

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WESTINGHOUSE AIR BRAKE TECHNOLOGIES CORPORATION
Petitioner

v.

RAILWARE, INC.
Patent Owner

IPR2026-00133
Patent 9,517,782

**DECLARATION OF LORI KAUFMAN, Ph.D.
IN SUPPORT OF PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,517,782**

TABLE OF CONTENTS

EXHIBIT LIST	xiii
LISTING OF CLAIMS	xvi
I. INTRODUCTION	1
II. QUALIFICATIONS	3
III. MATERIALS CONSIDERED	13
IV. UNDERSTANDING OF LEGAL PRINCIPLES	14
A. Claim Construction.....	15
B. Priority	15
C. Obviousness.....	16
V. BACKGROUND OF THE TECHNOLOGY.....	20
A. Known Problem to Protect Railway Workers.....	20
B. Known CTC Systems to Control Track Blocking and Unblocking	22
C. Known Secret Code Employed for Safety and Security	32
D. Known Workers Operating Mobile Device to Take Possession or Control of Worksite	35
VI. OVERVIEW OF THE '782 PATENT	38
A. Summary	38
B. Prosecution History	41
C. Priority Date	41
VII. LEVEL OF ORDINARY SKILL IN THE ART	41
VIII. IDENTIFICATION OF CHALLENGES	43
IX. CLAIM CONSTRUCTION	44
A. “release code” (claims 1-8)	45
B. “railway control apparatus” (claims 1-8)	48

C.	“to respond to prompts displayed thereon” (claims 1, 5) and “to respond to the message to release the block” (claims 2, 6)	48
D.	“user terminal” (or “terminal”) (claims 1, 2, 4, 5)	49
E.	“from the user terminal in return” (claims 1 and 5)	49
F.	Remaining Claim Terms	49
X.	GROUND 1: CLAIMS 1-8 ARE OBVIOUS OVER FRA- REPORT AND KRUIJSWIJK	50
A.	Summary of FRA-Report	50
1.	One Reference or Motivation to Combine	50
2.	Accessible to Interested Members of the Relevant Public.....	52
3.	FRA-Report Overview	53
4.	Analogous Art	59
5.	Prior -1179 IPR	60
B.	Summary of Kruijswijk and Analogous Art	61
C.	Analysis of Independent Claims 1, 5	63
1.	1[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”	63
	5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”	63
2.	1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”	66
3.	1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and	

to permit the railway field worker to respond to prompts displayed thereon;”	76
5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”	76
4. 1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”	88
5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”	88
5. 1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	94
5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	94
6. 1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”	108
5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”	108

D.	Analysis of Dependent Claims 2-4, 6-8	122
1.	Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”	122
	Claim 6: “The method of claim 1 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”	122
2.	Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”	124
	Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”	124
3.	Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	125
	Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	125
XI.	GROUND 2: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT, KRUIJSWIJK, AND MACEY	126

A.	Summary of FRA-Report and Analogous Art	126
B.	Summary of Kruijswijk and Analogous Art	126
C.	Summary of Macey and Analogous Art.....	126
D.	Analysis of Independent Claims 1, 5	129
1.	[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”	129
5[Pre]:	“A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”	129
2.	1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”	129
3.	1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”	130
5[A]:	“configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”	130
4.	1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”	130
5[B]:	“providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track	

sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”	130
5. 1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	131
5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	131
6. 1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”	131
5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”	131
E. Analysis of Dependent Claims 2-4, 6-8	135
1. Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”	135
Claim 6: “The method of claim 4 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”	135

2.	Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”	136
	Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”	136
3.	Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	136
	Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	136
XII.	GROUND 3: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT AND SCHMITZ.....	137
A.	Summary of FRA-Report and Analogous Art	137
B.	Summary of Schmitz and Analogous Art	137
C.	Analysis of Independent Claims 1, 5	140
1.	[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”	140
	5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”	140
2.	1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”	140

3.	1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”	140
	5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”	141
4.	1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”	141
	5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”	141
5.	1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	142
	5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	142
6.	1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”	149

5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”	149
D. Analysis of Dependent Claims 2-4, 6-8	155
1. Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”	155
Claim 6: “The method of claim 1 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”	155
2. Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”	156
Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”	156
3. Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	156
Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	156

XIII. GROUND 4: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT, BYFORD, AND MACEY	157
A. Summary of FRA-Report and Analogous Art	157
B. Summary of Byford and Analogous Art	157
C. Summary of Macey and Analogous Art.....	159
D. Analysis of Independent Claims 1, 5	159
1. [Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”	159
5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”	159
2. 1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”	160
3. 1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”	160
5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”	160
4. 1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”	160

5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”	160
5. 1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	161
5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”	161
6. 1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”	168
5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”	168
E. Analysis of Dependent Claims 2-4, 6-8	173
1. Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”	173
Claim 6: “The method of claim 4 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and	

permitting the railway field worker to respond to the message to release the block.”	173
2. Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”	174
Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”	174
3. Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	174
Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”	174
XIV. CONCLUSION.....	175

EXHIBIT LIST

Exhibit Number	Description
1001	U.S. Patent No. 9,517,782 (the “’782 Patent”)
1002	File History of U.S. Patent No. 9,517,782
1003	Declaration of Dr. Lori Kaufman including Curriculum Vitae (“Kaufman”)
1004	Vols. 1 and 2 of U.S. Department of Transportation, Federal Railroad Administration, <i>Supporting Railroad Roadway Worker Communications with a Wireless Handheld Computer</i> , Report Nos. DOT/FRA/ORD-04/13.i and DOT/FRA/ORD-04/13.ii (October 2004) (“FRA-Report”)
1005	PCT Publication No. WO 2007107554 A1 to Kruijswijk <i>et al.</i> (“Kruijswijk”)
1006	U.S. Patent No. 6,078,908 to Schmitz (“Schmitz”)
1007	PCT Publication No. WO 2010/012040 A1 to Macey (“Macey”)
1008	U.S. Patent No. 6,300,873 to Kucharczyk <i>et al.</i> (“Kucharczyk”)
1009	U.S. Patent No. 5,708,422 to Blonder <i>et al.</i> (“Blonder”)
1010	U.S. Patent No. 8,406,943 to Brand <i>et al.</i> (“Brand”)
1011	U.S. Patent No. 6,581,161 to Byford (“Byford”)
1012	Federal Railroad Administration, Research Reports, available at https://web.archive.org/web/20050211025837/http://www.fra.dot.gov:80/us/content/412
1013	Federal Railroad Administration, Research Reports, available at https://web.archive.org/web/20060922194521/http://www.fra.dot.gov/us/content/412

1014	Federal Railroad Administration, Research Reports, available at https://web.archive.org/web/20080212192107/http://www.fra.dot.gov:80/us/content/412
1015	Federal Railroad Administration, Research Reports, available at https://web.archive.org/web/20090320043352/http://www.fra.dot.gov/us/content/412
1016	Internet Archive Affidavit for URLs including EX1012-1015: https://web.archive.org/web/20050211025837/http://www.fra.dot.gov:80/us/content/412 https://web.archive.org/web/20060922194521/http://www.fra.dot.gov/us/content/412 https://web.archive.org/web/20080212192107/http://www.fra.dot.gov:80/us/content/412 https://web.archive.org/web/20090320043352/http://www.fra.dot.gov/us/content/412
1017	Excerpt of File History from U.S. Pat. RE49115
1018	Oral Argument Transcript regarding Wabtec’s Motion to Quash and Railware’s Motion to Compel held on March 26, 2025, before The Honorable Mark R. Hornak, Chief District Judge of the Western District of Pennsylvania. <i>See Railware, Inc. v. Southeastern Pennsylvania Transportation Authority</i> , Case No. 2:24-mc-01283-MRH, ECF No. 41 (W.D. Pa.).
1019	PCT Publication No. WO 2005/047074 A1 to Makkinga (“Makkinga”)
1020	US20120176217 to Tamaribuchi <i>et al.</i> (“Tamaribuchi”)
1021	U.S. Department of Transportation, Federal Railroad Administration, <i>Impact of Data Link Technology on Railroad Dispatcher Operations</i> , Report No. DOT/FRA/ORD-04/11 (October 2004) (“Malsch”)
1022	[RESERVED]

1023	[RESERVED]
1024	Railware’s Opening Claim Construction Brief, <i>Railware, Inc. v. Southeastern Pennsylvania Transportation Authority</i> , Case No. 2:24-cv-02963-JMY, ECF No. 40 (E.D. Pa. May 9, 2025).
1025	[Redacted] Declaration of Mehdi Ahmadian, Ph.D. in Support of Railware Inc.’s Claim Construction Submissions, <i>Railware, Inc. v. Southeastern Pennsylvania Transportation Authority</i> , Case No. 2:24-cv-02963-JMY, ECF No. 40-20 (E.D. Pa.).
1026	Defendant Southeastern Pennsylvania Transportation Authority’s Opening Claim Construction Brief, <i>Railware, Inc. v. Southeastern Pennsylvania Transportation Authority</i> , Case No. 2:24-cv-02963-JMY, ECF No. 39 (E.D. Pa. May 9, 2025).
1027	Excerpts from the Transcript of the March 28, 2025 Deposition of Medhi Ahmadian, Ph.D. as Part of Defendant Southeastern Pennsylvania Transportation Authority’s Opening Claim Construction Brief Submission (Exhibit 1017), <i>Railware, Inc. v. Southeastern Pennsylvania Transportation Authority</i> , Case No. 2:24-cv-02963-JMY, ECF No. 39-18 (E.D. Pa.).
1028	U.S. Department of Transportation, Federal Railroad Administration, <i>Communication and Coordination Demands of Railroad Roadway Worker Activities and Implications for New Technology</i> , Report No. DOT/FRA/ORD-07/28 (November 2007) (“Roth”)
1029	[RESERVED]
1030	<i>Railware v. Peninsula Corridor Joint Powers Board d/b/a Caltrain</i> (“Caltrain”), Case No. 5:25-cv-05725-BLF, ECF No. 1, Complaint (N.D. Cal. Jul. 8, 2025)
1031	<i>Railware v. Peninsula Corridor Joint Powers Board d/b/a Caltrain</i> (“Caltrain”), Case No. 5:25-cv-05725-BLF, ECF No. 15, Proof of Service (July 24, 2025).

LISTING OF CLAIMS
including January 13, 2018 Certificate of Correction

Claim Designation	Claim Language
Claim 1	
1[Pre]	A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:
1[A]	a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network; and
1[B]	a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,
1[C]	wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;
1[D]	a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and
1[E]	a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.
Claim 2	
[2]	The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.

Claim 3	
[3]	The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.
Claim 4	
[4]	The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.
Claim 5	
5[Pre]	A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:
5[A]	configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;
5[B]	providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;
5[C]	generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and
5[D]	permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.
Claim 6	
[6]	The method of claim 4 5 ¹ , further comprising:

¹ This change is based on the January 13, 2018 Certificate of Correction. EX1001, last page.

	displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.
Claim 7	
[7]	The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.
Claim 8	
[8]	The method of claim 2 ⁷² , wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.

² This change is based on the January 13, 2018 Certificate of Correction. EX1001, last page.

I, Lori Kaufman of Earlysville, Virginia, declare that:

I. INTRODUCTION

1. I have personal knowledge of the facts stated herein, and if called upon to testify to those facts I could and would competently do so.

2. I have been retained by Venable LLP, counsel for Westinghouse Airbrake Technologies Corporation (“Wabtec”), to analyze U.S. Patent No. 9,517,782 (“’782 Patent”) (EX1001) and to provide my opinions regarding the patentability of claims 1-8 of the ’782 Patent.

3. I understand that Wabtec is requesting that the Patent Trial and Appeal Board (“PTAB” or “Board”) to institute an *inter partes* review (“IPR”) proceeding of the ’782 Patent.

4. I have been asked to provide my independent analysis of the ’782 Patent based on the prior art cited in this declaration.

5. Petitioner’s counsel has asked me to consider whether certain references disclose or suggest, alone or in combination, the features recited in certain claims of the ’782 Patent. I have also been asked to consider the state of the art and the prior art available before the time of the alleged invention of the ’782 Patent. My opinions are provided in this Declaration.

6. My opinions in this Declaration are based on my review of the documents above, my understanding as an expert in the relevant field, and my

education, training, research, knowledge, and personal and professional experience, as well as the materials cited herein.

7. I am being compensated for my time at my standard hourly consulting rate of \$350 per hour. My compensation does not depend on the outcome of this matter or the specifics of my testimony. I have no financial interest in the outcome of this matter.

8. To my knowledge, I have no financial interest in Petitioner. Counsel for Petitioner has informed me that Railware, Inc. (“Railware”) purports to own the ’782 Patent. To the best of my knowledge, I have no financial interest in Railware and, to my recollection, have had no contact with Railware or the named inventor, Mr. Ross Pirtle, of the ’782 Patent. To the best of my knowledge, I do not have any financial interest in the ’782 Patent.

9. To the extent any mutual funds or other investments that I own have a financial interest in the Petitioner, Railware, or the ’782 Patent, I am not aware of, and do not control, any financial interest that would affect or bias my judgment.

10. This Declaration summarizes the opinions I have formed to date. I reserve the right to modify my opinions, if necessary, based on further review and analysis of information that I receive subsequent to the filing of this report, including in response to positions taken by Railware or its experts that I have not yet seen,

including any secondary consideration evidence that Railware or its expert may consider and present.

II. QUALIFICATIONS

11. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

12. A copy of my curriculum vitae (“CV”) is being submitted herewith as Appendix 1 to this declaration.

13. As set forth in my CV, I obtained a Bachelor of Science in 1987, Master of Science in 1993, and Doctor of Philosophy in 1997, all in Electrical Engineering from the University of Virginia in Charlottesville, Virginia.

14. For my doctoral dissertation, I performed an in-depth quantitative analysis of software failures in safety-critical systems. As part of my research, I developed a collection of statistical models to assess rare event failures that combined Markov modeling with Statistics of the Extremes. The success of my research led to several publications, and my obtaining a postdoctoral research position within the Department of Electrical Engineering at the University of Virginia beginning in the summer of 1997.

15. Initially, the focus of my postdoctoral research involved work for the Nuclear Regulatory Commission (“NRC”) in which I performed risk analysis for

safety-critical control systems. During this time period, the Department of Electrical Engineering received funding from the Federal Railroad Administration (“FRA”) to develop a risk assessment model for Positive Train Control (“PTC”) that would satisfy the FRA’s Office of Safety requirements for granting approval to a given PTC system.

16. Based upon my doctoral research as well as my on-going postdoctoral research, I was brought in to support the risk analysis for the North American Joint PTC (“NAJPTC”) Project (commonly referred to as the Illinois Department of Transportation (“IDOT”) PTC) and the CSX Communications-Based Train Management (“CBTM”) system in approximately mid-1998. The initial documentation that I was provided to support developing a risk assessment model for a given PTC system included documentation from Conrail, CSXT, and Norfolk Southern entitled PTC ON-BOARD PLATFORM System Requirements Document 1997-1998 Conrail, CSXT, and Norfolk Southern. From this system requirements document, I was able to extend the modeling concepts from my dissertation and NRC work to that of a risk informed model using simulation to develop a repeatable experiment to provide a quantified assessment of expected PTC performance with evidence from a safety perspective.

17. The premise of my train control risk assessment modeling was based on the concept of a three-state Markov model to represent all CBTM and PTC components; that is, any device found on or along the track infrastructure or on board a consist could be in one of three states: (1) Operational: the device is functioning as designed; (2) Failed Safe: the device has failed in a known way that is detectable by the overarching system design; (3) Failed Unsafe: the device has failed in an unknown way that potentially places the overall system at risk. Each of the CBTM and PTC model components was referred to as an “object”.

18. For each “object” defined by the Conrail, CSXT, and Norfolk Southern document above, I applied the three-state Markov model to create a module to support a simulation-based risk assessment. The three state Markov model allowed for the discrete simulation of the communications to the wayside devices and movement authorities (both via signal and verbal commands). I also incorporated static models of computer controlled braking curves for the consists taken from information provided by Wabtec (PTC) and CSX (CBTM). The key parametric data required to support this simulation was the equipment failure rate data that we obtained from the FRA and CSX for CBTM, and from the Union Pacific Railroad (“UPRR”), Lockheed Martin, Union Switch and Signal, and the FRA for the NAJPTC program.

19. Once I was engaged in my PTC research in 1998, I met and worked with railroad experts from CSX, Burlington Northern Santa Fe (“BNSF”), UPRR and Norfolk Southern that included current and former wayside workers, engineers, dispatchers, and others. Additionally, I met and worked with representatives from several labor unions such as the Brotherhood of Locomotive Engineers (“BLE”) and Brotherhood of Railroad Signalmen (“BRS”), various offices within the FRA, the Association of American Railroads (“AAR”), the NAJPTC, and Railroad Safety Advisory Committee (“RSAC”). The BRS and BLE made available various engineers and wayside workers for me to meet. I also travelled to Spartanburg, South Carolina, to ride aboard a PTC-equipped CSX train (CBTM) and witness an FRA brake test.

20. These meetings allowed for the refinement of the “object” model parameters and introduced the concept of extending the “object” models to include human factors (that is, the role of the dispatcher, engineer, conductor, and railway workers in train control operations).

21. In addition to the aforementioned modeling, I also applied my knowledge of discrete event simulation from my graduate studies to develop the requirements that defined the needed Monte Carlo simulation environment to produce the necessary data to support a statistically valid PTC risk assessment.

While I did not participate in any development of the software to support the simulation, I supported the selection of algorithms for the random number generation to support the Monte Carlo simulation and the Use Cases to test various train movement algorithms.

22. The combination of my “object” modeling and simulation work resulted in the development of the Axiomatic Safety-Critical Assessment Process (“ASCAP”) that simulated the movement of trains as the interaction of a collection of discrete objects using a Monte Carlo simulation. ASCAP modeled the various hardware/software functions (operations) and human in the loop actions as: onboard objects (*e.g.*, onboard computer, engineer, conductor, wheel sets, displays, and radio), wayside objects (*e.g.*, monitored switches, grade crossings, signals (absolute and intermediate) wayside interface units (“WIUs”), work crews with radios, and broken rail detection circuits), and dispatcher objects.

23. The FRA knew that the system functionality was not particularly unique between different PTC systems. From my meetings with the RSAC, CSX, FRA, BLE, BRS and others, I understood the requirements for a PTC system to be universal across the industry. In particular, the functionality of the onboard, wayside, and dispatch center equipment was similar, and from a risk assessment modeling perspective, it was identical. For example, the modeling of CBTM monitored

switches and onboard enforcement of penalty braking was reused in PTC. It was this fact that allowed for concurrent modeling of CBTM and the NAJPTC project.

24. The state of each object at the time of intersection was determined via a Monte Carlo “draw” and the outcome on train movement was defined by a well-defined set of outcomes derived from the General Code of Operating Rules (“GCOR”), CBTM, and PTC operational requirements. The fact that the three-state Markov model for the objects for the CBTM project (Conrail, CSXT, and Norfolk Southern document above) and the NAJPTC project provided the same functionality allowed for their reuse. The only required changes were the difference in GCOR for Direct Traffic Control (“DTC”), Centralized Traffic Control (“CTC”), and PTC operations.

25. From my multiple interactions with the FRA, RSAC, CSX, BLE, BRS, and others, and my own study of GCOR, train control systems, and documentation for the CBTM and the NAJPTC effort, I developed a very strong understanding of rail operations (DTC, Track Warrant Systems (“TWS”), CTC, CBTM, and PTC) in general by the fall of 2000 to further refine my modeling.

26. The paper entitled “The Axiomatic Safety-Critical Assessment Process (ASCAP) Simulation Methodology,” from the Proceedings of the 9th IFAC Symposium on Control in Transportation Systems, Braunschweig, Germany, 2000,

was one of the papers that I published describing the ASCAP concept for quantitative modeling of PTC-based systems for risk assessment. In this paper, I presented an overview of the three-state Markov model concept used in fault tolerant computing and its application to modeling PTC system objects as defined in the Conrail, CSXT, and Norfolk Southern document above. This three-state Markov model provided the flexibility to model both hardware and software systems required to implement train control systems such as DTC, TWS, CTC, CBTM, and PTC, as well as the human factors impact of dispatchers, train crews, and rail workers on operations.

27. As a result of my on-going NAJPTC and CSX CBTM modeling efforts, my postdoctoral position led to my becoming a Principal Scientist with the Department of Electrical Engineering at the University of Virginia in the fall of 2000.

28. To further refine the accuracy of the ASCAP simulation, I actively engaged with Wabtec on the NAJPTC project to develop the braking profile models for normal and emergency braking of the consist for use in the ASCAP simulation. These models required ASCAP to model the consist as a distributed mass rather than a point to capture a realistic braking profile that incorporated the track grade, curve and elevation, and the effects of pressure distributed across each wheel set brakes.

29. To provide the level of detail expected from my PTC risk assessment work with regard to the impact of human factors, I travelled to the CSX dispatch center in Jacksonville, Florida, and the Norfolk Southern dispatch center in Roanoke, Virginia, to further my knowledge of rail operations by watching and interviewing engineers, conductors, and dispatchers within their operational environments.

30. As a Principal Scientist, I continued to grow my understanding of PTC, and expanded my areas of rail safety research to include the upgrade of the New York City Transit Authority (“NYCTA”) Canarsie Line. By 2002, my work was concentrated almost exclusively in extending the modeling and simulation constructs that I developed for CBTM and PTC to the NYCTA effort. As part of my NYCTA support, I successfully completed Track Safety School in 2002 to further my understanding of NYCTA operations, and to ensure the alignment of my modeling and simulation work with actual operational practice.

31. Additionally, the same model constructs for CBTM and PTC objects (onboard, wayside and dispatch) were reusable for the NYCTA Canarsie Line risk assessment project. Again, this reuse was permissible due to similar nature of requirements across the platforms.

32. By 2002, after approximately four years, I had developed an in-depth understanding of PTC operations, how CBTM could be considered a PTC system,

why PTC could function as a non-vital overlay, the importance of human-in-the-loop modeling to better analyze the potential benefit of a PTC system, identified the range of ASCAP objects for all PTC equipment required by the CBTM and NAJPTC efforts (note: they were the same collection of objects), and understood how these concepts in many ways were similar, if not identical, to the NYCTA Carnarsie Line upgrade. I had leveraged my educational knowledge and expertise in stochastic analysis and rare event modeling, to develop a collection of reusable modeling objects that could effectively represent any PTC system.

33. I continued this work until I left the Department of Electrical Engineering at the University of Virginia in February 2004 for other business pursuits, primarily IT and Department of Defense related. In 2005 while employed at Commonwealth Computer Research, Inc., I received an award from the FRA to review safety analysis reports in support of the on-going IDOT PTC system development.

34. In 2006, I supported the development of requirements for a generalized train movement simulator to the support quantification of PTC systems using multiple routing algorithms. While at Booz Allen (in or around 2007), I worked with my colleague to identify potential accident scenarios that could arise due to communication issues with the IDOT PTC system (NAJPTC). Concurrent with this

activity, I quantified the maximum allowable communication timeout period for the communications architecture so that the PTC system would not pose a greater risk of train collisions, derailments, and accidents, as compared to a traditional cab signal system.

III. MATERIALS CONSIDERED

35. My opinions contained in this Declaration are based on the documents I reviewed, my professional judgment, as well as my education, experience, and knowledge of the field.

36. In preparing this declaration, I have reviewed and/or considered the documents cited in the Exhibit List and the documents referenced in this declaration.

37. In addition, I have reviewed the below documents:

- U.S. Provisional Application No. 61/893,547 to Pirtle
- U.S. Patent RE47,835 (the “RE’835 Patent”)
- File History of RE’835 Patent
- U.S. Patent RE49,115 (the “RE’115 Patent”)
- File History of RE’115 Patent
- Petition for *Inter Partes* Review, IPR2023-01179, Paper 2, Jul. 6, 2023 (’782 Patent)
- Patent Owner Preliminary Response, IPR2023-01179, Paper 7, Oct. 23, 2023 (’782 Patent)
- PTAB Decision Denying Institution of *Inter Partes* Review, IPR2023-01179, Paper 8, Jan. 22, 2024 (’782 Patent)

- Petition for *Inter Partes* Review, IPR2023-01180, Paper 2, Jul. 6, 2023 (RE’835 Patent)
- Patent Owner Preliminary Response, IPR2023-01180, Paper 7, Oct. 23, 2023 (RE’835 Patent)
- PTAB Decision Denying Institution of *Inter Partes* Review, IPR2023-01180, Paper 8, Jan. 22, 2024 (RE’835 Patent)
- Petition for *Inter Partes* Review, IPR2023-01181, Paper 2, Jul. 6, 2023 (RE’115 Patent)
- Patent Owner Preliminary Response, IPR2023-01181 Paper 7, Oct. 23, 2023 (RE’115 Patent)
- PTAB Decision Denying Institution of *Inter Partes* Review, IPR2023-01181, Paper 8, Jan. 22, 2024 (RE’115 Patent)

IV. UNDERSTANDING OF LEGAL PRINCIPLES

38. I am not a lawyer, and I will not provide any legal opinions in this IPR declaration. Although not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

A. Claim Construction

39. I understand that claim construction in an *Inter Partes* Review is controlled by the standard in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*).

40. I have been informed that claim construction begins with the language of the claims. The words are given their “ordinary and customary meaning,” which is “the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application.”

41. The specification and prosecution history are sources of intrinsic evidence that informs the meaning of the claim language. Extrinsic evidence, such as expert testimony and dictionaries, may be useful in educating judges regarding the field of the invention or helping determine what a person of ordinary skill in the art (“POSITA”) would understand claim terms to mean. However, extrinsic evidence in general is viewed as less reliable than intrinsic evidence.

42. I understand that in this proceeding, any claim term that is not construed should be given its plain and ordinary meaning.

B. Priority

43. I understand that a continuation application is a later-filed application that has the same disclosure (specification and figures) as an earlier filed application

to which the later-filed application claims priority. A continuation is generally entitled to the same priority date as the later-filed application to which it claims priority.

C. Obviousness

44. I have been informed by counsel and understand that a prior art reference can render a patent claim obvious to one of ordinary skill in the art if the differences between the subject matter set forth in the patent claim and the prior art are such that the subject matter of the claim would have been obvious at the time the alleged invention was made.

45. In analyzing obviousness, I understand that it is important to consider the scope of the claims, the level of skill in the relevant art, the scope and content of the prior art, the differences between the prior art and the claims, and any secondary considerations.

46. I have been informed by counsel and understand that a single reference can render a patent claim obvious if any differences between that reference and the claims would have been obvious to a person of ordinary skill in the art. Alternatively, the teachings of two or more references may be combined in the same way as disclosed in the claims, if such a combination would have been obvious to one having ordinary skill in the art.

47. In determining whether a combination based on either a single reference or multiple references would have been obvious, I have been informed by counsel and understand that it is appropriate to consider the following factors:

- Whether the teachings of the prior art references disclose known concepts combined in familiar ways, and when combined, would yield predictable results;
- Whether a POSITA could implement a predictable variation, and would see the benefit of doing so;
- Whether the claimed elements represent one of a limited number of known design choices, and would have a reasonable expectation of success by those skilled in the art;
- Whether a POSITA would have recognized a reason to combine known elements in the manner described in the claim;
- Whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent;
- Whether the innovation applies a known technique that had been used to improve a similar device or method in a similar way; and

- Whether there was a design need or problem known to the POSITA that would have motivated the POSITA to combine the elements, as claimed.

48. I been informed by counsel and understand that a POSITA has ordinary creativity and is not an automaton.

49. I been informed by counsel and understand that all prior art references are to be looked at from the viewpoint of a POSITA.

50. I been informed by counsel and understand that, in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the patent being considered, and that obviousness is analyzed from the perspective of a POSITA at the time of the invention.

51. I been informed by counsel and understand that when the claimed subject matter involves combining pre-existing elements to yield no more than one would expect from such an arrangement, the combination is obvious. I also I been informed by counsel and understand that in assessing whether the claimed subject matter is obvious, one must consider whether the claimed improvement is more than the predictable use of prior art elements according to their established functions.

52. I been informed by counsel and understand that there need not be a precise teaching in the prior art directed to the specific subject matter of a claim

because one can take account of the inferences and creative steps that a person of skill in the art would employ.

53. I been informed by counsel and understand that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art. I been informed by counsel and understand that in an obviousness analysis, neither the motivation nor the avowed purpose of the alleged inventor controls the inquiry. Any need or problem known in the field at the time of the invention and addressed by the patent can provide a reason for combining elements. For example, I been informed by counsel and understand that it is important to consider whether there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. I been informed by counsel and understand that known techniques can have obvious uses beyond their primary purposes, and that in many cases a person of ordinary skill can fit the teachings of multiple pieces of prior art together like pieces of a puzzle.

54. I been informed by counsel and understand that, when there is a reason to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. I further have been informed by counsel and understand that, if this leads to the anticipated success, it is likely the product not of innovation but of

ordinary skill and common sense, which bears on whether the claim would have been obvious.

55. I been informed by counsel and understand that secondary considerations can include, for example, evidence of commercial success of the invention, evidence of a long-felt need that was solved by an invention, evidence that others copied an invention, or evidence that an invention achieved a surprising result. I further have been informed by counsel and understand that such evidence must have a nexus or causal relationship to the elements of a claim, in order to be relevant.

56. I am unaware of any such secondary considerations asserted by Railware for the '782 Patent.

V. BACKGROUND OF THE TECHNOLOGY

A. Known Problem to Protect Railway Workers

57. The '782 Patent allegedly is directed to a conventional centralized railway control system to generate a release code when a block is placed, transmit the release code to a railway worker's conventional mobile device, and receive the release code in return to remove the block. EX1001, 2:38-39, 2:43-67, 1:21-2:3, Fig. 3A, 6:18-41, 9:2-5, Fig. 3B, 6:4-11.

58. I believe that before the Priority Date (discussed further below) it was a known problem to a POSITA of protecting railway workers from removal of a

block by the dispatcher or another, intentionally or inadvertently, while maintenance track work is performed.

59. For instance, the prior art discusses that the CTC dispatcher and worker communicate to ensure the track block is safely removed only when the worker has left the subject area. EX1004, Vol. I: 6 (“[w]hen a dispatcher [grants] a request for roadway worker protection the track is placed off-limits (blocked) for other uses. In Central Traffic Control (CTC) territory, blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track.”), 36 (“worker can retrieve a list of Form Ds ... under his/her authority ... [and] [f]ollowing the link[] ‘Cancel/Fulfill’ ... the roadway worker is able to give some track under his authority back to the dispatcher”), 1 (“Voice radio communications are vital to the safe and efficient operation of the railroads. Voice radio supports two types of communication tasks. The first type includes safety-critical communications related to train movements and allocation of track between roadway workers and trains.”), 9 (proposed that any future systems/applications should include a “verification system that prevent[s] or minimize[s] common human error”), 27 (“prompt the roadway worker for confirmation” before “giving any section of track back to the dispatcher”); Vol. II: 12 (“[o]nce a track is blocked, the dispatcher temporarily loses authority over that track.”), 11 (“Blue ... track section is authorized

for maintenance ... [which means the] track has been protected [T]he dispatcher temporarily loses control over that section of track.”).

