Chapter 5

SECURING POSITIVE TRAIN CONTROL SYSTEMS

Mark Hartong, Rajni Goel and Duminda Wijesekera

Abstract Positive train control (PTC) systems are distributed interoperable systems that control the movement of passenger and freight trains, providing significant safety enhancements over traditional methods of operating railroads. Due to their reliance on wireless communications, PTC systems are vulnerable to attacks that can compromise safety and potentially cause serious accidents. Designing PTC systems that can mitigate the negative effects of wireless-based exploits are mandatory to ensuring railroad safety. This paper employs use cases and misuse cases to analyze the effects of exploiting vulnerabilities in PTC systems. Use cases specify operational interactions and requirements, while misuse cases specify potential misuse or abuse scenarios. A distributed trust management system is proposed to enable PTC use cases and eliminate identified misuse cases.

Keywords: Railroad security, positive train control, use cases, misuse cases

1. Introduction

Railroads are a critical component of the U.S. transportation and distribution system. The rail infrastructure consists of approximately 141,000 miles of track used by 549 freight railroads to move 25% of all intercity freight by tonnage and 41% of all freight by ton-miles [2, 34].

Positive train control (PTC) systems are used to control the movement of passenger and freight trains, providing significant safety enhancements over traditional methods of operating railroads. Less than 5% of route-miles in the U.S. [3] currently use PTC systems for positive train separation, speed enforcement and roadway worker protection. However, the implementation of PTC systems in the railroad infrastructure is expected to increase over the next decade.

PTC systems use wireless networks to distribute train position data, signals and switch position monitor data, and movement authorities generated by a

Hartong, M., Goel, R. and Wijesekera, D., 2008, in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 57–72.

central office for controlling railroad operations. However, their reliance on wireless networks exposes PTC systems to a slew of attacks that can significantly impact the safety of railroad operations.

This paper employs use cases and misuse cases to analyze the effects of exploiting vulnerabilities in PTC systems. Use cases specify operational interactions and requirements, whereas misuse cases specify potential misuse or abuse scenarios. A distributed trust management system is proposed to enable PTC use cases and eliminate identified misuse cases.

2. Business Context of Railroads

Railroads in the United States are categorized as Class I, Class II or Class III based on their annual revenue. Currently, there are six Class I freight railroads, with the remainder being Class II and Class III railroads.

In 2000, Class I railroads invested 17.8% of their revenues in capital improvements, compared with an average of 3.7% for all manufacturing industries. Between 1991 and 2000, railroad re-investments totaled $54 billion: 67% for roadways and structures, and 33% for equipment. Unfortunately, the total stock market value of railroads is one-fifth of its 1980 value. This has reduced the amount of capital available for improvements and maintenance. The difference between capital expenditures and the amount railroads can invest from their own revenues is about $2 billion annually. As private corporations, it is difficult for railroads to justify spending on new technological initiatives that do not directly support recapitalization requirements.

Domestic policy initiatives do not favor public investment in railroads. In 1998, for example, federal and state expenditures on highway improvements were 33 times greater than the expenditures on passenger rail and freight rail combined. The public sector invested $108 billion in highways, $11 billion in transit, $9 billion in airways and airports, but just $3 billion in railroads [1].

Public sector investment in railroad security is even worse. In 2006, only 2% of all critical infrastructure protection grants from the Department of Homeland Security were designated for railroad security; all of these grants were earmarked for enhancing passenger rail security [9].

3. Consequences of Disrupting Rail Operations

The Congressional Research Service of the Library of Congress [29] and the President's National Security Telecommunications Advisory Committee [26] have identified hacker attacks as a serious threat to wireless networks such as those used in PTC systems. Although no attacks are known to have occurred on the railroad control infrastructure, the General Accountability Office reports that successful attacks have been launched against industrial control systems in other sectors [13].

