Chapter 12

USE-MISUSE CASE DRIVEN ANALYSIS OF POSITIVE TRAIN CONTROL

Mark Hartong, Rajni Goel and Duminda Wijesekera

Abstract Forensic analysis helps identify the causes of crimes and accidents. Determination of cause, however, requires detailed knowledge of a system's design and operational characteristics. This paper advocates that "use cases," which specify operational interactions and requirements, and "misuse cases," which specify potential misuse or abuse scenarios, can be used to analyze and link forensic evidence and create post-incident reconstructions. Use-misuse case analysis techniques involving non-probabilistic and probabilistic methods are described and applied to Positive Train Control (PTC) Systems – a network-based automated system that controls the movements of passenger and freight trains.

Keywords: Use-misuse case analysis, Bayesian belief networks, Positive Train Control (PTC) systems

1. Introduction

A forensic investigation involves the collection and analysis of evidence from the scene of an incident. Currently, investigators in the transportation sector, such as the National Transportation Safety Board (NTSB), make extensive use of the "Swiss Cheese Model" [23] to identify proximate and precursor causes of accidents. As an alternative, this paper presents a forensic analysis process rooted in the software development life cycle, which advocates that all the phases of system design should actively participate in and support incident investigation functionality.

The proposed forensic analysis process uses a software engineering technique called use-misuse case analysis, which examines system vulnerabilities and potential ways to exploit them [24–26]. Permissible interaction patterns provided by use cases constrain the scope of an investigation and convey knowledge about its operational domain in a succinct

manner, reducing the time spent by investigators to understand the domain and acquire evidence. Conversely, misuse cases, which incorporate known vulnerabilities and ways in which they can be exploited, provide investigators with alternative scenarios to pursue and identify potential evidence items.

Evidence found during a forensics examination may map completely (non probabilistically) to the evidence trait set defined by a misuse case. If the forensic evidence does not map completely, i.e., it is probabilistic in nature, techniques such as Bayesian Belief Networks (BBNs) [12, 14] can be used to obtain a probabilistic estimate about the misuse case that resulted in the incident.

In addition to describing the forensic analysis methodology, this paper compares its results with those from a traditional NTSB investigation of the June 2002 collision between Amtrak and MARC passenger trains in Baltimore, Maryland [18]. In fact, the NTSB recommendation relating to the use of Positive Train Control (PTC), a network-based system that conveys control messages for passenger and freight trains, is supported by the methodology.

The following section describes Positive Train Control (PTC) systems, use cases and misuse cases; it also shows how PTC functional requirements and potential misuse/abuse can be modeled via use-misuse cases. Section 3 discusses the NTSB forensic investigation of the Amtrak-MARC train accident, and shows how it can be viewed as an instance of a use-misuse case. Section 4 discuses the derivation of evidence traits from misuse cases. Section 5 describes a non-probabilistic mapping of evidence traits to misuse cases. Section 6 focuses on the probabilistic analysis of evidence using Bayesian Belief Networks (BBNs). The final section provides concluding remarks.

2. PTC System Use-Misuse Case Modeling

Positive Train Control (PTC) systems are increasingly used to ensure the safe operation of freight trains and passenger trains in the United States [8–11]. PTC offers significant enhancements in safety by providing for adequate train separation, enforcing speed restrictions, and protecting roadway workers. In a communication-based PTC implementation, functional subsystems are interconnected by a wireless network. Consequently, they are subject to the same vulnerabilities as other control systems that communicate using wireless networks. Although the vulnerabilities arise from common shortcomings of communicating subsystems, they manifest themselves in a specific control aspect by disrupting system functionality in a predictable manner.