60. There are other examples that discuss this two-way communication to protect the railway worker. EX1019, 5:1-11 (“the responsibility for unblocking the work zone” should be put in the hands of the railway worker to make it “technically impossible” for the central dispatcher to route trains on that section of track); EX1020, [0009] (“in the rail transportation system, the workers may be in danger due to erroneous situation recognition or manipulation mistake of an ordering person in an operation control center, even if workers are performing maintenance work inside the railroad line area.”), [0150], [0151] (“since the worker can initiate the maintenance work after confirming that the safety measure is maintained, it is possible to prevent the safety measure from not being performed due to erroneous situation recognition or manipulation mistake of the ordering person and to prevent the worker from being in danger.”), [0152]; EX1007, 16:1-21 (a railway worker must enter “a specific code before it is deemed the target zone 108 is safe for the passage of the vehicle.”), 13:35-14:4.

B. Known CTC Systems to Control Track Blocking and Unblocking

61. The ‘782 Patent acknowledges it was well-known to operate “centralized traffic control” or track display to control interlocking signals (via an

interface) for track blocking and unblocking control track by transmitting a signal, *e.g.*, blocking signal or unblocking signal, to track interlocks.

Interlocking signals govern movement within a sector controlled by an interlock.

* * *

Interlocking systems usually incorporate a 3-color system by which the train, or train conductor, is informed to proceed at regular speed, is informed to proceed at a reduced speed or ***is prohibited from proceeding through the upcoming section.***

* * *

One method of ***controlling all of the interlocks*** within a rail system is through a ***centralized traffic control (CTC)***, or traffic control system (TCS). A ***CTC*** is used ***for monitoring, tracking and operating trains traversing tracks throughout a network.*** ***The CTC is controlled by a single person known as a train dispatcher.***

* * *

Information regarding track conditions, train traffic, scheduling, etc., ***are presented on a control console which may include a map of the entire rail system controlled by the CTC.*** ***Through the control console, the dispatcher has control of each interlock signal (that is, the dispatcher controls the train traffic and flow of train traffic using the interlocks) and is constantly made***

aware of the positions of trains in the railway system as such positions are electronically reported by signals present throughout the railway system. In addition, in order to provide for safe traffic control and avoid accidents or collisions, signals are provided throughout the track network, or interlocks.

The ***interlocks may be controlled from the CTC in any of various different ways***, including, e.g., direct wiring, by pulse codes sent over a wire to distant locations, etc. In addition, interlocks can also be controlled by a native mechanism detecting presence of a train on the track. That is, ***when a train occupies a certain section of track, the interlock prevents other trains from proceeding onto the same***

EX1001, 1:27-2:17 (emphasis added).

62. Railware's expert, Mehdi Ahmadian, Ph.D, in the SEPTA litigation (defined below) agrees that CTC systems with dispatcher console or interface to control track blocking and unblocking via interlocks were known. Dr. Ahmadian cites a 2010 public document before the Priority Date in support.

CTC systems typically include control consoles, which may take a variety of forms and have a variety of back-end and front-end components, that display various pieces of information, such as track conditions, train traffic, and scheduling. Through the control console, the dispatcher can view and control the movement of trains throughout the railway network. Movement

of trains within a sector of track is typically governed by interlocking signals, which are controlled by the dispatcher via a control console. Shown below is an example of a control center where dispatchers control train traffic using a CTC system [Footnote 1: Pratima Bhattacharyya, Reporter's Notebook Taking a look at SEPTA control, DAILY PENNSYLVANIAN (Oct. 5, 2010), https://www.thedp.com/article/2010/10/reporters_notebook_taking_a_look_at_septa_control]:

EX1025, ¶ 14.

63. From the 2010 public document, Dr. Ahmadian cites the below image, showing a CTC dispatcher console to control track blocking and unblocking.



Id.

64. Dr. Ahmadian further discusses that the '782 Patent acknowledges it was known to control interlocking signals from the dispatcher's interface:

According to the '782 patent, in a standard railway system, “[i]nterlocking signals govern movement within a sector controlled by an interlock.” *Id.* at 1:27-28. “[A] track may be divided into sections,” and an “interlocking signal” is exhibited at the entrance to each track section. *Id.* at 1:28-32. “[T]he interlocking signal displays a color system which instructs the conductor of the train, or the train operating by automated response, how to move through the upcoming section of track.” *Id.* at 1:32-35.

Id., ¶¶ 22, 23; *see supra* ¶ 61 (discussing the '782 Patent interlocking statements).

The '782 patent further explains that “all of the interlocks” within a railway system may be controlled electronically through “a centralized traffic control (CTC).” *Id.* at 1:40-44. “The CTC is controlled by a single person known as a train dispatcher.” *Id.* at 1:46-47. “Information regarding track conditions, train traffic, scheduling, etc.” is displayed to the dispatcher “on a control console,” and “[t]hrough the control console, the dispatcher has control of each interlock signal.” *Id.* at 1:48-59.

EX1025, ¶ 24.

65. Further, Dr. Ahmadian cites a 2002 dictionary (Railway Age's Comprehensive Railroad Dictionary, 2nd Ed. (2002)) to assert that CTC was well-known: "a commonly used railroad dictionary at the time defines 'centralized traffic control' to mean 'a system of rail operation by means of which the movement of trains over routes and through blocks on a designated section of track or tracks is directed by signals controlled from a designated central point.'" *Id.*, ¶ 204. This also supports my opinion, given this 2002 inclusion, that CTC systems were well-known to a POSITA.

66. The prior art also teaches that it was known for a dispatcher to operate a track display to control interlocking signals (via an interface) for track blocking and unblocking control track by transmitting a signal, *e.g.*, blocking signal or unblocking signal, to track interlocks.

67. For example, this is shown in the FRA-Report below, particularly Figure 1 and associated Table 2 describing the track status.

Table 2. Representation of Color Code for Monitoring Track Status

Color	Meaning
White	Indicates that the track segment is available for routing trains or other uses.
Red	Means train or track vehicle occupancy. A train currently occupies that block.
Green	Indicates that the track segment has been cleared (authorized for use) for train movement. The train has not yet entered this block.
Blue	Indicates that a track section is authorized for track maintenance. This means that a portion of track has been protected for use by maintenance of way crews or track equipment. When the dispatcher gives track authority to a work crew, the dispatcher temporarily loses control over that section of track. Trains cannot enter this track segment unless authorized by the roadway worker responsible for that block.

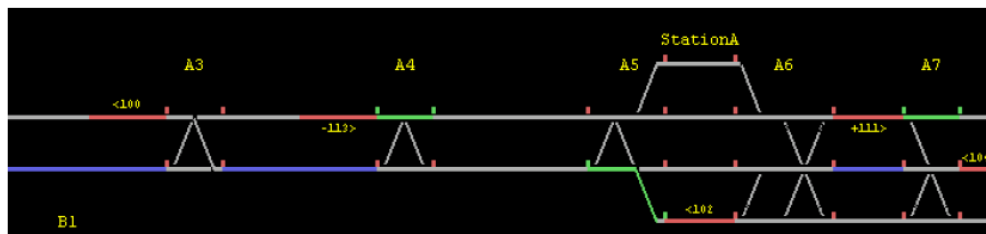


Figure 1. Track Chart Display

EX1004, Vol. II: 11 (Fig. 1, Table 2), 10; Vol. I: 1 (“[i]n centralized traffic control territory, switches and signals receive commands from the dispatcher’s computer.”), 6 (“In Central Traffic Control (CTC) territory, blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track.”).

68. This is also shown in Malsch (EX1021 or “DOT/FRA/ORD-04/11”), which was accessible to interested members of the relevant public. EX1021, front page (“This document is available to the public through the National Technical Information Service, Springfield, VA 22161. This document is also available on the FRA website at www.fra.dot.gov”), Report Documentation Page (“12a. Distribution/Availability Statement”), notice page (“This document is disseminated

....”); EX1012, 1; EX1013, 1; EX1014, 3; EX1015, 3 (see “DOT/FRA/ORD-04/11”); EX1016.

69. Malsch shows in Figure 3 below “Active Track Layout” and Figure 8 below “Track Layout,” both with “Block Track” and “Unblock Track” buttons for the interlockings.

70. Malsch’s “routing interface displayed the track layout and was modeled after a Central Traffic Control (CTC) based signal system. It ***simulated routing activity for a track network on the Northeast Corridor.***” EX1021, 6 (emphasis added), 8 (display updated “when a train passed an interlocking. Stations and interlockings were named.”).

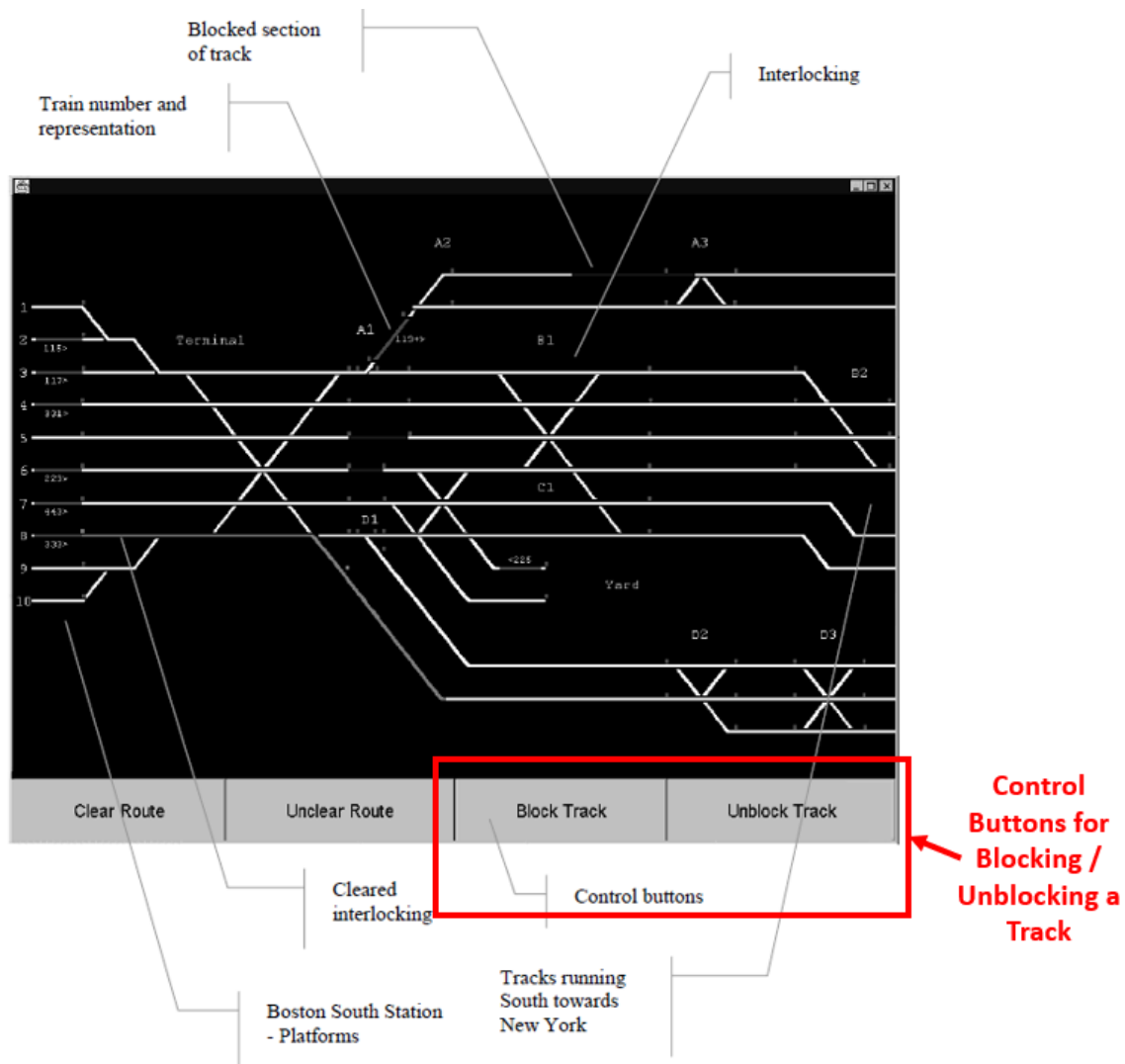


Figure 3. Active Track Layout

EX1021, 10 (Fig. 3) (annotated), 9 (“The main routing tasks were accomplished using mouse-activated buttons located at the bottom of the screen; clearing and unclearing a route as well as blocking and unblocking tracks. . . . The dispatcher blocked a track to enable roadway workers and their equipment to occupy the track. Unblocking the track removed this protection for the roadway worker crew and equipment and made the track available for train movements or other MOW crews.

The simulator propagated the state of the signal to the adjacent block.”)



Figure 8. Track Layout

Id., Fig. 8, 1 (“In CTC territories, the dispatcher monitors train position via signals communicated by track circuitry, on a visual display (i.e., a computer display or mimic board) and monitors events through two-way radio communications with railroad crews in the field.”), 59 (“**Centralized Traffic Control (CTC)**: A signal system that allows the dispatcher to know which blocks are occupied by trains and roadway workers, and to control switches and signals remotely from the dispatch center.”) (emphasis in original).

71. Other references likewise discuss similar known CTC systems. *See e.g.*, EX1020, [0002] (“The present invention relates to a control system for controlling a target device having an influence on safety of maintenance work, and a terminal device for maintenance worker and a control device included in the control system.”), [0060] (“The central control device 100 . . . for controlling the rail transportation control system 1”).

C. Known Secret Code Employed for Safety and Security

72. As discussed below, the ‘782 Patent allegedly recites a secret code according to Railware.

73. I believe a secret code, including “one-time password” (“OTP”), was generated and transmitted in railway and other industries before the Priority Date.

- EX1005, 8:14-16 (“generating, at the server station, the personal secret code, e.g. a random number of a predetermined number of

digits.”), 12:13-21 (The secret code is transferred over a network such as the Internet to a “railroad track ... technician[.]”), 4:3-8 (secret code is sent to a specific user and to ensure secret, the code can be “terminate[d]” after “a one-time use”).

- EX1009, 13:66-14:8 (“generates a confirmation code and supplies that code to the customer” where the code is “randomly generated so as not to be predictable,” and “will be known only to the customer” or the relevant person), 15:7-27.
- EX1006, 6:63-7:4 (“authentication computer [server] 2 generates the transaction authorization number TAN or the comparable password” using “a random number generator 5 ...”), 7:16-18 (“The transaction authorization number TAN or the comparable password can be a one-time usable transaction authorization number TAN or a one time usable password.”), Fig. 2 (“Authorization Computer 2” and “Random Number Generator 5”), Abstract.
- EX1008, Abstract (“one-time use access code ... may be issued by a server ... [and] may be generated using a cryptographically strong random number generator”), 7:30-42 (“every access code issued by server 30 ... will be unique to the requester. That requester, and only that requester, will know the access code”), 9:41-44.
- EX1011, 4:31-38 (server generating a “cipher lock code” for a specific user and transmitting the code in “encrypted form” over the Internet to the user’s wireless device which “decrypt[s]” it), 5:7-14 (user permitted “one-time access”).

74. I also believe a POSITA knew before the Priority Date that secret codes were transmitted to a central system in railway and other industries for safety and security.

- EX1007, 16:1-21 (railway worker must enter on their mobile device “a specific code before it is deemed the target zone [] is safe for the passage of the vehicle.”), 13:35-14:4, 15:16-35 (a railway worker enters a secret code “such as a PIN (personal identification number) or password only known to the user” which “[u]pon the successful entry of this code to the interface [of the remote command center, it] ... transmit[s] a signal to the signalling device” which changes “from a red light [(blocked track)] to a green light [(unblocked track)] and signals the operator of the train to proceed.”), 20:31-37.
- EX1005, 2:8-13 (“transfer[s] a message containing the personal secret code from the [] communication device via the communication network to the server station” which verifies it), claim 1, 7:1-17, Abstract, 6:1-9.
- EX1009, 14:18-25 (“Then, the confirmation code which was supplied for the given transaction is compared to the confirmation code that was received ... to ensure that the customer is, in fact, providing a proper confirmation of the authorization.”).
- EX1006, 7:8-15 (code “is transmitted again to the authorization computer” which “verifies” the code to control, *e.g.*, a locking

mechanism or “physical access controls.”), Abstract, 5:7-9, 5:24-48, 7:60-61.

75. Thus, a POSITA was aware and employed secret codes before the Priority Date across a range of fields, including railway systems.

D. Known Workers Operating Mobile Device to Take Possession or Control of Worksite

76. Before the Priority Date, it was conventional for railway workers to operate a mobile device for communicating with a central control system (dispatcher) for controlling a track.

77. The named inventor acknowledged to the USPTO (as shown below) in the application leading to RE’115 Patent that mobile phones, text messaging, and email were conventional before the Priority Date and thus indicated that these known communication methods could be applied to railway systems. EX1017, 8 (¶¶ 5-7), 15-16.



Android Developers Blog

The latest Android and Google Play news for app and game developers.

Speech Input API for Android

05 March 2010

People love their mobile phones because they can stay in touch wherever they are. That means not just talking, but e-mailing, texting, microblogging, and so on. So, in addition to search by voice and voice shortcuts like "Navigate to", we included a voice-enabled keyboard in Android 2.1, which makes it even easier to stay connected. Now you can dictate your message instead of typing it. Just tap the new microphone button on the keyboard, and you can speak just about anywhere you would normally type.

Id., 15 (excerpt).

78. Several prior references state that workers operated mobile devices for track control, such as to take possession and return possession of a work zone, with a CTC system. *See e.g.*, EX1004, Vol. I: 13, 29 ("The PDA also enabled the roadway worker to request a variety of work authorizations (Form D and Foul Time)."), 6 ("If the dispatcher grants permission to work the track is placed off-limits (blocked) ... [and] blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track."), 36 (FRA-Report describes that the "worker can retrieve a list of Form Ds ... under his/her authority ... [and] [f]ollowing

the link[] ‘Cancel/Fulfill’ ... the roadway worker is able to give some track under his authority back to the dispatcher.”); EX1020, Abstract (“A terminal device carried by a maintenance worker transmits, to a central control device, a request to maintain a first state in which a central control device controls a target device so that maintenance work is safely performed.”), [0068], [0082] (“After the worker performs the selection of the safety measure . . . the worker touch[es] a button B11 . . . [to] request for approval (Request PTW).”), Figs. 2 and 4, [0097] (the worker on the PDA interface selects “in FIG. 4, an unlock request button B32 for requesting the release of the PIN lock.”); EX1019, 7:1-18 (“The external workstation is therefore able to take over a part of the functionality of the traffic control system such that the operator of the external workstation can ensure blocking of the work zone.”), 11:3-17 (“In step 41 the withdrawal of the work zone is transferred to the traffic control system from the mobile workstation In step 43 the traffic control system sends a confirmation of receipt of the withdrawal data and this results in situation 44 wherein the occupied work zone is once again available to the traffic control system. In step 45 the work zone is unblocked within the traffic control system”)

VI. OVERVIEW OF THE '782 PATENT

A. Summary

79. The '782 Patent (having Application No. 15/177,506) was filed on June 9, 2016, claiming alleged priority to Application No. 14/519,727 (now U.S. Patent No. 9,403,545) filed on October 21, 2014, and a provisional with Application No. 61/893,547 filed on October 21, 2013. EX1001, front page; EX1002, 2-3.

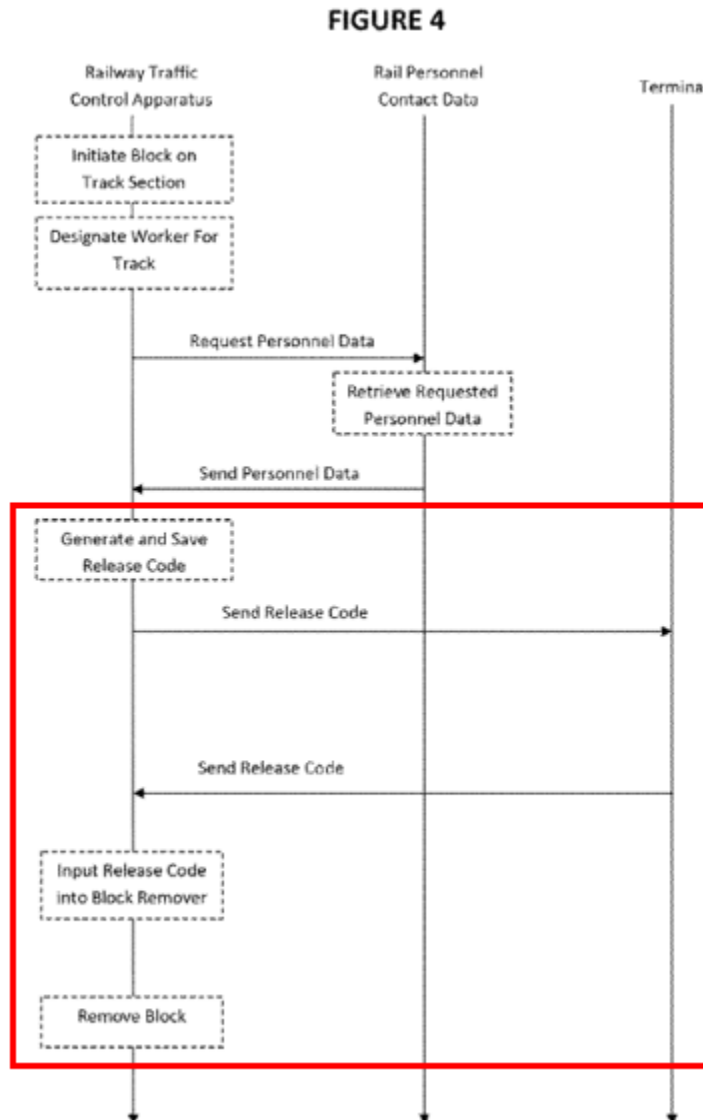
80. I believe the '782 Patent combines known CTC systems with conventional mobile devices and a known code for authorization or authentication. *See supra* Sections V.B-D.

81. Specifically, the '782 Patent describes adapting conventional blocking mechanisms in conventional CTC systems by implementing a “release code” that is generated, sent to a worker, and then received from the worker before releasing a block on the track. EX1001, Abstract (“[t]ools . . . to control traffic over a railway track section . . . [and] when traffic over the track section is to be blocked, a release code is generated and sent to . . . the railway worker. Traffic through the track section is blocked until the release code is entered in the system.”), 2:53-58 (similar), 1:42-2:67.

82. I understand Railware refers to this back-and-forth transmission of the code as the “crux of the inventive aspect”: “a code is sent out to the railway worker

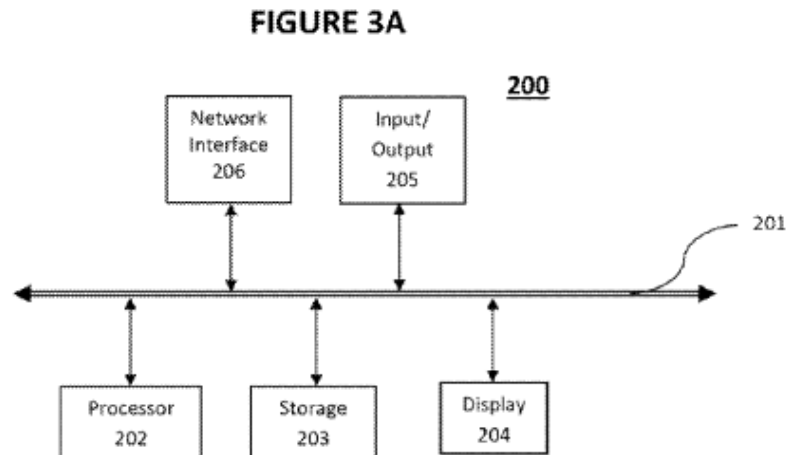
in the field and the block can only be released when that railway field worker provides the code back to the dispatcher.” EX1018, 30:17-24.

83. This is also shown in Figure 4 below.

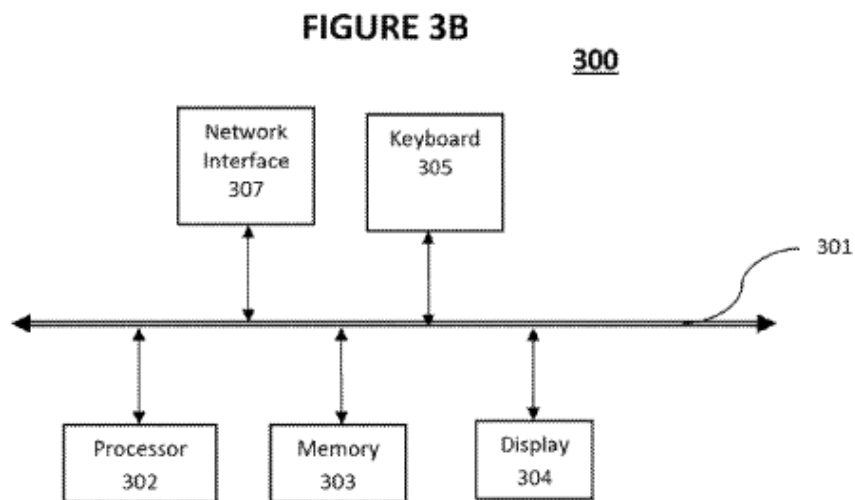


Id., Fig. 4 (annotated).

84. The specification acknowledges that it invokes generic hardware, as shown in Figures 3A (user terminal) and 3B (railway control apparatus) below for such functionality.



Id., Fig. 3A, 6:18-41, 9:2-5 (“The terminal 103 could be any communication device such as, but not limited to, mobile phone or smartphone, tablet, WIC (or another) pager, PDA, etc.”).



Id., Fig. 3B, 6:4-11 (“The user interface 101D may be a mobile application, a web page or some other software component, on a terminal device.”), 6:42-7:20.

B. Prosecution History

85. During prosecution, the ’782 Patent never received a substantive office action, and the Examiner issued a notice of allowance allowing the as-filed claims 1-8. EX1002.

86. A Certificate of Correction was issued on January 13, 2018 to change claim 6’s reference of claim 1 to claim 5 and claim’s 8 reference of claim 2 to claim 7. EX1001, last page.

C. Priority Date

87. I have been asked to assume for the purpose of this declaration a priority date of October 21, 2013 (the “Priority Date”), which is the date of the provisional application, but to reserve the right to offer opinions about this priority date (and priority chain) before the PTAB or otherwise if asked.

VII. LEVEL OF ORDINARY SKILL IN THE ART

88. I have been informed that a POSITA is a hypothetical person who is presumed to have the skill and experience of an ordinary worker in the field at the time of the alleged invention.

89. I believe a POSITA as of the Priority Date would have had at least a bachelor’s degree in electrical, mechanical, or related engineering, and would have

had at least two (2) years of experience in railway operations or railway control systems. A higher level of education or skill might make up for less experience, and vice-versa.

90. Railware's expert offered a similar POSITA description in the dismissed SEPTA litigation.

It is my opinion that a person of ordinary skill in the art of the Asserted Patents would have (i) at least a bachelor's degree in electrical, mechanical, industrial or related engineering, and (ii) would have had at least two (2) years of experience in railway safety, railway operations, and/or railway control systems. A higher level of education or specific skill might make up for less experience, and vice-versa.

EX1025, ¶ 63; EX1024, 24.

91. I was a POSITA at the time of the Priority Date as discussed in my Qualifications (*see* Section II) and CV.

92. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II).

93. Based on my knowledge and experience, I believe that I am considered to be a POSITA in the field of the '782 Patent.

94. Also, based on my knowledge and experience, I understand and know of the capabilities of persons of ordinary skill in the field before the Priority Date.

VIII. IDENTIFICATION OF CHALLENGES

95. This Declaration explains the conclusions that I have formed based on my analysis.

96. To summarize those conclusions:

97. **Ground 1:** Based upon my knowledge and experience, I believe that claims 1-8 of the '782 Patent are obvious by FRA-Report (EX1004) and Kruijswijk (EX1005).

98. **Ground 2:** Based upon my knowledge and experience, I believe that claims 1-8 of the '782 Patent are obvious by FRA-Report, Kruijswijk, and Macey (EX1007).

99. **Ground 3:** Based upon my knowledge and experience, I believe that claims 1-8 of the '782 Patent are obvious by FRA-Report and Schmitz (EX1006).

100. **Ground 4:** Based upon my knowledge and experience, I believe that claims 1-8 of the '782 Patent are obvious by FRA-Report, Byford (EX1011), and Macey.

IX. CLAIM CONSTRUCTION

101. I have generally applied the plain and ordinary meaning of the terms recited in the claims, as would have been understood by persons of skill in the art as of the Priority Date. I understand in *Railware, Inc. v. Southeastern Pennsylvania Transportation Authority*, Case No. 2:24-cv-02963-JMY (EDPA) (the “SEPTA litigation”) the parties filed proposed constructions for Claim 5 (and certain dependent claims) of the ’782 Patent. *Id.*, ECF 41; EX1024-1027. Claim 1 was not asserted in the SEPTA litigation. The SEPTA litigation was dismissed.

102. I understand Petitioner does not believe any claim terms require express construction for purposes of this IPR given the prior art disclosure herein.

103. Nonetheless, I have been asked to (i) explain herein how the prior art satisfies even Railware’s (and SEPTA’s) proposed constructions in the SEPTA litigation as well as the Board’s discussion of the claimed code in the ’782 Patent IPR (IPR2023-01179 (“-1179 IPR”)) and (ii) reserve the right to respond to any proposed constructions advanced by Railware in this proceeding.

104. For purposes of this IPR only, I have been asked to apply their constructions, along with the Board’s discussion of “release code” in the prior institution-denied -1179 IPR.

105. I have been asked to reserve the right to respond to any claim construction arguments in any proceeding.

A. “release code” (claims 1-8)³

Railware	SEPTA
“A code that is not readily available to the terminal user (<i>i.e.</i> , the dispatcher).” EX1024, 17.	Indefinite. EX1026, 23-24.

106. I understand that Railware’s expert in the SEPTA litigation contended “those skilled in the art that ‘secret,’ as applied to the Code Terms, means a code that is not readily available to the dispatcher” EX1025, ¶¶ 152, 113 (“Code Terms that is transmitted to the railway field worker ... but otherwise remains ‘secret’ from the dispatcher.”), 114, 148 (“Asserted Patents are resolute in their indication that the Code Terms are secret.”), 83, 128-130; EX1024, 18 (“Asserted Patents [’782 Patent, RE’835 Patent, RE’115 Patent] repeatedly ... refer to the Code Terms as ‘secret’ from the dispatcher. Ahmadian Decl. ¶ 83.”), 23, 19-21, 7.

107. I understand Railware’s expert asserted that, “a code qualifies as not readily available to the dispatcher based on whether the ***dispatcher can see or easily access*** the code before it is time for removal the block.” EX1025, ¶154 (emphasis added); EX1024, 27.

³ Railware and SEPTA in their briefs list only certain claims for each term herein. See EX1024, EX1026.

108. I understand Railware’s expert asserted that, “there are *a lot of parameters that are involved* there that, *absent of knowing those parameters*, then the *secretness of the code to the dispatcher or its availability or lack of cannot* be *definitively ascertained*.” EX1026, 28 (emphasis added); EX1027, 100:6-102:2. I agree.

109. I understand the Board previously denied -1179 IPR challenging the claims of the ’782 Patent, finding that the prior art did not show the claimed “release code.”

110. While the Board stated it was not construing release code, the Board did discuss it as shown below:

The ’782 patent makes clear that the release code is “only” received by the relevant railway field worker and an internal storage ... Although the ’782 patent describes alternative means for retrieving the release code from internal storage when the field worker is unavailable, accessibility to a “release code” is limited and this alternative access is only provided where “no maintenance worker [is] available to transmit the random secret code.” *See id.* at 10:19–22; *see also id.* at 5:58–60, 9:32–34, 9:65–10:5, 10:10–26 (consistently describing the release code as “secret”).

IPR2023-01179, Paper 8, 19-20 (Jan. 22, 2024) (citing EX1001) (internal citations omitted), n.3 (“no material difference” between release code and secret code).

111. The Board also noted in -1179 IPR, while not resolving, that the '782 Patent specification fails to inform Railware's proposed construction or how a POSITA "would have distinguished a code that is 'readily available' to the dispatcher from a code that is not 'readily available.'" *Id.*, 20 n. 11; EX1026, 26.

112. I agree with the Board the '782 Patent specification does not state when the release code is "'readily available' to the dispatcher from a code that is not 'readily available'" because, for instance, the specification never uses the words "readily available" and "a lot of parameters that are involved" as discussed above. Also, "whether the dispatcher can see or easily access the code before it is time for removal the block" compounds this issue as Railware has introduced another subjective term ("easily access") not defined in the specification on top of "readily available."

113. Additionally, Railware alleges in a July 8, 2025 Complaint: "software that will only allow the dispatcher to release track and time authority after both the RWIC [Roadway Worker In Charge] and one authorized person in the work group has entered a special pin code into the system." EX1030, ¶ 89.

B. “railway control apparatus” (claims 1-8)

Railware	SEPTA
“[n]o construction necessary or plain and ordinary meaning” EX1025, ¶183.	“centralized traffic control (CTC) console used by the train dispatcher” EX1026, 21.

114. I understand that Railware’s expert believes the term should be “broadly understood and encompasses a number of hardware (such as processor and memory components) and software components beyond just the dispatcher’s console.” EX1025, ¶¶194, 200-201, 183-186, 192, 210, 223.

C. “to respond to prompts displayed thereon” (claims 1, 5) and “to respond to the message to release the block” (claims 2, 6)

Railware	SEPTA
“do not need construction, or should be afforded their plain and ordinary meaning” EX1025, ¶301.	Claim 5: “to respond through the mobile user device user interface to prompts displayed thereon” Claim 6: “to respond through the mobile user device user interface to the message to release the block” EX1026, 19-20

115. I understand Railware’s expert alleges this covers any “standard type of user interface” and “does not require that the response take any particular format or serve any particular purpose.” EX1025, ¶¶308, 313-314 (“broadly”), 321.

D. “user terminal” (or “terminal”) (claims 1, 2, 4, 5)

Railware	SEPTA
“user terminal of a terminal user (i.e., the dispatcher)” EX1024, 29; EX1025, ¶¶247-248, 266, 251, 259	“railway field worker’s mobile user device” EX1026, 6-7

116. Railware asserts that the “user terminal” in Claim 5 refers to the dispatcher’s terminal and Claim 1 refers to the worker’s terminal. EX1024, 41, 38.

E. “from the user terminal in return” (claims 1 and 5)

Railware	SEPTA
“[n]o construction necessary or plain and ordinary meaning” EX1025, ¶¶276-277, 279, 296, 321	“transmitted from the user terminal (as previously defined)” EX1026, 15-16.

117. Railware’s expert asserts in Claim 5, “[g]iven the breadth of descriptions regarding how the removal or release code can be returned or transmitted ... the *code can be returned in a number of different ways ...*” and is *not “limited to ... only via the user terminal of the railway field worker*” EX1025, ¶¶287 (emphasis added), 288, 293-299.

F. Remaining Claim Terms

118. For the remaining claim terms of the ’782 Patent, I have applied their plain and ordinary meaning as understood by a POSITA as of the Priority Date.

X. GROUND 1: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT AND KRUIJSWIJK

A. Summary of FRA-Report

119. *Supporting Railroad Roadway Worker Communications with a Wireless Handheld Computer* (“FRA-Report”) (EX1004) is a two-volume report that was published by the U.S. Department of Transportation, Federal Railroad Administration in October 2004.

120. Volume I of FRA-Report (“Vol. I”) discusses the study from the perspective of the “Usability for the Roadway Worker” and Volume II (“Vol. II”) discusses the study as to the “Impact on Dispatcher Performance.” EX1004, Vol I: Title Page, Vol II: Title Page.

121. This report was developed to support the development of data link (digital communications) technologies from the roadway worker perspective to improve their safety.

1. One Reference or Motivation to Combine

122. A POSITA would have understood FRA-Report to be an omnibus multi-volume publication that constitutes a single publication for the points outlined below.

- Vol. II states that it is “***continuing development and evaluation of the [Vol. I] application***” EX1004, Vol. II: 3 (emphasis added), Abstract (“This ***report*** is the ***second in a series***”

documenting the development and evaluation of a software application to facilitate communications for railroad roadway workers.”) (emphasis added), ix, 5 (“The information described here adds to [Vol I] ...”), 72. As such, Vol. I and Vol. II form a single publication.

- Both FRA-Report volumes were published by the U.S. Department of Transportation, FRA. EX1004, Vol. I and Vol. II: cover page.
- Both FRA-Report volumes were published with the same report number (“DOT/FRA/ORD-04/13.” with a “i” and “ii”) and on the same date of October 2004. EX1004, Vol. I and Vol. II: Report Documentation Page, Boxes 2 and 10.
- Both FRA-Report volumes share overlapping authors. EX1004, Vol. I, Vol. II: Report Documentation Page, Box No. 6.
- A POSITA accessing FRA-Report publicly would have found them together as shown below.

Federal Railroad Administration

Research Reports

Reports are listed by their corresponding report numbers starting with the most recent published document. Click on the "Report Number" for a pdf copy of the report, if available. Additionally, all these reports are also available to the U.S. public through the [National Technical Information Service](#) in Springfield VA.



RESEARCH & DEVELOPMENT (R&D;) REPORTS	
REPORT NUMBER	TITLE
DOT/FRA/ORD-04/13.i	Supporting Railroad Roadway Worker Communications with a Wireless Handheld Computer: Volume I - Usability for the Roadway Worker
DOT/FRA/ORD-04/13.ii	Supporting Railroad Roadway Worker Communications with a Wireless Handheld Computer: Volume II - Impact on Dispatcher Performance

See e.g., EX1012, 1.

- Both volumes are in the field of, and solve the problem of, railway control for safe maintenance work and both have substantially similar network architecture. EX1004, Vol. I: Abstract, 1, 6, 14 (Fig. 2), 29, 37-38; Vol. II: Abstract, ix, 3, 5, 10-12, 16 (Fig. 4).

123. Given the significant overlapping aspects discussed above, I believe that a POSITA would have considered FRA-Report Vol. I and Vol. II to be one publication that would have been consulted by a POSITA together.

124. Alternatively, I believe a POSITA would have been motivated to combine the two volumes with a reasonable expectation of success for the reasons above.

2. Accessible to Interested Members of the Relevant Public

125. I believe the FRA-Report was accessible to interested members of the relevant public based on the FRA's statements, including that FRA-Report was generally "available to the public": "This document is *available to the public* through the National Technical Information Service, Springfield, VA 22161. This document is also available on the FRA website at www.fra.dot.gov." EX1004, Vol. I, Vol. II: front page (emphasis added), Report Documentation Page ("12a. Distribution/Availability Statement"), notice page ("This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange.")

126. Also, I believe the Internet Archive confirms FRA-Report was available to the relevant public at www.fra.dot.gov in, for instance, 2005, 2006, 2008, and 2009 and under “Research Reports.” EX1012-1015 (see “DOT/FRA/ORD-04/13.i” and “DOT/FRA/ORD-04/13.ii”); EX1016 (Internet Archive affidavit for the websites in EX1012-1015). It would have been normal for a POSITA to visit the FRA in 2005-2009 to keep updated on current information such that the POSITA would have reviewed or seen the FRA-Report.

127. I further believe the FRA-Report was accessible to interested members of the relevant public because, as discussed above, they were published together.

3. FRA-Report Overview

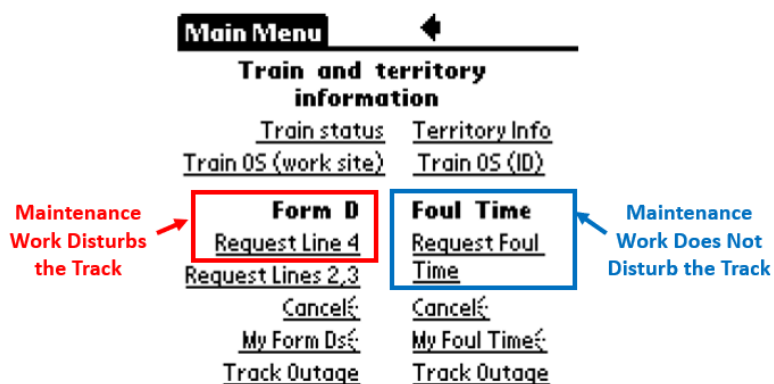
128. FRA-Report explains that current communications technology “offers the opportunity to improve productivity and safety in railroad operations” and that the Report “documents the design and evaluation of a digital communication device intended to improve roadway worker safety and productivity.” EX1004, Vol. I: iii; Vol. II: ix-x.

129. It also teaches that “[c]ommunications are vital in making railroad operations safe and efficient,” and that providing mobile devices to roadway workers for digital communications between them and central dispatch improves both safety and productivity. *Id.*, Vol. I: 1-2; Vol. II: 1-2.

130. FRA-Report describes a CTC system that, upon a railway worker's request from a mobile phone (PDA), blocks the track to "protect[] the roadway worker since it prevents the dispatcher from routing trains on that track" (*id.*, Vol. I: 6, 11-14) because "the dispatcher temporarily loses authority over that track" to the worker. *Id.*, Vol. II: 12.

131. The work authorization can include that a "track is placed off-limits (blocked) for other uses" via "Foul Time" or "Form D, Line 4." *Id.*, Vol. I: 6-8. "Foul Time" (sometimes called "track and time") is used when a worker needs a track taken out of service (*i.e.*, blocked) for maintenance work, but the work does not disturb the track. *Id.*, Vol. I: 8-9. "Form D, Line 4" is used when a worker needs a track taken out of service (*i.e.*, blocked) for maintenance work, and the work involves on-track equipment or will disturb the track. *Id.*

132. The Figure below depicts the roadway worker's mobile device interface for requesting blocking of the track under both Form D, Line 4 and Foul Time.



Id., Vol. I: 16 (Fig. 4, annotated); *see also* Vol. II: 17 (Fig. 5).

133. When the worker clicks “Request Line 4” or “Request Foul Time,” the worker is brought to a subsequent screen where the worker inputs information for the maintenance request, such as the worksite location, track number, and timing.

Field	Value	Label
Form D Line 4 Request		
Work site	185.1 Providence between/at 188.6 Lawn	Location
Track #	2	Track
Start time	11:23 am	Start
Duration	1 hour (estimated)	End
Send request Main Menu		
Request Foul Time		
Track #	2	Track
Between/at	73.6 Mill River Jct to 81.4 Branford Station	Location
Start time	12:05 pm	Start
End time	12:25 pm	End
Send request Main Menu		
Foul Time Request		
Track #	1	Track
Between/at	72.3 New Haven to 72.7 Fair St	Location
Start Time (24h)	12:00	Start
End Time (24h)	14:00	End
Send request Main Menu		

Id., Vol. I: 34 (Fig. A-3 (Left), annotated), 35 (Fig. A-4 (Center), annotated); Vol. II: 19 (Fig. 8 (right), annotated).

134. The roadway worker’s request for blocking of a track is transmitted to the dispatcher, such as via a “wireless data link” (*i.e.*, wireless access to the internet). *Id.*, Vol. I: Abstract (“A prototype communications device was developed for roadway workers to request train and territory information and to request track protection from the dispatcher. The device uses a wireless data link to send and receive information in digital form.”), iii, x, 13-14 (Fig. 2); Vol. II: ix-x, 15-16 (Fig. 4).

135. The worker who requested the block track will be sent by the CTC system information, including “Form D number (automatically assigned by system),

Form D recipient, date, direction of travel, track number, track location, and information about trains or track cars ahead.” *Id.*, Vol. I: 38.

136. The CTC requests confirmation by the railway worker. *Id.*, Vol. I: 34-35 (Figs. A-3, A-4). The confirmation request includes such information as: (1) date, (2) worker’s identity, (3) track and location, and (4) the dispatcher granting the request. *See id.*

Form D ◀ ▾ History Please confirm Form D 0001 Date: 01/28/2000 Delivered to: Oriol 4. 2 track out of service between/at Providence and Lawn in charge of Oriol Dispatcher North East Corridor Ask time Eff. Cancel Form D	Foul Time ◀ ▾ History Please confirm Foul Time Date: 01/28/2000 Delivered to: Oriol Permission to foul 2 track between/at Mill River Jct and Branford Station Issued: 9:05p Allowed: 9:25p Dispatcher: North East Corridor Accept Do not Accept	Please confirm Foul Time Date: 09/15/2000 Delivered to: HMSL Permission to foul 1 track between/at New Haven and Fair St Issued: 12:00p Allowed: 2:00p Dispatcher: NorthEastCoridor Accept Do not Accept
--	---	---

Id., Vol. I: 34 (Fig. A-3 (left)), 35 (Fig. A-4 (center)); Vol. II: 20 (Fig. 11 (right)).

137. The dispatcher operates a workstation can have multiple monitors that is used to control the switches and signals in the field which will block and unblock the track. *Id.*, Vol. II: 10 (“Each dispatcher is in charge of a specific territory where he/she has authority to route the trains, take tracks out of service, and grant work authorizations. Each dispatcher has a workstation to control the switches and signals.”), 11, 28.

138. The dispatcher workstation displays a color-coded representation of the track which the dispatcher operates to control a plurality of railways and interlocks.

For instance, Figure 1 below shows the interlocks for the tracks in blue have been controlled or selected by the dispatcher to block the track while the tracks in green have been unblocked.

Table 2. Representation of Color Code for Monitoring Track Status

Color	Meaning
White	Indicates that the track segment is available for routing trains or other uses.
Red	Means train or track vehicle occupancy. A train currently occupies that block.
Green	Indicates that the track segment has been cleared (authorized for use) for train movement. The train has not yet entered this block.
Blue	Indicates that a track section is authorized for track maintenance. This means that a portion of track has been protected for use by maintenance of way crews or track equipment. When the dispatcher gives track authority to a work crew, the dispatcher temporarily loses control over that section of track. Trains cannot enter this track segment unless authorized by the roadway worker responsible for that block.

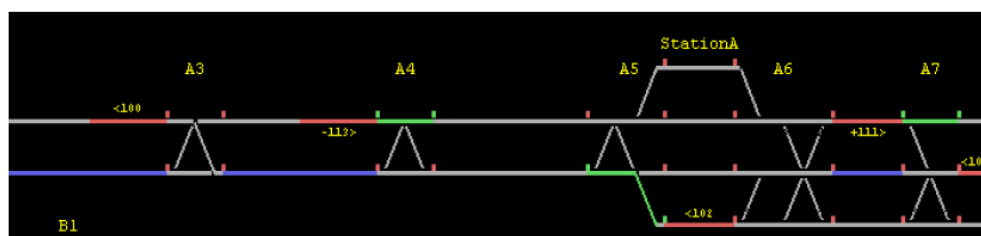


Figure 1. Track Chart Display

Id., Vol. II: 10-11 (Fig. 1, Table 2).

139. “If the dispatcher grants permission to work, (under Foul Time, Form D, or verbal permission) the track is placed off-limits (blocked) for other uses.” *Id.*, Vol. I: 6. In CTC systems, “blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track.” *Id.* In other words, “[s]witch operation is restricted, and the signals (wayside and in-cab) for the blocked track will display a stop signal at both ends to prevent movement by unauthorized

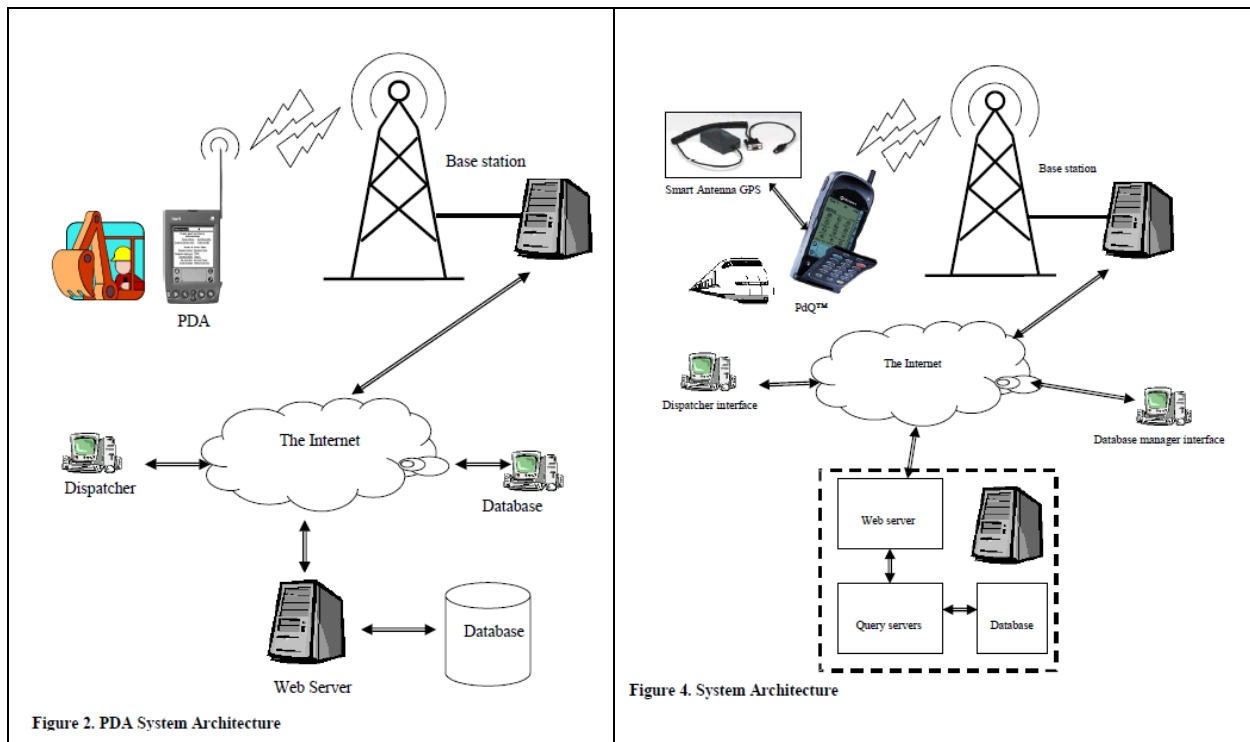
track vehicles.” *Id.*; Vol. II: 11 (“After receiving the request, the dispatcher decided whether to grant, modify, or deny the request. ... If the dispatcher intended to grant the work authorization, the dispatcher proceeded to protect the requested track.”).

140. Placing a block on the track transfers authority over that track to the worker, and the “dispatcher will not be able to reverse or normalize a switch that is part of the blocked track.” *Id.*, Vol. I: 6 (“Once authorization for track use is granted to a roadway crew and the track is blocked, the dispatcher has delegated authority over that track to the roadway crew.”); Vol. II: 12 (“Once a track is blocked, the dispatcher temporarily loses authority over that track.”). A dispatcher also cannot route trains over a blocked track. *Id.*, Vol. I: 6; Vol. II: 12-13.

141. After performing any work, the worker selects on the mobile phone “the links [or prompts] ‘Cancel/Fulfill’ or ‘Clear’ to give some track under his authority back to the dispatcher.” *Id.*, Vol. I: 36-37, 32 (Fig. A-1), 6; Vol. II: 12.

142. The dispatcher uses the workstation to unblock the track and make it available for other uses. *Id.*, Vol. I: 6; Vol. II: 12 (“Once the job is complete, the roadway worker returns control of the track to the dispatcher, who releases the track for other uses.”), 10-11.

143. Figure 2 of Volume I, and Figure 4 of Volume II depict the system architecture.



Id., Vol. I: 14 (Fig. 2 (left)); Vol. II: 16 (Fig. 4 (right)).

4. Analogous Art

144. Based on my review of the '782 Patent's prosecution history (EX1002), FRA-Report was not considered during prosecution of the '782 Patent.

145. In my opinion, FRA-Report is analogous art to the '782 Patent because FRA-Report is from the same field of endeavor as the '782 Patent of workers, railway work, or access control. EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36; EX1004, Vol. I: 6, 36-37, Abstract, 32 (Fig. A-1); Vol. II: 10-12, 18-20, Abstract and summary of the FRA-Report discussed above.

146. I believe Railware's expert's description in the SEPTA litigation of the '782 Patent supports this field of endeavor. EX1025, ¶¶20 ("control traffic over a

railway track section when a railway worker is working on or near the track section”), 54, 57; EX1024, 6, 13-14.

147. FRA-Report, as shown in my analysis above, is also reasonably pertinent to any purported problem addressed in the ’782 Patent, namely, controlling or authorizing access to a location or a region, such as by workers or railway traffic. EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36.

5. Prior -1179 IPR

148. I understand that Petitioner relies on the same primary reference (FRA-Report) as -1179 IPR, but in combination of new references not considered in the prior IPR.

149. As discussed above, (and more below), I believe the FRA-Report teaches blocking and unblocking the track at the worker’s request or control from his or her mobile device.

150. I further note that the FRA-Report is combined with new prior art (Kruijswijk, Schmitz, Macey and others) that teaches transmitting and/or returning a secret code from the relevant person to control access, such that the FRA-Report’s CTC system will not unblock the track until the relevant worker provides the code, *e.g.*, sending the code via the cancel/fulfill link or conveying the code by calling or texting the dispatcher. EX1005, 8:14-20, 3:29-34; EX1006, 6:63-7:4, 8:19-21, 5:58, 2:57-3:5, Abstract; EX1007, 15:22-35; EX1008, Abstract, 7:30-42, 9:41-44. I

further outline below with corroborating references that it was known to a POSITA to generate, transmit, and return a secret code, e.g., for safety and security, and the problem of protecting railway workers, among other reasons, which would have led a POSITA to apply the secret-code references (as the claimed release code) in FRA-Report. See *e.g.*, *infra* ¶¶ 233-238, 262-263.

151. In my opinion, based on these new references, the instant Petition renders the '782 Patent obvious.

B. Summary of Kruijswijk and Analogous Art

152. PCT Pub. No. WO 2007/107554 A1 (EX1005, “Kruijswijk”) published on September 27, 2007 and is therefore prior art under at least AIA 35 U.S.C. § 102(a) without any § 102(b) exceptions.

153. Kruijswijk discloses a system used for railway safety, that involves comparing a communicated “secret code” for identity verification. EX1005, Abstract, 12:13-21 (“railway track” “technicians” using this system for railway “safety checks”).

154. Kruijswijk teaches “generating, at the server station, the personal secret code, e.g. a random number of a predetermined number of digits.” *Id.*, 8:14-16, 3:30.

155. The secret code is transferred over a network such as the Internet to a railway worker or “railroad track ... technician[.]” *Id.*, 12:13-21, 13:25-28, 1:11-17, 3:29-34, 8:21-25.

156. Thereafter, the worker “transfer[s] a message containing the personal secret code from the [] communication device via the communication network to the server station” which verifies it with the saved code. *Id.*, 6:1-9 (“database includes, for a particular user ... the personal secret code itself, and/or verification data for verifying that a code entered indeed is the personal secret code of the respective user.”), 2:8-13, 11:8-17, Abstract.

157. Based on my review of the ’782 Patent’s prosecution history (EX1002), Kruijswijk was not considered during prosecution of the ’782 Patent.

158. In my opinion, Kruijswijk as shown in my above analysis is analogous art to the ’782 Patent because Kruijswijk is from the same field of endeavor as the ’782 Patent of workers, railway work, or access control. EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36; EX1005, 12:13-21, Abstract, 3:29-34, 8:14-25; EX1025, ¶¶20, 54, 57; EX1024, 6, 13-14.

159. For instance, Kruijswijk describes workers, railway work, and access control below:

One application of the invention is to use it for safety checks that must be performed by at least two technicians. Regulations (by the company or the government) may require some kind of proof that the safety checks were really performed by the technicians. With this invention, it can be proved that the technicians were at least at the same physical position. For instance, after the repair

of a railroad track, regulations may require inspection by two technicians.

Id., 12:13-21.

160. A POSITA would have understood that Kruijswijk is a form of “access control” because it verifies the railway workers are in the correct location, otherwise, they would have been asked to move to the proper location (or be denied access to the current location if not in the correct area).

161. Additionally, Kruijswijk, as shown in my analysis above, is reasonably pertinent to any purported problem addressed in the ’782 Patent, namely, controlling or authorizing access to a location or a region, such as by workers or railway traffic. EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36; EX1005, 12:13-21, Abstract, 3:29-34, 8:14-25.

C. Analysis of Independent Claims 1, 5

1. 1[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”

5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”

162. I understand that a preamble may or may not be limiting and believe that the FRA-Report teaches Limitations 1[Pre] and 5[Pre].

163. FRA-Report discloses a system and method for enhanced railway control to protect the safety of railway workers on or near tracks because it teaches a worker blocking and unblocking a track from a user terminal (mobile device) for worker safety. EX1004, Vol. I: Preface (“This report documents the design and evaluation of a digital communication device intended to improve roadway worker safety and productivity.”), Abstract (“A prototype communications device was developed for roadway workers . . . to request track protection from the dispatcher.”), 1 (“safety-critical communications related to train movements and allocation of track between roadway workers and trains.”), 2 (“Advances in communication technology have the potential to improve railroad safety and productivity.”), 2 (“Data link improved train and roadway worker safety, and situation awareness while lowering the dispatcher’s perceived workload compared to voice radio.”), 6 (“Roadway workers’ tasks include inspection, construction, maintenance, and repair of the track infrastructure (i.e., track, bridges, signal, and communication systems, and electric traction systems) on or near the track.”), iii (“This report documents the design and evaluation of a digital communication device intended to improve roadway worker safety and productivity.”); Vol. II: Abstract, 2 (“New technology in the form of digital data link communications and location finding systems such as GPS offer the potential to improve the safety and productivity of railroad operations. The use of

digital telecommunications has been proposed as a communication medium to supplement voice radio.”), 10 (“Dispatchers route trains and allocate track to roadway workers. Their most important responsibilities are to ensure safe movement of trains and personnel on the tracks”), 1.

164. Railway workers operate a PDA interface and request track protection, *e.g.*, Form D request to block the track from the CTC system. *Id.*, Vol. I: Abstract (“[a] prototype communications device was developed for roadway workers ... to request track protection from the dispatcher.”), 29 (“The PDA also enabled the roadway worker to request a variety of work authorizations (Form D and Foul Time).”), 32 (Fig. A-1) and 34 (Fig. A-3), 37; Vol. II: 16-17 (requesting “work authorization”), 18-20.

165. Dispatchers located at the CTC accept the requests and remotely place blocks on track sections from their workstations, thus ensuring the safety of the railway workers as they continue to directly communicate and interact with them: “[w]hen a **dispatcher [grants] a request for roadway worker protection** the **track is placed off-limits (blocked) for other uses**. In **Central Traffic Control (CTC)** territory, **blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track.**” *Id.*, Vol. I: 6 (emphasis added), 1; Vol. II: 12 (“[o]nce a track is blocked, the dispatcher temporarily loses authority

over that track.”), 11 (“When a dispatcher received a request for roadway worker protection, . . . [and if] the dispatcher intended to grant work authorization, the dispatcher proceeded to protect the requested track. At the Traffic Control Center, the dispatcher could use the track display to protect the track segment in question using software that controlled various switch[es] and signals in the field.”).

