CYBERSECURITY:

For Safe and Secure Mobility

ALSTOM
• mobility by nature •

B
Dhoby Ghaut
Kallang A ↑
Theatre
i

Editorial

Cybersecurity: the “must-have” for smart systems

Eddy Thesee
Vice President,
Cybersecurity
Products &
Solutions,Alstom

In many respects, a computer system bears a remarkable likeness to living organisms. Like them, it grows, develops, and explores new territory.

Above all, it seamlessly interlocks with its surrounding ecosystem, which for its part is constantly changing, and it sees new species regularly appear.

There is a lot more to a railway system than its computer system. Computer systems, however, are acquiring more and more importance within the networks, in the control centres or the drivers’ cabins, as well as track equipment and traveller information systems. This increasingly prominent role offers a fantastic opportunity for creating value, as digitisation brings added intelligence to railway networks, in terms both of their development and operational needs and of their maintenance requirements.

This added element of intelligent systems is nevertheless accompanied by an added element of fragility, if the overall security of the digital systems used is not taken seriously, and adequately matched by the safety and security culture that is typical of the railway world. Because computer systems are “living” systems, this demands of those playing their various roles in the railway universe permanent vigilance, combined with a solid ability to anticipate and adapt.

The leading players in the transport world have, during the last few years, entered the era of cybersecurity. In the railway world, attacks are still rare. As the networks modernise, however, exposure increases apace. The challenge is thus clear: cybersecurity must be placed at the very heart of our culture of excellence and security.

We have, for the most part, embraced this transformation with success. We are today able to equip the systems we deploy, operate and maintain with the required levels of protection and solidity, even in contexts in which cyber-threats are particularly critical, as is the case in Israel.

It should be remembered, however, that we have not embarked upon this transition alone. Cybersecurity does not have a weak link, and we are working with all our partners, and particularly with Airbus, on setting the benchmark standards and sharing the key processes throughout the entire value chain. This will ensure that regardless of the means of transport used, the traveller can continue to enjoy both a smooth and safe journey. ●

Experts in this issue

Alstom Experts

Carlos Galan Arnillas
REM Project
Cybersecurity Manager,
Alstom

Serge Benoliel
Cybersecurity
Management Office
Manager, Alstom

Baptiste Fouques
Cyber Defense Expert
for systems and core
frameworks, Alstom

Jean-François Gillot
Cybersecurity
Platform Manager,
Alstom

Thierry Renouf
Cybersecurity
Platform Manager,
Alstom

Sangeeta Chomal
Cybersecurity Leader
MEA Region, Alstom

External Experts

Gilles Desoblin
Director, Strategy and
Programmes Department,
IRT-SystemX

Quentin Rivette
Industrial Information
Security Officer, SNCF
Voyageurs, Rolling Stock

Yseult Garnier
Industrial Information
Security Officer,
SNCF Réseau

Jean Thersiquel
Head of Product
Security, Apsys-Airbus

Serge Van Themsche
VP Strategic Alliances,
Cylus

Dr Leonardo J. Valdivia
Professor of Engineering,
Panamerican University
Zapopan, Jalisco, Mexico

Christian Schlehuber
Head of IT Security,
DeutscheBahn Netz

Christophe Ponchel
Technical Coordinator,
Innovation Products,
Airbus

Sebastien Rummelhardt
Head of Digital Security
Red and Blue Teams,
Airbus

Selected quotes

“If the same importance is given to cybersecurity as to safety, then the mind-set of transport professionals would change, and they would see cybersecurity as a necessity and not as an extra.”

Dr Leonardo J. Valdivia,
Professor of Engineering, Panamerican University Zapopan, Jalisco, Mexico

“Our product portfolio encompasses everything from individual components to entire trains, and they all need to be resilient to cyber attacks.”

Thierry Renouf,
Cybersecurity Platform Manager, Alstom

“With digital trains, the number of cyber attacks and their effectiveness will increase, so we all collectively have to find countermeasures...We have entered an era of collective intelligence – we can’t fight cyber attacks without it.”

Gilles Desoblin,
Director, Strategy and Programmes Department, IRT-SystemX

“A software system is not something that is static... It’s a living product – the threats evolve, both because the system itself is evolving and because attackers find new ways to assault the system.”