Disruptions to railway networks can have a significant negative impact on the U.S. economy. Service problems resulting from Union Pacific's inability to position and move their equipment (although not the result of a deliberate

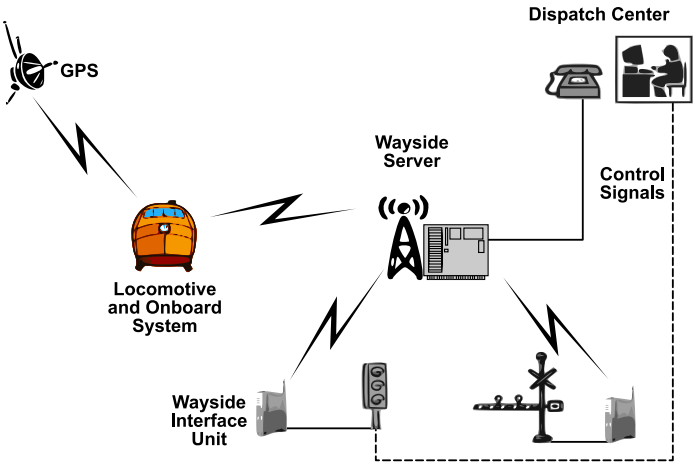

Figure 1. Generic PTC architecture.

attack) resulted in direct costs of $1.093 billion and an additional $643 million in costs to consumers [37]. More recently, commuter and CSX freight rail service on the East Coast experienced cancellations and delays of up to 48 hours because of the accidental introduction of a virus that disabled the computer systems at the CSX headquarters [28].

Vulnerabilities in the rail control infrastructure have been highlighted in several reports (see, e.g., [6, 24]). While these studies were unable to reach conclusions about the threat level and degree of risk, they uniformly emphasize the possibility of serious accidents. For example, a single successful attack on a PTC system can re-position a switch from a mainline to an occupied siding, which would almost certainly result in a collision.

4. PTC Systems

The generic PTC functional architecture (Figure 1) has three major functional subsystems: wayside units, mobile units and a dispatch/control unit. The wayside units include highway grade crossing signals, switches and interlocks; mobile units include locomotives and other equipment that travels on rail along with their onboard controllers; the dispatch/control unit is the central office that runs the railroad. Each major functional subsystem consists of a collection of physical components (information processing equipment and databases) linked via wireless networks.

Table 1 summarizes the five PTC levels and their functionality [10, 11]. Each higher PTC level includes all the functions of the lower levels along with additional functionality. Note that each level maps to multiple security requirements.

The complexity of analyzing security needs increases with the level of PTC functionality. We employ misuse cases to determine potential threat profiles

Table 1. PTC levels and functionality.

Level	PTC Functionality
0	None
1	Prevent train-to-train collisions Enforce speed restrictions Protect roadway workers
2	PTC Level 1 functions plus Digital transmission of authorities and train information
3	PTC Level 2 functions plus Wayside monitoring of the status of all switch, signal and protective devices in the traffic control territory
4	PTC Level 3 functions plus Wayside monitoring of all mainline switches, signals and protective devices Additional protective devices such as slide detectors, high water and bridge interlocks Advanced broken rail detection Roadway worker terminals for dispatcher and train communications

and their effects on railroad safety. Previous work on PTC security has considered possible problems in the rail infrastructure [4], examined communications systems [7, 8], and discussed potential threats [15]. However, security requirements for operating PTC systems without disruption have not been specified as yet. Before we can derive these security requirements, it is necessary to discuss sample misuse cases and show how they can impact PTC functionality.

5. Analyzing Railroad Safety and Security

Recent regulatory initiatives [36] and industry efforts [14] at deploying wireless PTC systems have significantly increased the level of risk. Several techniques have been proposed to analyze non-security related risks. They include:

- Soft systems methodology (SSM) [5]
- Quality function deployment (QFD) [27]
- Controlled requirements expression (CORE) [23, 35]
- Issue-based information systems (IBIS) [21]
- Joint application development (JAD) [38]

