Whitepaper

PTC FOR RAILS

AN OPPORTUNITY TO IMPROVE CYBERSECURITY

by Courtney Schneider, Cyber Policy Research Manager
Waterfall Security Solutions

The greatest security risk to rail networks is arguably online rather than onboard. With cyber attacks on railway networks speckling the globe in recent years, the growth in rail cyber security awareness is on the rapid uptick. As bad actors have successfully compromised rail networks in Denmark, the UK, San Francisco, Germany, Poland and more, governments and standards bodies have been responded to require security best practices to protect railways' geographically dispersed critical infrastructure.

Contemporaneously, railway infrastructure is undergoing government mandated large-scale safety upgrades for accident prevention, particularly in the United States where Positive Train Control (PTC) implementation for Class 1 railways was enacted into law in the Rail Safety Improvement act of 2008 (RISA). Scheduled for completion in 2020, the PTC roll-out is occurring at a time when accident prevention - both by human operator, and by cyber-attack – is front of mind for operators, lawmakers, and regulators alike.

PTC

Class 1 railroads across the US have invested close to $11 billion in the development, installation and implementation of PTC. The technology is meant to prevent four main types of accidents: train collisions, derailments due to speeding, trains entering maintenance track sites, and a train traveling through an improperly aligned switch. PTC technology achieves this through locomotive-borne devices linked to a central dispatching system via wireless communications. If an operator exceeds an authorized speed or movement authority, automation on the locomotive brings the train to a full stop. PTC eliminates many risks of accident and mis-operation due to human error.

Cybersecurity

Unfortunately, locomotive and signaling system mis-operation is not limited to human error. Rail system operators are increasingly aware of the risk of cyber sabotage. The simplest cyber attacks – common malware and ransomware – can impair operations so thoroughly that rail systems must be shut down for safety reasons while computers systems are restored from backups. More sophisticated and more malicious attacks can have more serious consequences.

PTC represents a step in a long trend towards increased connectivity for rail automation systems. The increased wireless communications for PTC reduce errors and improves safety records. Communicating locomotive locations and predicted arrival times to freight customers and passengers' cell phones across the Internet increases customer satisfaction. Communicating live equipment usage status information to maintenance scheduling and optimizing applications increases efficiencies and reduces costs. As with most modern automation, all these initiatives demand increased connectivity.

The problem here is that all cyber attacks are information, and every bit of information can be an attack. A single bit – a "one" bit saying "open the switch" when the switch should be closed – can be an attack. Increased connectivity means increased flows of

messages into and out of signaling systems from IT networks and even the Internet. Each of these messages is a threat to continuous, correct, efficient and safe operations.

PTC As Opportunity

PTC projects generally include budgets to upgrade communications to increase connectivity with trackside and on-board automation, and to deploy commensurate cybersecurity. This budget for cybersecurity represents an opportunity to address steadily-increasing risks due to the long-standing trend towards increased attack sophistication and increased connectivity with IT systems and customers. To address these risks thoroughly, it makes sense to look to what the most cybersecure railway systems are doing.

The most secure rail sites are not concerned with the steadily increasing sophistication of cyber attacks, nor with the steadily increasing rate of disclosure of new attack vulnerabilities in control system, network, firewall and other security software. This is because the most secure sites protect their automation systems from cyber attacks physically, with hardware-based solutions, not just with software solutions.

Physical Protection from Cyber Attacks

Thoroughly secured rail system operators define their on-board, trackside, signaling system, and PTC control assets as a single, control-critical WAN. They forbid routers and firewalls between any control-critical asset and a non-critical asset or network. They permit only Unidirectional Security Gateways at the so-called “IT/OT interface” – the interface between control-critical components and non-critical components. Unidirectional Security Gateways are physically able to transmit information in only one direction – from OT control critical networks to IT systems and the Internet.

Unidirectional Gateways replicate database servers and other servers unidirectionally. The replica databases on the IT networks provide IT users, customers and passengers with the same data as would have been sourced from control-critical databases, without ever sending even one message from IT networks back into control-critical networks. It does not matter how sophisticated attacks become or how clever our attackers are - if no information enters control-critical networks, no attacks enter either.

Security Is Essential to Safety

Increased connectivity within critical rail control systems and between such systems and IT networks is part of a long trend towards increased automation, efficiency, and safety but results in increased cyber risk. Modern rail system operators embrace both increased efficiencies and reduced risk by deploying physical, unidirectional protections from cyber attacks as part of on-going PTC and other automation improvements.

Better yet, the physical protections provided by Unidirectional Security Gateway deployments reduce operating costs. Security update programs are essential to software-based cybersecurity but are notoriously expensive due to the potential for

malfunction of the new, updated software. Continuous testing of new security updates for continued correct and safe operations is very costly and has limited value – new security vulnerabilities continue to be announced very frequently. Physical protection from attack information means that these costly programs can be scaled back to reflect the limited benefits that security updates bring to unidirectionally-protected networks.

PTC programs present an opportunity to deploy modern, robust cybersecurity protection in the form of Unidirectional Security Gateways. The gateways not only assure safe, continuous and efficient operations, they reduce the cost of the most-costly elements of software-based security programs, thus reducing overall cybersecurity program costs. Strong unidirectional cybersecurity is essential to safe and reliable operations and improves overall efficiency as well.