Chapter 20

PROTECTION AND RECOVERY OF RAILROAD EVENT RECORDER DATA

Mark Hartong, Rajni Goel and Duminda Wijesekera

Abstract Passenger and freight locomotives in the United States are required to carry event recorders for collecting data that can be used in post-accident investigations. There are, however, shared management, labor and government concerns about maintaining the integrity, confidentiality and non-repudiation properties of the collected data. This paper proposes a cryptographic technique based on secret sharing that protects event recorder data while supporting data recovery by authorized parties.

Keywords: Event data recorders, railroad accident investigations, secret shares

1. Introduction

Railroad accidents are relatively rare events in the United States. In 2006, the total incident rate was 16.25 per million train miles [13]. This rate is very low, but it still equates to more than 13,100 separate incidents. Train accidents (collisions or derailments) and highway grade crossing incidents accounted for 22.2% of the incidents; the remaining 55.6% involved trespassers on railroad property or railroad personnel performing their job-related activities.

Locomotive event data recorders are used by railroad companies, the Federal Railroad Administration (FRA) and the National Transportation Safety Board (NTSB) to determine the root cause of incidents. In fact, the lead locomotive of any train operating faster than 30 mph is required to be equipped with an event recorder [34]. But the regulations only require event data recorders to capture information about a limited number of parameters; they do not mandate the recording of onboard communications or the crash hardening of all recorders until 2009.

The lack of evidence pertaining to crew actions was highlighted in the aftermath of the February 1996 collision of MARC and AMTRAK trains in Silver Spring, Maryland. In particular, the NTSB/FRA investigation was hampered by the lack of voice records of the train crew in the moments leading up to the accident. Indeed, the NTSB subsequently recommended that voice communications of crew members be recorded for exclusive use in accident investigations [27].

Railroad management, labor organizations and the government have strong interests in using event data recorders to collect forensic data about railroad incidents and to maintain the integrity and confidentiality of the data. This paper discusses the current requirements for locomotive event recorders and proposes cryptographic mechanisms for protecting the recorded data from unauthorized release, tampering and misuse.

2. Railroad Event Recorder Requirements

The use of event data recorders to assist in accident investigations goes back almost 50 years. Aircraft flight data recorders capture critical flight parameters while cockpit voice recorders record all flight deck communications. Without information from these devices, the sequences of events that resulted in several major aviation incidents (e.g., the ValueJet Flight 592 crash in Miami, Florida on May 11, 1996) would have remained unknown.

The use of event data recorders in railroads is a more recent development. The Rail Safety Improvement Act of 1988 [35] provides statutory authority for the use of event recorders in the United States. Based on this statutory authority, Section 229.135 of Title 49 of the Code of Federal Regulations [34] defines the minimum requirements for locomotive event recorders. It differs from the original regulations by adding the requirement for a certified survivable version and phasing out magnetic tape recordings by 2010. The federal technical performance standards generally mirror the IEEE standard for event recorders [15]. The recovery of data from locomotive event recorders is governed by Association of American Railroads (AAR) standards [5]. These mandatory industry standards define manufacturer-independent physical and logical download interfaces, download methods and the serial protocol used to recover data from event recorders.

There are six original equipment manufacturers (OEMs) for locomotive event recorders in the United States (Table 1). While the data storage formats used by the manufacturers may differ, the primary method of data download is a serial DB-9 RS232 (19,200 bps) interface to a personal computer using the Xmodem 1K CRC file transfer protocol [9].

Table 1. Event recorder manufacturers.

Manufacturer	**URL**
Bach Simpson	www.bach-simpson.com
Electromotive Diesel	www.emdiesels.com
GE Transportation Systems	www.getransportation.com
Q-tron – A WABTEC Company	www.wabtec.com
Quantum Engineering	www.qei.biz
WABTEC Railway Electronics	www.wabtec.com

This simple file transfer protocol, which does not distinguish between text and binary files, uses a 16-bit cyclic redundancy check for error detection. Other approved downloading mechanisms include a PCMCIA interface using the ANSI AT Attachment (ATA) protocol and a serial download data port connected to a radio for wireless download using the Xmodem protocol.

3. Cryptographic Protection of Data

This paper proposes the use of cryptographic techniques to achieve data integrity, authentication and non-repudiation. Currently, all event recorder manufacturers utilize checksums to provide integrity protection against accidental and non-malicious errors, but not against malicious attacks. Also, checksums (on their own) do not provide for data non-repudiation and confidentiality. Event recorder data is not random and is interpreted within a particular context; consequently, the surreptitious modification of checksums is extremely difficult. Nevertheless, certain bit manipulations are possible [21].

