Transportation Systems Resilience
Preparation, Recovery, and Adaptation

Prepared by

Transportation Systems Resilience Section
Standing Committee on the Logistics of Disaster Response and Business Continuity
Standing Committee on Emergency Evacuations
Standing Committee on Critical Transportation Infrastructure Protection

Transportation Research Board

November 2017

Transportation Research Board
500 Fifth Street, NW
Washington, D.C.
www.TRB.org
Benefits and Needs for an Integrated Approach to Cyber–Physical Security for Transportation

RAE ZIMMERMAN
New York University Wagner Graduate School of Public Service

MICHAEL G. DINNING
U.S. Department of Transportation Volpe Center

Physical and cyber security mechanisms protect people and infrastructure assets for transportation from hazards, both natural and human-initiated. Both physical and cyber security mechanisms are diverse in size, function, deployment, and cost, and have proliferated. Since they are often colocated and functionally interdependent they need to be compatible. These physical and cyber mechanisms accomplish multiple security functions and reinforce one another for cost savings and conflict avoidance. First, connections between cyber and physical systems are presented in the context of interdependencies and resilience. Second, patterns and trends in cyber-attacks on transportation set the stage for typologies for both physical and cyber systems with illustrative cases. Third, social and economic effects and organizational arrangements are introduced to begin shaping solutions. Finally, conclusions are drawn as lessons learned.

Characteristics of Cyber–Physical System Combinations

Interdependency and Resilience Principles Applicable to Cyber–Physical Systems

Interconnections and interdependencies among infrastructure sectors are well-recognized. Rinaldi, Peerenboom and Kelly (1) identified these concepts, and detailed typologies were identified by Petit et al. (2). Furthermore, resilience has become linked with infrastructure interdependencies (3). Resilience, traditionally defined as returning to a previous state, subsequently has signified withstanding adverse changes, and moving to a stronger state (adaptation) (4). Furthermore, the concept is multidisciplinary (4, 5). Qualifications have been made, for example, the element of withstanding adverse changes has been interpreted as robustness (6), however, robustness has been considered an element of resilience (7). Resilience has been adapted with metrics for cyber systems (6), and integrates risk assessment and risk management (8).

Colocation and Cofunctionality of Cyber and Physical Security

Physical and cyber systems in transportation have become increasingly colocated and functionally dependent on one another. The U.S. Department of Transportation (DOT) (9) reported increases in information technology (IT) deployment in physical transportation support systems for 72 metropolitan areas.

IT and control systems and physical transportation components connect in many ways. Signals and switches that control transit train routing and track alignment involve control system connections (10). Computer-controlled highway systems include traffic lights, signage,
automatic toll collection, and infrastructure such as pumping apparatus at gasoline stations. Road vehicles themselves are becoming increasingly connected to computers and electronic control systems, and braking systems and air bags are among those that, if disabled, could compromise safety (11–14). Automated vehicles could increase this risk if security is not considered in designs. While functional dependencies of physical and cyber systems in the transportation sector are beneficial, they may create vulnerabilities, since disabling a cyber system can disable the physical transportation system it is supporting and vice versa.

CYBER AND CYBER–PHYSICAL ATTACKS ON TRANSPORTATION SYSTEMS

Patterns and Trends in Selected Cyberattacks on Transportation Systems

Cyber-attacks directly against transportation control systems are small in number relative to other industry sectors, however in 2014 and 2015, according to Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT), they escalated, and from 2012 to 2015 the number more than quadrupled (15–18). These only represent the ones reported to ICS-CERT, and other sectors with higher attack incidents—e.g., energy—indirectly affects transportation. Also, cyber-attacks can disrupt traditional IT systems, like tolling management and airline reservation systems.

Need for Designing Cybersecurity into Physical Security Systems

Physical security systems—such as access control, intrusion detection, and video systems—are becoming increasingly reliant on networked digital technologies. Many are connected as part of the Internet of Things (IoT). Unlike older stand-alone security systems, these are potentially vulnerable to cyber-attacks, putting physical security systems at risk.

Many physical security system managers lack knowledge and skills in cybersecurity, and many (incorrectly) feel that their networks are separate and not at risk. Physical security systems are treated as industrial control systems in most organizations, not under the purview of IT professionals. Some physical security vendors have not included adequate cyber protections in their technologies (19).

Adversaries can use cyber-attacks to disrupt physical security systems in many ways. As illustrated by Krebs (20), cyber-attacks can block alarms from intrusion-detection systems, compromise access-control systems, and spoof video and inspection system images. As elements of the IoT, physical security systems can also be used as vectors for large-scale cyber-attacks. In 2016, IoT devices—such as video cameras and digital video recorders—were exploited by hackers to create a distributed denial-of-service attack which caused widespread disruption to Internet infrastructure services (20).

Physical security system technologies and designs must include cybersecurity protections similar to those used in other IT systems, and be monitored for intrusions as other IT networks are. Organizations need to treat physical security technologies as part of their IT networks, and ensure that cybersecurity is part of system design, management, and operations.
Examples of Attacks

Transportation systems face several types of physical and cyber-attacks, including attacks by terrorists, criminals, politically motivated groups, and disgruntled employees. Cyber- and physical attacks may be directed separately or combined as hybrid attacks.