Christophe Ponchel,
Technical Coordinator, Innovation Products, Airbus

Contents

Editorial 03

Experts in this issue 04

Selected quotes 05

Part one: Anticipate

INFOGRAPHIC
Railway systems, an emerging target for cyber criminals– Towards stronger regulations and standards 08

ANALYSIS
Cyber-secure mobility solutions are the only ones that will perform in the future 10

INSIGHT
Joint visions for cybersecurity collaboration 12

Part two: Develop & Deliver

INSIGHT
From risk analysis to cybersecurity architecture 14

ANALYSIS
Safety and security: orchestrating complementarity........ 17

CASE STUDY
REM Montreal 19

CASE STUDY
Tel Aviv, A flagship cybersecurity project in Middle East Africa........ 20

Part three: Operate & Maintain

INSIGHT
From awareness to expertise: cybersecurity, the other digital transformation 22

INSIGHT
Cybersecurity during maintenance of legacy train systems........ 23

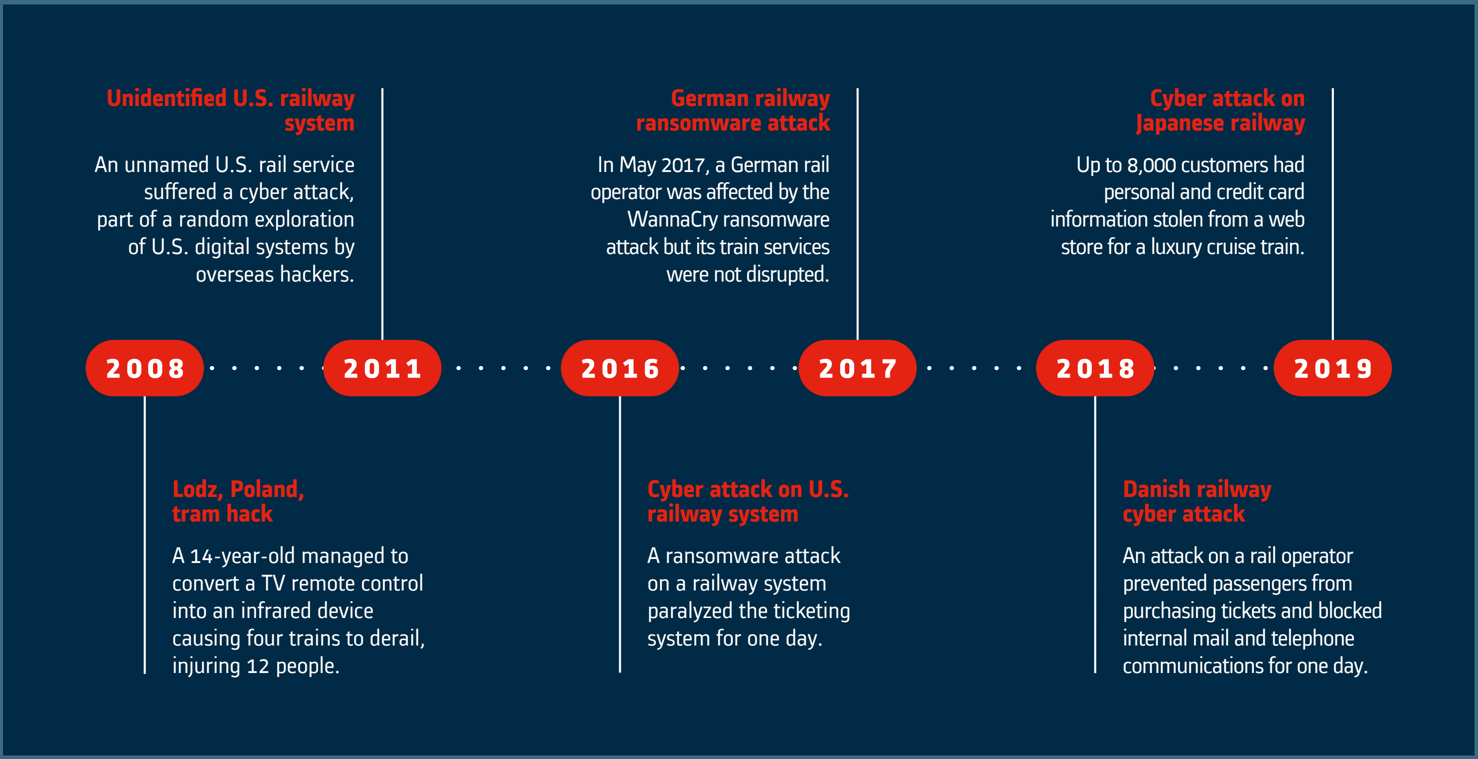
ANALYSIS
Cybersecurity is a continuous and permanent process 25