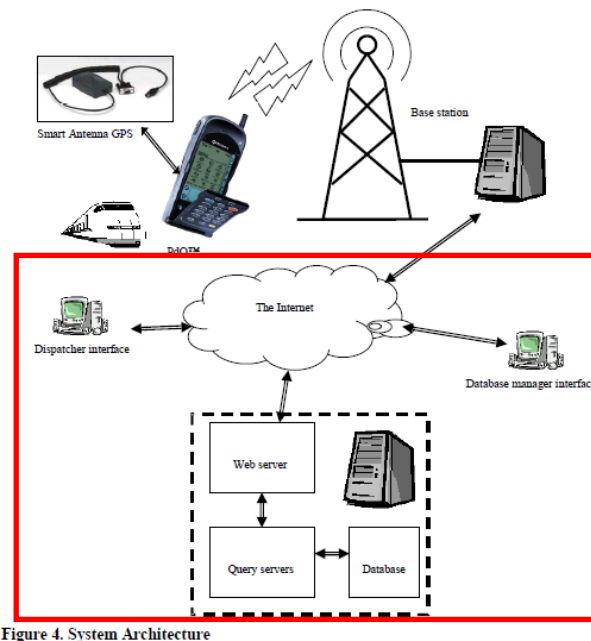
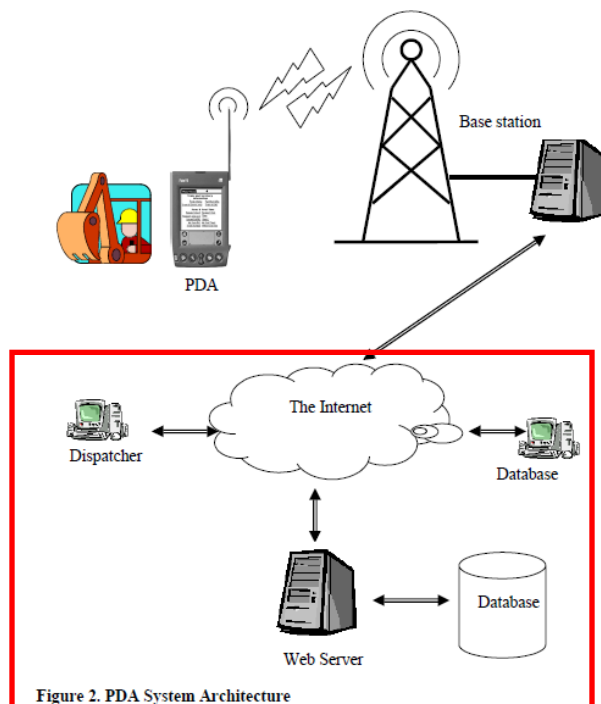
166. After the work, and the worker clicks on a link, “Cancel/Fulfill” or “Clear,” displayed by the CTC on the user terminal interface, “the roadway worker is able to give some track under his authority back to the dispatcher [CTC].” *Id.*, Vol. I: 36-37, 6 (“Once authorization for track use is granted to a roadway crew and the track is blocked, the dispatcher has delegated authority over that track to the roadway crew. . . . When the job is completed, the responsible crew foreman releases the track back to the dispatcher. In CTC territory, the dispatcher unblocks the tracking making it available for other uses.”), 7 (“Give control of the track back to the dispatcher.”), 14 (Figs. 2), 32 (A-1), 34 (A-3), 29; Vol. II: 12 (“Once the job is complete, the roadway worker returns control of the track to the dispatcher, who releases the track for other uses.”), 10-11.

2. **1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”**

167. I believe that FRA-Report teaches Limitation 1[A].

168. As explained above in Section V.B, CTC systems were well-known in the art and within the POSITA's general knowledge and skill.

169. As shown below, FRA-Report discloses a railway control apparatus or CTC dispatcher's computer (e.g., processor, non-transitory medium or storage), database, and web server and query server with associated database to communicate with railway workers.



EX1004, Vol. I: 14 (Fig. 2 (annotated)), 13, 31, 36-39, 1, 6; Vol. II: 16 (Fig. 4 (annotated)), 43-46; Limitations 1[Pre], 5[Pre] (discussing CTC control).

170. The railway control apparatus with the dispatcher's computer, web server, and/or query server each have a processor and a non-transitory medium such

as a hard drive or other storage for storing one or more programs of executable instructions because it was known computers (and servers) would have included processors and storage (such as RAM or hard drive) which store software or other computer programs containing instructions. Specifically, it was known to a POSITA that computers (servers) would have hard drive(s), memory (such as RAM), and other storage to store data necessary for the computer. It was common for computers to have processors to execute software (or instructions) residing on the computers as they are invoked, such as an operating system and other applications. *See e.g.*, EX1020, [0067] (“The control unit 190 includes a CPU (Central Processing Unit) for reading and executing a program from the storage unit 140 and controls each unit of the central control device 100.”), [0351] (“Also, a program for realizing all or some of the functions of the central control device 100 or the terminal device 200 may be recorded in a computer-readable recording medium. The program recorded in this recording medium may be read and executed with a computer system to perform a process of each unit. Also, the ‘computer system’ cited herein includes an OS or software of a peripheral device and the like.”), [0353].

171. A dispatcher’s computer with a processor would execute such software or computer programs to perform various functions, *e.g.*, for controlling switches and signals to block and unblock the tracks. EX1004, Vol. II: 10-11; *infra* ¶174.

172. A POSITA would further understand the dispatcher's CTC workstation or computer could be a standalone computer or multiple computers or in combination with one or more servers (or accesses the software on a central server or series of servers) because a railway system may require several computers or servers to operate a railway system. For instance, a POSITA would have made a design choice for a dispatcher's CTC workstation to consist of multiple computers in combination with multiple servers to provide a level of availability (fault tolerance) necessary to ensure that the system is operational and functional upon demand.

173. FRA-Report further teaches computers and software.

174. The FRA-Report describes that "the dispatcher would communicate with the roadway worker through the computer aided dispatch (CAD) system." *Id.*, Vol. II: 18. This includes that "[e]ach dispatcher has a workstation to control the switches and signals" and "[a]t the Traffic Control Center, the dispatcher could use the track display to protect the track segment [or block the track] in question using software that controlled various switche[s] and signals in the field." *Id.*, Vol. II: 10-11, 11 (Fig. 1 and Table 2), 28 ("The dispatcher can view the track on two monitors and can allocate track to trains, and track equipment or roadway workers using a variety of keyboard and mouse commands."); Vol. I: 1 ("In centralized traffic control

territory, switches and signals receive commands from the dispatcher's computer. These commands determine the track over which the train will travel ..."), 14 (Fig. 2) (showing dispatcher and other computers), 31 ("dispatcher's terminal," web server, and query servers described as a "computer"), 36 ("The web server is now running on a computer," "query servers used in this study were mainly written in Java (Sun Microsystems, 2001) ... [A] Common Gateway Interface (CGI) script ... [was] used as an interface between the web server and the query servers. It reads the HTML forms as sent by the PDA ... and returns the requested information to the PDA."), 38-40, 32-40 (Figs. A-1-A-5), 12 (Fig. 1 ("Dispatcher's terminal"))).

175. Figure 1 below illustrates a dispatcher's track display with a plurality of railways and interlocks. For instance, the dispatcher via the railway control apparatus selected the blue tracks to control the corresponding interlocks such that they are "protected for use" or blocked. Likewise, the dispatcher selected the tracks in green to control the corresponding interlocks such that they have been "cleared" or unblocked. As such, the dispatcher in FRA-Report controls from the display the blocking and unblocking of the tracks.

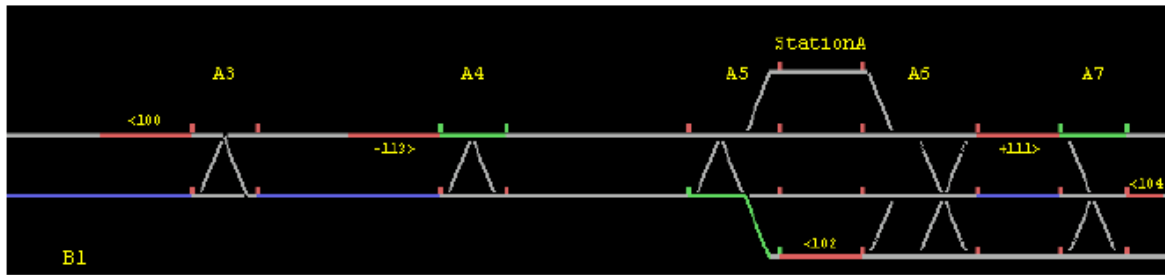


Figure 1. Track Chart Display

Table 2. Representation of Color Code for Monitoring Track Status

Color	Meaning
White	Indicates that the track segment is available for routing trains or other uses.
Red	Means train or track vehicle occupancy. A train currently occupies that block.
Green	Indicates that the track segment has been cleared (authorized for use) for train movement. The train has not yet entered this block.
Blue	Indicates that a track section is authorized for track maintenance. This means that a portion of track has been protected for use by maintenance of way crews or track equipment. When the dispatcher gives track authority to a work crew, the dispatcher temporarily loses control over that section of track. Trains cannot enter this track segment unless authorized by the roadway worker responsible for that block.

Id., Vol. II: 11 (Fig. 1 and Table 2 as well as related text), 10 (“Each dispatcher is in charge of a specific territory where he/she has authority to route the trains, take tracks out of service, and grant work authorizations. Each dispatcher has a workstation to control the switches and signals.”), 11 (“At the Traffic Control Center, the dispatcher could use the track display to protect the track segment in question using software that controlled various switch[es] and signals in the field.”); Vol. I: 6 (“If the dispatcher grants permission to work, ... the track is placed off-limits (blocked for other uses. In Central Traffic Control (CTC) territory, blocking a track protects the roadway worker since it prevents the dispatcher from routing

trains on that track When the job is completed, the responsible crew foreman releases the track back to the dispatcher. In CTC territory, the dispatcher unblocks the track making it available for other uses.”).

176. A POSITA would also have recognized that, in practice, other inputs may be used, such as touch screen to interact with the dispatcher’s track display, *e.g.*, Figure 1 above.

177. FRA-Report teaches another dispatcher interface below that a POSITA would combine with the above interface or use separately, where the dispatcher has assigned worker, “Oriol,” for “1 track out of service between/at 81.5 Branford and 90.4 Guilford”:

Requested Active Rejected and cancelled	
Requested Form Ds 0003, Oriol - Read 0002, Oriol - Read	Requested Foul Time 10.00a-10.30a, Oriol - Read
Form Ds waiting for time effective 0004, Oriol - Read	

Form D 0003 is Requested

Foreman: **Oriol** would like to work in 1 track at/between **Branford** and **Guilford**
 Desired starting time: **11.00a**
 Expected duration of work: **1 hour**

Form D #: **0003**
 Delivered to: **Oriol**
 Date: **01/28/2000**

Line 4: track out of service between/at
 and in
 charge of

Train: **North East Corridor**
 Dispatcher:

Please select 'Confirm' to grant permission to work or 'Deny' to disregard this form D request and then press 'Send Response'

☒ Confirm
☐ Deny Reason:

Figure A-5. Dispatcher Interface

EX1004, Vol. I: 40 (Fig. A-5).

178. The '782 Patent acknowledges it was known for a CTC system to control interlocks, block and unblock a track, in a railway network from a dispatcher's console. EX1001, 1:25-2:3 (background section describing a “control console which may include a map of the entire rail system ... [where] the dispatcher has control of each interlock signal ...”); Section V.B.

179. According to Railware, the below 2010 public document before the Priority Date shows a “control center where dispatchers control train traffic using a CTC system.” EX1025, ¶¶ 14, 22-23; Section V.B.



Id.

180. The railway control apparatus also has a network interface, as discussed above, through which it communicates via a network (*e.g.*, “Internet” in Figures 2 and 4) with the worker’s PDA, such as for work authorization. *See supra* ¶ 169 (discussing Figures 2 and 4); EX1004, Vol. I: 37 (“**Dispatcher Query Server.** Handles requests sent by the PDA that need dispatcher interaction such as requests that have to do with work permissions and answers sent by dispatcher to the PDA”) (emphasis in original), 36, 14 (Fig. 2 (“Internet”)), 13 (“[T]he server redirected the message to the appropriate destination via the Internet. Through this transaction, the PDA sent and received information to a web server. A number of servers look for requests sent by the PDA, the dispatchers, or a database manager.”), 1 (“Each dispatcher manages a portion of the track network.”); *see infra* 1[B], 5[A] (discussing worker’s mobile device or PDA access the Internet and communicates with the railway control apparatus).

181. Additionally, a POSITA would have understood that because the dispatcher (as discussed above) is remotely controlling switches and signals along the track, the railway control apparatus would have a network interface that is used to communicate with the signals and switches. *See supra* ¶¶ 174-175.

182. Thus, FRA-Report teaches Limitation 1[A]. I also thus believe FRA-Report teaches a railway control apparatus under Railware's construction, which is "broadly understood and encompasses a number of hardware ... software components beyond just the dispatcher's console" (*see supra* ¶ 114) because FRA-Report discloses a dispatcher's console or computer and other hardware and software (such as the database and servers) to control track blocking and unblocking.

183. Additionally, FRA-Report likewise discloses SEPTA's construction of a railway control apparatus because FRA-Report teaches a CTC "console used by the train dispatcher" for, *e.g.*, blocking and unblocking tracks. *See supra* ¶ 114.

184. Nonetheless, a POSITA would have understood that FRA-Report teaches SEPTA's construction because it is simply a design choice for the dispatcher's console to contain the software and hardware to perform the railway control apparatus functionality, and a POSITA would recognize that hardware and software can be stored on one computer or divided between different computers or servers to perform functionality.

3. **1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”**

5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”

185. I believe that the FRA-Report teaches Limitations 1[B] and 5[A].

186. As explained above in Sections V.A-D, it was within the POSITA’s general knowledge and skill for railway workers with mobile devices to communicate with a central control system.

187. FRA-Report discloses providing the railway worker with a user terminal (PDA or smartphone) which communicates via a network (such as the Internet or wireless network) with the railway control apparatus for work authorization or to block the track for work. EX1004, Vol. I: 13 (“[T]he server redirected the message to the appropriate destination via the Internet....[T]he PDA sent and received information to a web server. A number of servers look for requests sent by the PDA, the dispatchers, or a database manager. ... A work authorization was sent to the dispatcher while an information request was answered by the system”), 29 (“The PDA also enabled the roadway worker to request a variety of

work authorizations (Form D and Foul Time.”), 11 (“[A] software application was developed for use on a PDA with wireless communication capabilities. ... The application was specifically designed for use on the railroad, and was intended to facilitate communication between roadway workers and dispatchers.”).

188. FRA-Report explains that a “***device was selected that had wireless access to the Internet, and could be used anywhere along the track.***” *Id.*, Vol. I: 13 (emphasis added), x (“a personal digital assistant (PDA) with wireless access to the Internet.”), iii (“The prototype device was designed as a handheld information appliance with wireless access to the Internet. Roadway workers tested this data link device prototype as part of a usability evaluation.”), 14 (Fig. 2), 31; Vol. II: ix-x, 15-16 (Fig. 4).

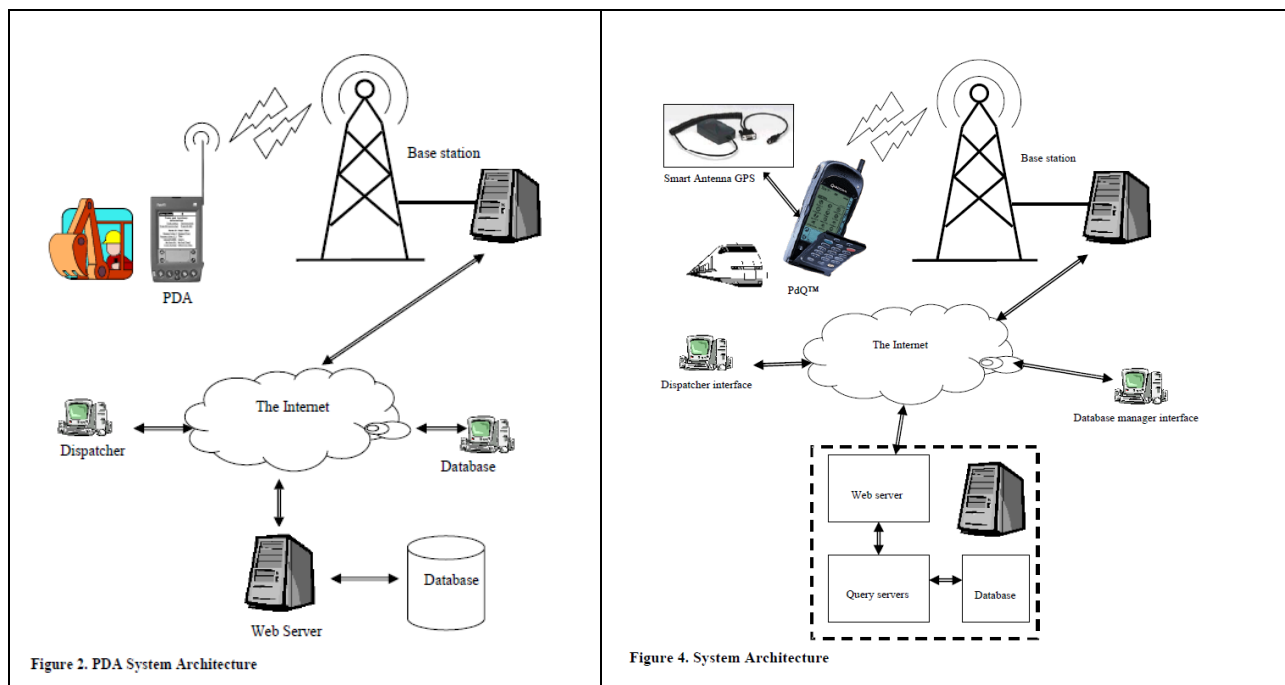
189. The worker may interface with the device using a stylus and touchscreen and the device’s menu driven interface. *Id.*, Vol. I: 13, 29; Vol. II: 16-17. They may also input information such as text using the buttons on the cell phone keypad. *Id.*, Vol. II: 15 (Fig. 2), 21.

190. FRA-Report also explains “the dispatcher would communicate with the roadway worker through the computer aided dispatch (CAD) system.” *Id.*, Vol. II: 18; Vol. I: 13 (“A number of servers look for requests sent by the PDA, the

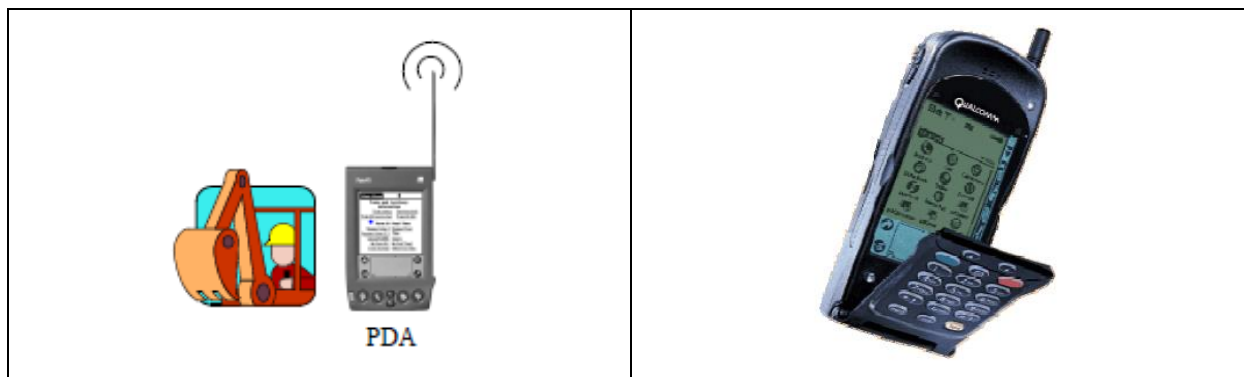
dispatchers, or a database manager. These servers represent the core of the system as they redirect the request to the appropriate recipient.”)

191. FRA-Report teaches that the railway control apparatus and worker communicate via a network or Internet. *Id.*, Vol. I: 14 (Fig. 2 (“Internet”)), 13 (“[T]he server redirected the message to the appropriate destination via the Internet.... A number of servers look for requests sent by the PDA, the dispatchers, or a database manager.”), 37 (dispatcher query server responds to “requests sent by the PDA” such as “work permissions and answers sent by dispatcher to the PDA”), 11 (“PDA with wireless communication capabilities”), 1, 36; Limitations 1[Pre], 5[Pre], 1[A] (discussing network or Internet communication between dispatcher and worker).

192. For instance, Figures 2 and 4 below show two-way communication between the user terminal (mobile device) of the railway worker and the railway control apparatus via a network, such as the Internet.



Id., Vol. I: 14 (Fig. 2) (left); Vol. II: 16 (Fig. 4) (right)



Id. (excerpts).

193. FRA-Report discloses a software application that runs on the mobile device and enables “the operator to ... request information related to operating conditions, and request work authorization. The application was specifically

designed for use on the railroad, and was intended to facilitate communication between roadway workers and dispatchers.” *Id.*, Vol. I: 11.

194. FRA-Report discloses that the railway worker’s mobile device (PDA) provides a user interface that displays information including prompts over the network from the railway control apparatus.

195. For example, Figure A-1 below displays information including prompts, *e.g.*, “Main Menu,” “My Form D’s,” “My Foul Time,” “Clear,” and “Cancel/Fulfill,” “You own these form Ds 0003 ... and the form D # 0003 has been cancelled,” among many others, received over the network from the railway control apparatus.

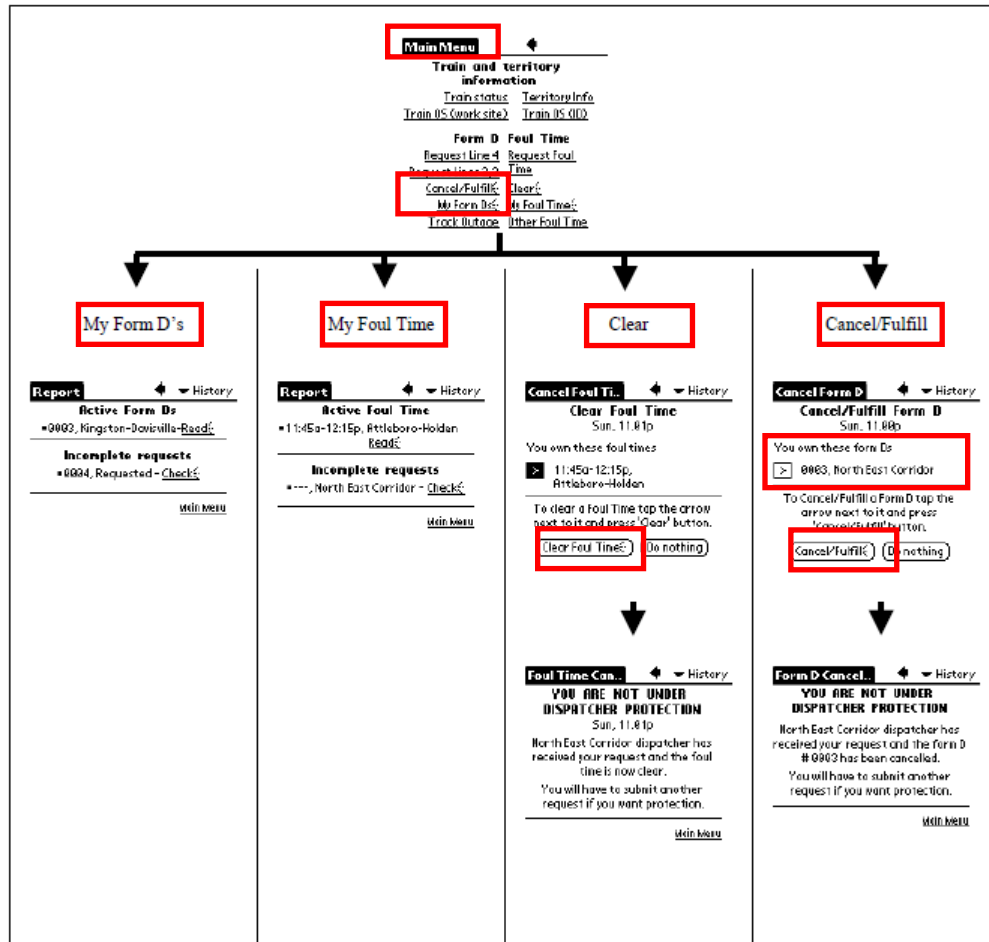


Figure A-1. PDA Screen Shots (1)

Id., Vol. I: 32 (Fig. A-1) (annotated), 31 (“**Web server**. This server hosts the master files that are used as templates to send information back to the PDA.”) (emphasis in original), 36 (“The query servers ... read[] the HTML forms as sent by the PDA ... and returns the requested information to the PDA”).

196. In Figure A-3 below, the railway control apparatus displays information including prompts on the worker’s interface, such as “Ask time Eff” and “Cancel Form D” buttons and “North East Corridor dispatcher has received your request ...”

in charge of Oriol.”

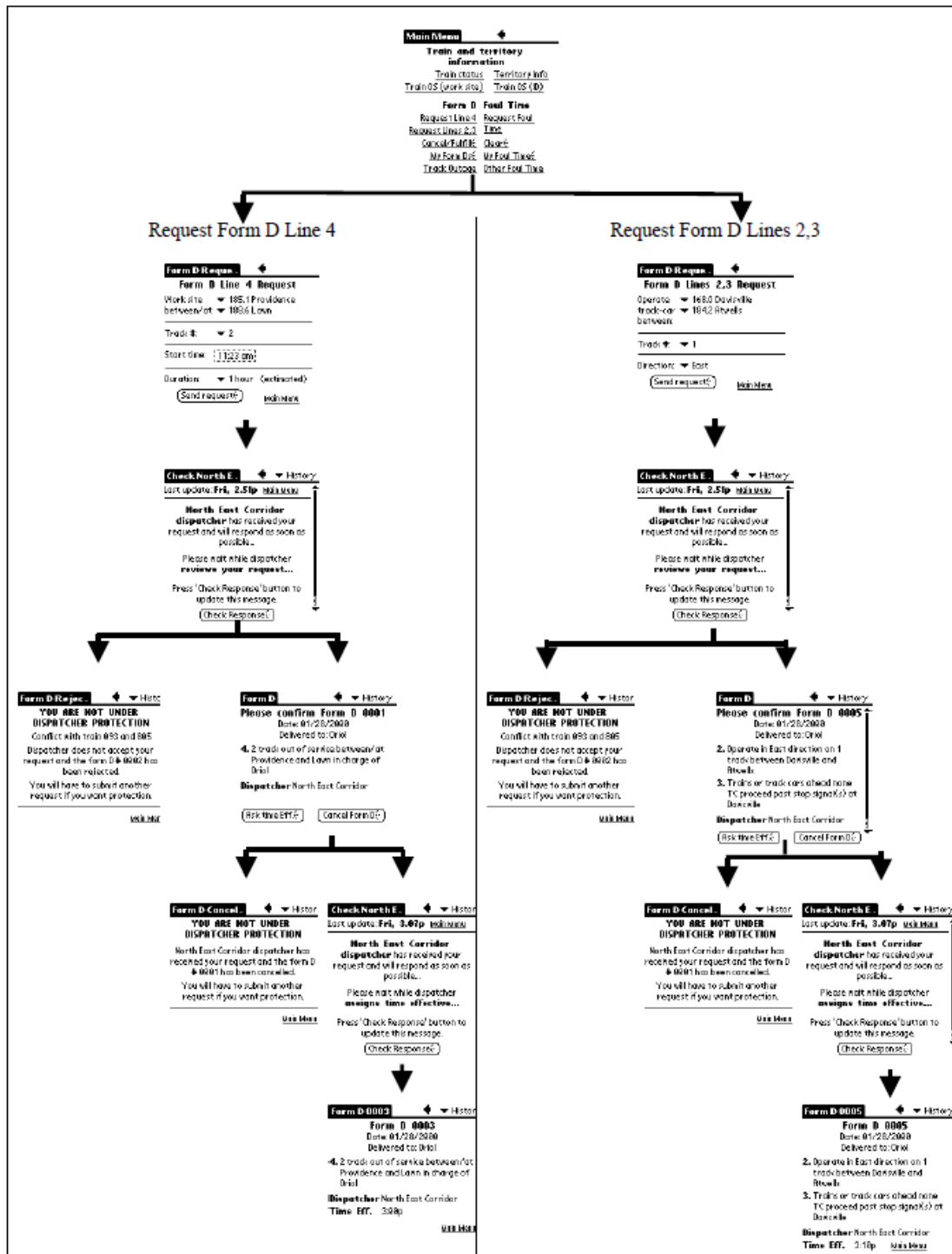
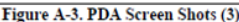


Figure A-3. PDA Screen Shots (3)



197. As another example in Figure A-4 below, the railway worker may be prompted to accept or not accept foul time.

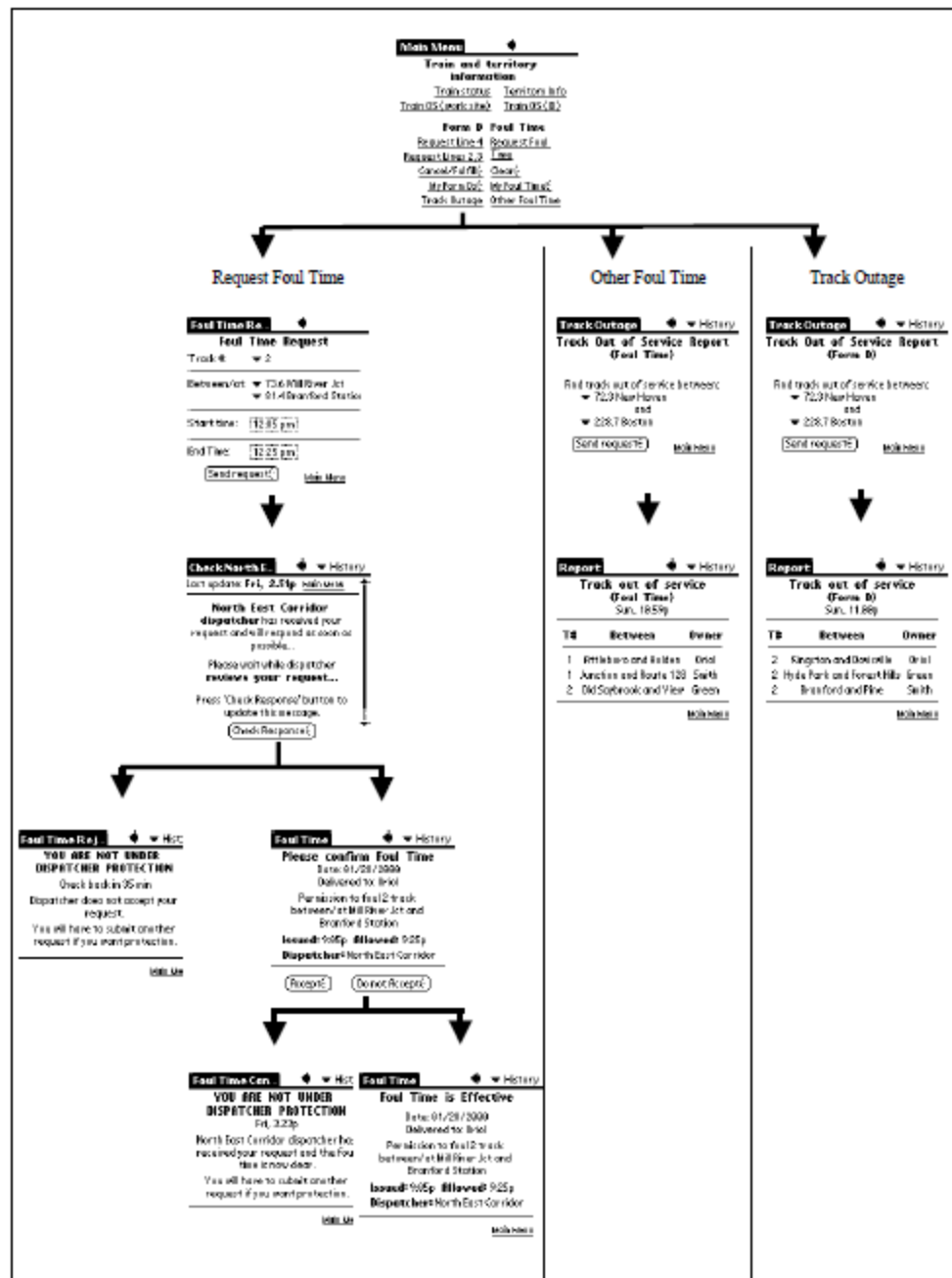
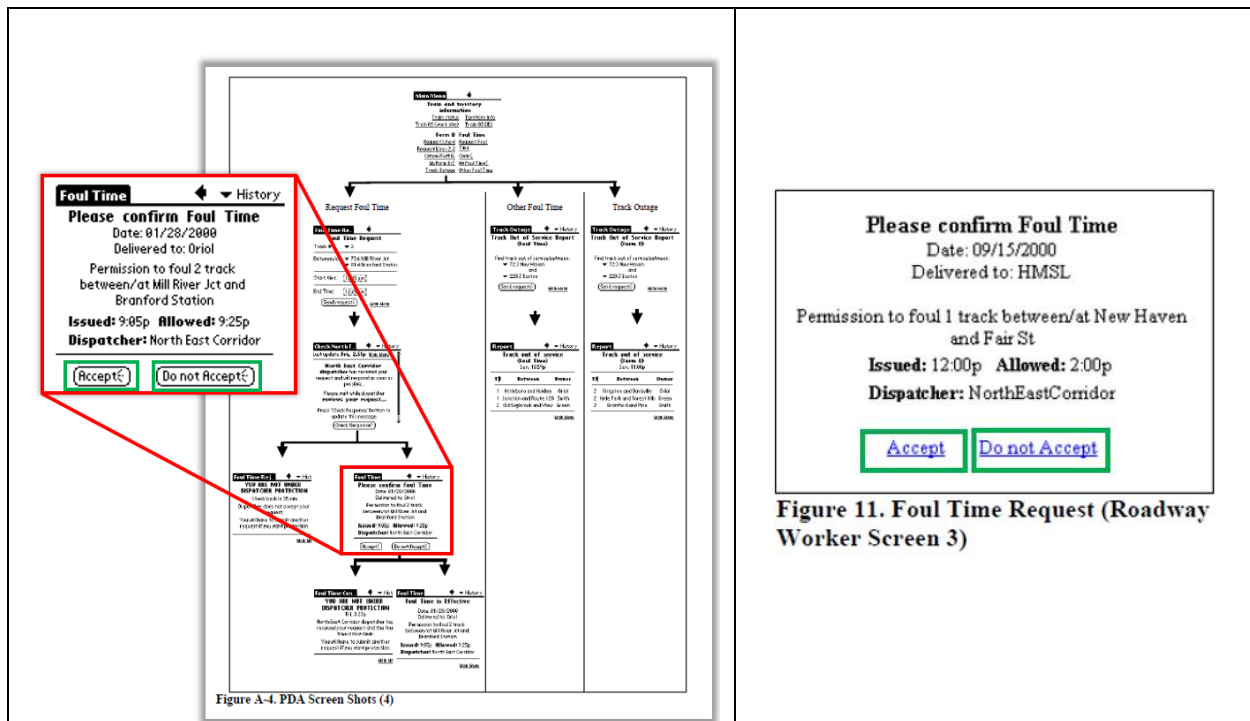