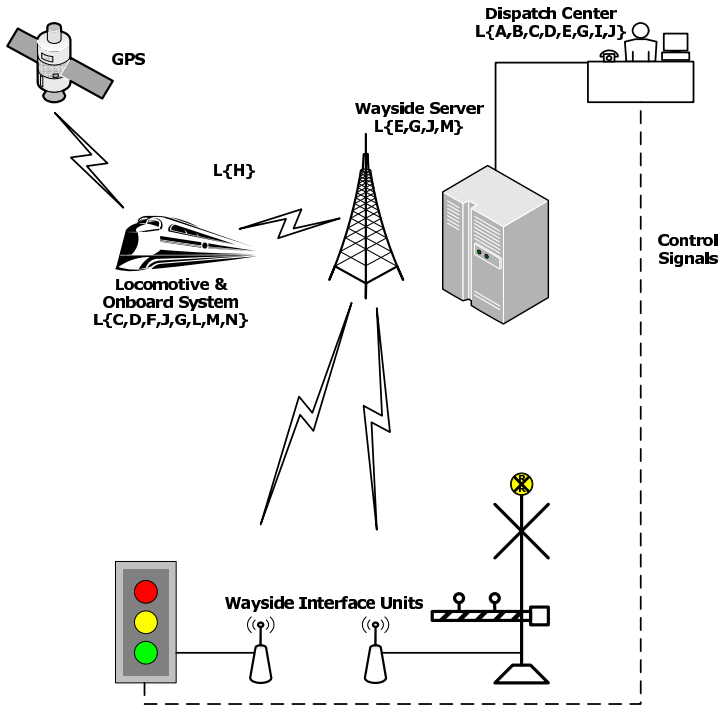

Figure 1. Simplified PTC architecture.

A simplified PTC architecture is presented in Figure 1. The architecture incorporates three major functional subsystems: wayside units, mobile units and a dispatch/control unit. The wayside units consist of elements such as highway grade crossing signals, switches and interlocks, and maintenance of way workers. The mobile units are locomotives and other rail equipment with onboard computers and location systems. The dispatch/control unit is the central office that runs the railroad. Each major functional subsystem consists of a collection of physical components implemented using databases, data communications systems and information processing equipment. Forensic evidence relevant to misuse cases for PTC systems is located in various subsystems. L{A} through L{N} in Figure 1 denote items of forensic evidence that relate to a specific misuse case. Note that these evidence items must be collected from multiple locations.

All PTC systems have the same core functional requirements. Table 1 specifies the functional requirements for various PTC levels [8, 9]. Note that each subsequent level imposes additional requirements.

Table 1. PTC levels and functionality.

Level	Functionality
0	None
1	Prevent train to train collisions; enforce speed restrictions; protect roadway workers and equipment
2	Level 1 functionality plus Digital transmission of authorities and train information
3	Level 2 functionality plus Monitor the status of all wayside switches, signals and protective devices in traffic control territory
4	Level 3 functionality plus Monitor the status of all mainline wayside switches, signals and protective devices, and additional devices (e.g., slide detectors, high water, hot bearings); implement advanced broken rail detection, roadway worker terminals for communications between dispatch and trains

In addition to functionality, PTC systems are also classified by the extent to which they augment railroad operations. Full PTC systems modify or replace the existing modes of railroad operation. Overlay PTC systems, on the other hand, provide their functionality while maintaining the existing modes of operation.

Deployed PTC systems operate with multiple components at the same time, forming a network of systems. Therefore, security and forensic aspects must be considered at the device level and at the network level. At the network level, it is necessary to identify sensitive network resources and components, and implement appropriate access control mechanisms. It is also important to prevent sabotage and misuse of PTC devices and network resources. The implementation of network management and security systems to protect, monitor and report on PTC systems without adversely impacting performance requires significant technical and financial resources.

2.1 Use Cases

Use cases capture how the users of a system will interact with the system. Ideally, they describe all possible interactions between an end user (person, machine or another system) and the system under consideration. Use cases also convey system requirements and constraints, and describe the essential features and rules under which the system and users operate. Use case diagrams are graphical instantiations of use cases (see Figure 2).