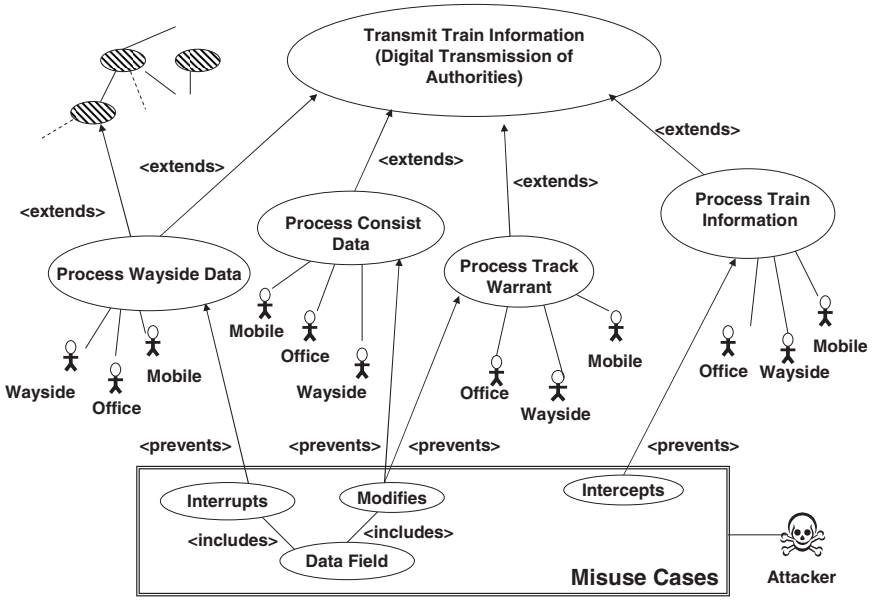

Figure 2. PTC use cases, misuse cases and their relationships.

- Feature-oriented domain analysis (FODA) [20]
- Accelerated requirements method (ARM) [18]
- Use/misuse case analysis [31, 32]

We employ use/misuse cases to analyze the effects of exploiting vulnerabilities in PTC systems. Use cases specify operational interactions and requirements. On the other hand, misuse cases specify potential misuse or abuse scenarios.

5.1 Use Cases for PTC Operations

Use cases are widely employed for capturing functional requirements [19, 30]. They define the set of interactions between actors (users) and a system. Constructs such as <includes> and <extends> may be used to create complex use cases from simple ones. The <includes> relationship is analogous to a use case subroutine, while <extends> specifies an enhancement of the basic interaction pattern.

Figure 2 presents PTC use cases, misuse cases and their relationships. Use cases are represented as ovals, actors as traditional stick figures, and relationships as single lines connecting actors to use cases or intra use case relationships. The shaded ovals in the top left-hand corner of Figure 2 denote additional use cases that have not been fully defined in this example.

5.2 Misuse Cases for PTC Operations

Due to the misuse and/or abuse of system flaws and vulnerabilities by various malicious actors (mal-actors), use cases are augmented with misuse cases to facilitate the task of eliminating known mal-actions during system design. Employing use cases and misuse cases together simplifies the process of specifying and reviewing system interactions, and deriving system security requirements.

High-speed rail control requires timely signal dissemination and reaction to enforce system requirements and to prevent foreseeable mal-actions. Potential mal-actors are abstracted as a single attacker in misuse cases. All actors (including the mal-actor) communicate by exchanging messages. Figure 2 represents the mal-actor using a skull and crossbones, and misuse cases as ovals in the box labeled "Misuse Cases." Misuse cases relating to PTC operations are categorized as: (i) passive eavesdropping, (ii) active denial of control, and (iii) active assumption of control.

- **Passive Eavesdropping:** This involves the surreptitious gathering of information, possibly using a wireless network analyzer. The actor is unaware of the eavesdropping because the mal-actor does not actively interfere with an executing use case by transmitting or disturbing the actor's signal. The ability to exploit the results of a passive misuse case depends on the attacker's technical sophistication (e.g., ability to bypass or overcome protection mechanisms).

- **Active Denial of Control:** This involves a technique such as broadband jamming of the frequency spectrum to disable communications between an actor and the PTC system. This misuse case prevents the actor from issuing commands to the PTC system. Note that the mal-actor does not need to have any knowledge about the parameters in the messages sent by the actor to the PTC system. The Interrupts misuse case in Figure 2 is an example of active denial of control.