Table 2 presents the minimum requirements for data collection by event recorders for the purposes of accident reconstruction, disciplinary actions or locomotive health monitoring. In all cases, it is critical that data integrity and confidentiality be maintained and that the data be attributed to particular entities without non-repudiation. Unfortunately, tampering with event recorder data has been observed. In a 1982 collision, the crew reported that the event recorder was working properly prior to the accident. However, several hours after the accident, a railroad official discovered that the case had been broken open and the tape was missing (the locomotive cab itself was not damaged) [26]. In another collision [25], certain attributes of the recorded data were found to have been modified. The union that represents railroad engineers has agreed, in principle, to the use of event recorders, but it is concerned about the

Table 2. Minimum data required to be collected by event recorders.

Train Speed
Direction of Motion
Time
Distance
Throttle Position
Application and Operation of Automatic Air Brakes by Engineer
Application and Operation of Automatic Air Brakes by On-Board Computer
Application and Operation of Independent Brakes
Application and Operation of Dynamic Brakes (if equipped)
Cab Signal Aspects (if equipped)
Loss of End of Train (EOT) Communications
Electronic Controlled Pneumatic (ECP) Braking Messages (if equipped)
EOT Armed Emergency Brake Command and Emergency Brake Application
Indication of EOT Valve Failure
EOT Brake Pipe Pressure
EOT Marker Light Status
EOT "Low Battery" Status
Status of Lead Locomotive Headlights
Status of Lead Locomotive Auxiliary Lights (Ditch Lights)
Horn Control Activation
Locomotive Number
Locomotive Position in the Consist
Tractive Effort (Pulling Capability)
Cruise Control Status
Safety Critical Train Control Information Routed to Engineer's Display

misuse, improper interpretation, public disclosure, tampering and use of the data beyond the purposes of accident investigation [8].

Most of these concerns can be addressed by having at least two entities actively participate in the recovery of event recorder data. Railroad management and labor, for example, could jointly obtain data to evaluate locomotive performance and determine maintenance requirements, an activity in which the government has no regulatory interest. Labor and government could retrieve locomotive operating parameters (e.g., speed and horn settings) to support or refute labor claims during a federal locomotive engineer review board hearing. Likewise, railroad management and government could obtain locomotive operating parameters to support or refute the validity of railroad violations identified by the government.

The secret sharing technique [7, 30] – also known as secret splitting or split knowledge – enables cryptographic keys to be distributed between the various stakeholders. In secret sharing, N secrets (e.g., pieces of the

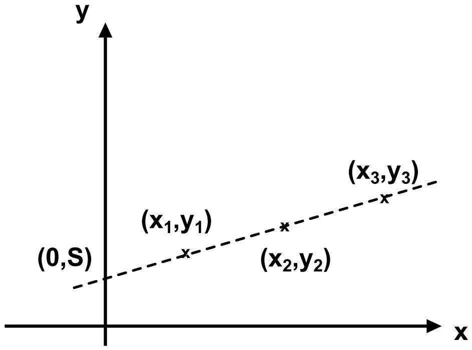

Figure 1. Secret shares.

key used to encrypt data) are shared among M entities where $M < N$ such that all M entities can collaborate to recover the original data, but no group with $M - 1$ or fewer entities can do so.

Multiple mathematical results are available to support the creation and reconstruction of secret shares [32]. In the case of event recorder data, any two of the three stakeholders (management, labor and government) should be able to recover the data by combining their secret shares. This situation is modeled using three distributed secrets (S_1, S_2, S_3). Each stakeholder is given two of the three secrets, (S_1, S_2), (S_1, S_3) or (S_2, S_3), and agreement by any two of the three stakeholders is sufficient to recover all three distributed secrets, enabling the key to be reconstituted and the data to be recovered.

4. Secret Sharing and the Primary Use Case

The critical use case in the forensic analysis of a railroad incident is the recovery of encrypted event recorder data. We use an implementation of Shamir's N of M secret sharing scheme to ensure that no single party can unilaterally recover the cryptographic key and modify or release the data. Three parties are involved, railroad management, railroad labor and government ($M = 3$). Any pair of the secret shares held by management, labor and government is sufficient to reconstruct the cryptographic key (i.e., $N = 2$).