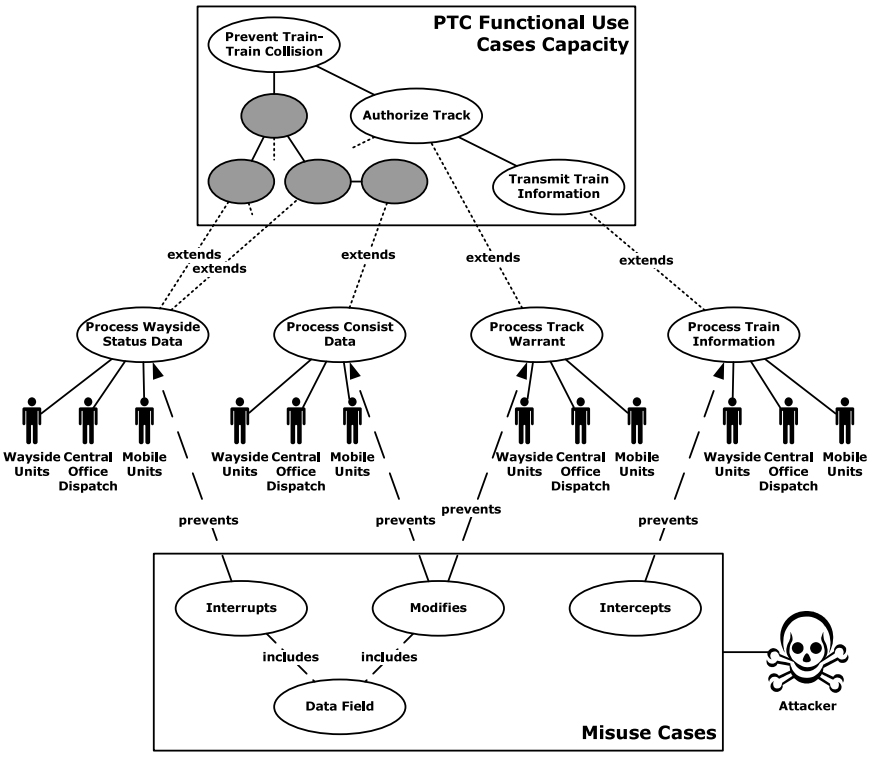

Figure 2. Use-misuse case relationships.

2.2 Misuse Cases

Misuse cases [24, 25] specify the external view of system behavior with respect to interactions between actors and/or mal-actors and the system. PTC actors in the use cases in Figure 2 include office/dispatch, wayside and mobile unit operators. Potential mal-actors are abstracted to a single attacker in the misuse cases. Figure 2 demonstrates how misuse cases can affect four use cases: (i) Process Wayside Status Data, (ii) Process Consist Data, (iii) Process Track Warrant, and (iv) Process Train Information. All actors – and the attacker — communicate by exchanging messages using the PTC system. Note that message formats used in PTC systems are implementation dependent.

A secure PTC system ensures that the safety services provided for the various PTC functions are available even in an exploitable communications environment. The repeated application of use-misuse case analysis to the functional requirement, Prevent Train-Train Collision, for exam-

ple, yields the security requirements of confidentiality, integrity, availability, authentication, accountability and identification. This process is repeated as required for each PTC functional requirement in Table 1. By analyzing additional postulated misuse cases, it is possible to obtain the aggregated security requirements for PTC Levels 1 through 4.

In the following, we describe a specific misuse case, Modify Track Warrant,in the format specified by Sindre and Opdahl [25]. In particular, we discuss how the misuse case leads to the generation of security requirements, and the establishment of a set of defining evidence traits needed for forensic analysis.

Misuse Case: Modify Track Warrant

Summary: Track warrant message is modified. This message conveys information that prevents train to train, train to on-track equipment, on-track equipment to on-track equipment, and train to roadway worker collisions.

Basic Path: The track warrant message is transmitted from the office/dispatch system to a mobile unit. The CRC is modified while the message is en route, rendering the message invalid. The mobile unit receives the invalid message. Acting on the invalid message, the mobile unit strikes another train, a track vehicle or roadway workers.

Alternate Paths: The track warrant message is relayed through the wayside subsystem and, during transmission, the CRC of the message is modified between the office/dispatch subsystem and the wayside subsystem, or the wayside subsystem and the mobile unit.