Part I

Anticipate

RAILWAY SYSTEMS, AN EMERGING TARGET FOR CYBER CRIMINALS

The rise of cyber threats on railway systems



2008

Lodz, Poland, tram hack

A 14-year-old managed to convert a TV remote control into an infrared device causing four trains to derail, injuring 12 people.

2011

Unidentified U.S. railway system

An unnamed U.S. rail service suffered a cyber attack, part of a random exploration of U.S. digital systems by overseas hackers.

2016

Cyber attack on U.S. railway system

A ransomware attack on a railway system paralyzed the ticketing system for one day.

2017

German railway ransomware attack

In May 2017, a German rail operator was affected by the WannaCry ransomware attack but its train services were not disrupted.

2018

Danish railway cyber attack

An attack on a rail operator prevented passengers from purchasing tickets and blocked internal mail and telephone communications for one day.

2019

Cyber attack on Japanese railway

Up to 8,000 customers had personal and credit card information stolen from a web store for a luxury cruise train.

TOWARDS STRONGER REGULATION

On track for a pan-European standard

Since February 2018, Alstom, along with several experts, has contributed to the CENELEC workgroup 26 to define a new European standard for cybersecurity railway application, which will apply to signalling, rolling stock and fixed installation.

NIST CSF-SP800 Series

Operational security requirements

Bundesamt für Sicherheit in der Informationstechnik

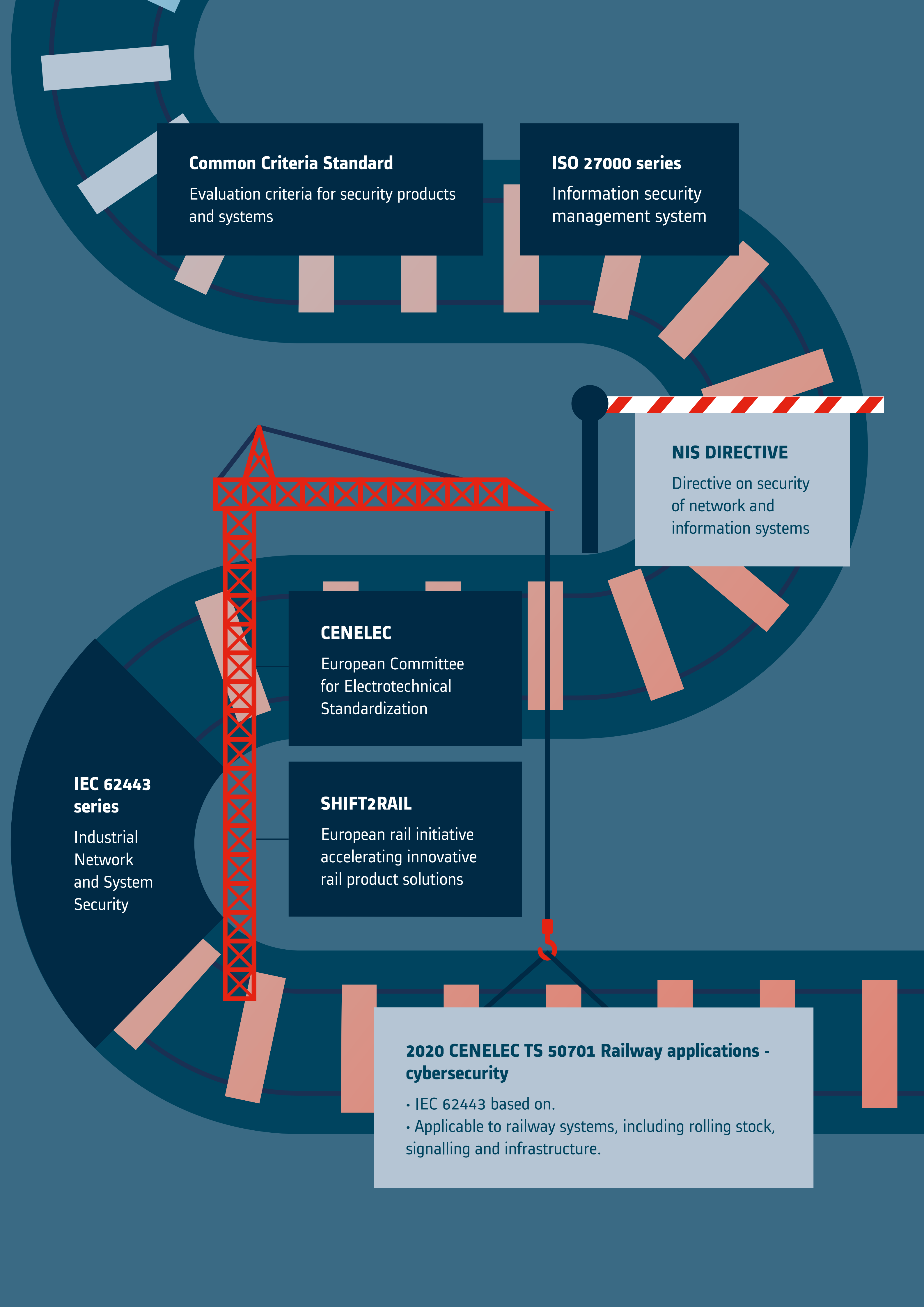
Protection of critical infrastructures; IT security-detailed measures