The secret sharing technique is illustrated in Figure 1. First, the point (0, S) on the y-axis corresponding to the cryptographic key S is located. A line containing the point (0, S) is then drawn, and three points, (x_1, y_1), (x_2, y_2) and (x_3, y_3), on the line are selected. These three points represent the shares that are distributed to railroad management, labor and government.

Table 3. Recovery of event recorder data use case.

Number	Description
1	**Summary**: Railroad management, labor or government recovers cryptographically-protected data from a locomotive event recorder for forensic analysis of a locomotive accident (collision/derailment), locomotive health monitoring or crew disciplinary actions.
2	**Basic Path**: The event recorder captures forensic data. After a locomotive collision or derailment, government accident investigators combine their secret share with the secret share held by railroad management or labor to generate the cryptographic key. Cryptographically-protected data is downloaded from the event recorder. Using the cryptographic key, the government decrypts the downloaded data and verifies its authenticity and integrity; the data is then forensically analyzed.
3	**Alternate Paths**: (1) Health Analysis – The event recorder captures forensic data. Railroad management combines its secret share with the secret share held by railroad labor to generate the cryptographic key. Cryptographically-protected data is downloaded from the event recorder. Using the cryptographic key, railroad management decrypts the downloaded data and verifies its authenticity and integrity. Railroad management conducts locomotive health analysis using the decrypted data. (2) Engineer Discipline – The event recorder captures forensic data. Railroad management combines its secret share with the secret share held by the government to generate the cryptographic key. Cryptographically-protected data is downloaded from the event recorder. Using the cryptographic key, railroad management and government decrypt the downloaded data and verify its authenticity and integrity. Railroad management and government review the data to determine if engineer decertification is warranted.
4	**Capture Points**: The event recorder captures recorder attributes. Management, labor and government analyze the downloaded and decrypted forensic data.

At least two of the three shares must be known in order to recover the key S. Knowing two shares means that two points on the line are available, enabling the specification of the equation of the line. The cryptographic key S is then obtained by determining the intersection of the line with the y-axis. One share (or point) is insufficient to determine S. An infinite number of lines go through this point, corresponding to an infinite number of intersections with the y-axis (possible key values). The key is secure because, regardless of the computing power available, the key cannot be reconstructed without at least two shares (points).

The secret sharing technique enables the use case described in Tables 3 and 4. However, it does not protect against data corruption due to

Table 4. Recovery of event recorder data use case (continued).

Number	Description
5	**Triggers**: (1) Management and labor determine the need for forensic analysis of the event recorder data. (2) Management and government determine the need for forensic analysis of the event recorder data. (3) Labor and government determine the need for forensic analysis of the event recorder data.
6	**Attacker Profile**: Not applicable.
7	**Preconditions**: (1) Railroad management, labor and government each have a secret share. (2) Event recorder attributes have been successfully captured in the event recorder.
8	**Post Conditions (Worst Case)**: (1) Event recorder is damaged and data cannot be recovered. (2) Data confidentiality, integrity and non-repudiation are lost. (3) Event recorder is not damaged, but data has been manipulated to preclude data recovery.
9	**Post Conditions (Best Case)**: (1) Data is recovered from the event recorder. (2) Data confidentiality, integrity and non-repudiation are maintained.
10	**Business Rules**: (1) Management, labor and government place their secret shares in escrow. (2) Secret shares held in escrow must be released if ordered by a court. (3) In the case of an accident, data that is recovered may not be used in civil suits by the affected parties (management, labor, government or the public).

event recorder damage or the deliberate manipulation of data. Storing event recorder data in a crash-hardened memory module reduces the probability of data loss, but does not completely address data corruption and malicious data modification. Data loss can be mitigated using a fault tolerant storage mechanism such as Rabin's Information Dispersal Algorithm (IDA) [28]. This algorithm is conceptually similar to the secret sharing technique in that it breaks a file or block of data into M pieces and permits complete data recovery using any N pieces. This requires that event recorder designs implement multiple independent storage mechanisms, each of which holds one of the M pieces. Note, however, that IDA does not protect against malicious data modification.

Protection against unauthorized data alteration can be achieved by storing a hash value of each of the M pieces. The hash value of each piece is validated prior to using the piece to recover the complete file or block. If a hash value is determined to be invalid, it is assumed that the corresponding piece has been altered and that piece is not used to reconstruct the original file or block. Only subsets of the M pieces that have not been corrupted are used in reconstruction. The original

Algorithm 1 Data collection.

```
while event_recorder_is_enabled do
  for required_event_attributes do
    Read(required_event_attribute)
    Store(required_event_attribute)
  end for
end while
```

data can be reconstructed as long as the cardinality of the subset of uncorrupted pieces is no less than N.

5. Implementation Issues

This section discusses the principal implementation issues related to data collection and recovery. These include modifications to the event recorder as well as trust management and key escrow.

5.1 Data Collection

Event recorders capture continuous streams of data. Algorithm 1 specifies the steps involved in data collection.

Algorithm 2 Secure data collection.

```
Process_command_line_options
while event_recorder_is_enabled do
  for all required_event_attributes do
    Read(required_event_attribute)
    encrypted_required_event_attribute ←
       Encrypt(required_event_attribute, common_key)
    Store(encrypted_required_event_attribute)
  end for
end while
```

Algorithm 2 incorporates an additional encryption step to protect event recorder data. Encryption would be implemented using a cryptographic module that is resistant to reverse engineering. The device would have to be programmed after mass production so that the key and key escrow information are entered once and maintained without external electrical power. Data written to the EEPROM must be prevented from being erased, altered or cleared by service personnel or crash investigators. Detailed technical standards for cryptographic modules have been specified [23] along with compliant implementations [22]. Using such a cryptographic module with an appropriate trust management system can ensure that event recorder data is adequately protected.

A major technical issue arises because IDA operates on blocks of data. This precludes its use with analog data and also limits its application to digital data. Digital event recorders capture their information as continuous streams of closely-spaced "snapshots" in time. Therefore, the cryptographic module must encrypt each snapshot and write the encrypted information to the EEPROM before the next snapshot arrives. Consequently, the sampling rate of event recorder inputs is limited by the cycle time for encryption and storage. But reducing the sampling rate decreases the fidelity of the collected data. Specifying the required fidelity of event recorder data is, therefore, an important issue.

The worst-case scenario occurs when an event recorder captures crew conversations. The sampling rate must be high enough for the recorded conversations to be intelligible on replay. According to the Shannon-Nyquist theory [31], the sampling rate should be twice the frequency of the highest frequency that is sampled. A frequency range of 0-4 kHz is required for most phonemes, which corresponds to a sampling rate of 8 kHz or a cycle time of 125 microseconds. Assuming that 8-bit pulse coded modulation (PCM) is used, the required system throughput is 64 kbps. FPGA-based encryption engines can support throughputs that are two magnitudes higher [11]. Therefore, an FPGA coupled with EEPROM technology with fast write times [36] would satisfy the 125 microsecond cycle time requirement.

5.2 Data Recovery

Several standards have been established for trust management in operational environments [2–4, 16–20]. While a detailed discussion of trust management is beyond the scope of this paper, an examination of the use cases for normal and abnormal data recovery provides valuable insights into the requirements of a trust management system.

Algorithm 3 presents the steps involved in normal event recorder data recovery for the purposes of monitoring locomotive health and engineer discipline. The data recovery process uses a non-secure network connection or a direct connection to the event recorder. A non-secure connection can be used because the AAR data transfer protocol, which is data-format neutral, allows data to be transferred in encrypted form. Likewise, when a direct connection is employed, data can be recovered in an encrypted format and is decrypted only in a secure environment during an investigation.

In the case of data recovery for the purpose of evaluating locomotive health, the *recovered_common_key* in Algorithm 3 is reconstructed from the key shares held by railroad management and labor. The recovered

Algorithm 3 Normal data recovery.

```
if locomotive_healh_recovery then
    recovered_common_key ←
        Recover_key(railroad_management_share, railroad_labor_share)
    for all encrypted_required_event_attributes do
        Read(encrypted_required_event_attribute)
        required_event_attribute ←
            Decrypt(encrypted_required_event_attribute, shared_key)
    end for
else if engineer_discipline then
    recovered_common_key ←
        Recover_key(railroad_management_share, government_share)
    for all encrypted_required_event_attributes do
        Read(encrypted_required_event_attribute)
        required_event_attribute ←
            Decrypt(encrypted_required_event_attribute, recovered_key)
    end for
end if
```

data enables management to proactively determine degradations in locomotive behavior that may have an adverse impact on the capability of a crew to operate a train safely, which would, of course, be of great interest to labor. However, in the unlikely event that labor refuses to participate and provide its key shares (e.g., during a strike), data recovery could still proceed by management obtaining key shares from the government.