Capture Points: The track warrant message is invalid because one or more fields are modified: source, type, message payload and message identifier.

Triggers: Attacker places a transmitter within range of the subsystem's receiver and/or transmitter.

Attacker Profile: Attacker can capture the original message, read and interpret the message, modify one or more message fields, and retransmit the message.

Preconditions:

1. The office/dispatch subsystem is transmitting a track warrant message to a mobile unit.
2. The office/dispatch subsystem and the mobile unit subsystem are operating normally.

Post Conditions (Worst Case):

1. The mobile unit receives an invalid track warrant message, causing a train to train, train to on-track equipment, track to on-track equipment or train to roadway worker collision.
2. Unauthorized modifications of track warrant messages disable accountability and non-repudiation of specific operational restrictions and authorizations for potentially high hazard events such as commingling of roadway workers and trains.

3. An invalid track warrant message halts mobile units at the limits of its authority, producing a significant operational and safety impact.

Post Conditions (Best Case):

1. Message origin information is authenticated and data integrity is maintained.
2. Track warrant message modifications are identified and isolated.
3. Two entities do not commingle although they operate on altered track warrant messages.

Business Rules:

1. Only the office/dispatch subsystem originates valid track warrant messages.
2. The office/dispatch subsystem may push a valid track warrant message to a mobile or wayside subsystem.
3. The mobile subsystem may pull or request pulling a valid track warrant message from the wayside subsystem or the office/dispatch subsystem.
4. The wayside subsystem may pull a valid track warrant message from the office/dispatch subsystem only after the receipt of a request to pull a track warrant message from a mobile subsystem unit.

3. Railway Accident Investigation

Before discussing our methodology, we illustrate how collected evidence and pre-analyzed use-misuse cases can be used to determine probable cause in a documented railway accident investigation. We consider the June 2002 collision of Amtrak and MARC trains in Baltimore, Maryland [18].

We assume that pre-defined use-misuse cases associated with the operation of a locomotive by an engineer are already available. These use-misuse cases are created prior to an accident by analyzing the engineer's interactions with the locomotive, wayside systems and other systems, and identifying possible failure modes. Figure 3 presents a portion of the use-misuse case diagram for locomotive operation.

Forensic evidence gathered by investigators after an accident may include locomotive event recorder data, statements from the crew and other witnesses, recordings from the dispatch center, test data related to the operation of wayside devices (switches, signals, etc). The investigation of the Amtrak-MARC accident revealed that the engineer concentrated on monitoring speed to prevent flat spots, did not see the stop signal, and did not know how to apply the direct release air brakes.

Upon marking these facts in Figure 3 and tracing back to the root node for each misuse case, it is determined that the root causes of the accident were task fixation and lack of knowledge. Furthermore, failure to counter the misuse cases, task fixation and lack of knowledge,

