Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**12 November 2020**

PIN Number

**20201112-001**

Please contact the FBI with any questions related to this Private Industry Notification at your local **Cyber Task Force**.

Local Field Offices: [http://www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

# Addressing Risks Associated with Rail Industrial Internet of Things and Commercial Off-the-Shelf System Solutions

### Summary

Industrial equipment manufacturers are increasingly developing Commercial Off-the-Shelf (COTS) solutions that can be marketed to a variety of clients in different industries, leading a growing segment of US critical infrastructure to incorporate industrial internet of things (IIoT) devices into their networks. This type of IoT, as it applies to rail systems, replaces proprietary technology—originally designed only to support rail operations—with COTS technology. Although connected IIoT devices and systems offer expanded options for US rail infrastructure to streamline train operations, satisfy regulatory directives, and ensure interoperability throughout freight and multimodal shipping operations, they also increase rail systems' cyber risk. Since these devices may be used in multiple industries, they may face more attempts at exploitation by malicious cyber actors researching potential devices to compromise and use as entry points into US infrastructure networks.

**COTS IoT in Industrial Networks**

The increased integration of new devices and COTS systems increases potential entry points malicious cyber actors or advanced persistent threats may attempt to exploit, which enables cyber actors to more easily target multiple industries. Depending on the scope of a compromise, the impact could include disruption of rail operations, damage to rail infrastructure, theft of private data, safety liabilities, reputational and branding risks, financial losses, or scheduling and communications breakdowns. Recent malicious cyber activity against US rail entities demonstrates the importance of proactively addressing the cyber threat posed to IIoT devices and solutions as rail entities continue to streamline and modernize operations.

Factors driving rail modernization include goals of higher efficiency and safety. Technology upgrades occur at varying rates across freight and passenger rail operations, except where required by regulatory directives. For example, most US freight rail infrastructure is expected to implement a safety system known as Positive Train Control (PTC) by the end of 2020, as a result of a federal mandate.[a] In an effort to comply with this mandate, some companies have selected COTS components and solutions. On a broader level, the global railway aftermarket—which includes upgrades of train components and infrastructure—is projected by some market researchers to grow to $131 billion by 2026.

**Risks Associated with Rail IIoT Modernization**

The FBI has identified a number of emerging risks to the rail industry associated with IIoT modernization efforts, to include the shift towards COTS system solutions and how criminal actors may seek to exploit potential vulnerabilities in the near future. Rail IIoT faces similar vulnerability concerns as general IoT technology used in areas of critical infrastructure outside the rail industry (see PIN 20200521-001, TLP: WHITE, on www.ic3.gov). Concerns specific to devices and technologies used in rail operations include the following.

- IIoT devices added to trains connect or can be designed to connect with all aspects of

[a] The Surface Transportation Extension Act of 2015 mandated passenger and major freight railroads to implement PTC on most track lines by 31 December 2018. PTC is a system designed to prevent train-to-train collisions, derailments caused by excessive speeds, unauthorized train movements in work zones, and the movement of trains through switches left in the wrong position. PTC networks enable real-time information sharing between trains, sensors near train crossings, and "back office" applications monitoring train movement, speed restrictions, and the state of signal and switch devices that guide trains from one track to another. *(Source:* (U) Website | Railwayage.com | "Cyber Resiliency: A Clear and Urgent Necessity for Modern Railroads" | 21 March 2019 | https://www.railwayage.com/analytics/cyber-resiliency-a-clear-and-urgent-necessity-for-modern-railroads/ | accessed on 28 April 2020.)

train operations, including onboard GPS, brake, wheel, and engine sensors; passenger flows; environmental conditions; rail car temperatures; CCTV; alarm systems; and internet-connected or automated safety systems such as PTC. Each device can also have built-in remote access features that track the data being generated from the train activity in real-time. Remote accessibility increases the number of potential intrusion vectors a malicious cyber actor could exploit for stealing data or introducing malware. Rail operations data can include real-time overviews of locomotive fleet movements throughout geographic regions, their condition, and peak passenger patterns, which can also be used to drill down into individual travel activities.

- If a vulnerability arises in a COTS system installed on or used by multiple rail networks, cyber threat actors may be able to exploit the vulnerability to target multiple victims in one attack. For example, the WannaCry ransomware targeted internet-connected Windows 7 operating systems, impacting victims across multiple industries, including the German rail sector.
- Mission-critical control systems on the same networks as remotely accessible IIoT devices, passenger payment, or entertainment systems create a vulnerability for access to a train's operation network through the public access network.
- A Department of Transportation research team developed common attack scenarios through which cyber actors could attack rail-based IIoT. The most common scenarios identified included loss of train operation monitoring, malfunction or takeover of the signaling systems, and malfunction of wayside devices (such as switch controllers) due to cyber attacks. These scenarios could lead to unexpected train stops, delays, or disruption of service. In addition, if the rail fail-safe mechanisms were tampered with, these attacks could lead to train derailment, collision, or loss of life.[b]

Since 2003, there have been a variety of cyber incidents impacting rail companies in the United States and overseas. While most of the cyber incidents only disrupted minor operations, led to monetary losses, or resulted in malware being introduced into rail company computer networks, one incident in Lodz, Poland, resulted in train derailments.[c] The most recent breach, which occurred in August 2020, prevented a US transportation authority from sharing travel information with its customers. To mitigate the spread of malware, the US transportation authority temporarily shut down its real-time travel data sharing service and suspended employee email, payroll, and remote timekeeping capabilities.

