ITS AMERICA

ISSUE BRIEF: CYBERSECURITY

Is Cybersecurity a Core Safety Issue for Transportation?

This cybersecurity issue brief from the Intelligent Transportation Society of America (ITS America) explores the evolving nature of our transportation system's cybersecurity needs and what challenges practitioners face in the field. By diving into the threats our systems face today, we look to spread awareness of cybersecurity best practices for connected transportation infrastructure projects and encourage continued collaboration among private sector technology developers, public sector technology deployers, and Federal security practitioners.

July 2024

www.itsa.org

1100 New Jersey Ave SE Ste. 850 Washington,
DC 20003

Issue Brief: Is Cybersecurity a Core Safety Issue for Transportation?

From traffic operations centers and Advanced Traffic Management Systems (ATMS) to field signal cabinets and traffic control devices, transportation systems classically combine digital and automated components to manage physical processes – namely, the movement of people and goods across our transportation system. Public and private sector stakeholders have increased the deployment of digital transportation solutions to achieve a variety of beneficial outcomes, foremost among those being improving transportation safety for all road users.

As these digital components become increasingly prevalent in our transportation infrastructure, more can be done to secure these systems from increasingly sophisticated cyberattacks from bad actors and adversaries. Positive developments, such as increasingly intelligent transportation systems, automated features, and technological connectedness, which are deployed to improve safety, mobility, sustainability, and resiliency often simultaneously enhance the threat landscape for the controlled, safe, and reliable operation of transportation systems. Given the attractiveness and visibility of transportation systems, and the potential for disruption or damage, roadways and transportation networks are clear targets for cybersecurity attacks. Therefore, the transportation industry must utilize robust cybersecurity best practices to mitigate the threat from hostile incursions whenever it deploys innovative transportation solutions. These best practices must be incorporated at the beginning of the lifecycle of connected transportation infrastructure projects and should represent the biproduct of close collaboration among private sector technology developers, public sector technology deployers, and Federal security practitioners.

The Evolving Nature of The Transportation Environment

State departments of transportation (DOTs) for years have focused primarily on “bricks and mortar” improvements to their physical infrastructure. However, increasingly, the data they generate is essential to management of the transportation system. Just as in other industries, the “digitalization” of the transportation system is an ongoing evolution.

DOTs are like other industries in that they have an Information Technology (IT) environment on which the enterprise relies for business systems such as human resources systems, timecard/payroll, financial, accounting, etc. However, DOTs differ from most other state agencies in that they also rely upon Operational Technology (OT) systems (also called “cyber physical systems”). A key distinction between IT and OT systems is that OT controls systems in the built environment and as such can impact motorist and pedestrian safety.

For example, while a cyber related disruption can be of concern to IT systems at a DOT, such as MS Office or employee timecard systems, these systems being "down" for a period does not generally have safety of life ramifications. Whereas an OT system, such as traffic signals, can have significant public safety impacts if it is offline for even a brief period.

The OT environment also differs from the IT environment in that it is a distributed environment reaching a variety of endpoint devices spread across an entire jurisdiction. These OT networks have typically evolved over time with additional devices being added by different parts of the transportation organization. Consequently, this network is usually a combination of fiber and wireless elements with multiple service providers from telecom to Internet Service Providers (ISPs) as well as the DOTs own communications assets. The complexity and diversity of this network provides other challenges to security. For example, there can be equipment running a quite simple firmware all the way to end devices utilizing stripped down or full Window's operating systems. This makes for a complex Vulnerability Management (VM) strategy.

What Are the Unique Cybersecurity Issues in Transportation Systems?

Information Technology – The standard for IT cybersecurity is the well-known Confidentiality, Integrity, and Availability (CIA) triad. Enterprise data is considered proprietary intellectual property that is often the crown jewels of an organization's business advantage. Keeping digital assets safely under lock and key has therefore been the primary objective of IT cybersecurity strategies. This is followed by the need to ensure the integrity of digital assets. Organizations must not only keep their data out of competitors' hands, but they must also ensure that data is not corrupted in any way, intentionally or otherwise. Finally, at the lowest priority, that data needs to be available internally to appropriate employees and partners, and potential customers.

Operational Technology – The standard for OT cybersecurity, however, requires a broader and a re-ordered set of priorities, namely Control, Availability, Integrity, and Confidentiality, or CAIC. Maintaining *control* of all physical assets to ensure their safe operation is the main objective of OT cybersecurity and overrides all other concerns. If a facility or endpoint device cannot be run safely, then it should not be run at all. The next most important goal for OT cybersecurity is *availability*. OT is present in all critical infrastructure facilities, and critical infrastructure typically needs to always be available. *Integrity* is also important, particularly to the degree it ensures safety and availability. *Confidentiality* of OT data is far less of a concern than it is for IT data.