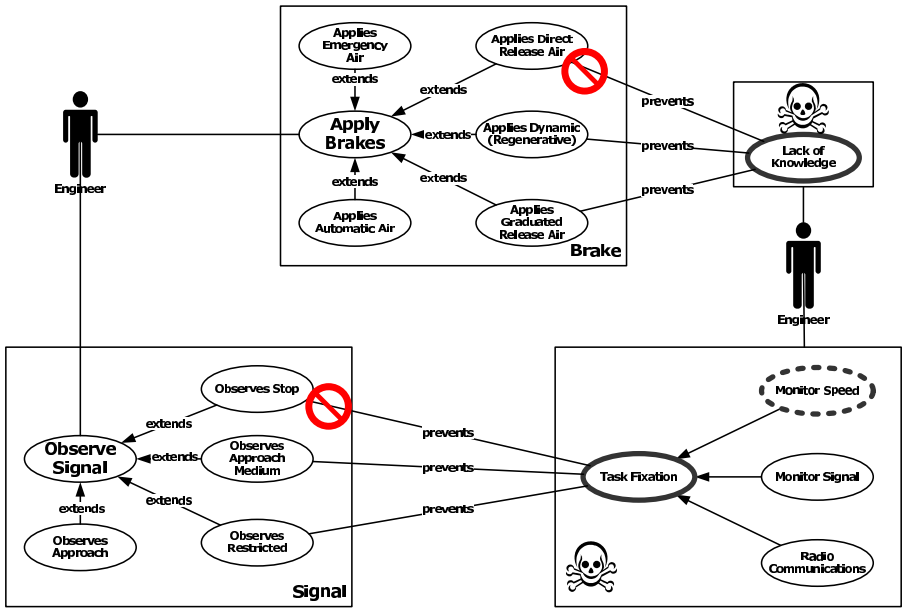

Figure 3. Amtrak-MARC use-misuse case diagram.

also contributed to the accident. These results closely match the NTSB probable cause findings of loss of situational awareness, lack of familiarity and proficiency, and absence of a PTC system [18].

4. Evidence Traits

Evidence traits provide detailed definitions of use cases and misuse cases. The notion of an evidence trait is a simple refinement of the concept presented in Section 3. However, unlike in Section 3, where the evidence gathered represents an entire use case or misuse case, the granularity of evidence is increased to include other attributes of use cases, such as pre conditions, post conditions and business rules. These evidence traits are captured from textually-specified use-misuse cases by analyzing nouns and verbs via a technique called "noun-verb extraction" [17]. Noun-verb extraction identifies specific characteristics of use cases and misuse cases that could represent evidence, i.e., behavior that is directly observed or conclusively inferred from observed behavior. The extraction process can be done manually by an engineer or by using specialized tools [20].

Table 2 presents the results of noun-verb extraction for the misuse case: Modify Track Warrant. The extractions identify the forensic ev-

Table 2. Evidence traits for PTC system.

Trait	Description
A	Text of message conveys authorization to occupy section of track
B	Message transmitted by office/dispatch system to mobile unit
C	CRC of message modified en-route, rendering message invalid
D	Mobile unit strikes another train, track vehicle or roadway workers
E	Message relayed to a wayside subsystem
F	Message invalid due to one or more modified fields: (i) source, (ii) type, (iii) payload, (iv) identifier
G	Attacker's transmitter placed within range of subsystem's receiver and/or transmitter
H	Attacker captures, reads, interprets, modifies and retransmits message
I	Office/dispatch subsystem transmits message to a mobile unit
J	Office/dispatch subsystem and mobile unit operates normally
K	Office/dispatch subsystem originates messages
L	Invalid message halts mobile units at limits of its current authority
M	Unauthorized modifications of messages disable accountability and non-repudiation of operational restrictions/authorizations for potentially high hazard events
N	Invalid message received causing train to train, train to track equipment, track to on-track equipment, train to roadway worker collisions

idence traits. Note that the physical locations of Evidence Traits A through N in Table 2 are identified in Figure 1.

5. Non-Probabilistic Forensic Analysis

Bogen and Dampier [1] and Pauli and Xu [21] have developed strategies for planning digital forensic examinations by systematically organizing, analyzing and identifying the most relevant concepts in a security incident, and determining the relations between these concepts. Our methodology, on the other hand, uses digital evidence to create an identifying signature. This signature is then matched with a set of previously identified misuse cases to identify a specific misuse case. Alternatively, the signature may be used to formulate a previously unidentified misuse case and generate the associated security requirements.

In non-probabilistic forensic analysis, the collected evidence represents a single identifying signature that has a one-to-one correspondence with a specific misuse case. This signature assists in mapping to a misuse case once evidence has been discovered. Also, it provides the forensic investigator with an initial set of traits and their locations, which facilitate the investigation.