  More sophisticated forms of active denial of control such as denial of service (DoS) and distributed denial of service (DDoS) attacks require knowledge of the message parameters. A more specialized misuse case is Power Exhaustion, in which a mal-actor prevents a wayside device from communicating by draining its power.

- **Active Assumption of Control:** This involves a mal-actor who impersonates an actor and gains active control of the PTC system or system component. An example misuse case is a mal-actor spoofing a dispatch center and requesting a locomotive to stop.

6. Deriving Security Requirements

We use a four-step process to derive security requirements from use cases and misuse cases.

- **Step 1:** Specify detailed use cases and misuse cases along with the relationships between them.
- **Step 2:** Specify operational and environmental constraints.
- **Step 3:** Derive system requirements.
- **Step 4:** Infer security objectives.

The following sections describe the four steps in detail.

6.1 Specifying Use Cases and Misuse Cases

As mentioned above, use cases specify functional requirements while misuse cases specify the abuses to be avoided or eliminated in a system being designed. Analyzing the effects that stated misuse cases have on the stated use cases is one of the principal security objectives. Graphical and textual representations such as those in Figure 2 and Tables 2 and 3 facilitate this activity.

Returning to our example, consider the impact of the misuse case Modifies on the use case, Transmit Train Information (Digital Transmission of Authorities) (Level 2). Figure 2 shows that this use case is extended into four use cases: Process Wayside Data, Process Consist Data, Process Track Warrant and Process Train Information by the actors: Office, Wayside and Mobile. The Prevents relationship existing between the Process Track Warrant use case and the Modifies misuse case shows which use cases executed by the actors are affected by misuse cases executed by the mal-actor. Tables 2 and 3 provide a detailed description of the Modify Track Warrant misuse case along with all its relationships.

6.2 Specifying Constraints

Constraints are obtained from the textual descriptions of use cases and misuse cases by employing the "noun-verb" extraction technique [25]. In noun-verb extraction, actions and elements correspond to (ad)verbs and (pro)nouns, respectively, in the text. This process may be performed manually or using automated tools [22]. After the actions and elements have been determined, they become system constraints from the point of view of the actors.

For example, applying the noun-verb extraction technique to the first sentence in the Summary section of the misuse case in Table 2 yields "Text carrying specific authorizations for a mobile unit to occupy a particular section of track," which appears in the first row of the first column of Table 4. Repeating this process for the text in Tables 2 and 3 yields the constraints in Tables 4 and 5.

6.3 Deriving System Requirements

The system requirements follow from the definitions of the constraints. The extracted nouns and verbs that make up the constraints are examined and recast into positive assertions regarding required system behavior. For example,

Table 2. Use/misuse case for Modify Track Warrant.

Number	Description
1	**Summary:** Text carrying specific authorization for a mobile unit to occupy a particular section of track is modified. This track warrant text provides information that prevents train-to-train, train-to-on-track-equipment, on-track-equipment-to-on-track-equipment and train-to-roadway-worker collisions.
2	**Basic Path:** The track warrant text is transmitted from the office/dispatch system to a mobile unit. The CRC is modified while the message is en route, rendering the track warrant text invalid and preventing the mobile unit from receiving a valid track warrant. Mobile units acting on invalid warrants collide with other trains, track vehicles or roadway workers.
3	**Alternate Paths:** The message is relayed through the wayside subsystem and the CRC is modified during transmission between: (i) the office/dispatch subsystem and the wayside subsystem, or (ii) the wayside subsystem and the mobile unit.
4	**Capture Points:** The track warrant message is invalid because one or more of the following message fields are modified: (i) source, (ii) type, (iii) message payload, (iv) message identifier.
5	**Triggers:** A transmitter is placed within range of the defender's receiver and/or transmitter.
6	**Attacker Profile:** The originator's message is captured, read and interpreted, bits in the message are substituted, and the message is retransmitted.

the constraint "Text carrying specific authorizations for a mobile unit to occupy a particular section of track" from the first row and first column in Table 4 is recast to the positive assertion "Authorization to occupy a specific section of track shall be in text." This assertion becomes the requirement in the second column of the first row in Table 4. This process is repeated for each constraint in the first column of Tables 4 and 5 to produce the corresponding requirement in the second column of the two tables.