In scenarios involving engineer discipline, the *recovered_common_key* is reconstructed using the key shares held by labor and government or by management and government. The government serves as the neutral party in these scenarios, which involve the certification, recertification or decertification of locomotive engineers [33]. Both management and labor have a vested interest in these proceedings and would, therefore, provide their key shares to government upon request.

The steps involved in accident data recovery (Algorithm 4) are similar to those performed during normal data recovery. However, there are two primary differences. First, data recovery is conducted in a controlled environment (i.e., the event recorder is moved from the accident site to a laboratory). Second, because the determination of the cause of an accident is in the interest of all three stakeholders, there would be few objections to providing key shares. Damage to the event recorder may complicate the task of data recovery. Possible solutions are to implement data distribution schemes or to perform off-board recording of data [14].

Management and labor could collude to prevent the recovery of accident data, but this is unlikely because of the mutual distrust that exists

Algorithm 4 Accident data recovery.

```
if key shares held by government and labor then
  $recovered\_common\_key \leftarrow \mathsf{Recover\_key}(railroad\_labor\_share,$
      $government\_share)$
else if key shares held by government and management then
  $recovered\_common\_key \leftarrow \mathsf{Recover\_key}(railroad\_management\_share,$
      $government\_share)$
  for all $encrypted\_required\_event\_attributes$ do
    $\mathsf{Read}(encrypted\_required\_event\_attribute)$
    $required\_event\_attribute \leftarrow \mathsf{Decrypt}(encrypted\_required\_event\_attribute,$
        $recovered\_common\_key)$
  end for
end if
```

between labor and management. Collusion could be mitigated by having a trusted third party hold all the key shares and release them to an authorized entity only upon receiving a court order. However, this escrow approach has several problems that would have to be resolved [1].

6. Conclusions

Evidence recovered from locomotive event data recorders is extremely important in accident investigations. Secret sharing provides an elegant cryptographic mechanism for preserving the integrity, confidentiality and non-repudiability of accident data. Indeed, it is expected that cryptography will be broadly adopted in devices that store potentially valuable data [10, 24, 29]. However, secret sharing introduces additional costs. These include adapting event data recorders to support encryption, securing the secret shares and operating the required infrastructure. Nevertheless, secret sharing is an attractive solution to the problem of securing critical shared data [6, 12].

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] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller and B. Schneier, The risks of key recovery, key escrow and trusted third-party encryption, *World Wide Web Journal*, vol. 2(3), pp. 241–257, 1997.

[2] American National Standards Institute, Financial Institution Multiple Center Key Management, ANSI Standard X9.28:1991, Washington, DC, 1991.

[3] American National Standards Institute, Financial Institution Key Management (Wholesale), ANSI Standard X9.17:1995, Washington, DC, 1995.

[4] American National Standards Institute, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, ANSI Standard X9.63:2001, Washington, DC, 2001.

[5] Association of American Railroads, Locomotive Event Recorder Download Standard, AAR Standard S-5512, Section M, *AAR Manual of Standards and Practices*, Washington, DC, 2004.

[6] M. Azer, S. El-Kassas and M. El-Soudani, Threshold cryptography and authentication in ad hoc networks: Survey and challenges, *Proceedings of the Second International Conference on Systems and Network Communications*, p. 5, 2007.

[7] G. Blakely, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317, 1979.

[8] Brotherhood of Locomotive Engineers, Locomotive event recorders seeking a balance of safety and privacy in the real world of railroad operations, presented at the *NTSB/SAE Vehicle Recorder Topical Technical Symposium*, 2003.

[9] J Campbell, *C Programmer's Guide to Serial Communications*, Sams, Indianapolis, Indiana, 1993.

[10] E Casey, Practical approaches to recovering encrypted digital evidence, *International Journal of Digital Evidence*, vol. 1(3), 2002.

[11] A. Dandalis, V. Prasanna and J. Rolim, A comparative study of performance of AES final candidiates using FPGAs, *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 125–140, 2000.

[12] Y. Desmedt, Some recent research aspects of threshold cryptography, *Proceedings of the First International Workshop on Information Security*, pp. 158–173, 1997.