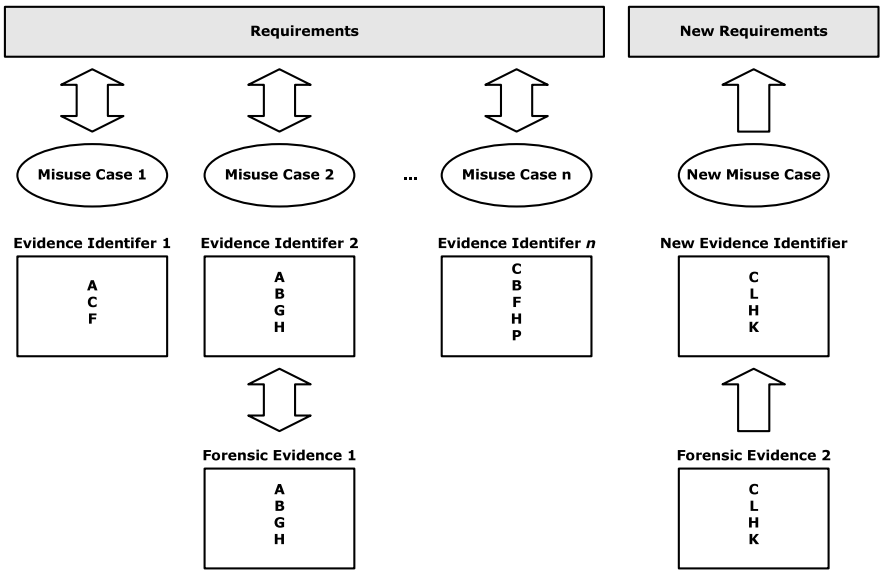

Figure 4. Non-probabilistic process.

The non-probabilistic process is outlined in Figure 4. The set of defined misuse cases (Misuse Case 1 to Misuse Case n) generates a corpus of known security requirements. Each misuse case is uniquely fingerprinted in terms of its own set of evidence traits (Evidence Identifier 1 to Evidence Identifier n). Forensic evidence obtained from an incident is compared to each fingerprint. In Figure 4, the collected evidence (Forensic Evidence 1) maps to the evidence trait Evidence Identifier 2. Evidence Identifier 2 uniquely identifies Misuse Case 2. This validates the requirements of Misuse Case 2 because the evidence is proof that Misuse Case 2 has occurred.

On the other hand, forensic evidence (Forensic Evidence 2) collected from another incident does not correspond to any existing evidence traits. Consequently, a new evidence trait set (New Forensic Identifier) is created for a new misuse case (New Misuse Case). The PTC system design may have to be adapted to account for the misuse case that yields the new set of evidence traits and identifies new security requirements. Note that the new misuse case and the associated requirements integrate into the corpus of known conditions.

6. Probabilistic Forensic Analysis

The evidence available to an investigator is often incomplete and may not match a misuse case fingerprint. A probabilistic match is required in such a situation. Bayesian Belief Networks (BBNs) [12, 14] offer a promising approach for probabilistically matching forensic evidence with evidence traits and associated misuse cases.

BBNs are directed acyclic graphs that capture probabilistic relationships between variables. Using a BBN to capture probabilistic relationships has several advantages. BBNs do not require exact or complete historical knowledge about the relationships between the variables. They may be created based on the available knowledge; however, as additional evidence is gathered, the relationships between variables may be adjusted to reflect the new evidence and compensate for missing information. Their easily understandable graphical structure simplifies their creation, modification and maintenance by domain experts, while providing opportunities for efficient computation. BBNs also support the determination of cause from effect just as easily as effect from cause; this enables them to be used to reason in a forward or backward manner with the available data.

Figure 5 shows an example BBN. An investigator is assumed to have discovered forensic evidence items A, C, F and G (represented by "true" conditions or complete (100%) certainty). On the other hand, the forensic evidence items B, H and L have not been discovered. The inability to obtain evidence does not imply it does not exist; consequently, it is assumed to exist with some probability. In the example, the evidentiary items B, H and L are assumed to be equally likely to be "true" or "false" (i.e., 50% probability).

Mathematical equations are set up that define the probability of each node of the BBN in terms of the probabilities of its parents. When the system of Bayesian equations associated with the nodes in Figure 5 is solved using a BBN tool (e.g., Netica), the probability of the evidence matching Misuse Case 1 is computed to be 89.6%. The high probability for Misuse Case 1 indicates a need to implement the requirements that arise from Misuse Case 1. However, it does raise the issue whether some or all of the requirements arising from Misuse Cases 2 and 3 should also be implemented. The answer is a technical as well as managerial decision, involving the level of risk and the economics of the situation, which are outside the scope of this paper.