In addition to having different priorities and goals as they relate to cybersecurity, the technology used in physical systems is often quite different from the technology used in information systems. These differences can significantly affect not only the cybersecurity

posture of the systems but also the means available to secure them. OT systems often include legacy equipment that is built to have a 30-year operational life cycle. This equipment may well have been designed for an era when the entirety of OT was safely air-gapped from the rest of the world.

Is Cybersecurity a Safety Issue in the Transportation Sector?

Traffic management centers are increasingly using digital information to manage the OT network and the operations systems they control, such as traffic signals systems, weather stations, pavement sensors, video cameras, speed detection, deicing systems, etc. Given the importance of these systems to traffic operations, they are clearly safety critical.

As safety critical systems, another distinction between IT and OT systems is the concept of "availability." Uptime in these systems is important to continue to drive activities in the physical environment. OT systems do not usually carry confidential information, such as Personally Identifiable Information (PII), and given the simplicity of interactions with the endpoint device, integrity of the information may be of a lesser concern. This difference in priorities, combined with the potential physical impacts of a transportation hack, reinforces the idea that, in the transportation world, cybersecurity is more analogous to safety than it is to data protection.

There are multiple scenarios in which a cyberattack against an OT network could directly impact the safety of the transportation system. For example, Signal Phase and Timing (SPAT) data that informs system management and connected vehicle communications could be corrupted. It is also possible to simply crash the system, including through a recurring hack that will automatically re-crash the system each time it is restored. In addition, it is often overlooked that the OT traffic system provides another pathway for a hacker to use as an entry point to attack IT systems.

What are the Cyber Dangers to the Transportation Sector?

Threats to DOT systems can come from a host of threat actors. These actors are typically classified by their motivations or their connection to the organizations they attack. For example, a hacktivist might be motivated by the belief that a manufacturer has unacceptable environmental practices, while an employee might be motivated by a desire for revenge stemming from perceived mistreatment by his employer. Terrorists or nation-states might be motivated by a desire to create chaos or to otherwise achieve a political objective. "Script kiddies" are typically just looking for notoriety and easy pickings.

Historically, OT systems have been beyond the reach (both literally and figuratively) of all but the most persistent attackers. We have seen, however, that with enough time and effort, even the most well-protected sites can be vulnerable to attack. For most organizations, the ability to maintain a true air gap between IT and OT systems is effectively impossible.

In addition to intentional threats from hostile governments, terrorist groups, disgruntled employees, and malicious intruders, organizations also face unintentional threats, such as those caused by system complexity or accidents, and natural threats, such as floods and earthquakes. In some cases, cyber defense systems can also provide protections against these additional safety risks.

Conclusion

Various governmental bodies and industries continue to grapple with securing cyber-physical systems. With both digital and physical impacts, DOT OT systems and the potential safety impacts of an interruption to these systems pose potential safety ramifications. Faced with mounting cyber threats and the potential implications from a cyber-attack, it is imperative that the U.S. Department of Transportation (USDOT) and its industry partners move expeditiously to address existing risks to protect the safety and reliability of the transportation system.

Treating OT cybersecurity as a critical safety issue can serve as a starting point for the international transportation industry, utilizing tested best practices while adopting emerging trends to tackle challenges such as future-proofing cyber defenses and creating a cyber-secure culture analogous to the industry's safety culture norm. The transportation industry itself can make strides in its own mandatory or voluntary standards to ensure the safe, controlled, and reliable operation of traffic systems everywhere.

Cybersecurity is a 21st Century issue, but it is no longer a future issue. Instead of viewing it as a standalone challenge, the industry would be better served by considering it a new element to be baked into processes and projects, just as safety was decades ago. Funding is of course necessary but, when done efficiently, cyber defense costs will be only a tiny portion of most transportation projects.

A simple first step (of many) that can be taken by transportation executives and project managers daily is to add one more question to their review processes – "What are the cybersecurity risks of this project and how are we addressing them?"

If you would like to learn more about best practices, network with industry cybersecurity experts, and help move cybersecurity forward in the transportation ecosystem be sure to join our ITS America Cybersecurity Community of Practice. For more information, please contact Tina Williams at twilliams@itsa.org.

On behalf of the ITS America Cybersecurity Community of Practice, John Contestabile, Paul Lennon, Christopher Lyons, and Rick Tiene developed this paper.

ITS AMERICA

www.itsa.org

1100 New Jersey Ave SE Ste. 850
Washington, DC 20003