Figure A-4. PDA Screen Shots (4)



Id., Vol. I: 35 (Fig. A-4, left annotated); Vol. II: 20 (Fig. 11, right annotated), 19 (“After granting the initial request, the roadway worker receives a message ... [and] must acknowledge receiving the Foul Time request granted by the dispatcher by selecting ‘Accept’ or reject”)

198. The worker operating the PDA’s user interface—as shown in, *e.g.*, Figures A-1 and A-3-A-4 above—responds to prompts displayed thereon such as: **Fig. A-1**: “Cancel/Fulfill” or “Clear” (“Clear Foul Time”) button or link and “My Form Ds” link; **Fig. A-3**: “Ask for Time Effective” or “Cancel Form D” or “Check Response” buttons; or **Fig. A-4**: “Accept” button, among others, while requesting blocking and unblocking a track for work. *Id.* Vol. I: 32 (Fig. A-1, showing worker can select links), 34 (Fig. A-3, showing PDA interface and worker responding to

prompts displayed from the railway control apparatus), 36 (“Following the links ‘Cancel/Fulfill’ or ‘Clear,’ the roadway worker is able to give some track under his authority back to the dispatcher.”), 27 (“[b]efore giving any section of track back to the dispatcher, the system should prompt the roadway worker for confirmation.”), 16 (Fig. 4), 37 (“**Requests sent by PDA:** Request Form D line 4: ... to perform a work that will require a Form D line 4 authorization.”) (emphasis in original), 37 (“This request receives just the acceptance or rejection of the Form D as input. If the roadway worker accepts the Form D, the dispatcher will assign a time effective and it will become rule until it is cancelled or fulfilled.”), 11; Vol. II: 19 (“The roadway worker must acknowledge receiving the Foul Time request granted by the dispatcher by selecting ‘Accept’”), 18, 20-21

199. FRA-Report also discloses that the railway control apparatus and railway worker’s device can also communicate via the Short Message Service (SMS) (*i.e.* text messages). *Id.*, Vol. II: 15 (“The current prototype also exhibited the ability to send and receives short text messages (SMS). This enabled the dispatcher or roadway worker to alert each other when a request for track authorization was initiated or answered.”), 63 (“Short message service (SMS) is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as web servers, electronic mail,

paging, and voice-mail systems. Messages must be no longer than 160 alphanumeric characters. SMS is a reliable, low-cost communication mechanism for brief messages.”).

200. A POSITA would have understood that the mobile device has an interface (i.e., display screen) to display the SMS messages received from the railway control apparatus, and an interface, such as keyboard or touchscreen, to input and send SMS messages to the railway control apparatus.

201. In other words, the railway worker can respond to a prompt received in any SMS message, such as following a hyperlink to automatically execute an action or replying to the text message, which are both well-known to a POSITA.

202. Accordingly, FRA-Report teaches Limitations 1[B], 5[A], including “to respond to prompts displayed thereon.” It also teaches these limitations under Railware’s construction of any “standard type of user interface” and SEPTA’s construction to respond to the prompts displayed on the worker’s device. *See supra* ¶ 115.

4. **1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”**

5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”

203. I believe that FRA-Report teaches Limitations 1[C] and 5[B].

204. Using a centralized traffic control computer program to place blocks on one or more track sections to permit railway field workers to enter the track sections while blocking railway traffic to the track sections was well-known in the art and within the POSITA’s general knowledge and skill. *See* Section V.B; *see supra* ¶¶ 178-179. The ’782 Patent acknowledges this point, as discussed previously. EX1001, 1:22-2:3.

205. Claim 1 recites the “railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part [1[C]]. . . a code generation part [1[D]] . . . and a block removal part [1[E]]”

206. Claim 5 does not recite such parts.

207. The '782 Patent specification discusses the railway control apparatus implementing such “parts” as software and/or hardware. EX1001, 2:58-67 (“Such process may be largely automated via programming” including “the block placing part . . . a code generation part . . . [and] a block removal part”), 2:47-49 (“a centralized railway control system may be adapted (such as via computer hardware, software, or combination) ...”), 6:42-45 (“FIG. 3B shows an exemplary constitution of a computer 300 which can be configured by appropriate programming to operate as the railway traffic control apparatus 105 (FIG. 1A).”).

208. FRA-Report discloses implementing these three parts in software and/or hardware via the railway control apparatus’ processor. *See* Limitation 1[A] (describing railway control apparatus’ software and hardware); EX1004, Vol. I: 14 (Fig. 2), 31, 36-39, 40 (Fig. A-5).

209. As discussed in Limitations 1[B], 5[A], FRA-Report discloses that a railway worker may request via a link on a PDA interface to block the track, which “prevents the dispatcher from routing trains on that track.” EX1004, Vol. I: 6 (“If the dispatcher grants permission to work, (under Foul Time, Form D, or verbal permission), the track is placed off-limits (blocked) for other uses. In Central Traffic Control CTC) territory, blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track.”), 32 (Fig. A-1), 34 (Fig.

A-3), 29, 37, 1; Vol. II: 11 (“At the Traffic Control Center, the dispatcher could use the track display to protect the track segment in question using software that controlled various switch[es] and signals in the field.”), 10, 12; see Limitations 1[B], 5[A].

210. Specifically, the worker selects a Form D work authorization link on the worker’s mobile device interface, such as “Request Form D Line 4” or “Request Form D Lines 2, 3” in Figures A-1 or A-3, and transmits such work authorization to the railway control apparatus. EX1004, Vol. I: 16 (Fig. 4), 37 (“**Requests sent by PDA: Request Form D line 4**: ... to perform a work that will require a Form D line 4 authorization.”) (emphasis in original), 29 (“The PDA also enabled the roadway worker to request a variety of work authorizations (Form D and Foul Time).”), 37 (“**Dispatcher Query Server**. Handles requests sent by the PDA that need dispatcher interaction such as requests that have to do with work permissions and answers sent by dispatcher to the PDA”) (emphasis in original), 32 (Fig. A-1), 34 (Fig. A-3); see Limitations 1[Pre], 5[Pre]; 1[B], 5[A].

211. As discussed, FRA-Report teaches a dispatcher with a track display or terminal user interface via the railway control apparatus to place a block on one or more specified track sections (shown in blue). See Limitation 1[A]. This was also known to a POSITA. *Id.*

212. FRA-Report discloses that the “dispatcher would communicate with the roadway worker through” the CAD system. EX1004, Vol. II: 18; see Limitation 1[A].

213. The CAD system includes software that allows the dispatcher to remotely control the tracks via switches and signals using keyboard and mouse commands. See Limitation 1[A] (describing dispatcher’s computer); EX1004, Vol. II: 11-12, 28 (“The dispatcher can view the track on two monitors and can allocate track to trains, and track equipment or roadway workers using a variety of keyboard and mouse commands.”); Vol. I: 1 (“In centralized traffic control territory, switches and signals receive commands from the dispatcher’s computer. These commands determine the track over which the train will travel”).

214. Based on the worker’s Form D request—or request to block the track—the railway control apparatus’ processor executes a block placing part (software / hardware) to block the track, also denoted as “out of service” for maintenance.

Answer request for Form D line 4: ***Used by a dispatcher to grant or deny the requested Form D lines 4. If the dispatcher grants the Form D, the appropriate information will be sent to the roadway worker*** who requested it ... [such as] Form D number (automatically assigned by system) ... foreman in charge ***of the track out of service.***

EX1004, Vol. I: 38 (emphasis added), 36-37, 6 (“When a dispatcher receives a request for roadway worker protection [and if] the dispatcher grants permission to work, (under Form D) the track is placed off-limits (blocked) for other uses.”), 6 (“blocking a track protects the roadway worker,”); Vol. II: 12 (“Once a track is blocked, the dispatcher temporarily loses authority over that track. The dispatcher will not be able to reverse or normalize a switch that is part of the blocked track.”).

215. This block placing part software/hardware is also shown in Figure A-3 where the railway control apparatus blocks a track based on a work authorization request, particularly “***Form D Request Line 4 ... Send Request ... North East Corridor dispatcher has received your request ... 2 track out of service*** between/at Providence and Lawn in charge of Oriol.” *Id.*, Vol. I: 34 (Fig. A-3) (emphasis added); see ¶ 197 (showing Figure A-3).

216. A POSITA would have understood the reference to “track out of service” refers to “blocking” the track.

217. Figure 1 below shows that the dispatcher operating the computer has selected the blue tracks to block them: “Blue ... track section is authorized for maintenance ... [which means the] track has been protected [T]he dispatcher temporarily loses control over that section of track.” A POSITA would have

understood the reference to “track has been protected” as referring to “blocking” the track.

218. Likewise, the dispatcher has selected the tracks in green to unblock them: “track segment has been cleared (authorized for use) for train movement.” A POSITA would have understood the reference to “track segment has been cleared” as referring to “unblocking” the track.

Table 2. Representation of Color Code for Monitoring Track Status

Color	Meaning
White	Indicates that the track segment is available for routing trains or other uses.
Red	Means train or track vehicle occupancy. A train currently occupies that block.
Green	Indicates that the track segment has been cleared (authorized for use) for train movement. The train has not yet entered this block.
Blue	Indicates that a track section is authorized for track maintenance. This means that a portion of track has been protected for use by maintenance of way crews or track equipment. When the dispatcher gives track authority to a work crew, the dispatcher temporarily loses control over that section of track. Trains cannot enter this track segment unless authorized by the roadway worker responsible for that block.

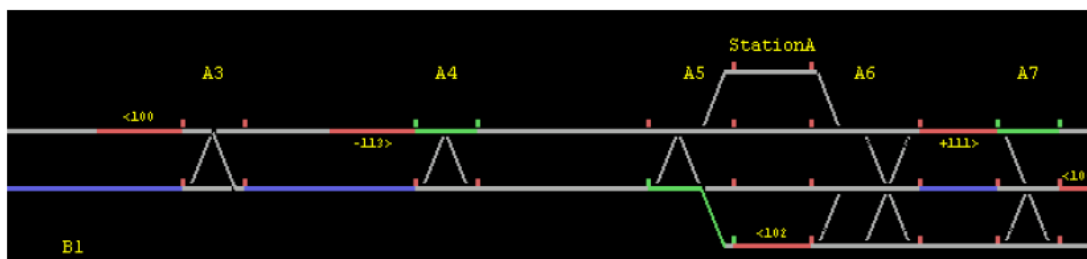


Figure 1. Track Chart Display

Id., Vol. II: Table 2, Fig. 1.

219. While the track is blocked (colored in blue on the “Track Chart Display” in Figure 1 above), the railway worker can enter the track to perform, *e.g.*,

maintenance work, because the worker—not the dispatcher—has authority over the track. *Id.*, Vol I: 32 (Fig. A-1), 34 (Fig. A-3 with track “out of service” until worker cancels the request), 6 (“If the dispatcher grants permission to work the track is placed off-limits (blocked) ... [and] **blocking a track protects the roadway worker since it prevents the dispatcher from routing trains on that track.**”) (emphasis added), 36-37 (“the links [or prompts] ‘Cancel/Fulfill’ or ‘Clear’ to give some track **under his authority back to the dispatcher.**”) (emphasis added); Vol. II: 11 (“Blue ... track section is authorized for maintenance ... [which means the] track has been protected When the dispatcher gives track authority to a work crew, the dispatcher temporarily loses control over that section of track.”), 12; *see infra* Limitations 1[E], 5[D] (unblocking the track). Thus, FRA-Report teaches Limitations 1[C], 5[B].

5. **1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”**

5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”

220. FRA-Report and Kruijswijk disclose and render obvious Limitations 1[D], 5[C].

221. FRA-Report teaches that a worker transmits a work authorization or request to block the track from the PDA's interface. See Limitations 1[C], 5[B]. Thereafter, the dispatcher in the track display via the railway control apparatus: blocks the track, generates a Form D number, and transmits that number and other information (*e.g.*, track related) to the worker's PDA or electronic contact address.

If the dispatcher grants the Form D [blocks the track], the ***appropriate information*** will be ***sent to the roadway worker who requested it***. This information includes ***Form D number*** (automatically assigned by system), ***Form D recipient***, date, track number, track location, and foreman in charge of the track out of service.

EX1004, Vol. I: 38 ("Form D line 4") (emphasis added), 34 (Fig. A-3) ("Delivered to: Oriol"); Limitations 1[A] (dispatcher computer with track display to block the track); 1[C], 5[B].

222. The worker has an electronic contact address for the PDA.

223. Specifically, the Form D number and other information above are "sent to the roadway worker who requested it" and the worker's PDA device ID is registered in the railway control apparatus database. EX1004, Vol. I: 39 ("The database includes ... Roadway workers (MWForemen.txt). Includes information about registered PDAs and their owner."), 57 ("Each Palm VII device had a built in device ID [and this] device ID was used to identify which roadway worker was

sending each request.”), 13 (“querying the database” to respond to work authorization); see Limitation 1[A] (discussing database).

224. Additionally, it would have been known to a POSITA that the PDA includes electronic addresses, *e.g.*, a MAC address, device ID, or IP address, and that some or all of that information would have been stored in the railway control apparatus’ database used for communicating with workers.

225. The Form D and other information transmitted by railway control apparatus to the worker is accessible on the worker’s user terminal (PDA) interface. See Limitations 1[B], 5[A] (displaying information, including prompts, on the worker’s interfaces); EX1004, Vol. I: 34 (Fig. A-3) (“Form D Line 4 Request ... North East Corridor dispatcher has received your request ... Please confirm Form D 0001 ... Delivered to: Oriol ... 2 track out of service between/at Providence and Lawn in charge of Oriol”), 32 (A-1) (“You own these form Ds 0003, NorthEast Corridor ... NorthEast Corridor dispatcher has received your request and the form D # 0003 has been cancelled.”), 31 (“**Web server**. This server hosts the master files that are used as templates to send information back to the PDA.”) (emphasis in original), 36 (“The query servers ... read[] the HTML forms as sent by the PDA ... and returns the requested information to the PDA”).

226. As mentioned, Claim 1 recites a code generation part (1[D)). A POSITA would have understood that the hardware (*e.g.*, processor) and software used to place a block would have included corresponding hardware and software to generate the code below or code generation part given the railway control apparatus CAD system controls switches and signals to block and unblock the track. See Limitations 1[A]; 1[C], 5[B].

(a) FRA-Report and Kruijswijk Combination

227. As discussed above, FRA-Report discloses that the dispatcher operates the track display (or another interface) via the railway control apparatus to block the track and generate and transmit information (*e.g.*, track-related) to the worker's electronic contact address accessible by the worker's PDA interface. See Limitations 1[C], 5[B]; 1[D], 5[C].

228. Kruijswijk supplies the "release code" such that the dispatcher in FRA-Report operates the track display via the railway control apparatus and blocks the track as well as generates (code generation part: software and/or hardware) and transmits the "release code" (as taught in Kruijswijk) to a worker's electronic contact address accessible by the worker's PDA interface.

229. Specifically, Kruijswijk teaches "generating, at the server station, the personal secret code" such as "a random number," and "cryptographical methods

may be applied” based on user data. EX1005, 8:14-20, 3:29-34. “Subsequently the personal secret code is transferred” by the server to the railway worker (“railroad track” “technician”), *e.g.*, mobile phone (such as SMS, email), over the network or Internet. EX1005, 8:21-25, 12:12-21 (railway worker “safety checks”), 11:8-17, Abstract, 13:25-28, 5:3-6, 3:29-34.

230. Thus, FRA-Report and Kruijswijk disclose and render obvious Limitation 1[D], 5[C]. Given the foregoing, they also disclose these limitations under the Board’s discussion of release code (*see supra* ¶¶ 110-111), including Kruijswijk’s secret code discloses and renders obvious the claimed “release code”: [a] Kruijswijk describes its code as a “secret code” and only received by the relevant worker; [b] to ensure secrecy, the code can be “terminate[d]” after “a one-time use”; and [c] the relevant worker transmits the secret code to the server, and the server verifies the relevant worker as part of “safety checks” after track maintenance is performed. EX1005, 12:13-21, 4:3-8, 9:8-10, 6:1-9 (“verification data for verifying that a code entered indeed is the personal secret code of the respective user.”), 7:1-17 (server verifying secret code entered).⁴

⁴ Kruijswijk discusses in a separate embodiment the secret code “may” be shared between workers, and Railware contends this is a secret code. EX1005, 11:19-24; EX1030, ¶89; *see supra* ¶ 113. Notably, as described above, Kruijswijk’s several

231. Further, FRA-Report and Kruijswijk disclose and render obvious Limitations 1[D], 5[C] under Railware’s construction, including Kruijswijk discloses and renders obvious the “release code” or a “code that is not readily available to the terminal user (*i.e.*, the dispatcher)” for the above reasons [a]-[c]. As such, the code taught in Kruijswijk is secret to the relevant person or “not readily available” to the dispatcher when Kruijswijk combined with the FRA-Report.

232. I understand Railware’s expert states that, “***any method of generating the string of symbols to serve as the Code Terms would be within the scope of the inventions.***” EX1025, ¶¶163 (emphasis added), 166; EX1024, 28. This understanding further supports that Kruijswijk teaches a secret code.

other embodiments teach a “secret code” that is only known to the relevant person (railway worker), including the server verifying the relevant worker provided the secret code. EX1005, 3:29-34 (“In an embodiment ... transferring the personal secret code to the second user”), 6:1-9 (“In particular the database includes, for a particular user, control data corresponding to a personal secret code PSC 23, for example the personal secret code itself, and/or verification data for verifying that a code entered indeed is the personal secret code of the respective user.”), 9:27-10:4 (“In an embodiment ... a message containing the personal secret code is transferred”), 8:14-35, 7:1-17.

233. Additionally, FRA-Report and Kruijswijk also disclose and render obvious Limitations 1[D], 5[C], including under the Board and Railware's understanding of release code, because a POSITA would have had a motivation to combine and reasonable expectation of success to implement Kruijswijk as a release code or secret code in FRA-Report as generating and transmitting a secret code, *e.g.*, for safety and security, only received by the relevant worker was taught before the Priority Date. EX1008, Abstract ("one-time use access code ... may be issued by a server ... [and] may be generated using a cryptographically strong random number generator"), 7:30-42 ("every access code issued by server 30 ... will be unique to the requester. ***That requester, and only that requester, will know the access code***") (emphasis added), 9:41-44; EX1007, 15:22-35 ("specific code" is "only known to the" railway worker), 20:25-37; EX1009, 13:66-14:8 ("generates a confirmation code and supplies that code to the customer" where the code is "randomly generated" and "will be known only to the" relevant person), 15:7-27; EX1011, 4:31-38 (server generating a "cipher lock code" for the relevant user), 5:7-14 (user permitted "one-time access"), 3:61-4:3, Abstract, 5:25-30. Thus, it would have been predictable or obvious to try in implementing Kruijswijk as the claimed release code or secret code in FRA-Report.

234. Additionally, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Kruijswijk as a release code or secret code in FRA-Report to address the known problem of protecting railway workers from removal of a block by the dispatcher while track work is performed. *See* Section V.A. In other words, such a release code would have ensured that it is only known to the worker and the track can only be released by the worker returning that code.

235. Similarly, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Kruijswijk as a “release code” or secret code because it was known to a POSITA that a worker uses a mobile phone for controlling track possession, including to take control of a work zone and return it to the central system, and thus implementing a code only known to the worker would have been obvious to try for safety and security. *See* Section V.D.

236. Likewise, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Kruijswijk as a “release code” or secret code given the use of one-time password or one-time code for authorization or authentication was prevalent before the Priority Date, as shown above and other prior art. *See* Section V.C.

237. In my view, a POSITA would have been motivated with a reasonable expectation of success to use a one-time code in the railway industry, including the

FRA-Report, because the one-time code would have improved safety and security of the worker such that only the worker would know the code and would return the one-time code to release the track block.

238. Also, such known authentication systems would have driven a POSITA to apply such authentication to ensure the code is only known to the worker and the track is only unblocked when the railway control apparatus receives the code transmitted by the worker. Thus, it would have been predictable in implementing Kruijswijk as the claimed release code or secret code in FRA-Report.

239. Accordingly, FRA-Report and Kruijswijk disclose and render obvious Limitations 1[D], 5[C]. I further believe FRA-Report and Kruijswijk teach “user terminal” under Railware’s construction (dispatcher’s terminal) in Claim 5 because, as discussed above (*see supra* ¶¶ 220-226, Limitations 1[A]; 1[C], 5[B]), the dispatcher operates a computer to block the track as well as generate and transmit the release code to a worker’s electronic contact address accessible by the worker’s PDA interface. For the same reasons, they teach SEPTA’s construction in Claim 5 and both parties’ construction in Claim 1 as the worker’s terminal (*see supra* ¶ 116).

(b) Motivation to Combine FRA-Report and Kruijswijk with a Reasonable Expectation of Success

240. A POSITA would have had a motivation to combine with a reasonable expectation of success such that the dispatcher operates the track display via the

railway control apparatus and blocks the track as well as generates and transmits the “release code” (as taught in Kruijswijk) to a worker’s electronic contact address accessible by the worker’s PDA interface given Kruijswijk and FRA-Report involve railway technology and worker safety. See Sections X.A.3-4, X.B. Kruijswijk teaches that its invention is applied in the railway field (EX1005, 12:13-21, “after the repair of a railroad track”), is an Internet-based system—as with the FRA-Report, and thus would have been a natural and predictable option for a POSITA to look to when modifying the FRA-Report. See Sections X.A.3-4, X.B. And further, FRA-Report (like Kruijswijk) also discusses improving safety based on where rail workers are when providing confirmations. EX1004, Vol. I: 20-21 (“work authorizations accepted in a location that was not the one requested.”); EX1005, 12:13-21.

241. CTC systems and secret-code verification systems were known, so modifying FRA-Report with the code taught in Kruijswijk would have been simply applying a known technique to a known device for safety and security improvement. See Sections V.B-C.

242. FRA-Report recognized that a secret-code system (or similar technologies) would have been implemented in the FRA-Report to augment worker safety: [1] “improve roadway worker safety and productivity” (EX1004, Vol. I: Preface); [2] “positively identify the person communicating” (*id.*, Vol. I: 57); and

[3] implement “a verification system that prevent[s] or minimize[s] common human error.” *Id.*, Vol. I: 9, 27 (“Before giving any section of track back to the dispatcher, the system should prompt the roadway worker for confirmation.”), iv (“develop intelligent railroad systems”), Report Documentation Page (“Subject Terms ... intelligent railroad systems”). Likewise, prior art discusses that technologies would have been applied to augment worker safety. EX1028, 4 (“the potential exists to develop portable roadway worker devices that combine technologies for ... reliable communication, as well as data storage, retrieval, and computation functions to support maintenance and inspection tasks”); EX1015, 1 (EX1028 referenced in March 2009); Sections V.A.D. Thus, such teachings provide the motivation to combine FRA-Report and Kruijswijk.

243. A POSITA would have been further motivated by the FRA-Report’s goals to “improve roadway worker safety and productivity” (EX1004, Vol. I: Preface) and implement a “verification system.” EX1004, Vol. I: 9 (“a verification system that prevent[s] or minimize[s] common human error.”), 27 (“Before giving any section of track back to the dispatcher, the system should prompt the roadway worker for confirmation.”), iv (“develop intelligent railroad systems”); Limitations 1[B], 5[A] (FRA-Report teaching two-way communication between the worker’s user terminal and railway control apparatus).

244. A POSITA would have thus recognized, to prevent the dispatcher from erroneously revoking a blocked track, that FRA-Report would implement a “handshake” or verification protocol where the code taught in Kruijswijk is associated with the blocked track and transmitted to the worker who later unblocks the track with the same code. Kruijswijk as described above teaches verifying the user with a secret code. EX1005, 6:1-9, 7:1-17.

245. This would have enhanced the prior worker and the dispatcher handshake or two-way communication over radio. EX1028, 14-15 (discussing dispatcher and worker communication, such as over radio, to block and unblock the track for worker safety).

246. Notably, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection.” EX1004, Vol. I: 57. FRA-Report even proposes various solutions including (i) a “device ID” to be sent with messages and/or (ii) “password-protected access to the system” such as a “personal password.” *Id.*, 57-58. Therefore, FRA-Report urges a need and readiness to implement robust verification measures (including password-based ones) to effectively verify roadway worker identities, and Kruijswijk teaches one such solution in the railway maintenance field.

247. A POSITA would have been motivated to incorporate Kruijswijk in FRA-Report for at least this reason.

248. A POSITA would have appreciated that modifying FRA-Report with Kruijswijk would have had a reasonable expectation of success. FRA-Report was published in October 2004, or nine (9) years before the Priority Date, and built and tested a railway worker and dispatcher CTC system containing a server(s) with software generating railway data and transmitting such data to the railway worker for controlling from a mobile device blocking and unblocking the track. Limitations 1[A]; 1[C], 5[B]; 1[D], 5[C]; 1[E], 5[D]. Further, the worker's PDA in FRA-Report has existing encryption and decryption technology (EX1004, Vol. I: 57), otherwise, this was known. EX1011, 4:25-24. Thus, it would have been predictable to generate and transmit a code in FRA-Report to the worker's device. *See also* EX1004, Vol. II: 15, 21, 27, 41, 63 (SMS "is a globally accepted wireless service that enables the transmission" and "is a reliable, low-cost communication mechanism."). FRA-Report notes that "[t]he system is designed to be highly configurable" (EX1004, Vol. I: 41); EX1021; EX1028. With such hardware and software, the FRA-Report would have had flexibility when the code is generated, such as before or after the block is placed, depending on the needs for the system, such as safety,

efficiency, and workflow, and would have been a predictable design choice for a POSITA designing or modifying a system as disclosed in FRA-Report.

249. Likewise, there would have been a reasonable expectation of success given that, for example, Kruijswijk was published in 2007 and Macey was published in 2010, which both involve a worker using a mobile phone and code in a rail system. EX1005, 8:14-25, 12:13-21, 11:8-17, Abstract, 13:25-28, 5:3-6, 3:29-34; EX1007, 15:16-35, 20:31-37, 16:1-21, 13:35-14:4. This shows that a code was implemented in railway systems. Also, from October 2004 to before the Priority Date, mobile device, server, and technology capabilities evolved, and with such enhanced technology, it would have been predictable for a POSITA to apply those capabilities to enhance FRA-Report with a code-based system. *See* Sections V.A-D; EX1017, 8 (¶¶ 5-7), 15-16 (named inventor acknowledged to the USPTO that mobile phones, text messaging, and email were conventional before the Priority Date).

250. A POSITA would further have been motivated to modify FRA-Report with a reasonable expectation of success for the worker's interface to receive and display (such as prompt or text box message) the release code taught in Kruijswijk given the worker's existing user interfaces in the FRA-Report and it is a design choice by a POSITA. Limitations 1[B], 5[A].

251. Alternatively, a POSITA would have been motivated to modify FRA-Report to transmit the code taught by Kruijswijk with a reasonable expectation of success to the worker's electronic contact address through other methods, including text message or email message given such methods would have provided an alternate form to the worker and text, email, and links were well-known. EX1004, Vol. II: 15, 21, 27, 63; EX1017, 15-16 ("05 March 2010 People love their mobile phone That means not just talking, but e-mailing, texting ..."). As another option, the text and email message would have included an embedded link to return the code.

6. **1[E]: "railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections."**

5[D]: "permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return."