6.4 Inferring Security Objectives

The first step is to decide which traditional security objectives (confidentiality, integrity, availability, authenticity, accountability and identification) must be enforced to ensure that each specific requirement defined above is met. This step is typically performed by an experienced security engineer. Formally, this involves specifying use cases that mitigate or prevent the stated misuse cases from being executed.

Table 3. Use/misuse case for Modify Track Warrant (continued).

Number	Description
7	**Preconditions:** (i) The office/dispatch subsystem is transmitting a track warrant message to a mobile unit, (ii) the office/dispatch subsystem and the mobile unit are operating normally.
8	**Postconditions (Worst Case):** (i) The mobile unit receives an invalid track warrant, which causes a train-to-train, train-to-on-track-equipment, on-track-equipment-to-on-track-equipment or train-to-roadway-worker collision, (ii) unauthorized modifications of track warrants disable accountability and non-repudiation of specific operational restrictions and authorizations for potentially high hazard events such as commingling of roadway workers and trains, (iii) an invalid warrant halts mobile units at the limits of its current authority, producing a significant operational (if not safety) impact.
9	**Postconditions (Best Case):** (i) Integrity (specifically data origin authentication and data integrity) is maintained, (ii) track warrant modification is identified and isolated, (iii) two entities do not commingle despite operating on altered track warrants.
10	**Business Rules:** (i) Only the office/dispatch subsystem may originate valid track warrant text, (ii) office/dispatch subsystem may push valid track warrant text to a mobile unit or wayside subsystem, (iii) mobile unit may pull or request pulling a valid track warrant text from the wayside subsystem or the office/dispatch subsystem, (iv) wayside subsystem may pull valid track warrant text from the office/dispatch subsystem only after the receipt of a request to pull track warrant text from a mobile unit.

For example, to satisfy the requirement in the second column of the first row in Table 4, namely "Authorization to occupy a specific section of track shall be in text," it is necessary to protect the "integrity" of transmitted track authorities between authenticated senders and receivers. This yields the security objective "Integrity of text" in the third column of the first row of Table 4. This process is repeated for each requirement in the second column of Tables 4 and 5 to produce the corresponding security objective in the third column of the two tables.

In some instances a constraint does not translate to a specific security objective because the requirement generated from the constraint is actually the specification of a higher level use case. For example the constraint "Mobile unit collides with another train, track vehicle or roadway workers" in the fourth row of Table 4 generates the requirement "Mobile unit shall be prevented from colliding with another train, track vehicle and roadway workers." This requirement is, in fact, one of the core use cases that defines a PTC system. Consequently the level of granularity of the requirement will directly impact the

Table 4. Constraints, requirements and security objectives.

Constraint	**Requirement**	**Security Objective**
Text carrying specific authorization for a mobile unit to occupy a particular section of track	Authorization to occupy a specific section of track shall be in text	Integrity of text
Track warrant transmitted from office/dispatch subsystem to mobile unit	Track warrant shall be transmitted from office/dispatch subsystem to mobile unit	Authenticity of sender and receiver
Track warrant invalid as CRC is modified en route	CRC shall be applied to track warrant to detect changes that would render track warrant invalid	Integrity of track warrant
Mobile unit collides with another train, track vehicle or roadway workers	Mobile unit shall be prevented from colliding with another train, track vehicle and roadway workers	
Message relayed to wayside subsystem	Message shall be relayed to wayside unit	Authenticity of receiver
Track warrant invalid as one or more message fields are modified: (i) source, (ii) type, (iii) message payload, (iv) message identifier	Track warrant shall be protected from modification	Integrity of track warrant
Transmitter within range of defender's receiver and/or transmitter	System shall operate when defender is within range of attacker's transmitter	Availability of communications
Attacker captures the originator's message, reads and interprets message, substitutes bits and retransmits the message	System shall operate in environment where originator's message is captured, read and interpreted, message bits are substituted and message is transmitted	Identity of originator; authenticity of sender and receiver; integrity of message

ability of a security engineer to devise mitigating use cases (and subsequently define the required security objectives). Increased granularity of the requirements is, therefore, critical to defining essential security-related use cases.

