White paper – August 2017

The state of cybersecurity in the rail industry

Rockwell Collins
Building trust every day

Introduction

The last thirty years have witnessed major technological advances in computing, networking and the industrial control systems (ICS) that help run critical infrastructure operations. Today, ICS control everything from ventilation in subterranean tunnels to high rise elevators to nuclear reactor cores. In rail, ICS have replaced the mainframes and obscure protocols that were once the backbone of the industry. SCADA control systems, the field devices and Remote Terminal Units they interface with and the PTC systems being implemented across the industry all depend on ICS.

But, as we now know from examples across many critical infrastructure industries, ICS also enables vulnerability via outside connectivity, creating continuous threats to public safety and continuity of operations. As ICS evolve and advance to support their industries so do the threats – and, so must the cybersecurity to protect them.

Up until 2010, when the world witnessed the first case of weaponized malware in Stuxnet, very little consideration was given to cybersecurity for ICS in critical infrastructure. Although Stuxnet is specific to the nuclear industry the precedent had been set. Cybersecurity experts around the globe, in all critical infrastructure industries, understood the implications. In the future, anything that could be accessed from the outside, and even some things that couldn't, would be possible targets. Simply being listed by the United States Government as *Critical Infrastructure* meant being an inevitable target. Very quickly industries like rail understood just how critical it was to focus on ICS cybersecurity, even if the *how* wasn't exactly clear yet.

Since Stuxnet, many studies have shown that the world has continued to see a significant increase in cyberattacks. From massive near-gigabit distributed denial of service (DDOS) attacks, ransomware, and attacks on financial institutions and credit card fraud – to critical infrastructure around the world. Just last year, Ukraine experienced one of the most infamous attacks on ICS when nearly 300,000 people found themselves without power in the middle of winter after an electric grid was compromised.

There is no denying the potential, ruthlessness and capability of modern day cyberattacks. With Nation State level malware and zero-day vulnerabilities being leaked regularly to the internet, even inexperienced “script-kiddies” have the potential to inflict significant damage. The damage experienced professionals can do is massive.

Additionally, physical security is under unprecedented exposure. In some instances, transportation authorities stretch their information systems and architecture over hundreds of square miles. This presents challenges to the entire organization. Integrating physical and cybersecurity is increasingly important to protect proprietary and customer information and more importantly the safety of passengers, the workforce and cargo.

Many rail and transportation authorities do have mechanisms in place which harden their cybersecurity posture, but these controls often lack a programmatic approach to securing the ICS backbone. We believe the path to success in cybersecurity begins with a logical, realistic approach – a baseline

The risks

The National Institute of Standards and Technology (NIST), Special Publication 800-82, revision 2[1], lists the following cyber-threats to ICS:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- ICS software or configurations settings modified, or ICS software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life.

Based on recent events within ICS from around the world, nearly every one of those situations has occurred. Again, look at the Ukrainian power plant cyberattack of 2016. After analyzing all of the information made available, cybersecurity experts believe the attack began with a spear phishing campaign in April of 2016. The phishing campaign targeted not only the power plant employees, but also their vendors – ultimately leading to multiple back-channel access points into the plant's enterprise network.

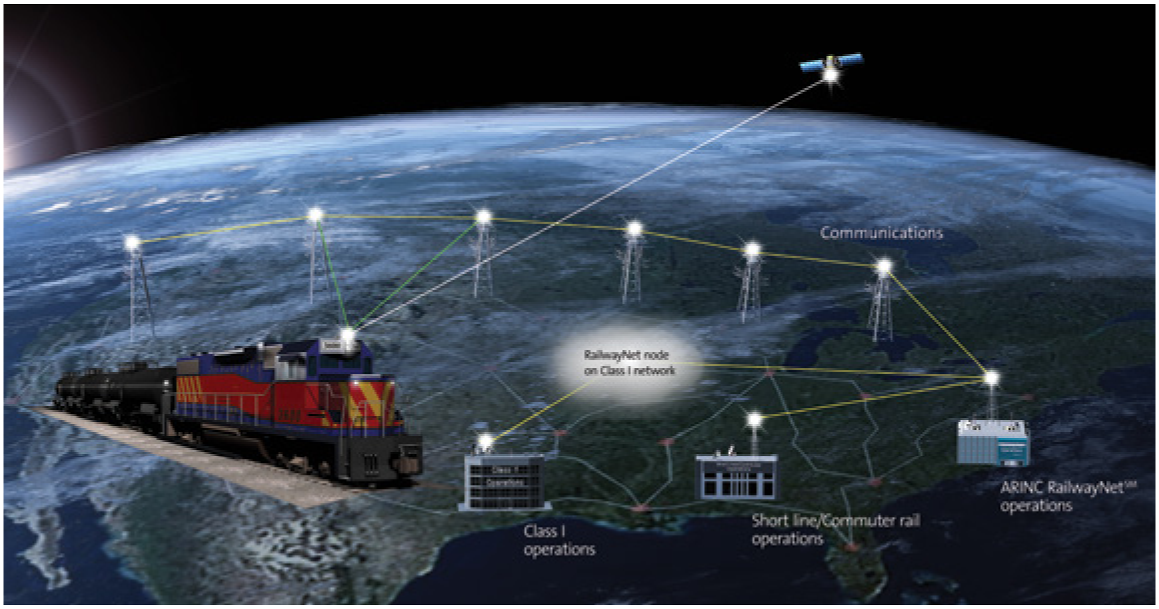
After a few months of reconnaissance the attackers had identified a route into the ICS zone and infiltrated accordingly. During propagation of the attack, they had full-remote access to workstations and were able to take control, change passwords, lock out authorized users and begin to shut down the power grid. All the while, the power plant operations staff were both unaware of what was going on and/or unable to do anything to stop it.

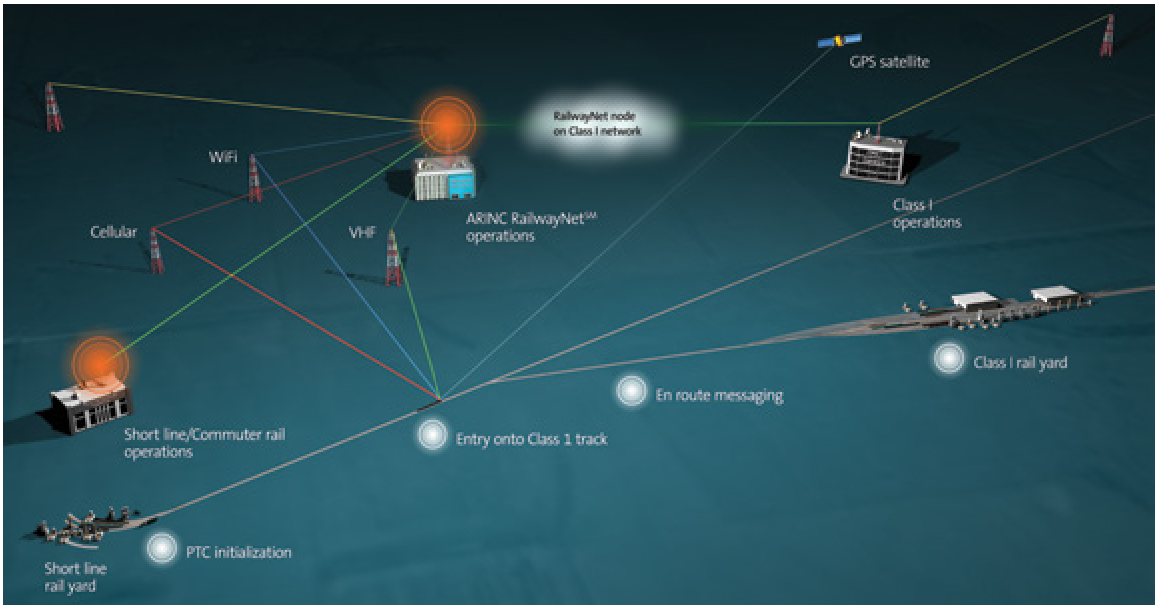
The plant actually had significant cyber-protections in place to prevent an attack of this scale, including multiple firewalls in place, layers of security controls from the border to the ICS zone, and the staff had cybersecurity training. But it still happened.

Cybersecurity Center of Excellence

It is well understood that there are significant risks associated with operating any type of electronic asset, let alone critical infrastructure level ICS. Rockwell Collins' Cybersecurity Center of Excellence has developed a three-phased approach to tackling cybersecurity challenges in critical infrastructure. As our advisors and engineers only work within the critical infrastructure verticals and have been supporting the rail industry for thirty years, we have a comprehensive knowledge base and understanding of the needs and challenges faced.

Rockwell Collins will assist and guide an operational assessment via the following three phases, which will lead to a cybersecurity program and increased maturity levels.


Communications
RailwayNet node on Class I network
ARINC RailwayNet℠ operations
Short line/Commuter rail operations
Class I operations



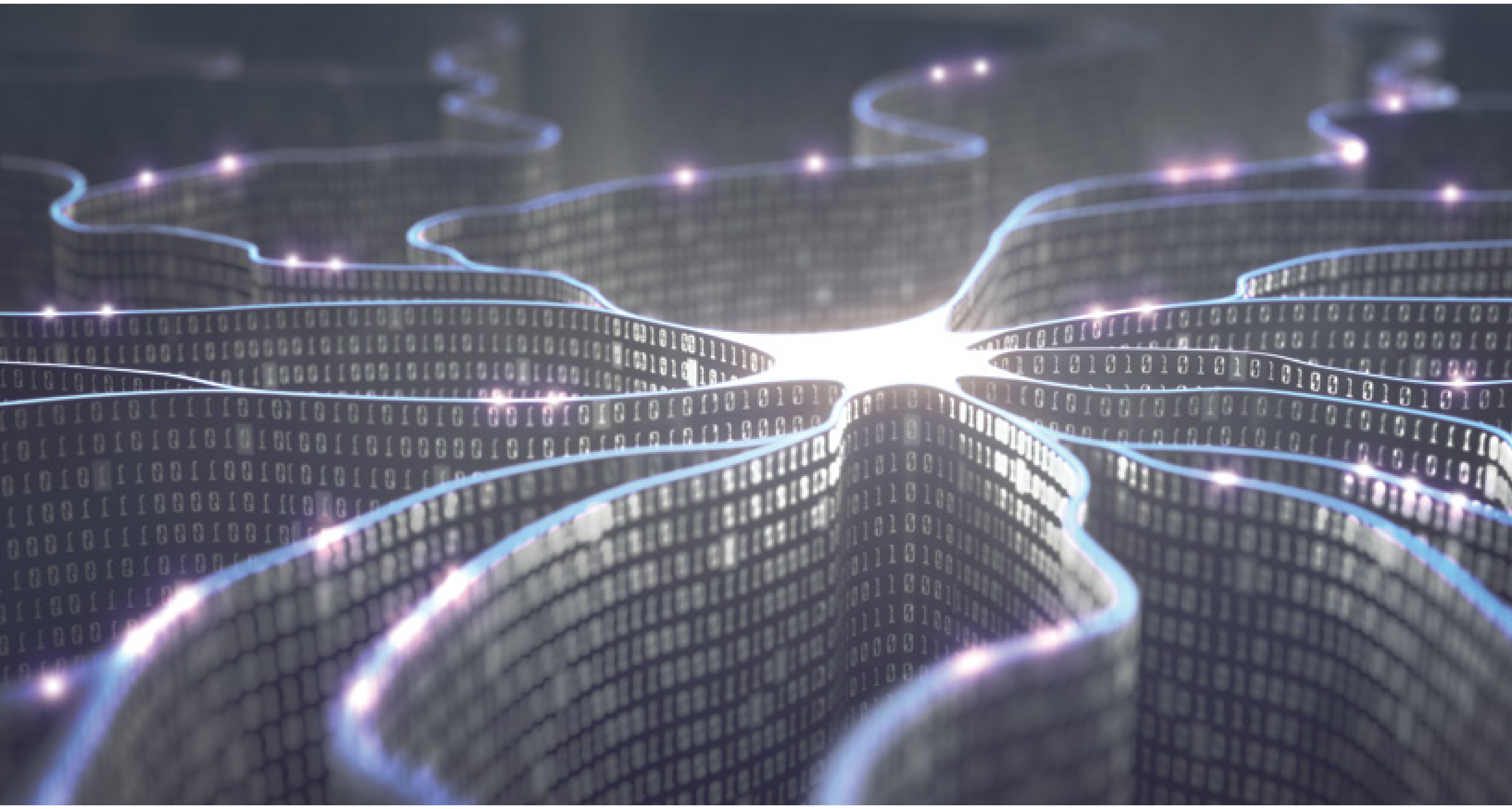
Phase One: Baseline

Securing infrastructure is not simple. It is easy to get wrong and hard to get right. Taking the time to take a hard honest look at your current maturity level and build a roadmap is essential to implementing successful cyber solutions. The more focus is placed on baselining 'as-is' posture with organizations such as the International Standards Organization (ISO), Control Objectives for Information and Related Technologies (COBIT), and NIST, the greater advantage to your operations. We will use these existing frameworks, the critical data and methodologies, to help develop a cybersecurity strategy that makes sense for your railroad and exiting ICS.

Phase Two: Secure

What do you do with all of this information and analyses? How do you implement new policies, procedures, controls and technologies in the most cost-effective and efficient manner? This is the same challenge that most of our customers have faced in the early stages of implementing and hardening new infrastructure.

Rockwell Collins has over a decade of experience helping the nuclear industry do just that. After Stuxnet was discovered, the U.S. Nuclear Regulatory Commission created cybersecurity regulations for all nuclear power generation facilities. From helping to develop policies and procedures, to designing new architecture and implementing new technology, we understand the challenges you face. We will help your railroad develop a solution that's right for your operations, one that is adaptable to the ever evolving cyber environment and any forthcoming regulations.



Phase Three: Maintain

Which leads to the critical phase of maintaining your cybersecurity. What has to be done to keep things up-to-date and ready for upgrades at an increased pace? What are the configuration challenges that will arise if certain technologies are updated but not others? How much will a program such as vulnerability management cost?

Rockwell Collins has extensive experience as systems integrators. Stemming from our experience in software development and platforms installed at nuclear installations, rail and transit authorities, and other critical infrastructure sites around the country, we are very familiar with these challenges. They are constant, on-going and if not well-maintained, produce significant threat and vulnerability to the owner. Rockwell Collins advisors and engineers work hand-in-hand with your technical and management teams to conquer these maintenance challenges and prepare your system for the future.

Physical and cybersecurity integration

Rockwell Collins is an industry leading expert in both physical and cyber environments. Today, over forty nuclear plants use our single-platform, integrated physical and cyber solutions. We understand the challenges and necessity of this task; our proven experience in critical infrastructure enables us to deliver customers the information they need to make the best decision for their operations.

Next steps

While many agree cybersecurity is often under-prioritized and under-funded, and it's undeniably difficult to put your arms around an executable strategy – it's also widely known this can't afford to keep being the case. In fact, in Forbes' 2017 Global Information Security Survey[2], 78 percent of executives and IT managers expressed this feeling. However, risk doesn't warrant haphazard expense. The very nature of cyberattacks and cybersecurity necessitate a vigilant and phased approach. Rockwell Collins will help your railroad take on the cyber challenges you're facing in manageable strategic steps as part of a roadmap you control.

Notes:

[1] U.S. Department of Commerce. National Institute of Standards and Technology. *Guide to Industrial Control Systems (ICS) Security*. By Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams and Adam Hahn Washington State University. May 2015. Special Publication 800-82 Revision 2. Retrieved August 2017 from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[2] Russ Banham, "Why Cybersecurity Should Be A No. 1 Business Priority For 2017," Forbes, March 20, 2017. Retrieved August 2017 from https://www.forbes.com/sites/eycybersecurity/2017/03/20/why-cybersecurity-should-be-a-no-1-business-priority-for-2017/#375187c71719

Building trust every day.

Rockwell Collins delivers innovative aviation and high-integrity solutions that transform commercial and government customers' futures worldwide. Backed by a global network of service and support, we are deeply committed to putting our solutions to work for you, whenever and wherever you need us. In this way, working together, we build trust. Every day.

For more information, contact:

Rockwell Collins
2551 Riva Road
Annapolis, MD 21401
866.633.6882 | +1.410.266.4000
security@rockwellcollins.com
rockwellcollins.com

Rockwell Collins
Building trust every day