Cyber Security Risk Management of Connected Railroads: A Literature Review, Industry Survey and Case Study

Zezhou Wang

Graduate Research Assistant, Rutgers University, the State University of New Jersey
Presentation Outline

• Research Motivation
• Cyber Risk Identification for Connected Railroads
• Industry Survey & Lessons Learned
• PTC Case Study – Preliminary Cyber Risk Identification
• Knowledge Gaps and Ongoing Research
Research Motivation

- A number of communications-based technologies are already or to be implemented in the railroad industry, such as:
  - Centralized Traffic Control (signaling) systems and PTC systems
  - remote controlled locomotives
  - remote traffic interoperability and configuration management among yards
  - power distribution and energy management
  - ridership and farebox management systems
  - others

- It is important to understand potential cyber security risks of the communication systems (focus of this research) to better serve the existing or upcoming intelligent network of connected railroad
Connected Railroad Systems:

Example: Positive Train Control System

Communications Infrastructure:
- Radio/cellular towers
- GPS antennas
- Fiber (or copper) backbone

Back Office:
- Back Office Servers
- Dispatch center

Connected Railroad Systems:
Example: Remote Control Locomotives

Research Goal and Current Framework

In the process of this project, we have provided a literature review over:

- The technologies, methodologies, and applications related to cyber security risk management in rail industry
- Conclusions of past rail cyber risk analysis and directions for future research

We also developed an industrial survey to understand:

- Company practices on cyber technologies and their security assurance
- Prevailing industry interests and cyber-related knowledge gaps

Our ultimate research goal:

- Fully understand connected railroad technologies and identify potential cyber attacks
- Assess level of impacts due to cyber attack and evaluate vulnerabilities
- Recommend effective strategies for risk mitigation & resiliency improvement
Literature Review and Case Study
### Identified Rail Cyber Attack Scenarios (Snapshot)

<table>
<thead>
<tr>
<th>Railway Systems</th>
<th>Potential Attack Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Various) Signaling &amp; train control systems</td>
<td>(General) Multiple attacks including electromagnetic interference, DoS jamming, etc.</td>
</tr>
<tr>
<td>e.g. PTC in the U.S.; ERTMS in Europe; CTCS in China</td>
<td>(Specific) Passive eavesdropping, brute force attacks, unauthorized access to the network, message modification, replay attack, etc.</td>
</tr>
<tr>
<td>Balise/transponder data systems (if available)</td>
<td>(General) Compromise the availability or integrity of the Balises/Transponders’ data,</td>
</tr>
<tr>
<td></td>
<td>(Specific) Jamming, electromagnetic interference, rewriting false data</td>
</tr>
<tr>
<td>Public address (PA) Systems for Passenger Services</td>
<td>Unauthorized intrusions</td>
</tr>
<tr>
<td>Traction power control systems (if available, e.g. SCADA System)</td>
<td>False data injection attacks, message modification, and unauthorized access to the network</td>
</tr>
</tbody>
</table>
General Cyber Security Risk Reduction Strategies

Technology-driven strategies
• Intrusion detection systems (IDS)
• Prevention mechanisms (e.g. authentication, authorization, access control, encryption, firewall and others)
• Impact mitigations and resiliency

Policy-driven strategies
• Training (e.g. improved cyber risk awareness)
• Configuration management (e.g. software patching and updating)
• System maintenance
• Other case-based strategies based on user needs
Case Study Example of PTC Cyber Attack: Risk Sources

Communications between back office and:
- Signaling points
- Wayside radios

Cyber security associated with devices:
- Switches
- Radio systems
- Wayside Interface Units (WIU)s

Example Types of attack:
- Forgery, Replay, DoS
- Bandwidth exhaustion attacks, jamming;
- Malware insertion into devices

Cyber risk details are driven by vendor specs, and won’t be released to public

Cyber Rail Industrial Survey
Industrial Survey

As part of this project, we are seeking input from industry experts to understand existing and emerging connected railroad technologies and cybersecurity issues.