252. FRA-Report and Kruijswijk disclose and render obvious Limitations 1[E], 5[D].

253. FRA-Report describes that the "worker can retrieve a list of Form Ds ... *under his/her authority* ... [and] [f]ollowing the link[] 'Cancel/Fulfill' ... the *roadway worker is able to give some track under his authority back to the dispatcher.*" EX1004, Vol. I: 36 (emphasis added), 37 ("Retrieve list of active Form Ds: Used whenever a roadway worker has finished their job or wants to cancel or

fulfill a Form D and is giving the track back to the dispatcher.”) (emphasis in original), 37 (“My Form Ds: Used to retrieve a list of current Form Ds . . . under the authority of the roadway worker holding the PDA.”) (emphasis in original), 38 (“Retrieve list of active Foul Time: Used whenever a roadway worker has finished their job or wants to clear a Foul Time and is giving the track back to the dispatcher.”) (emphasis in original), 38 (“My Foul Time: Used to retrieve a list of current Foul Times . . . under the authority of the roadway worker.”) (emphasis in original), 39, 31, 32 (Fig. A-1); see Limitations 1[B], 5[A].

254. After selecting a “Cancel/fulfill” link, the worker’s mobile device communicates to the railway control apparatus that a track block “under [worker’s] authority” may now be removed or unblocked. *Id.*, Vol. I: 36, 37 (“Cancel/Fulfill Form D: Works together with [Retrieve list of active Form Ds]. This is the step to actually cancel or fulfill the Form D.”) (emphasis in original), 38 (“Clear Foul Time: Works together with [Retrieve list of active Foul Time]. This step is required to clear the Foul Time.”) (emphasis in original), 16 and Fig. 4 (“Cancel” Form D and “Cancel” Foul Time), 32 and Fig. A-1 (“Clear Foul Time” and “Cancel/Fulfill Form D”); Vol. II: 15 (“The application can also be used to request and cancel work authorizations.”), 18 (“The application software also handles the several types of

work authorization requests and cancellations (Foul Time and Form Ds). ... Cancel work authorization (automatic).”); see Limitations 1[B], 5[A].

255. The railway control apparatus block removal part (software and/or hardware) unblocking the track is likewise shown in Figure A-1, particularly “***Cancel/Fulfill Form D ... You own these form Ds 0003, NorthEast Corridor ... Cancel/Fulfill ... Form D Cancel ... YOU ARE NOT UNDER DISPATCHER PROTECTION*** [track unblocked] NorthEast Corridor ***dispatcher has received your request*** and ***the form D # 0003 has been cancelled.***” *Id.*, Vol. I: 32 (Fig. A-1) (emphasis added), 37 (“Cancel/fulfill Form D: Works together with the previous request. This is the step to actually cancel or fulfill the Form D.”) (emphasis in original), 6 (“When the job is completed ... the dispatcher unblocks the track making it available for other uses.”).

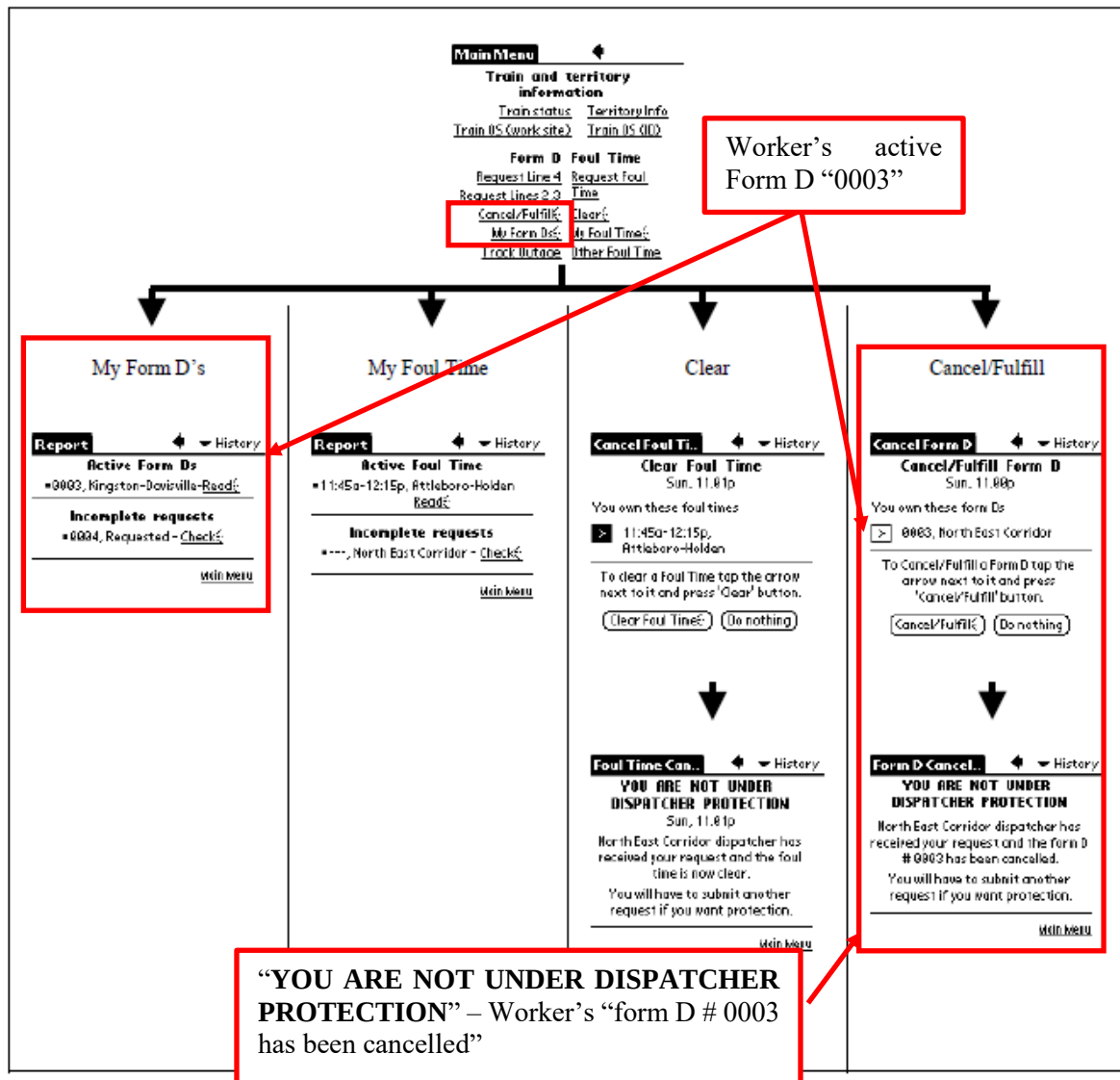


Figure A-1. PDA Screen Shots (1)

Id. (annotations added).

256. Claim 1, unlike Claim 5, recites a block removal part (1[E]). A POSITA would have understood that the hardware and software used to place a block (see Limitations 1[C], 5[B]) would have included corresponding hardware (*e.g.*, processor) and software to remove the block or block removal part given the railway

control apparatus CAD system controls switches and signals to block and unblock the track. See Limitations 1[A]; 1[C], 5[B].

(a) FRA-Report and Kruijswijk Combination

257. As discussed above, FRA-Report teaches the worker selects the “Cancel/fulfill” link on their PDA (user terminal) to transmit information to the railway control apparatus block removal part (software and/or hardware), which unblocks the track “under [worker’s] authority.” EX1004, Vol. I: 36-37, 6; Vol. II: 15, 18; Limitations 1[B], 5[A].

258. Kruijswijk supplies transmitting the “release code” such that the worker in FRA-Report transmits the code, *e.g.*, selecting the “Cancel/Fulfill” link (or, *e.g.*, by call, text, email), to the railway control apparatus, which will only unblock the track once the transmitted code is entered by the dispatcher or automatically by the railway control apparatus. EX1024, 11-12 (Railware asserting “dispatcher ... enters the removal or release code into the railway control apparatus” or automatically “without dispatcher intervention”); EX1025, ¶¶ 296 (asserting “numerous ways ... the release or removal code may be returned to the dispatcher or the railway control apparatus” including “manually” and “automatically”), 312-313, 321, 341, 350, 358.

259. Specifically, Kruijswijk teaches that the code must be returned to the server by the worker as, *e.g.*, a “safety check.” EX1005, 12:13-21. Kruijswijk

describes that “after the repair of [the] railroad track” (*id.*, 12:17-18), the worker’s mobile phone “request[s] ... to enter a personal secret code.” *Id.*, claim 1, 7:1-17, 2:8-11.

260. Thereafter, the worker (via the phone) “transfer[s] a message containing the personal secret code from the [] communication device via the communication network to the server station.” *Id.*, claim 1, 7:1-17, Abstract.

261. The “server station” then “verif[ies]” “the personal secret code” based on the worker’s code in the database. *Id.*, Abstract, 7:1-17 (“The personal secret code ... is verified using the user control data from the database.”), 6:1-9 (“verifying that a code entered indeed is the personal secret code”), 12:13-21 (worker “safety checks”). Thus, FRA-Report and Kruijswijk disclose and render obvious Limitations 1[E], 5[D].

262. Additionally, FRA-Report and Kruijswijk disclose and render obvious Limitations 1[E], 5[D] because a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Kruijswijk the transmitted release code in FRA-Report to the railway control apparatus, which will only unblock the track with the transmitted code given it was known. EX1007, 16:1-21 (railway worker must enter on their mobile device “a specific code before it is deemed the target zone [] is safe for the passage of the vehicle.”), 13:35-14:4; *see*

also EX1006, 7:8-15 (code “is transmitted again to the authorization computer” which “verifies” the code to control, *e.g.*, a locking mechanism), Abstract, 5:7-9, 5:24-48, 7:60-61.

263. Specifically, Macey teaches the railway worker enters a secret code “such as a PIN (personal identification number) or password ***only known to the user***” which “[u]pon the successful entry of this code to the interface [of the remote command center, it] ... transmit[s] a signal to the signalling device” which changes “from a red light [(blocked track)] to a green light [(unblocked track)] and signals the operator of the train to proceed.” EX1007, 15:16-35 (emphasis added), 20:31-37. Thus, it would have been a predictable design choice to implement from Kruijswijk the transmitted secret code in FRA-Report to unblock the track.

264. A POSITA would have had a motivation to combine and reasonable expectation of success to implement from Kruijswijk the transmitted release code in FRA-Report to unblock the track to address the known problem of protecting railway workers from improper removal of a track block. *See* Section V.A. Thus, a POSITA would have used the worker’s transmitted code to unblock the track to ensure the track can only be released by the worker returning that code.

265. Similarly, a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Kruijswijk the transmitted

release code in FRA-Report to unblock the track because it was known to a POSITA that a worker uses a mobile phone for controlling track possession, including to take control of a work zone and return it to the central system, and as such, implementing a code to only unblock a track with the release code (as taught by Kruijswijk) would have been obvious to try for safety and security. *See* Section V.D. Thus, the worker with the code would hold possession of the track and would transfer such possession by transmitting the code to the dispatcher to unblock the track.

266. Also, a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Kruijswijk the transmitted release code in FRA-Report to unblock the track given the use of one-time password or one-time code transmitted to a server for authorization or authentication for safety and security was prevalent before the Priority Date. *See* Section V.C.

267. In my view, such known authentication systems would have driven a POSITA or would been predictable to apply code authentication to railway systems to ensure a track block is only unblocked when the railway control apparatus receives the code transmitted by the railway worker. In other words, the release code would have ensured the dispatcher would neither intentionally nor inadvertently removes the track block without the worker's release code (explicit permission). Thus, it

would have been predictable or obvious to try to implement Kruijswijk in FRA-Report.

268. Alternatively, FRA-Report and Kruijswijk teach Limitations 1[E], 5[D] because Railware has apparently stated that these limitations include when a worker is unavailable to transmit the code in return, and thus a “Chief Traffic Controller” (or similar person) retrieves the code from the railway control apparatus’ storage. EX1024, 21-22; EX1025, ¶¶118-120; *see supra* ¶ 110 (“unavailable”); *see supra* ¶ 117 (“***the code can be returned in a number of different ways***” and is ***not “limited to ... only via the user terminal of the railway field worker”***) (emphasis added). Such a code lookup would have been obvious to try to a POSITA, where another person obtains the saved code from storage in the railway control apparatus and enters the code (or provides it to the dispatcher) to release the track block. It was routine and predictable, as outlined below, to store codes and use them to control another action, such as worker safety or control access. *See infra* ¶ 273.

269. As mentioned above, Railware asserted that the code can be manually entered by the dispatcher or automatically “without dispatcher intervention.” *See supra* ¶ 258. Moreover, Claims 1 and 5 do not recite entry of the release code.

270. Nonetheless, to the extent a dispatcher must enter the code, a POSITA would have been motivated with a reasonable expectation of success such that once

the worker transmits the release code to the railway control apparatus, to prompt or allow the dispatcher to enter the received release code via the dispatcher interface into the railway control apparatus because it would have ensured the dispatcher is alerted to the information provided, prevented the track block from being (improperly) released until the dispatcher enters the code, and reduced any miscommunication between the dispatcher and worker. The entry of a code into an interface was also known and a straightforward or design choice change, particularly given the existing hardware, software, and dispatcher interfaces in the FRA-Report. EX1010, 4:10-17 (“operator H to enter the displayed code”), 4:48-53, 5:24-30; Ground 1, Limitations 1[A]; 1[B], 5[A]; 1[C], 5[B].

271. Otherwise, a POSITA would have had a motivation to combine and reasonable expectation of success to automatically unblock the track block using the transmitted code as FRA-Report already automatically unblocks the track based on the worker as outlined above. *See supra* ¶¶ 252-256. Also, this is a design choice, such as it would have improved efficiency by automatically unblocking the track.

272. By either entering the code by the dispatcher or automatically by the railway control apparatus, FRA-Report’s railway control apparatus would compare the generated release code stored in the database (or other storage) with the worker’s

transmitted release code entered by the dispatcher or automatically and if the code matches, then the track is unblocked, otherwise the track remains blocked.

273. It was known to save a generated code in a database (or storage), e.g., password protected or encrypted to prevent improper access, and compare (or verify) codes to control another action. EX1005, 6:1-9, Abstract, 7:1-17, 11:8-17; EX1006, 7:8-15, Fig. 2; EX1007, 15:28-35; EX1008, 7:54-59; EX1009, Figs. 12, 14 (“received confirmation code = supplied confirmation code?”), 14:19-25, 15:17-27.

274. FRA-Report and Kruijswijk further teach “user terminal” under Railware’s construction (dispatcher’s terminal) in Claim 5 given the railway control apparatus will unblock the track with the release code. *See supra* ¶ 116. Likewise, they teach SEPTA’s construction in Claim 5 as the worker’s terminal (or PDA) transmits the code. *Id.*

275. Further, Railware’s understanding of “from the user terminal in return” further shows FRA-Report and Kruijswijk teach Limitations 1[E], 5[D] given “the code can be returned in a number of different ways” and is not “limited to ... only via the user terminal of the railway field worker” (*see supra* ¶ 117).

(b) Motivation to Combine FRA-Report and Kruijswijk with a Reasonable Expectation of Success

276. A POSITA would have modified FRA-Report with Kruijswijk because it would have been predictable given CTC systems and secret-code systems were

known, FRA-Report recognized that a secret-code system would have been implemented in the FRA-Report, and prior art discusses that technologies would have been applied to enhance worker safety. *See* Sections V.B-C; *supra* ¶¶ 178-179, 233, 242. As such, it would have been simply applying a known technique to a known device for increased safety.

277. A POSITA would have had a motivation to combine and reasonable expectation of success for the railway control apparatus to only unblock a track with the release code (as taught by Kruijswijk) transmitted by the worker in FRA-Report because it would have been a predictable option given it would “minimize[] common human error” and enhance the “verification system” in the FRA-Report. EX1004, Vol. I: 9, 27. A “handshake” or verification protocol, where the worker unblocks the track with the code taught in Kruijswijk, would have been obvious to try or a predictable next step. *See supra* ¶ 244; EX1028, 4, 14-15. Kruijswijk as described above teaches verifying the user with a secret code and Railware contends “the code can be returned in a number of different ways.” EX1005, 6:1-9, 7:1-17; *supra* ¶ 117.

278. Likewise, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection,” even offering various proposals on solutions towards this objective including a password-based one. EX1004, Vol. I: 57-58. A POSITA would have

been motivated to combine FRA-Report and Kruijswijk, given FRA-Report itself discloses a readiness to receive improvements—including password-based ones—towards verifying a track worker. *Id.*, Vol. I: 57-58.

279. Moreover, Kruijswijk and FRA-Report involve railway technology and worker safety including verification (Sections X.A.3-4, X.B) and thus a POSITA would have combined them, particularly as it would strengthen FRA-Report’s goal to “improve roadway worker safety and productivity” because the dispatcher would not unblock the track without the worker’s release code. EX1004, Vol. I: Preface.

280. Alternatively, a POSITA would have been likewise motivated to modify FRA-Report to transmit the release code by the worker [a] selecting the “Cancel/Fulfill” link (such as automatically or prompt the worker to enter the code), [b] calling, or [c] texting or emailing a message (such as via an embedded link activated to transmit the code) to the railway control apparatus to unblock the track. EX1005, 12:20-21 (“By using standard SMS-messages, the investments to implement this invention are very low.”); EX1004, Vol II.: 15, 21, 27, 63; EX1017, 15-16. This would have provided an efficient and alternative means to unblock the track, particularly as both the FRA-Report and Kruijswijk discuss text messages and text, email, and links were well-known. *Id.*

281. It was also within the general knowledge and skill of the POSITA to use control buttons and/or links to automatically execute an operation, such as returning information, such as the release code, to a central server.

282. A POSITA would have appreciated that modifying FRA-Report with Kruijswijk would have had a reasonable expectation of success. FRA-Report describes a CTC system with software to unblock a track at the worker's request from a mobile device. Limitations 1[D], 5[C]; 1[A]; 1[C], 5[B]; 1[E], 5[D]. FRA-Report states that "[t]he system is designed to be highly configurable" (EX1004, Vol. I: 41). Other prior art references also show a reasonable expectation of success and that before the Priority Date, mobile device, server, and other technology evolved. *See supra* ¶ 249. Thus, it would have been predictable to transmit the code from the worker device to the CTC system to unblock the track.

D. Analysis of Dependent Claims 2-4, 6-8

- 1. Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”**

Claim 6: “The method of claim 4 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”

283. FRA-Report and Kruijswijk disclose Claims 2 and 6, specifically transmitting the release code to the worker’s electronic address, displaying a message on the user terminal, and permitting the worker to respond to the message.

284. As discussed, the railway control apparatus generates a release code and transmits it and other information (*e.g.*, Form D, Form D recipient, date, track number, track location) as a message to the worker’s PDA or electronic contact address. See Limitations 1[D], 5[C]; EX1004, Vol. I: 34 (Fig. A-3) (“Form D Line 4 Request ... North East Corridor dispatcher has received your request ... Please confirm Form D 0001 ... Delivered to: Oriol ... 2 track out of service between/at Providence and Lawn in charge of Oriol”), 32 (A-1) (“You own these form Ds 0003,

NorthEast Corridor ... NorthEast Corridor dispatcher has received your request and the form D # 0003 has been cancelled.”).

285. A POSITA would recognize that the release code could be displayed, such as a prompt or text box message, on the worker’s interface in the FRA-Report and could be password protected. *See* Limitations 1[D], 5[C].

286. Alternatively, the release code would have been transmitted to the worker through other methods, including text message and email message. *Id.*

287. The railway worker would select or activate the “Cancel/Fulfill” embedded link which would transmit the release code to the railway control apparatus to unblock the track. *See* Limitations 1[E], 5[D].

288. Alternatively, upon activating the link, the system would prompt the worker to enter the release code and transmit it to the railway control apparatus. *Id.*

289. As another option, the worker would transmit the release code to the railway control apparatus to unblock the track by calling the dispatcher with the code or texting or emailing the code. *Id.* Alternatively, the text and email message would have included an embedded link to activate the return of the code to the railway control apparatus to unblock the track. *Id.*

290. These would have been straightforward changes given the hardware, software, and flexibility in the FRA-Report (*see supra* ¶¶ 248, 282), along with the

fact that it was within the general knowledge and skill of the POSITA to use control buttons and/or links to automatically execute an operation, such as returning information, such as the release code, to a central server. *See supra* ¶ 117 (Railware contending “the code can be returned in a number of different ways.”)

291. Accordingly, FRA-Report and Kruijswijk teach Claims 2, 6, including “to respond to the message to release the block” under Railware’s construction of any “standard type of user interface” and SEPTA’s construction to respond to the message. *See supra* ¶ 115.

2. **Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”**

Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”

292. FRA-Report and Kruijswijk disclose Claims 3 and 7.

293. FRA-Report and Kruijswijk disclose responding to the message and transmitting the release code to the railway control apparatus by [a] selecting or activating the “Cancel/Fulfill” or “Clear” links; [b] calling the dispatcher with the release code; or [c] texting or emailing the code to the dispatcher. *See* Claims 2, 6, Limitations 1[E], 5[D].

3. **Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”**

Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”

294. FRA-Report and Kruijswijk teach, as recited in Claims 4 and 8, specifically displaying on the user terminal a link for activating the return of the release code to the railway control apparatus.

295. As discussed, the worker’s user terminal displays a link, and upon selecting or activating the “Cancel/Fulfill” (or “Clear”) link (button) or a link in a text (or email) message on the worker’s mobile user interface, the release code would be transmitted to the railway control apparatus to unblock the track. *See* Claims 2, 6; Limitations 1[E], 5[D].

296. It was advantageous to embed the information in a button or link to simplify operation of a device and minimize data input (*i.e.*, retyping the release code) and distraction. Such a modification was a simple and predictable one, with a reasonable expectation of success. Accordingly, a POSITA would have been motivated with a reasonable expectation of success to implement a link to return the release code to the central railway control apparatus.

XI. GROUND 2: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT, KRUIJSWIJK, AND MACEY

A. Summary of FRA-Report and Analogous Art

297. My explanation of FRA-Report is above and incorporated here by reference. *See* Sections X.A.3-4.

B. Summary of Kruijswijk and Analogous Art

298. My explanation of Kruijswijk is above and incorporated here by reference. *See* Section X.B.

C. Summary of Macey and Analogous Art

299. PCT Pub. No. WO 2010/012040 (EX1007, “Macey”) published on February 4, 2010, and is therefore prior art under at least AIA 35 U.S.C. § 102(a) without any § 102(b) exceptions.

300. Macey discloses a system for enhancing railway worksite safety that involves comparing a secret code communicated by a railway worker before an approaching train is allowed to proceed through the worksite area. EX1007, 16:1-21, 1:5-8.

301. Macey further discloses an alert module that “may be a server or computer located at a central point, such as a headquarters or command cent[er] remote from” the tracks where railway workers are working for controlling over a

wireless (or wired) network a signaling device to prevent an approaching train from entering a worksite. *Id.*, 16:4-7, 15:28-35, 8:18-30, 14:22-35, 7:31-8:16.

302. The computer (or server) has “computer software implemented in any suitable computing language” and that “provides an interface 402 for the user to actively control and review the status of the detection device 200 and signalling device 300.” *Id.*, 14:6-15, 15:37-16:14.

303. Macey describes that a railway worker uses a device’s interface (e.g., a mobile phone, PDA, or laptop computer) to receive alerts of a train approaching the work site. *Id.*, 15:37-16:21, 8:3-8, 13:32-14:20, 14:28-15:8.

304. When a train proceeds towards a work zone, a detection device detects the presence of the train and sends a message to the alert module. *Id.*, 7:31-8:1, 14:37-15:8. The train then proceeds along the track where it will come upon the signaling device which shows a “stop” (or red) signal when railway workers are working on or near the track, and the worksite is not safe for a train to pass. *Id.*, at 8:18-9:6, 17:10-17, 18:1-9, 20:31-37.

305. After any work, the worker on the, *e.g.*, mobile device, enters “a specific code such as a PIN (personal identification number) or password only known to the user 112 to confirm that the status [of the track] is now safe for the passage of the vehicle.” *Id.*, 15:16-35, 13:25-14:4.

306. This code is transmitted to alert module at the central system, and the alert module communicates with the signaling device to unblock the track, *e.g.*, changing “a red light [blocked track] to a green light [unblocked track] and signals the operator of the train to proceed.” *Id.*, 20:31-37, 13:35-37 (“The alert module 400 comprises an interface 402 arranged for a user to enter an acknowledgement code 406....”), 15:28-35, 8:13-16, 8:35-9:6, 18:1-9.

307. Based on my review of the ’782 Patent’s prosecution history (EX1002), Macey was not considered during prosecution of the ’782 Patent.

308. In my opinion, Macey is analogous art to the ’782 Patent because Macey as shown in my analysis above is from the same field of endeavor as the ’782 Patent of workers, railway work, or access control. EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36; EX1007, 15:22-35, 16:1-21, 13:35-14:4, 20:31-37; EX1025, ¶¶20, 54, 57; EX1024, 6, 13-14.

309. For instance, Macey teaches railway worker safety and controlling railway traffic or physical access control by the working entering “a specific code such as a PIN (personal identification number) or password only known to the user 112 to confirm that the status [of the track] is now safe for the passage of the vehicle.” EX1007, 15:16-35, 20:31-37 (“Upon the code being entered into the

interface, an acknowledgement is transmitted to the signalling device and reports the safe status of the worksite for the train to proceed (509).”), 13:25-14:4.

310. Additionally, Macey, as shown in my analysis above, is reasonably pertinent to any purported problem addressed in the ’782 Patent, namely, controlling or authorizing access to a location or an area, such as by workers or railway traffic.

EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36.

D. Analysis of Independent Claims 1, 5

1. **[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”**

5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”

311. FRA-Report discloses Limitations 1[Pre], 5[Pre]. *See* Ground 1, Limitations 1[Pre], 5[Pre].

2. **1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”**

312. FRA-Report discloses Limitation 1[A]. *See* Ground 1, Limitation 1[A].

3. **1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”**

5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”

313. FRA-Report discloses Limitations 1[B], 5[A]. See Ground 1, Limitations 1[B], 5[A].

4. **1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”**

5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”

314. FRA-Report discloses Limitations 1[C], 5[B]. See Ground 1, Limitations 1[C], 5[B].

5. **1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”**

5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”

315. FRA-Report and Kruijswijk disclose and render obvious Limitations 1[D], 5[C]. *See* Ground 1, Limitations 1[D], 5[C].

6. **1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”**

5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”

316. FRA-Report and Kruijswijk disclose and render obvious Limitations 1[E], 5[D]. *See* Ground 1, Limitations 1[E], 5[D].

317. Likewise, the FRA-Report, Kruijswijk, and Macey disclose and render obvious Limitations 1[E], 5[D].

(a) FRA-Report, Kruijswijk, and Macey Combination

318. FRA-Report teaches the worker selects the “Cancel/fulfill” link to transmit information to the railway control apparatus, which unblocks the track. *See* Ground 1, Limitations 1[E], 5[D]; 1[B], 5[A].

319. Kruijswijk teaches a release code. *See* Ground 1, Limitations 1[D], 5[C].

320. Macey supplies the implementation of unblocking the track only based on the worker transmitting a secret code to a central system to protect the safety of the worker. *See supra* ¶¶ 262-263, Section XI.C.

321. Based on or following Macey's implementation, the worker would transmit the release code as taught in Kruijswijk to the railway control apparatus, which will only unblock the track once the transmitted code is entered by the dispatcher or automatically by the railway control apparatus. *See* Ground 1, Limitations 1[E], 5[D]. Thus, FRA-Report, Kruijswijk, and Macey disclose and render obvious Limitations 1[E], 5[D].

322. Additionally, a POSITA would have been motivated to combine with a reasonable expectation of success FRA-Report and Kruijswijk with Macey's implementation because it was predictable or obvious to try given known problem of protecting workers, a worker controlling a work zone, and one-time code. *See* Sections V.A-D. This would have ensured the dispatcher would not remove the track block without the worker's release code.

323. FRA-Report, Kruijswijk, and Macey further teach "user terminal" and "from the user terminal in return" for the reasons above. *See supra* ¶¶ 274-275.

324. It would have been obvious, as discussed, to automatically unblock the track or based on the dispatcher entering the code (or chief traffic controller retrieving the code from storage if the worker is unavailable). *See supra* ¶¶ 268-273.

(b) Motivation to Combine FRA-Report, Kruijswijk, and Macey with a Reasonable Expectation of Success

325. A POSITA would have been motivated to combine them with a reasonable expectation of success as it would have been predictable given CTC systems and secret-code systems were known, FRA-Report recognized that a secret-code system would have been implemented in the FRA-Report, and prior art discusses that technologies would have been applied to enhance worker safety. *See* Sections V.B-C; *supra* ¶¶ 178-179, 233, 242. As such, it would have been simply applying a known technique to a known device for increased safety.

326. FRA-Report’s “verification system” and goal to “minimize[] common human error” further enhance such motivation for the FRA-Report, Kruijswijk, and Macey combination. EX1004, Vol. I: 9, 27. A “handshake” or verification protocol, where the worker unblocks the track with the code taught in Kruijswijk, would have been a predictable next step. *See supra* ¶ 244; EX1028, 4, 14-15. In fact, Kruijswijk and Macey teach verifying the user with a secret code. EX1005, 6:1-9, 7:1-17; EX1007, 15:16-35, 20:31-37.

327. Notably, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection.” EX1004, Vol. I: 57. FRA-Report even proposes various solutions including (i) a “device ID” to be sent with messages and/or (ii) “password-protected access to the system” such as a “personal password.” *Id.*, 57-58. Thus, FRA-Report urges a need and readiness to implement robust verification measures (including password-based ones) to effectively verify worker identities, and Macey teaches one such solution in the railway maintenance field. As such, a POSITA would have been motivated to combine FRA-Report, Kruijswijk, and Macey to verify a track worker with the release code. EX1004, Vol. I: 57-58; EX1007, 15:16-35, 20:31-37.

328. A POSITA would have been motivated to combine FRA-Report, Kruijswijk, and Macey given they all involve railway technology and promote worker safety. *See* Sections X.A.3-4, X.B, XI.C. Moreover, all involve worker device communication with a central railway system for railway work and thus, such overlap would have further motivated a POSITA to combine them. *Id.* Thus a POSITA would have combined them, particularly as it would strengthen FRA-Report’s goal to “improve roadway worker safety and productivity.” EX1004, Vol. I: Preface; Ground 1, Limitations 1[E], 5[D] (verifying saved code with worker’s transmitted code to unblock the track).

329. Alternatively, a POSITA would have been motivated to modify FRA-Report to transmit the release code upon the worker [a] selecting the “Cancel/Fulfill” link (such as automatically or prompt the worker to enter the code), [b] calling, or [c] texting or emailing a message (such as an embedded link activated to transmit the code) to the railway control apparatus to unblock the track. *See supra* ¶ 280.