[13] Federal Railroad Agency, Accident/Incident Overview, 2006, Office of Safety Analysis, U.S. Department of Transportation, Washington, DC (safetydata.fra.dot.gov/OfficeofSafety), 2007.

[14] M. Hartong, R. Goel and D. Wijesekera, A framework for investigating railroad accidents, in *Advances in Digital Forensics III*, P. Craiger and S. Shenoi (Eds.), Boston, Massachusetts, pp. 255–265, 2007.

[15] Institute of Electrical and Electronics Engineers, IEEE Standard for Rail Transit Vehicle Event Recorders, IEEE Standard 1482.1-1999, Piscataway, New Jersey, 1999.

[16] International Organization for Standardization, Banking – Key Management (Retail) – Parts 1, 2 and 5, ISO Standards 11568-1:2005, 11568-2:2005, 11568-1:2007, Geneva, Switzerland, 2005–2007.

[17] International Organization for Standardization, Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks, ISO Standard ISO/IEC 9594-8:2005, Geneva, Switzerland, 2005.

[18] International Organization for Standardization, Health Informatics – Public Key Infrastructure – Parts 1, 2 and 3, ISO Standards ISO/TS 17090-1:2008, 17090-2:2008, 17090-3:2008, Geneva, Switzerland, 2008.

[19] Internet Engineering Task Force, RFC 1422: Privacy Enhancement for Internet Electronic Mail Part II: Certificate-Based Key Management, 1993.

[20] Internet Engineering Task Force, RFC 1424: Privacy Enhancement for Internet Electronic Mail Part IV: Key Certificate and Related Services (Standard), 1993.

[21] A. Menezes, P. van Oorschot and S. Vanstone *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 2001.

[22] National Institute of Standards and Technology, Module Validation Lists, Gaithersburg, Maryland (csrc.nist.gov/groups/STM/cmvp /validation.html).

[23] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, FIPS PUB 140-1, Gaithersburg, Maryland, 2001.

[24] National Research Council, *Cryptography's Role in Securing the Information Society*, National Academy Press, Washington, DC, 1996.

[25] National Transportation Safety Board, Railroad Accident Report – Side Collision of Two Missouri Pacific Railroad Company Freight Trains at Glasie Junction near Possum Grape, Arkansas, October 3, 1982, NTSB-RAR-83-06, U.S. Department of Transportation, Washington, DC, 1983.

[26] National Transportation Safety Board, Railroad Accident Report – Head-on Collision of National Railroad Passenger Corporation (Amtrak) Passenger Trains Nos. 151 and 168, Astoria, Queens, New York, July 23, 1984, NTSB-RAR-85-09, U.S. Department of Transportation, Washington, DC, 1985.

[27] National Transportation Safety Board, Railroad Accident Report – Collision and Derailment of Maryland Rail Commuter MARC Train 286 and National Railroad Passenger Corporation Amtrak Train 29 Near Silver Spring, Maryland on February 16, 1996, NTSB-RAR-97-02, U.S. Department of Transportation, Washington, DC, 1997.

[28] M. Rabin, Efficient dispersal of information for security, load balancing and fault tolerance, *Journal of the ACM*, vol. 36(2), pp. 335–348, 1989.

[29] Scientific Working Group on Digital Evidence, Proposed standards for the exchange of digital evidence, *Forensic Science Communications*, vol. 2(2), 2000.

[30] A. Shamir, How to share a secret, *Communications of the ACM*, vol. 22(11), pp. 612–613, 1979.

[31] C. Shannon, A mathematical theory of communication, *Bell System Technical Journal*, vol. 27, pp. 379–423 and pp. 623–656, 1948.

[32] D. Stinson and R. Wei, Bibliography on Secret Sharing Schemes, Research Report CORR 98-50, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Canada, 1998.

[33] U.S. Government, Qualification and Certification of Locomotive Engineers, *Title 49, Code of Federal Regulations*, Part 240, Washington, DC, pp. 743–791, 2006.

[34] U.S. Government, Railroad Locomotive Safety Standards, *Title 49, Code of Federal Regulations*, Part 229, Washington, DC, pp. 229–385, 2006.

[35] U.S. Government, Rail Safety Improvement Act of 1988, *Title 49, Code of Federal Regulations*, Part 1.49(m), Washington, DC, pp. 25–26, 2007.

[36] J. Wilson, Solid-state memory takes over niche military and aerospace applications, *Military and Aerospace Electronics*, vol. 12(12), 2001.