Cyber Security Risk Management for Connected Railroads (DTFR5317C00018)

3. What safety related systems do you have that use internet connections to pass data?

4. How do your dispatching systems communicate with wayside interlockings and control points?

https://docs.google.com/forms/d/10yU6yTd-D5j6yiPSmZzaDReWmyi9Yb6C-s KP k4yS0NA/edit
Survey Questions (Snapshot)

1. Your name and your company?
2. What is your contact information, email and/or phone number?
3. What safety related systems do you have that use internet connections to pass data?
4. How do your dispatching systems communicate with wayside interlockings and control points?
   4 (a). Is the communication path of your dispatching system through a dedicated closed network controlled by the railroad?
   4 (b). Does your railroad dispatching system use leased lines for this purpose?
   4 (c). Does your railroad dispatching system use a closed network? If yes, is there a way for an employee or contractor to access the system externally?
5. Does your railroad use a Supervisory Control and Data Acquisition (SCADA) system for traction control (electrified railroad) or for some other purpose?
   5 (a). If so, how does your SCADA system communicate with devices in the field? Is the communication path through a dedicated closed network controlled by the railroad?
   5 (b). Does your railroad SCADA system use leased lines for this purpose?
   5 (c). Does your SCADA system use a closed network? If yes, is there a way for an employee or contractor to access the system externally?
6. Does your railroad use remote control of locomotives in train consists or in yards?
   6 (a). If so, what security measures are in place to prevent someone else from taking control?
7. Does your railroad use radio code lines for control of switches and signals?
   7 (a). If yes, what security measures has your railroad taken to prevent unauthorized control of these devices?
Preliminary Survey Results

- PTC is the most-mentioned topic
- Some companies use leased lines from Internet Service Providers (ISPs) for data transmission, and some others use local network either via radio code lines or direct internal fibers
- For most of the respondents, the communication networks in dispatching system and SCADA (supervisory control and data acquisition) systems are dedicated closed networks.
- Commonly used cyber security measures include intrusion detection/prevention systems, firewalls, host intrusion prevention systems, authentication, firewall, anti-virus/malware tool and secure file transfer protocol, log collection, encryption, dedicated equipment etc.
Preliminary Survey Results (Cont.)

• Advanced Train Control System (ATCS), bridge remote control, and remote yard operations, sensor security are other connected railroad technologies that were mentioned of interest.

• Some other IT components/systems are also of interests, such as:
  • smart-link payment card system, ticket vending machines
  • access control and video security systems
  • building management systems, tunnel ventilation system
  • business systems
  • new Train Management Dispatch System (TMDS) at Application/Software level
  • very/ultra high frequency radio
Lessons Learned

- A lack of a unified framework to assess both likelihoods and consequences of specific cyber-attacks to railroads
- Limited prior work on evaluating the effectiveness of current/potential security mechanisms, and their respective costs and benefits
- Limited prior research regarding emerging wireless techniques (e.g. dynamic modulation and scaling, frequency hopping)
- Fail-safe design of vital systems is able to ensure safety to a base-line level
- Few studies considered the relationship between cyber security and railroad operational safety and level of operation impacts
- Several railroads are interested in generalized practices that can be customized for individual operational needs of each company
Ongoing Research

• Develop a unified rail cyber security risk framework (threats, vulnerabilities, consequences, prevention, mitigation and resiliency)
• Identification of several use cases (e.g. traction power control system, radio-controlled bridge, CTC Radio Code Line) in connected railroads,
• Developing customized risk assessment method for specific use cases
• Rail security risk management resource guide & recommended practices
Acknowledgement and Disclaimer

- Special Thanks to Federal Railroad Administration for sponsoring the project
  - Mr. Francesco Bedini Jacobini
  - Mr. Jared Withers

- Disclaimer:
  - The views and opinions expressed herein at that of the authors and do not necessarily state or reflect the Department of Transportation or the Federal Railroad Administration, and shall not be used for advertising or product endorsement purposes.
Thank You!

Contacts:

Xiang Liu, Ph.D.  (Principal Investigator)
xiang.liu@rutgers.edu;  (848)-445-2868

Zezhou Wang  (Graduate Research Assistant)
zezhou.wang@rutgers.edu;  (217)-721-2889

Please Contact Us if You Are Interested to Join the Industry Consortium for this Research