Note that in the example in Figure 5, based on the forensic evidence collected, there is also a relatively high probability (56.3%), of dealing with another, as yet undefined, attribute list (which, in turn could refer

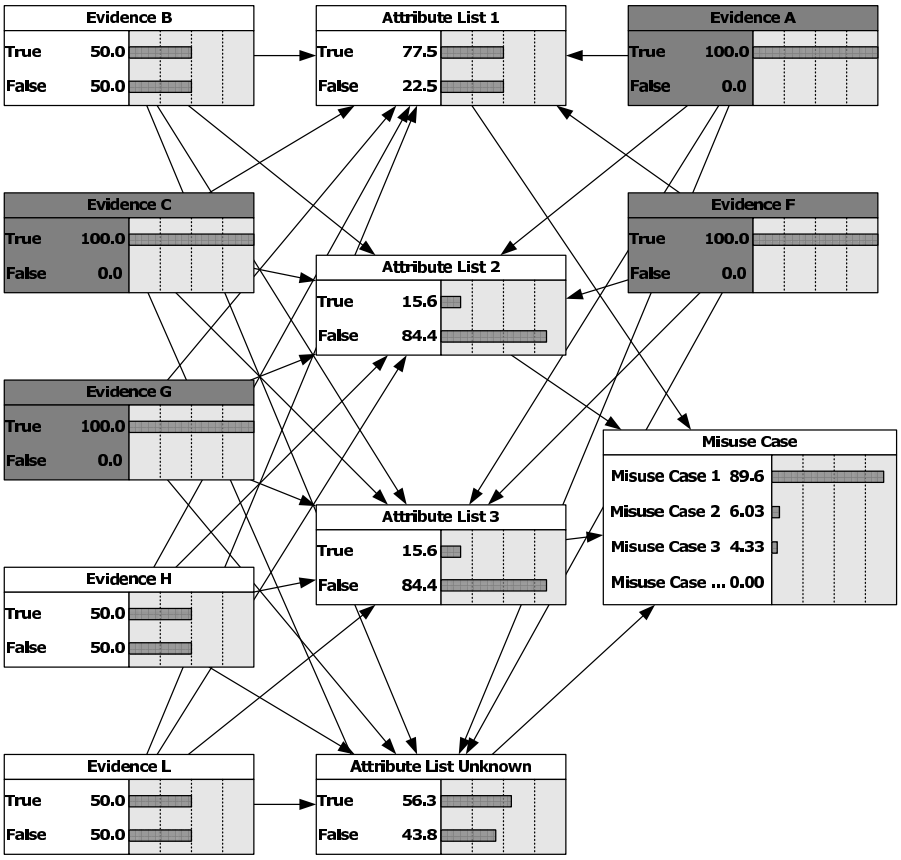

Figure 5. Probabilistic process using a Bayesian belief network.

to an unidentified misuse case and its associated security requirements). Additional forensic evidence is needed to confirm or deny the existence of undefined attribute list(s) and misuse cases.

7. Conclusions

Securing the railroad infrastructure is a high priority. Regulatory [6] and industry initiatives [11] related to the deployment of PTC systems have significantly increased railroad safety, but have also increased vulnerabilities [3]. A recent National Research Council (NRC) and National Security Telecommunications Advisory Committee (NSTAC) study [19] emphasizes that attacks on wireless networks can result in significant system degradation or disruption. PTC systems, because of their reliance on wireless networks, are prime targets for attack [13]. However,

previous work [2, 4, 5], while confirming the need to secure PTC systems and investigate security breaches, has not provided specific security requirements or developed decision processes for determining investigative scenarios [26].

Digital forensics has traditionally focused on electronic evidence gathered from computer systems and networks for use in legal proceedings. While considerable research has focused on using decision support systems to reason about evidence [7, 15, 22] and on generating crime scenarios from evidence using compositional reasoning [16], we believe that our use of use-misuse cases to determine the forensic evidence that should be collected for determining safety and security requirements is unique. The systematic analysis of forensic evidence from misuse cases proposed in this work will not only support accident investigations and contribute to the identification and prosecution of attackers, but will also increase the resilience of PTC systems to attack.

References

[1] A. Bogen and D. Dampier, Preparing for large scale investigations with case domain modeling, *Proceedings of the Digital Forensic Research Workshop*, 2005.

[2] A. Carlton, D. Frincke and M. Laude, Railway security issues: A survey of developing railway technology, *Proceedings of the International Conference on Computer, Communications and Control Technology*, pp. 1-6, 2003.

[3] 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.

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

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

[6] Department of Transportation, 49 CFR Parts 209, 234 and 236: Standards for the Development and Use of Processor Based Signal and Train Control Systems – Final Rule, Technical Report, Washington, DC, 2005.

[7] B. Falkenhainer and K. Forbus, Compositional modeling: Finding the right model for the job, *Artificial Intelligence*, vol. 51(1-3), pp. 95-143, 1991.

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

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

[10] Federal Railroad Administration, Benefits and Costs of Positive Train Control, Report in Response to the Request of Appropriations Committees, Department of Transportation, Washington, DC, August 2000.

[11] Federal Railroad Administration, Positive Train Control, Technical Report, Department of Transportation, Washington, DC (www.fra.dot.gov/us/content/1265), 2003.

[12] A. Gelman, J. Carlin, H. Stern and D. Rubin, *Bayesian Data Analysis*, Chapman and Hall/CRC, Boca Raton, Florida, 2003.

[13] General Accounting Office, Critical infrastructure protection challenges and efforts to secure control systems, GAO Testimony before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, House of Representatives, Washington, DC, March 2004.

[14] F. Jensen, *Bayesian Networks and Decision Graphs*, Springer, Heidelberg, Germany, 2001

[15] J. Keppens and Q. Shen, On compositional modeling, *Knowledge Engineering Review*, vol. 16(2), pp. 157-200, 2001.

[16] J. Keppens and J. Zeleznikow, A model based reasoning approach for generating plausible crime scenarios from evidence, *Proceedings of the Ninth International Conference on Artificial Intelligence and Law*, pp. 51-59, 2003.

[17] 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.

[18] National Transportation Safety Board, Collision of Amtrak Train No. 90 and MARC Train No. 436, Railroad Accident Brief DCA-02-FR-010, Washington, DC (www.ntsb.gov/publictn/2003/RAB0301.htm), May 12, 2003.

[19] Office of the President, The President's National Security Telecommunications Advisory Committee (NSTAC) Wireless Task Force Report, Washington, DC, January 2003.

[20] S. Overmyer, B. Lavoie and O. Rambow, Conceptual modeling through linguistic analysis using LIDA, *Proceedings of the Twenty-Third International Conference on Software Engineering*, pp. 401-410, 2001.

[21] J. Pauli and D. Xu, Threat-driven architectural design of secure information systems, *Proceedings of the Seventh International Conference on Enterprise Information Systems*, pp. 136-143, 2005.

[22] H. Prakken, Modeling reasoning about evidence in legal procedure, *Proceedings of the Eighth International Conference on Artificial Intelligence and Law*, pp. 119-128, 2001.

[23] J. Reason, *Human Error*, Cambridge University Press, Cambridge, United Kingdom, 1990.

[24] G. Sindre and A. Opdahl, Capturing security requirements through misuse cases, *Proceedings of the Ninth Norwegian Informatics Conference* (www.nik.no/2001/21-sindre.pdf), 2001.

[25] G. Sindre and A. Opdahl, Templates for misuse case description, *Proceedings of the Seventh International Workshop on Requirements Engineering: Foundations of Software Quality* (www.nik.no/2001 /21-sindre.pdf), 2001.

[26] G. Wimmel, J. Jurgens and G. Popp, Use case oriented development of security critical systems, *Information Security Bulletin*, vol. 2, pp. 55-60, 2003.