Malicious cyber actors are constantly working to improve their abilities to exploit weaknesses

[b] The report can be accessed at https://rosap.ntl.bts.gov/view/dot/49646/dot_49646_DS1.pdf?.

[c] The report can be accessed at https://www.masstransitmag.com/safety-security/article/21116419/securing-the-railroads-from-cyberattacks.

in networks. For example, cyber criminals work to advance their techniques and methods for gaining access to and exploiting systems in order to discover weak points in new connected systems. Their efforts can include holding competitions for developers to write or create proof-of-concepts on exploitable vulnerabilities, how to circumvent cyber security protocols, and the best way to conduct an advanced and persistent attack. The ongoing evolution of the cyber criminal threat increases the importance of proactively addressing cyber risk in critical infrastructure networks.

FBI investigations have revealed that malicious cyber actors actively search for and compromise vulnerable IoT devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks, participate in DDoS attacks, and use them as entry points for computer network exploitation. These activities can lead to a disruption of vulnerable IIoT software or hardware resulting in rail industry services interruptions or slowed Internet network connectivity. Additionally, cyber actors could deploy malware or execute ransomware on devices capable of spreading throughout all connected rail infrastructure networks, enabling theft of customer and employee data, physical disruptions, or the theft of intellectual property. For additional information on how cyber actors exploit general IoT devices, see https://www.ic3.gov/media/2018/180802.aspx and https://www.ic3.gov/media/2017/171017-1.aspx.

The FBI is providing the following indicators to help rail industry partners recognize when they may be the target of criminal activities seeking to exploit modernization efforts. *These indicators should be observed in context and not individually*. Suspicious activities/indicators include but are not limited to the following:

- increased interest and discussions on cyber criminal forums about rail technology vulnerabilities;
- increased reporting from rail companies and city transit authorities of cyber intrusions, such as phishing schemes or probing activities;
- persistent and undue interest in rail equipment or communications technical information, to include fail states, by individuals, including those who work in the rail industry but do not require this information for their jobs;
- procurement of rail infrastructure equipment by a person with no employment in or business connections to the rail industry; examples include wayside devices or connected braking systems. This activity is more significant as an indicator if the procurer shows no corresponding interest in equipment that is less modern or no longer widely used;
- non-rail entities using wireless equipment at frequencies used for automatic or connected rail functions, such as wayside monitoring device communication with the back office or

PTC;

- radio communications interference or failure, especially in rail yards, and including interference or failure of radio data transfer that may facilitate systems such as GPS or PTC;
- compromises of, or attempts to compromise, an industry or organization using IIoT technology or devices also used in the rail industry. An exhaustive approach to this indicator will rarely be practical; however, reporting on these activities will help rail organizations become aware of these threats and consider them in the context of common vulnerabilities.

In addition to standard cybersecurity best practices and insider threat countermeasures, the FBI has developed the following set of mitigation strategies and proactive measures that may help freight and passenger rail companies protect the connected rail devices from unauthorized access and exploitation.

- Work closely with manufacturers to ensure all internet-connected parts being introduced into trains and networks include built-in security features that are upgradable.
- Establish and perform risk assessments and penetration testing for each component of new systems to establish a clear view of the related cybersecurity risks.
- Establish continuous system scans to detect and quarantine potential anomalies.
- Patch critical vulnerabilities on all systems. Prioritize patching of Internet-connected servers for known vulnerabilities as well as software that processes Internet data, such as web browsers, browser plugins, and document readers. For additional guidance on identifying and patching the most commonly exploited vulnerabilities, refer to Alert (AA20-133A): Top 10 Routinely Exploited Vulnerabilities published by the FBI and CISA on 12 May 2020. [Reference link: https://www.us-cert.gov/ncas/alerts/aa20-133a]
- Strengthen credential requirements and implement multi-factor authentication to protect individual accounts. Change passwords, and do not use the same passwords for multiple accounts.
- Identify and suspend access of terminated employees and users exhibiting unusual activity, particularly through remote access or VPN solutions. Examples include uncharacteristic traffic, downloads, or login from an unusual location or unrecognized device.
- When possible, segment critical information on air-gapped systems. Use strict access control measures for critical data.
- Require technology services retained to be transparent in their contracts, services, and policies, particularly concerning data privacy and cybersecurity provisions.

**Reporting Notice**

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

**Administrative Note**

This product is marked TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

## Your Feedback Regarding this Product is Critical

**Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey**