

6 Emerging Rail
Cybersecurity
Standards Point to
**Unidirectional
Security Gateways**



4-5

INTRODUCTION

6-7

FRANCE: ANSSI

8-9

USA: NIST

10-11

USA: APTA

12-13

UK: DfT

14-15

USA: DHS

16-17

EU: ENISA

18-19

ABOUT WATERFALL SECURITY

INTRODUCTION

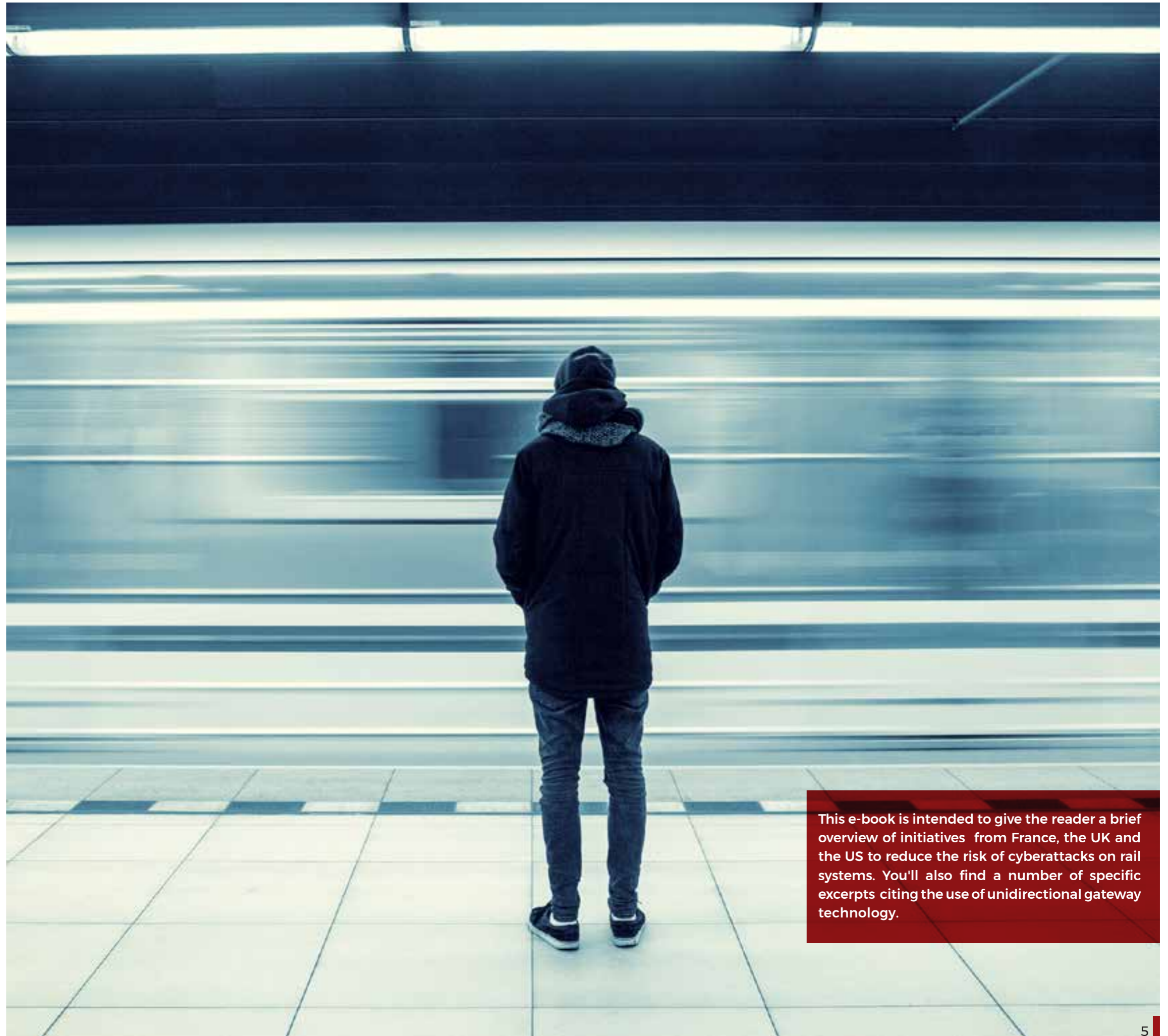
6 Emerging Rail Cybersecurity Standards Point to Unidirectional Security Gateways

A vital part of a country's national economy as a primary transportation mode for passengers and freight, many rail industries around the world are experiencing a rapid increase in digitization and modernization of safety, signaling and communication control systems. Accordingly, public and private investment can reach billions in capital expenditures.

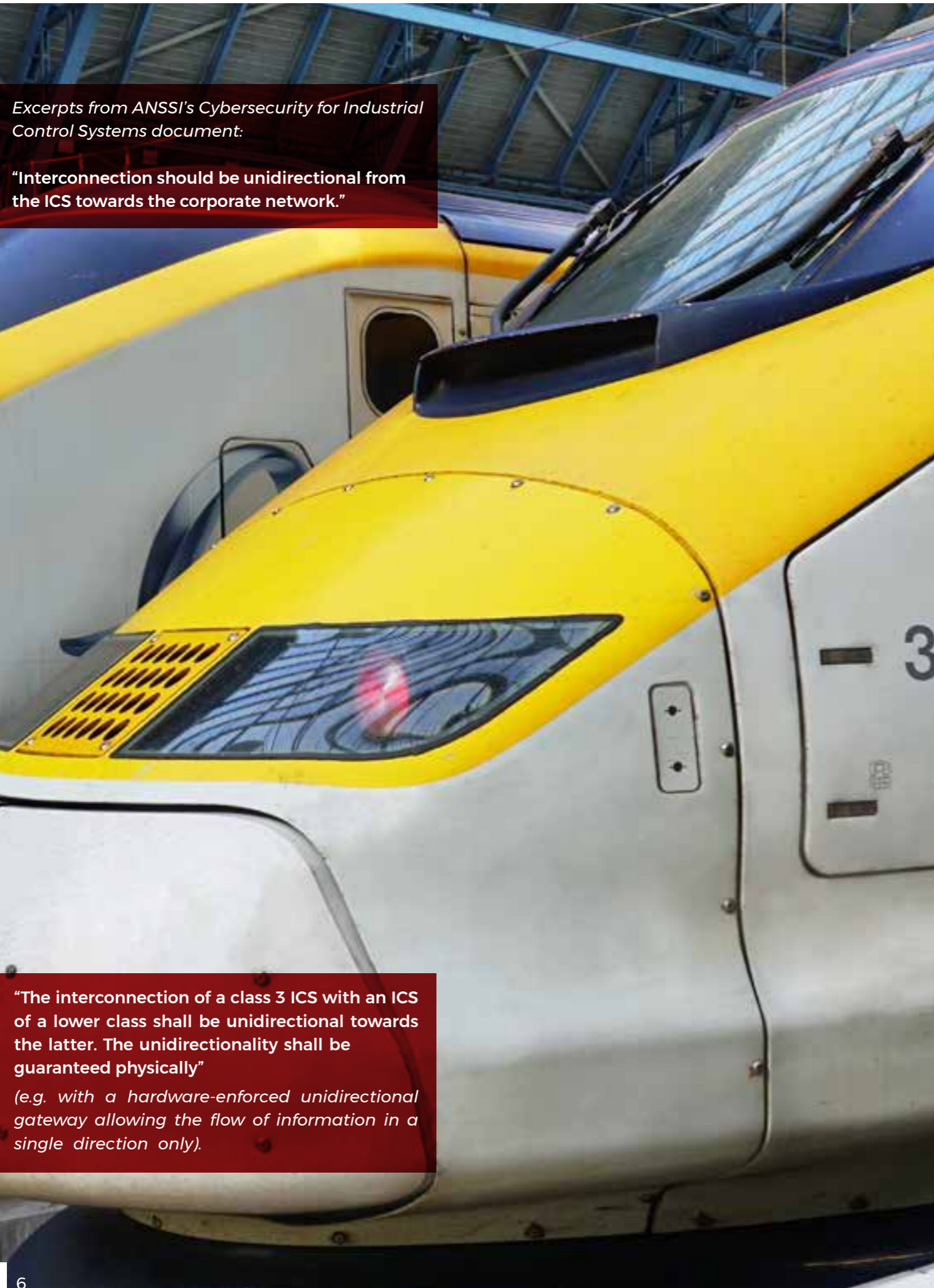
Unfortunately, the rise of digitization begets highly sophisticated cyberattacks, and rail systems' critical infrastructure is becoming more and more vulnerable.

Cyberattacks on rail systems are no longer a hypothetical threat.

Over the last few years, there have been reports of attacks on various railway systems in the U.K., U.S.A., Japan and many other countries. Due to interconnected systems, including entertainment devices and scheduling services, and the integration of digital signaling, the attack surface of modern rail systems continues to grow.



This e-book is intended to give the reader a brief overview of initiatives from France, the UK and the US to reduce the risk of cyberattacks on rail systems. You'll also find a number of specific excerpts citing the use of unidirectional gateway technology.



Excerpts from ANSSI's Cybersecurity for Industrial Control Systems document:

"Interconnection should be unidirectional from the ICS towards the corporate network."

"The interconnection of a class 3 ICS with an ICS of a lower class shall be unidirectional towards the latter. The unidirectionality shall be guaranteed physically"

(e.g. with a hardware-enforced unidirectional gateway allowing the flow of information in a single direction only).

FRANCE: ANSSI

The National Information System Security Agency

ANSSI discourages remote access and encourages the use of unidirectional gateways rather than firewalls

In France, the Agence nationale de la sécurité des systèmes d'information (ANSSI) is responsible for the country's digital security strategy and enforcement, and reports to the Secretary General for Defense and National Security. The French national digital security strategy, announced in 2015, is designed to support the digital transition of French society.

ANSSI divides its cybersecurity recommendations into three classes of industrial control systems (ICS), corresponding to their sensitivity. This classification can be applied to an entire site, to a specific portion, or to an ICS distributed over several sites. Class 3 relates to an ICS in which the risk or impact of an attack is critical.

ANSSI discourages remote access and encourages the use of unidirectional gateways rather than firewalls for these highly critical industrial systems classified as class 3 networks. The agency published a document entitled [Cybersecurity for Industrial Control Systems - Classification Method and Key Measures](#) in which railway switch automation is categorized as a class 3 critical network, and is composed of the following elements:

1. Programmable Logic Controllers (PLCs) connected to the switches on the railway tracts

2. Configuration work stations on a private network dedicated to the transport system - used for diagnostics and to configure routing maps

3. Maintenance work stations, outside the network

The use of firewalls is forbidden to connect any class 3 network, such as railway switching systems, to a lower class network or corporate network, and only unidirectional technology is permitted for these connections.

USA: NIST

National Institute of Standards and Technology of the U.S. Department of Commerce

Unidirectional gateways are recommended not only for network access restriction but also as network boundary protection, constituting major security objectives for SCADA control systems for railway networks.

The [second revision to the National Institute of Standards and Technology \(NIST\) 800-82 Revision 2](#) guidance for industrial control systems (ICS) security sets about explaining how to effectively implement security technology to protect unique ICS environments. One such environment that the document focuses on is railways.

Railways require particular attention, as they not only contain very critical control networks, but also these networks control geographically dispersed assets spanning large distances. Geographically distributed SCADA control technology operates “highly interconnected and dynamic systems” providing centralized monitoring and control for numerous processes. To protect these systems means restricting access to the ICS network whether that access be logical or physical.

Excerpts from [the National Institute of Standards and Technology \(NIST\) 800-82 Revision 2](#) guidance:

“Major security objectives for an ICS implementation should include the following: Restricting logical access to the ICS network and network activity. This may include using unidirectional gateways ... The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.”

“Unidirectional gateways restrict communications between connections to a single direction, therefore, segmenting the network.”

“Boundary protection devices control the flow of information between interconnected security domains to protect the ICS against malicious cyber adversaries and non-malicious errors and accidents.”

“Boundary protection controls include unidirectional gateways”

A unidirectional gateway “is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security or protection of critical digital systems, such as industrial control systems, from inbound cyberattacks.”

“All network-routable interfaces connecting the OCSZ to the SCSZ or FLSZ should use an isolation device to ensure security separation.”

“Higher security zones need to be behind perimeters in order to segregate them from lower-security zones.”

“Simply put, a transit agency needs to ensure that no one can interfere with its normal and proper operation.”

Excerpts from APTA's [Securing Control and Communications in Rail Transit Environments: Part IIIb Protecting the Operationally Critical Security Zone](#) document:

“In today's interconnected environment, it is conceivable and possible for someone acting remotely to access and modify a control system.”

“Antivirus, whitelisting, firewall and other current cyber-defense technologies that may inject delays in communications [in control systems] or block execution of programs carry the risk of unintentionally disrupting system functions...”

In late 2016, the American Public Transportation Association (APTA) published [Securing Control and Communications in Rail Transit Environments: Part IIIb Protecting the Operationally Critical Security Zone](#). The document draws out recommended practices for protecting the operationally critical security zones (OCSZ) in rail transit networks. Elements of an OCSZ are traction power SCADA, facilities monitoring, and centralized train control. Minimum system controls practices include placing electronic security perimeters around the OCSZ, how to securely connect security zones of different security levels, and creating physical and logical separation for OCSZ data transmission.

What this standard does particularly well is stress the importance of identifying and classifying different levels of criticality of operational networks. This method addresses the importance of secure connections from the most critical networks to networks of lesser importance or criticality.

Secondly, prevention is the single highest priority over detection and responding for rail, and the most important systems to protect are those that pose risks to life and property. The standard also points out the flaws and complications of using a software-only based strategy, such as firewalls, to protect operationally critical control networks.