330. A POSITA would have had a reasonable expectation of success in modifying FRA-Report and Kruijswijk with Macey’s implementation given the hardware and software in FRA-Report. *See supra* ¶ 248.

E. Analysis of Dependent Claims 2-4, 6-8

1. **Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”**

Claim 6: “The method of claim 4 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”

331. As discussed, the railway control apparatus transmits the code as a message (*e.g.*, prompt or text box message), text message, or email message to the

worker's PDA. *See* Ground 1, Claims 2, 6, Limitations 1[D], 5[C].

332. The worker would transmit the release code to the railway control apparatus by selecting or activating the “Cancel/Fulfill” embedded link, texting or emailing a message (such as an embedded link), or by calling the dispatcher with the code. *See* Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

2. **Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”**

Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”

333. *See* Claims 2, 6; Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

3. **Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”**

Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”

334. *See* Claims 2, 6; Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

XII. GROUND 3: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT AND SCHMITZ

A. Summary of FRA-Report and Analogous Art

335. My explanation of FRA-Report is above and incorporated here by reference. *See* Sections X.A.3-4.

B. Summary of Schmitz and Analogous Art

336. U.S. Patent No. 6,078,908 (EX1006, “Schmitz”) issued on June 20, 2000, and is therefore prior art under at least AIA 35 U.S.C. § 102(a) without any § 102(b) exceptions.

337. Schmitz discloses a data transmission system for verifying a user or relevant person’s identity using a secret password/code, including for controlling access to a secured location. EX1006, 1:37-2:7, 2:39, 2:57-3:5, 5:7-48.

338. Schmitz teaches that, upon the relevant person’s request, an “authentication computer [server] 2 generates the transaction authorization number TAN or the comparable password” using “a random number generator 5” *Id.*, 6:63-7:4, 8:19-21, 5:58, 2:57-3:5, Abstract, Fig. 2 (“Authorization Computer 2” and “Random Number Generator 5”).

339. The server transmits this code over the Internet to the relevant person’s receiver, *e.g.*, mobile phone, radio, email address. *Id.*, 2:21-24, 3:3-18, 5:3-6, 6:63-

7:4, 7:54-65, Abstract. “The receiver 3 can be a radio receiver incorporated into the data input apparatus 1.” *Id.*, 7:60-61.

340. Thereafter, relevant person enters the code into a “data input apparatus” of the receiver, and the code “is transmitted again to the authorization computer 2” which “verifies” the code to control access to a lock or “physical access controls.” *Id.*, 7:4-15, 5:7-9, 5:24-31.

341. Based on my review of the ’782 Patent’s prosecution history (EX1002), Schmitz was not considered during prosecution of the ’782 Patent.

342. In my opinion, Schmitz is analogous art to the ’782 Patent because a POSITA would have understood Schmitz, as shown in my analysis above, is in the same field of endeavor as the ’782 Patent of workers, railway work, or access control. EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36; EX1006, 5:7-9, 5:24-31, 5:35-48; EX1025, ¶¶20, 54, 57; EX1024, 6, 13-14.

343. For instance, Schmitz relates to access control as it provides a non-exhaustive list of fields of application, such as “computer centers,” “airports,” and “security regions,” (EX1006, 5:35-48) for employing its invention for, *e.g.*, “access controls” (*id.*, 5:7-9, 5:24-33). *See also id.*, 9:23-24 (“[t]he user obtains full access to or access limited to specific regions of the computer only after authorization.”), 5:12-18 (“The authorization computer checks and verifies this password, possibly

also in connection with the access permission to the concrete space at the concrete time.”).

344. A POSITA would have understood that Schmitz would have been applied to railway work (*e.g.*, “computer centers,” “security regions”). A POSITA would have also understood that Schmitz’s reference to a “user” is a broad term that could encompass numerous categories, such as a worker.

345. The broad applicability of Schmitz is further shown by “[t]he present invention can be universally employed in the region of data transmission systems. This holds for example also for the Internet and intranets, local area networks LAN, wide area networks WAN, etc.” *Id.*, 5:3-6.

346. Additionally, Schmitz, as shown in my analysis above, is reasonably pertinent to any purported problem addressed in the ’782 Patent of controlling or authorizing access to a location or a region, such as by workers or railway traffic, because like with the ’782 Patent, Schmitz controls access to locations or regions such as “security regions” (like railway traffic).

347. For example, Schmitz describes that it applies to “physical access controls” (EX1006, 5:7-9, 5:24-31) or “authorization of data transmission systems employing a transaction authorization number (TAN) or a comparable password.” *Id.*, 6:55-58. Also, Schmitz seeks to ensure a third-party cannot improperly “misuse”

or access the code, and the code could be “one-time” use. *Id.*, 1:11-33, 7:16-18 (“The transaction authorization number TAN or the comparable password can be a one-time usable transaction authorization number TAN or a one time usable password.”).

348. Once authorized, “[t]he user obtains full access to or access limited to specific regions of the computer only after authorization.” *Id.*, 9:23-24, 5:12-14 (“The authorization computer checks and verifies this password, possibly also in connection with the access permission to the concrete space at the concrete time.”)

C. Analysis of Independent Claims 1, 5

1. **[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”**

5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”

349. FRA-Report discloses Limitations 1[Pre], 5[Pre]. *See* Ground 1, Limitations 1[Pre], 5[Pre].

2. **1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”**

350. FRA-Report discloses Limitation 1[A]. *See* Ground 1, Limitation 1[A].

3. **1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display**

information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”

5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”

351. FRA-Report discloses Limitations 1[B], 5[A]. See Ground 1, Limitations 1[B], 5[A].

4. **1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”**

5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track sections;”

352. FRA-Report discloses Limitations 1[C], 5[B]. See Ground 1, Limitations 1[C], 5[B].

5. **1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”**

5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”

353. FRA-Report and Schmitz disclose and render obvious Limitations 1[D], 5[C].

(a) FRA-Report and Schmitz Combination

354. As discussed, FRA-Report discloses that the railway control apparatus blocks the track as well as generates and transmits a Form D number (and other information) to the worker’s electronic contact address. *See* Ground 1, Limitations 1[D], 5[C].

355. Schmitz supplies the “release code” to FRA-Report such that the dispatcher in FRA-Report operates the track display via the railway control apparatus and blocks the track as well as generates and transmits the “release code” (as taught in Schmitz) to a worker’s electronic contact address accessible by the worker’s PDA interface. *See* Ground 1, Limitations 1[D], 5[C]; 1[C], 5[B].

356. Specifically, Schmitz teaches generating and transmitting a release code. Schmitz describes that, upon a relevant person’s request, an “authentication

computer [authorization computer or server] 2 generates the transaction authorization number TAN or the comparable password” using “a random number generator 5” EX1006, 6:63-7:4, 8:19-21, 5:58, 3:29-33, 2:57-3:5, Abstract, Fig. 2 (“Authorization Computer 2” and “Random Number Generator 5”).

357. The server transmits this code over the Internet to the authorized relevant person’s electronic address, *e.g.*, mobile phone, radio, email address. *Id.*, 2:21-24, 3:3-18, 5:3-6, 6:63-7:4, 7:54-65, Abstract.

358. FRA-Report and Schmitz disclose and render obvious Limitations 1[D], 5[C]. Given the foregoing, they also disclose these limitations based on the Board’s discussion of release code (*see supra* ¶¶ 110-111) because the code taught in Schmitz (TAN or password) is randomly-generated and secret or only known to the relevant person. EX1006, 6:63-7:4, 8:19-21, 5:58, 2:57-3:5, Abstract 3:29-33.

359. Notably, Schmitz seeks to ensure a third-party cannot improperly “misuse” or access the code, and the code could be “one-time” use. *Id.*, 1:11-33, 7:16-18 (“The transaction authorization number TAN or the comparable password can be a one-time usable transaction authorization number TAN or a one time usable password.”).

360. Further, FRA-Report and Schmitz disclose and render obvious Limitations 1[D], 5[C] under Railware’s construction, including the code taught in

Schmitz is secret to the relevant person or “not readily available” to the dispatcher when combined with the FRA-Report. *See supra* ¶¶ 106, 110-111.

361. Additionally, FRA-Report and Schmitz disclose and render obvious Limitations 1[D], 5[C], including under the Board and Railware’s understanding of release code, because a POSITA would have had a motivation to combine and reasonable expectation of success to implement Schmitz as a release code or secret code in FRA-Report as generating and transmitting a secret code, *e.g.*, for safety and security, only received by the relevant worker was taught before the Priority Date. *See supra* ¶ 233; Section V.C. This would protect railway workers from an accidental (or even intentional) removal of a block by the dispatcher while the worker performed maintenance work. Thus, it would have been predictable or obvious to try in implementing Schmitz as the claimed release code or secret code in FRA-Report.

362. Moreover, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Schmitz as a release code or secret code, which is generated and transmitted in FRA-Report to the worker’s electronic contact address accessible by the user interface, for safety and security to address the known problem of protecting railway workers from removal of a block by the dispatcher while track work is performed. *See* Section V.A. Such a release code

would have ensured that it is only known to the worker and the track can only be released by the worker returning that code.

363. Similarly, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Schmitz as a “release code” or secret code because it was known to a POSITA that a worker uses a mobile phone for controlling track possession, including to take control of a work zone and return it to the central system, and thus implementing a code only known to the worker would have been obvious to try for safety and security. *See* Section V.D.

364. Likewise, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Schmitz as a “release code” or secret code given the use of one-time password or one-time code for authorization or authentication was prevalent before the Priority Date, as shown above and other prior art. *See* Section V.C.

365. In my view, such known authentication systems would have driven a POSITA (or would have been predictable) to apply such authentication to ensure the code is only known to the worker and the track is only unblocked when the railway control apparatus receives the code transmitted by the worker. Thus, it would have been predictable in implementing Schmitz as the claimed release code or secret code in FRA-Report.

366. Accordingly, FRA-Report and Schmitz disclose and render obvious Limitations 1[D], 5[C]. Given the foregoing, FRA-Report and Schmitz also teach “user terminal” under Railware and SEPTA’s construction (dispatcher’s terminal) because the dispatcher operates a computer to block the track as well as generate and transmit the release code to a worker’s PDA. *See supra* ¶¶ 220-226, 239; Ground 1, Limitations 1[A]; 1[C], 5[B].

(b) Motivation to Combine FRA-Report and Schmitz with a Reasonable Expectation of Success

367. A POSITA would have had a motivation to combine and reasonable expectation of success to generate and transmit the release code as taught in Schmitz in FRA-Report to the worker’s electronic contact address accessible by the user interface given both FRA-Report and Schmitz discuss controlling access to ensure protection and thus, a POSITA would have been motivated to modify the FRA-Report with the release code taught in Schmitz. *See* Sections X.A.3-4, XII.B. Schmitz expresses the “very secure, low cost” of implementing its system. EX1006, 6:24-26. Thus, a POSITA would have been motivated to modify the FRA-Report with the release code taught in Schmitz. *Id.*

368. Additionally, a POSITA would have modified FRA-Report with Schmitz because it would have been predictable given CTC systems and secret-code systems were known, FRA-Report recognized that a secret-code system would have

been implemented in the FRA-Report, and prior art discusses that technologies would have been applied to enhance worker safety. See Sections V.B-C; *supra* ¶¶ 178-179, 233, 242. As such, it would have been simply applying a known technique to a known device for increased safety.

369. Significantly, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection.” EX1004, Vol. I: 57. FRA-Report even proposes various solutions including (i) a “device ID” to be sent with messages and/or (ii) “password-protected access to the system” such as a “personal password.” *Id.*, 57-58. Therefore, FRA-Report urges a need and readiness to implement robust verification measures (including password-based ones) to effectively verify roadway worker identities, and Schmitz teaches one such code-based approach for identity verification. A POSITA would have been motivated to incorporate Schmitz for at least this reason.

370. A POSITA would have been further motivated with a reasonable expectation of success by the FRA-Report’s goals to “improve roadway worker safety and productivity” (EX1004, Vol. I: Preface) and implement a “verification system.” EX1004, Vol. I: 9, 27; Limitations 1[B], 5[A]. A POSITA would have thus recognized, to prevent the dispatcher from revoking a blocked track and increase security and safety, that FRA-Report would implement a “handshake” or

verification protocol where the code taught in Schmitz is associated with the blocked track and transmitted to the worker who later unblocks the track with the same code. *See supra* ¶ 244.

371. A POSITA would have appreciated that modifying FRA-Report with Schmitz would have had a reasonable expectation of success to generate and transmit a code in FRA-Report to a worker's device given the hardware and software in FRA-Report. Ground 1, Limitations 1[D], 5[C]; 1[A]; 1[C], 5[B]; 1[E], 5[D]; *supra* ¶ 248. Further, the worker's PDA in FRA-Report has existing encryption and decryption technology (EX1004, Vol. I: 57), otherwise, this was known. EX1011, 4:25-24.

372. Also, Schmitz describes the simplicity of implementing its system and technology evolved from FRA-Report to before the Priority Date, and with such enhanced technology, it would have been predictable for a POSITA to apply those capabilities to augment FRA-Report with a code-based system, such as Schmitz. EX1006, 6:24-26; *supra* ¶¶ 248-249. With such hardware and software, the FRA-Report would have had flexibility when the code is generated, such as before or after the block is placed, depending on the needs for the system, such as safety, efficiency, and workflow, or a design choice to a POSITA.

373. The POSITA would further have been motivated to modify FRA-Report with a reasonable expectation of success for the worker's interface to receive

and display (such as prompt or text box message) the release code taught in Schmitz given the worker's existing user interfaces and it is a design choice. Ground 1, Limitations 1[B], 5[A].

374. Alternatively, a POSITA would have been motivated to modify FRA-Report to transmit the code taught by Schmitz to the worker's electronic contact address through other methods, including text message or email message given such methods would have provided an alternate form to the worker and text, email, and links were well-known. EX1004, Vol. II: 15, 21, 27, 63; EX1017, 15-16. As another option, the text and email message would have included an embedded link to activate the return of the code.

6. **1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”**

5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”

375. FRA-Report and Schmitz disclose and render obvious Limitations 1[E], 5[D].

(a) FRA-Report and Schmitz Combination

376. As discussed, FRA-Report teaches the worker selects the “Cancel/fulfill” link to transmit information to the railway control apparatus, which unblocks the track. See Ground 1, Limitations 1[E], 5[D]; 1[B], 5[A].

377. Schmitz supplies transmitting the “release code” such that the worker in FRA-Report transmits the code, *e.g.*, selecting the “Cancel/Fulfill” link (or, *e.g.*, by call, text, email), to the railway control apparatus, which will only unblock the track once the transmitted code is entered by the dispatcher or automatically by the railway control apparatus. See Ground 1, Limitations 1[E], 5[D].

378. Specifically, Schmitz teaches the relevant person transmitting the release code to the server. The person enters the code (TAN or password) into “data input apparatus” of the receiver, and the code “is transmitted again to the authorization computer” which “verifies” the code to control, *e.g.*, a locking mechanism or “physical access controls.” EX1006, 7:8-15, Abstract, 5:7-9, 5:24-48 (applied across numerous “fields of application”), 7:60-61 (“The receiver 3 can be a radio receiver incorporated into the data input apparatus 1.”). Accordingly, FRA-Report and Schmitz disclose and render obvious Limitations 1[E], 5[D].

379. Additionally, a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Schmitz the transmitted release

code in FRA-Report to the railway control apparatus, which will only unblock the track with the transmitted code given it was known. *See supra* ¶¶ 262-263; Section XI.C. Thus, it would have been a predictable design choice.

380. Further, a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Schmitz the transmitted release code in FRA-Report to the railway control apparatus to unblock the track to address the known problem of protecting railway workers from improper removal of a track block. *See* Section V.A. Thus, a POSITA would have used the worker's transmitted code to unblock the track to ensure the track can only be released by the worker returning that code.

381. Similarly, a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Schmitz the transmitted release code in FRA-Report to the railway control apparatus to unblock the track because it was known to a POSITA that a worker uses a mobile phone for controlling track possession, including to take control of a work zone and return it to the central system. *See* Section V.D. As such, implementing a code (as taught by Schmitz) to unblock a track would have been obvious to try or predictable design choice for safety and security. Thus, the worker with the code would hold possession of the

track and would transfer such possession by transmitting the code to the dispatcher to unblock the track.

382. Also, a POSITA would have had a motivation to combine and reasonable expectation of success to implement from Schmitz the transmitted release code in FRA-Report to unblock the track given the use of one-time password or one-time code transmitted to a server for authorization or authentication for safety and security was prevalent before the Priority Date. *See* Section V.C.

383. In my view, such known authentication systems would have driven a POSITA to apply code authentication to railway systems to ensure a track block is only unblocked when the railway control apparatus receives the code transmitted by the worker. Thus, it would have been predictable or obvious to try to implement Schmitz in FRA-Report.

384. Thus, FRA-Report and Schmitz disclose and render obvious Limitations 1[E], 5[D]. Given the foregoing, FRA-Report and Schmitz further teach “user terminal” and “from the user terminal in return” for the reasons discussed previously. *See supra* ¶¶ 274-275.

385. It would have been obvious, as discussed, to automatically unblock the track or based on the dispatcher entering the code (or chief traffic controller retrieving the code from storage if the worker is unavailable). *See supra* ¶¶ 268-273.

(b) Motivation to Combine FRA-Report and Schmitz with a Reasonable Expectation of Success

386. A POSITA would have been motivated to combine them with a reasonable expectation of success as it would have been predictable given CTC systems and secret-code systems were known, FRA-Report recognized that a secret-code system would have been implemented in the FRA-Report, and prior art discusses that technologies would have been applied to enhance worker safety. *See* Sections V.B-C; *supra* ¶¶ 178-179, 233, 242. As such, it would have been simply applying a known technique to a known device for increased safety.

387. FRA-Report’s “verification system” and goal to “minimize[] common human error” would further enhance such motivation for FRA-Report and Schmitz. EX1004, Vol. I: 9, 27. A “handshake” or verification protocol, where the worker unblocks the track with the code taught in Schmitz, would have been a predictable next step. *See supra* ¶ 244; EX1028, 4, 14-15. Schmitz as discussed above teaches verifying the user with a secret code. EX1006, 7:8-15.

388. Likewise, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection.” EX1004, Vol. I: 57-58. Thus, a POSITA would have been motivated to combine FRA-Report and Schmitz to verify a track worker with the release code. *Id.*, Vol. I: 57-58.

389. A POSITA would have been motivated to combine FRA-Report and Schmitz with a reasonable expectation of success as both involve a verification system, along with access control (Sections X.A.3-4, XII.B), and thus it would have been obvious to try because it would strengthen FRA-Report's goal to "improve roadway worker safety and productivity" as the dispatcher would not unblock the track without the worker's release code. EX1004, Vol. I: Preface; EX1006, 7:8-15, 5:7-9, 5:24-48; Ground 1, Limitations 1[E], 5[D] (verifying saved code with worker's transmitted code to unblock the track).

390. Alternatively, a POSITA would have been motivated to modify FRA-Report to transmit the release code upon the worker [a] selecting the "Cancel/Fulfill" link (such as automatically or prompt the worker to enter the code), [b] calling, or [c] texting or emailing a message (such as via an embedded link activated to transmit the code) to the railway control apparatus to unblock the track. *See supra* ¶ 280.

391. A POSITA would have appreciated that modifying FRA-Report with Schmitz would have had a reasonable expectation of success given the hardware, software, and dispatcher and worker interfaces in the FRA-Report. *See supra* ¶¶ 248, 282. Thus, it would have been predictable to transmit the code from the worker device to the CTC system to unblock the track. *Id.*

392. Also, technology evolved from FRA-Report to before the Priority Date,

and with such enhanced technology, it would have been predictable for a POSITA to apply those capabilities to augment FRA-Report with a code-based system to unblock the track. *See supra* ¶¶ 248-249.

D. Analysis of Dependent Claims 2-4, 6-8

1. **Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”**

Claim 6: “The method of claim 4 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”

393. FRA-Report and Schmitz teach Claims 2 and 6.

394. As discussed, the railway control apparatus transmits the release code (taught in Schmitz) as a message (*e.g.*, prompt or text box message), text message, or email message to the worker’s PDA. *See* Limitations 1[D], 5[C]; Ground 1 Claims 2, 6, Limitations 1[D], 5[C]; EX1004, Vol. I: 34 (Fig. A-3), 32 (Fig. A-1).

395. The worker would transmit the release code to the railway control apparatus by selecting or activating the “Cancel/Fulfill” embedded link, texting or

emailing a message (such as an embedded link), or by calling the dispatcher with the code. See Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

2. **Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”**

Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”

396. FRA-Report and Schmitz teach Claims 3, 7. See Claims 2, 6, Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

3. **Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”**

Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”

397. FRA-Report and Schmitz teach these claims.

398. The worker’s user terminal displays a Cancel/Fulfill” (or “Clear”) link, and upon selecting or activating it, the release code would be transmitted to the railway control apparatus to unblock the track. See Claims 2, 6; Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D]. Alternatively, the worker would

transmit the release code to the railway control apparatus by activating or selecting a link in a text or email message. *Id.*

XIII. GROUND 4: CLAIMS 1-8 ARE OBVIOUS OVER FRA-REPORT, BYFORD, AND MACEY

A. Summary of FRA-Report and Analogous Art

399. My explanation of FRA-Report is above and incorporated here by reference. *See* Sections X.A.3-4.

B. Summary of Byford and Analogous Art

400. U.S. Patent No. 6,581,161 (EX1011, “Byford”) issued on June 17, 2003, and is therefore prior art under at least AIA 35 U.S.C. § 102(a) without any § 102(b) exceptions.

401. Byford discloses a system for “controlling access to a secure location” by generating and transmitting a secret code to a relevant person (or user). EX1011, 4:31-38, Abstract.

402. Byford teaches a server generating a “cipher lock code” for the relevant person and transmitting the code in “encrypted form” over the Internet to the relevant person’s wireless device which “decrypt[s]” it. *Id.*, 4:31-38, 3:61-4:3, Abstract, 5:7-14 (user permitted “one-time access”), 5:25-30, claims 1, 3.

403. Based on my review of the ’782 Patent’s prosecution history (EX1002), Byford was not considered during prosecution of the ’782 Patent.

404. In my opinion, Byford is analogous art to the '782 Patent because a POSITA would have understood Byford, as shown in my analysis above, is in the same field of endeavor as the '782 Patent of workers, railway work, or access control. EX1011, Abstract, 1:7-12, 3:61-65; EX1001, title, Abstract, 1:14-2:3, 2:43-3:7, 4:32-36; EX1025, ¶¶20, 54, 57; EX1024, 6, 13-14.

405. For instance, Byford relates to access control as it is titled, “System, apparatus and method for controlling access” where the “present invention is concerned ... [with] controlling access to a secure location” EX1011, Abstract. This could include, “controlling access to facilities by potential users of those facilities, for example physical access to a building or secure area or container, or access to a particular computer system” *Id.*, 1:7-11, 4:59-62 (“access control device may vary, depending on the requirements of the particular building or secure area”).

406. A POSITA would have understood that Byford would have been applied to railway work (*e.g.*, “secured location” or “secured area”). A POSITA would also have understood that Byford’s reference to a “user” is a broad term that could encompass numerous categories, such as a worker.

407. Additionally, Byford, as shown in my analysis above, is reasonably pertinent to any purported problem addressed in the '782 Patent of controlling or

authorizing access to a location or a region, such as by workers or railway traffic, because like with the '782 Patent, Byford controls access to locations or regions such as “secured location” or “secured area” (like railway tracks).

408. For instance, Byford teaches “controlling access to facilities by potential users of those facilities, for example physical access to a building or secure area ... or access to a particular computer system” *Id.*, 1:7-11. Also, Byford seeks to ensure a third-party cannot improperly obtain access by encrypting the code and providing “one-time access.” *Id.*, 5:7-14. Byford notes, “[t]his offers protection against an intruder who has, for example, observed a cipher lock setting being used and then reuses it to gain unauthorised access.” *Id.*

C. Summary of Macey and Analogous Art

409. My explanation of Macey is above and incorporated here by reference. See Section XI.C.

D. Analysis of Independent Claims 1, 5

1. **[Pre]: “A system to enhance railway control, to protect safety of railway workers on or near railway tracks, the system comprising:”**
5[Pre]: “A method to enhance railway control, to protect safety of railway workers on or near railway tracks, said method comprising:”

410. FRA-Report discloses Limitations 1[Pre], 5[Pre]. See Ground 1, Limitations 1[Pre], 5[Pre].

2. **1[A]: “a railway control apparatus comprising a processor, a non-transitory medium storing one or more programs of executable instructions, and a network interface through which the railway control apparatus communicates via a network;”**

411. FRA-Report discloses Limitations 1[A]. See Ground 1, Limitation 1[A].

3. **1[B]: “a user terminal provided to a railway field worker and configured to communicate via the network with the railway control apparatus and to provide a user interface to display information received from the railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon,”**

5[A]: “configuring a mobile user device of a railway field worker to provide a device user interface to display information received via a network from a railway control apparatus and to permit the railway field worker to respond to prompts displayed thereon;”

412. FRA-Report discloses Limitations 1[B], 5[A]. See Ground 1, Limitations 1[B], 5[A].

4. **1[C]: “wherein the railway control apparatus, by execution of said one or more programs of executable instructions by the processor, includes: a block placing part to place a block on one or more specified track sections to permit the railway field worker to enter the track sections while blocking railway traffic to said track sections;”**

5[B]: “providing a terminal user interface on a terminal to permit a terminal user of the terminal request the railway control apparatus to place a block on one or more specified track sections to permit a railway field worker to enter the track sections while blocking railway traffic to said track

sections;”

413. FRA-Report discloses Limitations 1[C], 5[B]. *See* Ground 1, Limitations 1[C], 5[B].

5. **1[D]: “railway control apparatus . . . includes . . . a code generation part to generate a release code and transmit the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”**

5[C]: “generating by the railway control apparatus a release code and transmitting the release code to an electronic contact address accessible by the railway field worker via operation of the user interface of the user terminal; and”

414. FRA-Report and Byford disclose and render obvious Limitations 1[D], 5[C].

(a) FRA-Report and Byford Combination

415. As discussed, FRA-Report discloses that the railway control apparatus blocks the track as well as generates and transmits a Form D number (and other information) to the worker’s electronic contact address. *See* Ground 1, Limitations 1[D], 5[C].

416. Byford supplies the “release code” to FRA-Report such that the dispatcher in FRA-Report operates the track display via the railway control apparatus and blocks the track as well as generates and transmits the “release code”

(as taught in Byford) to a worker's electronic contact address accessible by the worker's PDA interface. See Ground 1, Limitations 1[D], 5[C]; 1[C], 5[B].

417. Specifically, Byford teaches that after a server receives a request for access from the relevant person and validates such person, the server generates a "cipher lock code" and transmits this code in "encrypted form" over the Internet to the person's wireless device which "decrypt[s]" the code. EX1011, 4:31-40, 2:22-31, Abstract, 4:18-24, 5:25-30, claims 1, 3.

418. To prevent "unauthorized access," Byford provides "one-time access" code to the relevant person. *Id.*, 5:7-14. A POSITA would have recognized this "cipher lock code" could be, e.g., numeric (such as a random number) or alphanumeric for security. EX1005, 8:14-16; EX1006, 6:63-7:4, 2:65-3:1; see Section V.C, *supra* ¶ 233.

419. FRA-Report and Byford disclose and render obvious Limitations 1[D], 5[C]. Given the foregoing, they also disclose these limitations based on the Board's discussion of release code (*supra* ¶¶ 110-111), including the code taught in Byford is a secret code: encrypted ("cipher" code) for "one-time access" by the relevant person. Byford even validates the relevant person before providing the "cipher lock code."

420. Further, FRA-Report and Byford disclose and render obvious Limitations 1[D], 5[C] under Railware’s construction, including the code taught in Byford is secret to the relevant person or “not readily available” to the dispatcher when combined with FRA-Report. *See supra* ¶¶ 106, 110-111. Accordingly, FRA-Report and Byford disclose and render obvious Limitations 1[D], 5[C].

421. Additionally, FRA-Report and Byford disclose and render obvious Limitations 1[D], 5[C], including under the Board and Railware’s understanding of release code, because a POSITA would have had a motivation to combine and reasonable expectation of success to implement Byford as a release code or secret code, which is generated and transmitted in FRA-Report to the worker’s electronic contact address accessible by the user interface, as generating and transmitting a secret code, *e.g.*, for safety and security, only received by the relevant worker was taught before the Priority Date. *See supra* ¶ 233; *see* Section V.C. This would protect railway workers from an accidental (or even intentional) removal of a block by the dispatcher while the worker performed maintenance work. Thus, it would have been predictable or obvious to try in implementing Byford as the claimed release code or secret code in FRA-Report.

422. Additionally, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Byford as a release code or secret

code, which is generated and transmitted in FRA-Report to the worker's electronic contact address accessible by the user interface, for safety and security to address the known problem of protecting railway workers from removal of a block by the dispatcher while track work is performed. *See* Section V.A. Such a release code would have ensured that it is only known to the worker and the track can only be released by the worker returning that code.

423. Similarly, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Byford as a “release code” or secret code because it was known to a POSITA that a worker uses a mobile phone for controlling track possession, including to take control of a work zone and return it to the central system, and thus implementing a code only known to the worker would have been obvious to try for safety and security. *See* Section V.D.

424. Further, a POSITA would have had a motivation to combine and reasonable expectation of success to implement Byford as a “release code” or secret code given the use of one-time password or one-time code for authorization or authentication was prevalent before the Priority Date, as shown above and other prior art. *See* Section V.C.

425. Such known authentication systems would have driven a POSITA to apply such authentication to ensure the code is only known to the worker and the

track is only unblocked when the railway control apparatus receives the code transmitted by the worker. Thus, it would have been predictable in implementing Byford as the claimed release code or secret code in FRA-Report.

426. Thus, FRA-Report and Byford disclose and render obvious Limitations 1[D], 5[C]. In light of the foregoing, FRA-Report and Byford also teach “user terminal” under Railware and SEPTA’s construction because the dispatcher operates a computer to block the track as well as generate and transmit the release code to a worker’s PDA. *See supra* ¶¶ 220-226, 239; Ground 1, Limitations 1[A]; 1[C], 5[B].

(b) Motivation to Combine FRA-Report and Byford with a Reasonable Expectation of Success

427. A POSITA would have had a motivation to combine and reasonable expectation of success to generate and transmit the release code as taught in Byford in FRA-Report to the worker’s electronic contact address accessible by the user interface given both FRA-Report and Byford discuss controlling access to ensure protection and thus, a POSITA would have been motivated to modify the FRA-Report with the release code taught in Byford. *See* Sections X.A.3-4, XIII.B.

428. Additionally, a POSITA would have modified FRA-Report with Byford because it would have been obvious to try because CTC systems and secret-code systems were known, FRA-Report recognized that a secret-code system would have been implemented in the FRA-Report, and prior art discusses that technologies

would have been applied to enhance worker safety. See Sections V.B-C; *supra* ¶¶ 178-179, 233, 242. As such, it would have been simply applying a known technique to a known device for increased safety.

429. Notably, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection.” EX1004, Vol. I: 57. FRA-Report even proposes various solutions including (i) a “device ID” to be sent with messages and/or (ii) “password-protected access to the system” such as a “personal password.” *Id.*, Vol. I: 57-58. Therefore, FRA-Report urges a need and readiness to implement robust verification measures (including password-based ones) to effectively verify roadway worker identities, and Byford teaches one such code-based approach for identity verification. A POSITA would have been motivated to incorporate Byford for at least this reason.

430. A POSITA would have been further motivated with a reasonable expectation of success by the FRA-Report’s goals to “improve roadway worker safety and productivity” (EX1004, Vol. I: Preface) and implement a “verification system.” *Id.*, 9, 27; Limitations 1[B], 5[A]. A POSITA would have thus recognized, to prevent the dispatcher from revoking a blocked track and increase security and safety, that FRA-Report implement a “handshake” or verification protocol where the

code taught in Byford is associated with the blocked track and transmitted to the worker who later unblocks the track with the same code. *See supra* ¶ 244.

431. A POSITA would have appreciated that modifying FRA-Report and Byford would have had a reasonable expectation of success to generate and transmit a code in FRA-Report to a worker's device given the hardware and software in FRA-Report. Ground 1, Limitations 1[D], 5[C]; 1[A]; 1[C], 5[B]; 1[E], 5[D]; *supra* ¶ 248. Also, the worker's PDA in FRA-Report has existing encryption and decryption technology (EX1004, Vol. I: 57), otherwise, this was known particularly as technology evolved before the Priority Date. EX1011, 4:25-24 ("well-known encryption schemes"); *supra* ¶¶ 248-249. With such hardware and software, the FRA-Report would have had flexibility when the code is generated, such as before or after the block is placed, such as safety, efficiency, and workflow, or a design choice to a POSITA.

432. The POSITA would further have been motivated to modify FRA-Report with a reasonable expectation of success for the worker's interface to receive and display the release code taught in Byford given the worker's existing user interfaces in the FRA-Report and it is a design choice by a POSITA. Ground 1, Limitations 1[B], 5[A].

433. Alternatively, a POSITA would have been motivated to modify FRA-Report to transmit the code taught by Byford with a reasonable expectation of success to the worker by text message and email message. *See supra* ¶ 251.

6. **1[E]: “railway control apparatus . . . includes . . . a block removal part to remove only upon receiving the release code from the user terminal in return, the block placed by the block placing part on said one or more track sections.”**

5[D]: “permitting the block to said one or more track sections to be removed by the railway control apparatus only upon receiving the release code from the user terminal in return.”

434. FRA-Report, Byford, and Macey disclose and render obvious Limitations 1[E], 5[D].

(a) FRA-Report, Byford, and Macey Combination

435. As mentioned, FRA-Report teaches the worker selects the “Cancel/fulfill” link to transmit information to the railway control apparatus, which unblocks the track. *See* Ground 1, Limitations 1[E], 5[D]; 1[B], 5[A].

436. Byford teaches a release code. Macey supplies the implementation of unblocking the track only based on the worker transmitting a secret code to a central system (*see supra* ¶¶ 262-263, Section XI.C).

437. Based on or following Macey’s implementation, the worker would transmit the release code as taught in Byford to the railway control apparatus, which will only unblock the track once the transmitted code is entered by the dispatcher or

automatically by the railway control apparatus. *See* Ground 1, Limitations 1[E], 5[D]. Thus, FRA-Report, Byford, and Macey disclose and render obvious Limitations 1[E], 5[D].

438. Additionally, a POSITA would have had a motivation to combine and reasonable expectation of success to only unblock a track with the release code (as taught by Byford) following Macey's implementation in FRA-Report to address the known problem of protecting railway workers from improper removal of a track block. *See* Section V.A. Thus, a POSITA would have used the worker's transmitted code to unblock the track to ensure the track can only be released by the worker returning that code.

439. Similarly, a POSITA would have had a motivation to combine and reasonable expectation of success to only unblock a track with the release code (as taught by Byford) following Macey's implementation because it was known to a POSITA that a worker uses a mobile phone for controlling track possession, including to take control of a work zone and return it to the central system, and as such, implementing a code to only unblock a track with the release code (as taught by Byford) would have been obvious to try for safety and security. *See* Section V.D. Thus, the worker with the code would hold possession of the track and would transfer such possession by transmitting the code to the dispatcher to unblock the track.

440. Also, a POSITA would have had a motivation to combine and reasonable expectation of success to only unblock a track with the release code (as taught by Byford) following Macey's implementation given the use of one-time password or one-time code transmitted to a server for authorization or authentication for safety and security was prevalent before the Priority Date. *See* Section V.C.

441. Such known authentication systems would have driven a POSITA to apply code authentication to railway systems to ensure a track block is only unblocked when the railway control apparatus receives the code transmitted by the worker. Thus, it would have been predictable or obvious to try to implement Byford and Macey in FRA-Report.

442. Thus, FRA-Report, Byford, and Macey disclose and render obvious 1[E], 5[D]. Given the foregoing, FRA-Report, Byford, and Macey further teach "user terminal" and "from the user terminal in return" for the reasons discussed previously. *See supra* ¶¶ 274-275.

443. It would have been obvious, as discussed, to automatically unblock the track or based on the dispatcher entering the code (or chief traffic controller retrieving the code from storage if the worker is unavailable). *See supra* ¶¶ 268-273.

(b) Motivation to Combine FRA-Report, Byford, and Macey with a Reasonable Expectation of Success

444. A POSITA would have been motivated to combine FRA-Report, Byford, and Macey given they involve controlling access to a location or secured area. See Sections X.A.3-4, XIII.B, XI.C. Moreover, all involve worker device communication with a central server or system and thus, such overlap would have further motivated a POSITA to combine them. *Id.*

445. Additionally, a POSITA would have been motivated to combine them with a reasonable expectation of success as it would have been predictable given CTC systems and secret-code systems were known, FRA-Report recognized that a secret-code system would have been implemented in the FRA-Report, and prior art discusses that technologies would have been applied to enhance worker safety. See Sections V.B-C; *supra* ¶¶ 178-179, 233, 242. As such, it would have been simply applying a known technique to a known device for increased safety.

446. FRA-Report's "verification system" and goal to "minimize[] common human error" would further enhance such motivation. EX1004, Vol. I: 9, 27. A "handshake" or verification protocol, where the worker unblocks the track with the code taught in Byford, would have been obvious to try. See *supra* ¶ 244; EX1028, 4, 14-15.

447. Similarly, FRA-Report recognized the need “to positively identify the person communicating with the PDA by utilizing some form of password protection.” EX1004, Vol. I: 57-58. Thus, a POSITA would have been motivated to combine FRA-Report, Byford, and Macey with a reasonable expectation of success to verify the worker with the release code. EX1004, Vol. I: 57-58; Ground 1, Limitations 1[E], 5[D] (verifying saved code with worker’s transmitted code to unblock the track).

448. Alternatively, a POSITA also would have been motivated to modify FRA-Report to transmit the release code upon the worker [a] selecting the “Cancel/Fulfill” link, [b] calling, or [c] texting or emailing a message (such as via an embedded link activated to transmit the code) to the railway control apparatus to unblock the track to provide an efficient and alternative means to unblock the track and text, email, and links were well-known. *See supra* ¶ 280.

449. A POSITA would have appreciated that modifying FRA-Report and Byford with Macey’s implementation would have had a reasonable expectation of success given the existing hardware and software in FRA-Report. *See supra* ¶ 248. Thus, it would have been predictable to transmit the code from the worker device to the CTC system to unblock the track. *Id.*

E. Analysis of Dependent Claims 2-4, 6-8

- 1. Claim 2: “The system of claim 1, wherein upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, the user interface provided on the user terminal displays a message and permits the railway field worker to respond to the message to release the block.”**

Claim 6: “The method of claim 4 5, further comprising: displaying, upon the railway control apparatus placing the block of railway traffic to said one or more specified track sections and transmitting the release code to the electronic contact address accessible by the railway field worker, a message through the device user interface provided on the mobile user device and permitting the railway field worker to respond to the message to release the block.”

450. FRA-Report, Byford, and Macey teach Claims 2, 6.

451. As mentioned, the railway control apparatus transmits the code (taught in Byford) as a message (*e.g.*, prompt or text box message), text message, or email message to the worker’s PDA. *See* Limitations 1[D], 5[C]; Ground 1, Claims 2, 6, Limitations 1[D], 5[C]; EX1004, Vol. I: 34 (Fig. A-3), 32 (A-1).

452. The worker would transmit the release code to the railway control apparatus by selecting or activating the “Cancel/Fulfill” embedded link, texting or emailing a message (such as an embedded link), or by calling the dispatcher with the code. *See* Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

2. **Claim 3: “The system of claim 2, wherein upon the railway field worker responding to the message to release the block, the release code is returned to the railway control apparatus.”**

Claim 7: “The method of claim 6, further comprising: upon the railway field worker responding to the message to release the block, returning the release code to the railway control apparatus.”

453. FRA-Report, Byford, and Macey teach Claims 3, 7. *See* Claims 2, 6, Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D].

3. **Claim 4: “The system of claim 2, wherein the message displayed by the user interface on the user terminal includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”**

Claim 8: “The method of claim 2 7, wherein the message displayed by the device user interface on the mobile user device includes an embedded link for activating a return transmission of the release code to the railway control apparatus.”

454. FRA-Report, Byford, and Macey teach Claims 4, 8.

455. The worker’s user terminal displays a Cancel/Fulfill” (or “Clear”) link, and upon clicking or activating it, the release code would be transmitted to the railway control apparatus to unblock the track. *See* Claims 2, 6; Limitations 1[E], 5[D]; Ground 1, Claims 2, 6, Limitations 1[E], 5[D]. Alternatively, the worker would transmit the release code to the railway control apparatus by activating or selecting a link in a text or email message. *Id.*

XIV. CONCLUSION

456. For the foregoing reasons, it is my opinion that claims 1-8 of the '782 Patent are obvious in view of the prior art herein to a POSITA.

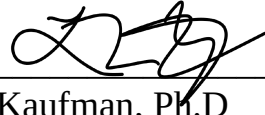
457. All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true.

458. I may receive additional documentation and other factual evidence over the course of this IPR that will allow me to supplement and/or refine my opinions.

459. I reserve the right to add to, alter, or delete my opinions and my declaration upon discovery of any additional information

460. Further, I am aware that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001, and may jeopardize the validity of the application or any patent issuing thereon.

461. I declare under penalty of perjury that the foregoing is true and correct.



Lori Kaufman, Ph.D

Executed on November 14, 2025

APPENDIX 1

LORI M. KAUFMAN, PhD.

530 Panorama Road

Earlysville, VA 22936

lori.kaufman@gmail.com

434.242.8467

EXPERIENCE SUMMARY: Lori Kaufman is an experienced Information Technology (IT) and Risk Analysis expert with over 25 years of both academic and professional experience. In the proposal industry, she has served as a Proposal Manager, Volume Lead, and a Technical Writer/SME. Technically, she has led and managed teams ranging from small-scale operations with 10+ members, proposal teams with 50+ members, and Integrated Product Teams (IPTs) and large-scale operations with 100+ members. The diversity of her expertise and experience includes system development lifecycle process management, agile software development process management, ITIL, DODAF, FEAF, cybersecurity, IT security, cloud computing, software and cyber security, software assurance, software life cycle management, virtualization, technology integration, fault tolerant systems, risk analysis and management (including train control systems), quality assurance, program management, systems engineering and various elements of C4ISR using a range of analytical and engineering skills.

CAPABILITIES: Lori Kaufman has over 20 years of leadership experience within both commercial and federal industry. She has led and written IT software/system assurance (including security and quality) plans for government agencies. She has provided analysis of cloud computing platforms for use within DOD and supported many IT programs from a life cycle management perspective throughout the federal government. She has overseen the development of several IT programs requiring the development of agile, ISO and CMMI processes. She has developed agile process management schema for both program management and software engineering and managed the development of FEAF/DODAF artifacts. She has also developed several ISO compliant logistics and supply chain models for various federal government agencies. Most recently, she has supported several cybersecurity and IA engagements using the RMF and the appropriate NIST/DCID requirements and integrating the DevSecOps pipeline into existing enterprises. She has supported various elements of C4ISR using a range of analytical and engineering skills. She has served as proposal manager for multiple federal opportunities, and has led the development of technical, management and staffing volumes. She is a recognized expert in railroad safety and supported various Positive Train Control (PTC) and Electronically Controlled Pneumatic (ECP) Brake safety assessments. She has served as an expert witness in a patent infringement case involving advanced rail control technology.

EXPERIENCE HIGHLIGHTS:

Panorama Consulting LLC, Charlottesville, VA, May 2011 – Present

Principal Consultant (Owner)

Provides subject matter expertise for IT system support and design (including cloud computing and enterprise architecture), cybersecurity, software security and risk analysis, software development and lifecycle management, FEAF/DODAF development, data mining and analytics, technical writing support and proposal support (including roles as capture manager and proposal manager) that includes FEDSIM. She has supported the development of DIACAP to Risk Management Framework (RMF) processes, and the implementation of the RMF. She has acted as a system architect supporting the integration of the DevSecOps pipeline within the existing systems engineering pipeline. In this capacity, she has developed the overarching framework for a DevSecOps pipeline with an emphasis on RMF compliance and meeting Authority to Operate (ATO) requirements for AWS and Azure platforms. She continues to develop analytic models for insider threat behavior and provides support across C4ISR program areas.

Supports various cloud computing initiatives and data center consolidation efforts that require internal and/or external cloud services and FedRAMP compliance; developing cyber security solutions; identifying server hardware to support distributed computing environments; providing software process management support; and providing management support for various IT initiatives. She is also developing an Indicators and Warnings (I&W) methodology for insider threat detection and the identification of anomalous behavior within the realm of cyber security. She continues supporting various Federal, State and Local proposal efforts as a subject matter expert in IT design and security for data centers and cloud environments. In addition, she also provides capture management, proposal management, and volume management for

technical opportunities that include cybersecurity and software lifecycle management.

Served as a subject matter expert (SME) to support a Department of Veterans Affairs (VA) data center enterprise architecture storage upgrade to a cloud service environment. She audited architecture requirements development to ensure functional and operational compliance to customer needs and business compliance; she defined the key performance indicators (KPIs) to ensure SLA/SLO compliance to both end users and backend business support; she reviewed system design and assessed compliance to all requirements; she led the development of DODAF/FEAF viewpoints and personally developed all Operational Viewpoints (OVs); she assisted with the development of test plans to ensure compliance to all operational and functional requirements; she identified the architecture elements required to provide disaster recovery/operational recovery compliance with existing VA policy; and she assisted with the development of data migration planning for the “To Be” environment and future expansion to a nationwide cloud infrastructure to support end user services.

Served as an expert witness for a railroad supplier in a patent infringement case.

Software Engineering Institute (SEI) | Carnegie Mellon, Pittsburgh, PA, November 2010 – April 2011

Senior Member of the Technical Staff – CERT

Assisted in the expansion of software assurance and risk management analysis to provide an engineering and human factors perspective in process management modeling. She also supported Department of Homeland Security (DHS) efforts to develop a control baseline from which both cloud computing users and providers can develop an audit and risk assessment framework, and a process for repeatable risk assessment for Critical Infrastructure Protection (CIP).

BAE Systems, Herndon, VA, December 2008 –October 2010

Deputy Chief Technology Officer

Responsible for overseeing IT mission assurance from a technology perspective with an emphasis on information assurance (IA) and cybersecurity. She managed a team of 10 individuals in developing an ITIL v3 compliant IT security model to support the BAE Systems enterprise approach to service delivery. The focus of this effort was to develop a reusable, Federal Information System Management Act (FISMA) compliant process that ensures confidentiality, integrity, availability (CIA), non-repudiation and authentication. The elements of this model are applicable to cloud computing. She also lent her expertise to develop several white papers on numerous security-related proposals whose net value exceeded several billion dollars for the defense and intelligence communities. For these proposal efforts, Lori provided leadership and support in developing the management, cost (including defining the labor force needed to support the opportunity) and technical volumes.

Served as capture manager and subject matter expert for IT opportunities within the defense intelligence community that included DOD and other agencies. She provided leadership for engagements requiring IT infrastructure design, operations and maintenance and lifecycle management related mission needs. As capture manager, she routinely led teams consisting of 50+ individuals. She also directly supported customer engagements to ensure that all mission needs were understood and met.

Assisted in the identification, design, and analysis of the virtualization and multiple security level (MSL) platforms to support the October 2010 awarded (\$300 million ceiling) Defense Intelligence Agency (DIA) Next Generation Desktop Computing Environment (NGDE).

Led and supported over one billion dollars in new business opportunities. Her contributions included both leadership and support in developing proposal technical, management, and cost volumes. Managed the technical writing teams, which consisted of 30+ domain experts, for both the technical volume and sample task order for the IT portion of the August 2010 awarded INSCOM OMNIBUS III IDIQ, which possesses a five-year \$492 million ceiling.

Booz Allen Hamilton, McLean, VA/Charlottesville, VA, January 2006 – December 2008

Associate

Provided subject matter expertise and leadership across multiple domains relying upon her software assurance, systems engineering, IT, data mining, quality assurance and risk management experience.

She assisted in the risk assessment of various transit and rail car programs for WMATA, Port Authority of New York and New Jersey and Amtrak. Her proposal management and support efforts yielded contracts in excess of \$50,000,000 from the Department of Transportation (DOT), the Department of Homeland Security (DHS), and the Department of Defense (DOD).

Air Force Space and Missile Systems Center MILSATCOM Joint Program Office, SMC Transformational Communication MILSATCOM System Engineering and Integration (SE&I) Segment Program, Transformational Satellite Communications System (TSAT) - provided expert analysis to support all phases of the software life cycle. Managed 100+ individuals from various organizations (including Lockheed Martin, The Aerospace Corporation, and the U.S. Air Force) in the coordination of TSAT software risk identification, mitigation strategies and the dissemination of information to the appropriate system concerns and across program segments. Additionally, she supported the emerging software assurance activities within the program including quality assurance planning and security.

SETA Support to the National Ground Intelligence Center (NGIC), Advanced Intelligence Projects Office (AIPO), Digital Reasoning Systems (DRS) Program Support –Worked with the NGIC AIPO to demonstrate the application of an entity extraction and conceptual query tool (Interceptor™) developed by Digital Reasoning Systems (DRS) to support the warfighter.

Federal Aviation Administration (FAA), Traffic Analysis and Review Program (TARP) Safety Risk Management Project –Developed a Safety Risk Management Document (SRMD) and performed the requisite risk analysis.

Transportation Security Administration (TSA), Checkpoint of the Future and Risk Management Analysis Tool –performed a review of data mining algorithms to provide a summary of the state-of-the-art practices in knowledge discovery and pattern recognition to improve airport screening.

Transportation Security Administration (TSA), Risk Management Task Force Project – Assisted in the development of a behavioral process model that allows for the identification of potential threats and vulnerabilities that can be exploited by either natural disasters or terrorist attacks.

Federal Railroad Administration, Test Plan Development for the General Train Movement Simulator for Safety Evaluation (GTMS-SE) - Using IEEE Standard 829-1998, developed a software test plan for the General Train Movement Simulator for Safety Evaluation (GTMS-SE). The GTMS-SE developed by DecisionTek, LLC, is a general train movement simulator that mimics real-life operations and scenarios of train movement over a specific territory.

Federal Railroad Administration, Optimum Communication Timeout Study - In this study, she and her colleagues identified the potential accident scenarios that may arise due to this timeout period. Concurrently with this activity, she quantified the maximum allowable communication timeout period for this architecture so that the PTC system would not pose a greater risk of train collisions, derailments, and accidents than a traditional cab signal system.

Independent Consultant, Charlottesville, VA, January 2006

Provided technical support to DecisionTek, LLC, to develop the software requirements and specification document for the General Train Movement Simulator for Safety Evaluation (GTMS-SE).

Commonwealth Computer Research, Inc., Charlottesville, VA, March 2004 – January 2006 Business Development Director

Responsible for identifying and writing proposals, and program management. In these roles, she successfully competed and managed a Department of Defense (DOD) Small Business Innovation Research (SBIR) Phase I award from Naval Air Systems Command (NAVAIR) to improve E-2C radar tracking capabilities. The success of her 8-person team in this Phase I effort led to the award of a Phase II contract. She successfully developed the bid for a DoD SBIR Phase I award from the Office of Naval Research (ONR). Concurrent with these activities, she developed proposals resulting in contracts from the Federal Railroad Administration (FRA), U.S. Army and Procter & Gamble. For the FRA award, she provided expertise to review safety analysis reports in support of the on-going development Illinois Department of Transportation (IDOT) Positive Train Control (PTC) system. During her tenure, she

expanded company research interests through contract awards and generated over \$1,400,000 in contracts.

University of Virginia, Charlottesville, VA, November 2000 – February 2004

Principal Scientist

Continued research assessing safety for railroad and transit railway signaling and processor-based control systems. She was responsible for ensuring that a simulation-based risk assessment of these systems complied with Department of Transportation (DOT) - Federal Railroad Administration (FRA) Proposed Rule 49 CFR Part 209, 234 and 236: Standards for Development and Use of Processor-Based Signal and Train Control Systems. She also continued to refine the model constructs as additional data became available.

SAIC, Charlottesville, VA, March – April 2003

Independent Consultant

Provided risk analysis expertise to the ARES Mars Airplane project. She derived parametric data from application experts and developed rudimentary models for baseline fault tree analysis.

University of Virginia, Charlottesville, VA, June 1997 - October 2000

Postdoctoral Research Associate

Engaged in research to assess safety for a Nuclear Regulatory Commission (NRC) control system for a reactor facility. She transitioned her research within the first few months of this postdoctoral term to support the safety analysis of railroad processor-based control systems. She was responsible for developing model constructs for the physical system and the associated railroad workers (engineers, conductors, dispatchers and maintenance of way workers) to support a simulation-based risk assessment of these systems compliant with Department of Transportation (DOT) - Federal Railroad Administration (FRA) Proposed Rule 49 CFR Part 209, 234 and 236: Standards for Development and Use of Processor-Based Signal and Train Control Systems.

University of Virginia, Charlottesville, VA, August 1991 - May 1997

Graduate Research Assistant

University of Virginia, Charlottesville, VA, January - May 1993

Graduate Teaching Assistant

Computer Systems Engineer, Department of Criminal Justice Services, Richmond, VA, August 1988 - June 1991.

Electronics Engineer, Carderrock Division, Naval Surface Warfare Center, Bethesda, MD, July 1987 - July 1988.

EDUCATION:

Ph.D. Electrical Engineering, University of Virginia, Charlottesville, VA, May 1997

School of Engineering and Applied Science

Dissertation: Dependability Analysis for Ultra-Dependable Systems using Statistics of the Extremes

M.S. Electrical Engineering, University of Virginia, Charlottesville, VA, May 1993

School of Engineering and Applied Science

Thesis: A Fault-Partitioning Based Parallel Automated Test Pattern Generation (ATPG) System

B.S. Electrical Engineering with Distinction, University of Virginia, Charlottesville, VA, May 1987

School of Engineering and Applied Science, Graduated with Distinction

AWARDS & HONORS:

- Tau Beta Pi - Engineering Honor Society
- Eta Kappa Nu - International Electrical Engineering Honor Society
- Raven Society - University of Virginia Honor Society

- 1993 Recipient of National Science Foundation Fellowship: NSF/GEE Minority Fellowship for Doctoral Studies in Engineering

PROFESSIONAL CERTIFICATIONS:

- ITIL v3 Foundation

PROFESSIONAL AFFILIATIONS:

- Senior Member IEEE
- Editor, *It All Depends* column for *IEEE Security and Privacy* magazine January 2009 – August 2011
- IEEE Reliability Society Administrative Committee 2000 - 2002
- IEEE Human Interface Technology Committee 2001 – 2002
- IEEE Reliability Representative to the Intelligent Transportation System (ITS) Council 2001 – 2002

PUBLICATIONS

Journals

Wolf, Joseph M., Lori M. Kaufman, Robert H. Klenke, James H. Aylor, and Ronald Waxman, "An Analysis of Fault Partitioned Parallel Test Generation," *IEEE Transactions on Computer-Aided Design*, Volume 15, Number 5, May 1996, pp. 517-534.

Kaufman, Lori M., Joanne Bechta Dugan, and Barry W. Johnson, "Using Statistics of the Extremes for Software Reliability Analysis," *IEEE Transactions on Reliability*, Volume 48, Number 3, September 1999, pp. 292-299.

Kaufman, Lori M., Joanne Bechta Dugan, and Barry W. Johnson, "Coverage Estimation Using Statistics Of The Extremes For When Testing Reveals No Failures," *IEEE Transactions on Reliability*, Volume 51, Number 1, January 2002, pp. 3-10.

Federal Publications

Kaufman, Lori M. and Barry W. Johnson, "Embedded Digital System Reliability and Safety Analysis," U.S. Nuclear Regulatory Commission NUREG/GR-0020, February 2001.

General Publications

Harauz, John, and Lori M. Kaufman, "A New Era of Presidential Security: The President and His Blackberry," *IEEE Security and Privacy*, Volume 7, Issue 2, March/April 2009, pp. 67-70.

Kaufman, Lori M., "Data Security in the World of Cloud Computing," *IEEE Security and Privacy*, Volume 7, Issue 4, July/August 2009, pp. 61-64.

Kaufman, Lori M., "Can a Trusted Environment Provide Security?" *IEEE Security and Privacy*, Volume 8, Issue 1, January/February 2010, pp. 50 - 52.

Kaufman, Lori M., "Can Public-Cloud Security Meet Its Unique Challenges?" *IEEE Security and Privacy*, Volume 8, Issue 3, July/August 2010, pp. 55-57.

Kaufman, Lori M., "How Private is the Internet?," *IEEE Security and Privacy*, Volume 9, Issue 1, January/February 2011, pp. 73 -75.

Refereed Conference Proceedings

Klenke, Robert H., Lori M. Kaufman, James H. Aylor, Ronald Waxman, and Padmini Narayan, "Workstation Based Parallel Test Generation," *Proceedings of the IEEE International Test Conference*, Baltimore, Maryland, October 1993, pp. 419-428.

Kaufman, Lori M., D. Todd Smith, Joanne Bechta Dugan and Barry W. Johnson, "Software Reliability Analysis Using Statistics of the Extremes," *Proceedings of the Reliability and Maintainability Symposium*, Philadelphia, Pennsylvania, January 1997, pp. 175-180.

Kaufman, Lori M., Joanne Bechta Dugan, and Barry W. Johnson, "Using Statistics of the Extremes for Software Reliability Analysis of Safety Critical Systems," *Proceedings of the Ninth International Symposium on Software Reliability Engineering*, Paderborn, Germany, November 1998, pp. 355-363.

Kaufman, Lori M., Ragavan Manian, Kiran Vemuri, and Joanne Bechta Dugan, "System-Reliability Analysis of an Embedded Hardware/Software System using Fault Trees," *Proceedings of the Reliability and Maintainability Symposium*, Washington D.C., January 1999, pp. 135-141.

Kaufman, Lori M., Ray Gretlein, and Ronald J. Hayne, "A Quantitative Assessment of the Application of Software Reliability to Reusable Code," *Proceedings of the Reliability and Maintainability Symposium*, Washington D.C., January 1999, pp. 165-170.

Kaufman, Lori M., Ted C. Giras and Nabil Ghali, "Reliability of a Computer Based Transit Car Door System," *Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, Volume 2*, Washington D.C., August 1999, pp. 941-946.

Kaufman, Lori M. Kaufman, Sanyukta Bhide and Barry W. Johnson, "Modeling of Common-Mode Failures in Digital Embedded Systems," *Proceedings of the Reliability and Maintainability Symposium*, Los Angeles, California, January 2000, pp. 350-357.

Tillack, Jonathan A., Lori M. Kaufman, Karthik Kannan and Barry W. Johnson, "Application of Design Standards to Safety-Critical Systems," *Proceedings of the Reliability and Maintainability Symposium*, Los Angeles, California, January 2000, pp. 345-349.

Kaufman, Lori M. and Ted Giras, "The Axiomatic Safety-Critical Assessment Process (ASCAP) Simulation Methodology," *Proceedings of the 9th IFAC Symposium on Control in Transportation Systems 2000, Volume 2*, Braunschweig, Germany, June 2000, pp. 534-539.

Joshi, Vikram V., Lori M. Kaufman and Ted C. Giras, "Human Behavior Modeling in Train Control Systems," *Proceedings of the Reliability and Maintainability Symposium*, Philadelphia, Pennsylvania, January 2001, pp. 183-188.

Monfalcone, Marc E., Lori M. Kaufman and Ted C. Giras, "Safety Assessment of a Direct Traffic Control (DTC) Train Control System using the Axiomatic Safety-Critical Assessment Process (ASCAP)," *Proceedings of the Reliability and Maintainability Symposium*, Philadelphia, Pennsylvania, January 2001, pp. 352-357.

Kaufman, Lori M. and Ted C. Giras, "Simulation of Rare Events in Transportation Systems," *Proceedings of the 2001 Winter Simulation Conference*, Washington D.C., December 2001, pp. 1380-1385.

Kaufman, Lori M., Maximo H. Salinas, Ronald D. Williams and Ted C. Giras, "Integrated Hardware/Software Device Testing for Use in a Safety-Critical Application," *Proceedings of the Reliability and Maintainability Symposium*, Tampa, Florida, January 2003, pp. 132-137.

Non-Refereed Conference Proceedings

Kaufman, Lori M. and Barry W. Johnson, "The Importance of Fault Detection Coverage in Safety Critical Systems," *Transactions of the Twenty-Sixth Water Reactor Safety Information Meeting*, U.S. Nuclear Regulatory Commission, NUREG/CP-0165, Bethesda, Maryland, October 1998, pp. 39-40.

Kaufman, Lori M. and Barry W. Johnson, "The Importance of Fault Detection Coverage in Safety Critical Systems," *Proceedings of the Twenty-Sixth Water Reactor Safety Information Meeting, Volume 2*, U.S. Nuclear Regulatory Commission, NUREG/CP-0166, Bethesda,

Maryland, October 1998, pp. 5-28.

KEY SPEAKING ENGAGEMENTS

Every Refereed and Non-Refereed Conference Proceeding Publication was presented at the cited conference for peer review and discussion.