Types of Intrusions on One System Followed by an Effect on the Other

1. Chicago Air Traffic Control Center Fire (21–23). On September 26, 2014, Federal Aviation Administration’s (FAA) Air Route Traffic Control facility outside of Chicago was closed by a massive fire, shutting down over 91,000 mi² of airspace and disrupting thousands of flights. The fire, set by a disgruntled contractor, provides insight into the challenges to making systems resilient to both physical and cyber-attacks. The facility was protected by physical security systems, including electronic access-control systems and video surveillance, but the trusted attacker had access privileges. The air traffic control system and the FAA employees adapted quickly and minimized the disruption by using air traffic control centers in other locations.

   The Chicago attack illustrates the importance of coordinated programs for physical, cyber, and personnel security. It also highlights the need for system redundancy and preparation to ensure the adaptability of processes and personnel.

2. Polish Tram Hacking Attack. American Public Transportation Association (APTA) (24) identified the hacking of track switching points on a Polish tram in 2007 resulting in several derailments. This exemplified a cyber-attack disabling an unprotected physical transportation component.

3. San Francisco Municipal Transportation Authority (SFMTA) Ransomware Attack. Ransomware attacks computer systems and data, but critical cyber–physical systems can also be impacted.

   The SFMTA ransomware attack occurred on November 25, 2016 (25), encrypting SFMTA’s information systems. To prevent malware from affecting their fare gates and ticket vending machines, SFMTA disconnected these systems from the network.

   This was an example of a cyber-attack affecting the physical operations of a transit system and creating disruption for users. The impact on physical control systems was minimized because SFMTA used a segmentation approach to separate operational control and communications systems from other IT systems. SFMTA had backed up its data, and received assistance quickly from the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation, and their IT vendors. The attack shows the importance of integrating IT and control system response plans into an organization’s overall incident response plans and keeping system documentation and response plans up to date (26).

Cyber and Physical Hybrid Attacks

Another type of attack is a joint or hybrid attack where both cyber and physical system attacks are coordinated over time.

1. Port of Antwerp Cyber–Physical Attack (27). From 2011 to 2013, drug smugglers reportedly hacked into the terminal management system that controlled container movements at
the Port of Antwerp (28). Smugglers used cyber-attacks to obtain security details for containers with illegal drugs hidden in legitimate cargo. They also physically broke into the terminal offices and installed monitors on computers to gain access to data on containers, which they then took control of. The drug smugglers’ attack on the Port of Antwerp illustrates the need for a comprehensive cyber–physical systems approach to security (28).

2. The Bay Area Rapid Transit (BART) Hacking and Physical Protests (late summer and early fall 2011). According to accounts by Barnard (29), Elinson (30), Geng (31), and Zimmerman’s summary (14), the attacks on the BART system involved both physical protests intended to disrupt rail transit service and cyber-attacks that reinforced one another. The attacks were conducted by different groups, but occurred in the same approximate time period, which exacerbated the impact (30, 31). This was a joint attack on the basis of timing, and it highlights the need to be prepared for simultaneous physical and cyber-attacks.

SOCIAL AND ECONOMIC IMPLICATIONS OF THE BREACHES

Social and economic effects of cyber and physical security breaches can be widespread given cascading effects of these attacks. They have economic impact on industry and workers, disrupt supply chains, and impact social services. Cyber–physical security breaches impact recovery time, which is a key resilience factor.

If both physical and cyber assets are damaged the response to attacks may be compromised. Organizations may not have access to key information or other resources for effective response and recovery. In addition, the public may be unable to get information on the extent of the disruption, how they should respond, or what alternative services are available. Both cyber and physical attacks can adversely impact public confidence in the safety, security, and reliability of the system.

Many public and private-sector initiatives are focused on improving transportation resilience. The National Infrastructure Protection Plan (32) and its transportation sector-specific plan (33), and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (34) provide guidance and standards. In addition, there are many professional organizations which are developing guidance and specifications on security and resilience for the various modes of transportation.

SOLUTIONS AND LESSONS LEARNED: NECESSITY FOR ACTION

Transportation system designs and operational procedure must be able to adapt to cyber and physical disruptions. Cyber, physical, and personnel security must all be addressed in a coordinated approach.

Challenges to Designing the Two Systems to Be Compatible and Resilient

Cyber and physical systems, and their respective security systems, are often managed independently, and traditional design configuration and asset management are often inadequate to address the two simultaneously. Based on the case studies in this paper four important challenges are:
Redundancy and back-up systems are needed to mitigate impacts of disruptions. They should be part of continuity of operations plans, and require training, management, and close oversight.

Cyber and physical systems, and their respective security system products, are specified and purchased independently from different sources. A systems approach to acquisitions should include security and resilience in system specifications. Where possible product designs should address both cyber and physical security.

Many organizations lack enterprisewide resiliency plans addressing all risks simultaneously. All hazards resiliency plans can reduce the impact of interrelated risks and cascading impacts.

Personnel must understand both cyber and physical risks and mitigation strategies. Some organizations are facing this challenge with workforce training programs, for example by NIST, DHS, ICS-CERT, and the Transportation Research Board Critical Transportation Infrastructure Protection Committee.

REFERENCES