UK: DFT

Department for Transport

The rail industry in the U.K. is undergoing a massive increase in demand for transporting passengers and freight, leading the government and other private sectors to significantly invest in digitization and modernization of safety, signaling and communication control systems. Unfortunately with the rise sophisticated cyberattacks, Britain's critical infrastructure is becoming more and more vulnerable.

"signaling systems should be protected with unidirectional gateways"


The inaugural Rail Cyber Security Summit was held in London in March of 2016 and the UK's Department for Transport (DfT) subsequently released [Rail Cyber Security - Guidance to Industry](#), which states clearly that signaling systems should be protected with unidirectional gateways and that there should be a clear separation between enterprise and operational rail networks. The DfT is also engaged in a UK Rail Safety and Standards Board (RSSB) led development of a cyber security strategy for the British rail industry.



Excerpts from the DfT's [Rail Cyber Security - Guidance to Industry](#) document:
"You should physically or electronically separate on-train networks for passengers from networks used for train control and signaling, particularly where WiFi is used."

"Signals should ideally contain unidirectional gateways."

"You should put security measures in place at interfaces between systems inside organisations and between different organisations. These form part of system boundaries, and need protection. Trust cannot be assumed."



Excerpts from the [Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies](#) document:

With unidirectional gateways “one can achieve the best of both worlds, enabling the connectivity required and assuring security. This holds true even if both the low and the high network are compromised, because the traffic flow control is physical in nature.”

“...regulators have encouraged the use of unidirectional gateways to protect equipment and processes in SISs” (safety instrumented systems).

USA: THE DEPARTMENT OF HOMELAND SECURITY

Industrial Control Systems Cyber Emergency Response Team

In September 2016, the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) released an updated version of [Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies](#). This document is a general industrial control systems guide and included in its target industries is railway ground transportation.

It comprises a collection of recommendations for ICS security programs on topics including risk management, security controls and technologies, as well as physical security and training/awareness. The document describes attack scenarios and essential limitations of security technologies as justification for specific recommendations. Unidirectional gateways are recommended as best practice for ICS network perimeter security - connecting highly critical networks to lower criticality networks and securing network communication flow.

ENISA:

Communication network dependencies for ICS/SCADA Systems

The European Union Agency for Network and Information Security (ENISA) cybersecurity guideline [Communication network dependencies for ICS/SCADA systems](#) provides insight into the communication network dependencies in ICS/SCADA environments, their potential impact on critical assets, and recommends security good practices to mitigate cyber risk. The guideline points to railway networks as one such SCADA environment highly dependent on WAN communications that are increasingly Internet Protocol based.

The guideline warns that cyber threats to critical infrastructure such as rail networks are likely to increase in the future as increased levels of communications expose SCADA systems to new Internet-based threats. The report focuses on how these threats - residing on less-trusted and Internet-exposed networks - can potentially exploit control networks in critical infrastructures, and provides recommendations to mitigate these threats.

One security control highlighted to protect SCADA networks from unauthorized access, malicious, code or cascading network outages is to harden network interconnections through unidirectional communications. In addition, unidirectional technology is also recommended as a means to provide security to systems using insecure protocols which traverse wide area networks - a central concern rail operators.



For control network monitoring, firewalls are not a universal solution and do not cover all the risks.

Unidirectional technology is recommended for hardening network interconnections and protecting sensitive SCADA and signaling systems.

ABOUT WATERFALL SECURITY



Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall products, based on its innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, rails, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases and protocols in the market.

For more information write:
info@waterfall-security.com

Waterfall's products are covered by U.S. Patents 8,223,205, 7,649,452, and by other pending patent applications in the US and other countries. "Waterfall", the Waterfall Logo, "Stronger than Firewalls", "In Logs We Trust", "Unidirectional CloudConnect", and "CloudConnect", and "One Way to Connect" are trademarks of Waterfall Security Solutions Ltd. All other trademarks mentioned above are the property of their respective owners. Waterfall Security reserves the right to change the content at any time without notice. Waterfall Security makes no commitment to update content and assumes no responsibility for any mistakes in this document.
Copyright © 2018 Waterfall Security Solutions Ltd. All Rights Reserved.



An aerial photograph of a large dam structure, possibly a concrete dam with a spillway. The image is heavily stylized with a red overlay that covers most of the frame, leaving only the edges in grayscale. The red overlay is semi-transparent, revealing the underlying structure of the dam. The dam's spillway is visible on the right side, and the reservoir is on the left. The overall composition is dynamic, with strong diagonal lines and a sense of scale.

www.waterfall-security.com
info@waterfall-security.com