Table 5. Constraints, requirements and security objectives (continued).

Constraint	Requirement	Security Objective
Office/dispatch subsystem transmits track warrant to mobile unit	Track warrant shall be transmitted from the office/dispatch subsystem to mobile unit	Authenticity of sender and receiver
Office/dispatch subsystem and mobile unit operate normally	Track warrant shall be transmitted from the office/dispatch subsystem to mobile unit when system is operating normally	Authenticity of sender and receiver
Office/dispatch subsystem originates track warrant	Office/dispatch subsystem shall originate track warrant	Accountability of originator
Invalid track warrant halts mobile unit at the limit of its current authority	Invalid track warrant shall halt mobile unit at the limit of its current authority	Integrity of track warrant
Unauthorized modification of track warrant disables the accountability and non-repudiation of specific operational restrictions and authorization for a potentially high hazard event such as commingling roadway workers and trains	Unauthorized modification of track warrant shall disable the accountability and non-repudiation of specific operational restrictions and authorization for a potentially high hazard event such as commingling roadway workers and trains	Integrity of track warrant; identity, accountability and authenticity of sender
Train-to-train, train-to-on-track-equipment, on-track-equipment to on-track-equipment or train to roadway-worker collision	System shall prevent train-to-train, train-to-on-track-equipment, on-track equipment to on-track equipment and train to roadway worker collision	

6.5 Drawbacks of the Process

A major drawback of our four-step process is the high degree of human involvement and skill required to infer the security objectives. As discussed in [33], employing a standard format for use cases and misuse cases simplifies

Table 6. Summary PTC requirements by functional capabilities.

	Confid.	**Integ.**	**Avail.**	**Auth.**	**Account.**	**Ident.**
Prevent train-to-train collisions	No	Yes	No	Yes	No	Yes
Enforce speed restrictions	No	Yes	No	Yes	No	Yes
Protect roadway workers	No	Yes	No	Yes	Yes	Yes
Wayside monitoring of traffic control territory	No	Yes	No	Yes	No	Yes
Wayside monitoring of all mainline switches	No	Yes	No	Yes	No	Yes
Additional wayside protection and detection devices	No	Yes	No	Yes	No	Yes
Advanced broken rail detection	No	Yes	No	Yes	No	Yes
Roadway worker terminals	Yes	Yes	No	Yes	Yes	Yes

the task, but does not automate it. Furthermore, it reduces but does not eliminate the need for extensive security engineering domain knowledge.

Consequently, we have pursued the translation of use cases and misuse cases to functional fault trees as an alternative to deriving system requirements and inferring security objectives [17]. This approach combines the user friendliness of graphical and textual specifications with the rigorous analysis provided by functional fault tree based tools.

7. Distributed Trust Management

We have designed a distributed trust management system to help mitigate stated misuse cases [16]. The system provides the use cases described in Figure 2 and includes the misuse case described in Tables 2 and 3 as well as other misuse cases related to communications and identity management. Upon analyzing these use cases and misuse cases, new requirements were generated and additional security objectives were inferred. Table 6 summarizes the security objectives. Each entry in the table indicates the necessity of a specific secu-

rity objective (confidentiality, integrity, availability, authenticity, accountability and identity).

Interoperability and network management aspects have a significant impact on the security requirements. This is because locomotives are often exchanged between railroads; therefore, onboard PTC subsystems must be compatible with various wayside and dispatch subsystems. Similarly, the logical and physical architectures of PTC systems, security policy issues, labor agreements, budgetary and schedule restrictions along with the skill level and availability of technical resources to manage a secure PTC system are important. The result is that no single optimal solution exists. Consequently, PTC security solutions should be tailored to address the specific railroad environment.

8. Conclusions

PTC systems can significantly enhance railroad safety by maintaining inter-train distances, enforcing speed restrictions and preventing train-to-wayside-worker accidents. Although they have been extensively analyzed for operational safety, PTC security issues have not been fully addressed. Due to their reliance on wireless networks, PTC systems are vulnerable to attacks that target wireless communications. Use/misuse case analysis is a systematic methodology for identifying how a mal-actor can negatively impact the functional objectives of a PTC system. The negative impacts on PTC use cases can be employed to design PTC systems that are resistant and resilient to misuse cases. Addressing these issues at the design stage rather than after deployment is an important security engineering practice.

PTC systems are currently not economically viable from the point of view of their safety business case alone [10, 11]. However, when combined with other advanced technologies, PTC systems can offer significant economic and safety benefits [12]. This will, however, depend on the ability to ensure that PTC systems are both resistant and resilient to attacks.

Note that the views and opinions expressed in this paper are those of the authors. They do not reflect any official policy or position of the Federal Railroad Administration, U.S. Department of Transportation or the U.S. Government, and shall not be used for advertising or product endorsement purposes.

References

[1] American Association of State Highway and Transportation Officials, Transportation: Invest in America – Freight-Rail Bottom Line Report, Washington, DC (freight.transportation.org/doc/FreightRailReport.pdf), 2002.

[2] Association of American Railroads, U.S. Freight Railroad Statistics, Washington, DC, 2004.

[3] Bureau of Transportation Statistics, Federal Railroad Administration National Rail Network 1:100,000 (Line), National Transportation Atlas Database 2003, Department of Transportation, Washington, DC, 2003.

[4] A. Carlson, D. Frincke and M. Laude, Railway security issues: A survey of developing railway technology, *Proceedings of the International Conference on Computer, Communications and Control Technologies*, vol. 1, pp. 1–6, 2003.

[5] P. Checkland and J. Scholes, *Soft Systems Methodology in Action*, John Wiley, Chichester, United Kingdom, 1999.

[6] C. Chittester and Y. Haimes, Risks of terrorism to information technology and to critical interdependent infrastructures, *Journal of Homeland Security and Emergency Management*, vol. 1(4), 2004.

[7] P. Craven, A brief look at railroad communication vulnerabilities, *Proceedings of the Seventh IEEE International Conference on Intelligent Transportation Systems*, pp. 345–349, 2004.

[8] P. Craven and A. Craven, Security of ATCS wireless railway communications, *Proceedings of the IEEE/ASME Joint Rail Conference*, pp. 227–238, 2005.

[9] Department of Homeland Security, FY 2006 Infrastructure Protection Program: Intercity Passenger Rail Security Program Guidelines and Application Kit, Washington, DC, 2006.

[10] Federal Railroad Administration, Railroad Communications and Train Control, Technical Report, Department of Transportation, Washington, DC, 1994.

[11] Federal Railroad Administration, Implementation of Positive Train Control Systems, Technical Report, Department of Transportation, Washington, DC, 1999.

[12] Federal Railroad Administration, Benefits and Costs of Positive Train Control, Report in Response to the Request of the Appropriations Committees, Department of Transportation, Washington, DC, 2004.

[13] General Accounting Office, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report to Congressional Requesters, GAO-04-354, Washington, DC, 2004.

[14] M. Hartong, R. Goel and D. Wijesekera, Communications-based positive train control systems architecture in the USA, *Proceedings of the Sixty-Third IEEE Vehicular Technology Conference*, vol. 6, pp. 2987–2991, 2006.

[15] M. Hartong, R. Goel and D. Wijesekera, Communications security concerns in communications-based train control, *Proceedings of the Tenth International Conference on Computer System Design and Operation in the Railway and Other Transit Systems*, 2006.

[16] M. Hartong, R. Goel and D. Wijesekera, Key management requirements for positive train control communications security, *Proceedings of the IEEE/ASME Joint Rail Conference*, pp. 253–262, 2006.

[17] M. Hartong, R. Goel and D. Wijesekera, Mapping misuse cases to functional fault trees in order to secure positive train control systems, *Proceedings of the Ninth International Conference on Applications of Advanced Technology in Transportation Engineering*, pp. 394–399, 2006.

[18] R. Hubbard, N. Mead and C. Schroeder, An assessment of the relative efficiency of a facilitator-driven requirements collection process with respect to the conventional interview method, *Proceedings of the Fourth International Conference on Requirements Engineering*, pp. 178–186, 2000.

[19] I. Jacobson, *Object-Oriented Software Engineering: A Use Case Driven Approach*, Addison-Wesley, Boston, Massachusetts, 1992.

[20] K. Kang, S. Cohen, J. Hess, W. Novack and A. Peterson, Feature-Oriented Domain Analysis Feasibility Study, Technical Report CMU/SEI-90-TR-021, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 1990.

[21] W. Kunz and H. Rittel, Issues as elements of information systems, Working Paper WP-131, Berkeley Institute of Urban and Regional Development, University of California, Berkeley, California, 1970.

[22] C. Lerman, *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and the Unified Process*, Prentice Hall, Upper Saddle River, New Jersey, 1998.

[23] G. Mullery, CORE: A method for controlled requirements specification, *Proceedings of the Fourth International Conference on Software Engineering*, pp. 126–135, 1979.

[24] National Research Council, *Cybersecurity of Freight Information Systems: A Scoping Study*, Transportation Research Board, National Academy of Sciences, Washington, DC, 2003.

[25] S. Overmyer, L. Benoit and R. Owen, Conceptual modeling through linguistic analysis using LIDA, *Proceedings of the Twenty-Third International Conference on Software Engineering*, pp. 401–410, 2001.

[26] President's National Security Telecommunications Advisory Committee (NSTAC), Wireless Security Report, Wireless Task Force Report, National Communications System, Arlington, Virginia (www.ncs.gov/nstac/reports/2003/WTF%20Wireless%20Security%20Report.pdf), 2003.

[27] QFD Institute, Frequently asked questions about QFD (www.qfdi.org/what_is_qfd/faqs_about_qfd.htm).

[28] W. Rash, Engaging in worm warfare, *InfoWorld*, January 9, 2004.

[29] J. Rollins and C. Wilson, Terrorist Capabilities for Cyberattack: Overview and Policy Issues, Report RL33123, Congressional Research Service, Library of Congress, Washington, DC, 2007.

[30] J. Rumbaugh, Getting started: Using use cases to capture requirements, *Journal of Object-Oriented Programming*, vol. 7(5), pp. 8–12, 1994.

[31] G. Sindre and A. Opdahl, Eliciting security requirements by misuse cases, *Proceedings of the Thirty-Seventh International Conference on Technology of Object-Oriented Languages and Systems*, pp. 120–131, 2000.

[32] G. Sindre and A. Opdahl, Capturing security requirements through misuse cases, *Proceedings of the Fourteenth Norwegian Informatics Conference*, 2001.

[33] G. Sindre and A. Opdahl, Templates for misuse case description, *Proceedings of the Seventh International Workshop on Requirements Engineering*, 2001.

[34] Surface Transportation Board, 2003 Statistics of Class I Freight Railroads in the United States, Department of Transportation, Washington, DC, 2003.

[35] Systems Designers Scientific, *CORE – The Method: User Manual*, SD-Scicon, London, United Kingdom, 1986.

[36] U.S. Government, Standards for the development and use of processor based signal and train control systems, *Federal Register*, vol. 70(232), pp. 72382–72385, 2005.

[37] B. Weinstein and T. Clower, The Impacts of the Union Pacific Service Disruptions on the Texas and National Economies: An Unfinished Story, Center for Economic Development and Research, University of North Texas, Denton, Texas, 1998.

[38] J. Wood and D. Silver, *Joint Application Development*, John Wiley, New York, 1995.