Department for Transport

Rail cybersecurity guidance to industry: cybersecurity assessements framework (CAF)

ANSSI

Industrial guide: detailed measures CSPN (criteria for first level evaluation)



Common Criteria Standard

Evaluation criteria for security products and systems

ISO 27000 series

Information security management system

NIS DIRECTIVE

Directive on security of network and information systems

CENELEC

European Committee for Electrotechnical Standardization

SHIFT2RAIL

European rail initiative accelerating innovative rail product solutions

IEC 62443 series

Industrial Network and System Security

2020 CENELEC TS 50701 Railway applications - cybersecurity

- IEC 62443 based on.
- Applicable to railway systems, including rolling stock, signalling and infrastructure.

Cyber-secure mobility solutions are the only ones that will perform in the future

Gilles Desoblin,
Director, Strategy and
Programmes Department,
IRT-SystemX

Quentin Rivette
Industrial Information
Security Officer, SNCF
Voyageurs, Rolling Stock

Yseult Garnier
Industrial Information
Security Officer,
SNCF Réseau

In a world that is increasingly connected and digital, cybersecurity is no longer simply an operational requirement – it is an economic necessity that is vital to the ongoing health of any business.

As the rail industry undergoes the transformation to a future in which digital technology plays a more important role, it will need to make cyber issues a central part of its strategy.

These will need to be addressed for three key aspects of the system – the command and control systems, which relate mainly to safety and signalling; rail traffic and operations, which focuses on keeping the trains running on schedule; and the corporate side of the business, which relates to the system's interaction with customers.

However, there is a discrepancy between the assets that railway operators are trying to protect – which can last for decades – and the nature of cyber threats, which evolve continuously. This creates challenges in ensuring that any updates to cyber defences do not compromise the safety or operational capabilities of the network.

Cyber defences need to be more robust than for other sectors because it is not just the risk of a data breach that has to be considered, but the safety of passengers and the health of critical infrastructure. At the same time, it is not realistic to protect everything, so operators need to prioritise protecting the most critical aspects of the system.

A large industrial company such as Alstom has many component suppliers, but Alstom is responsible for the end product. So how does it insure against the risk of a cyber attack that may come from a component provided by an external supplier?

It depends on the nature of the component and the technology involved, on legal and contractual issues, as well as what coverage insurers offer and at what cost, says Gilles Desoblin, Director of the Strategy and Programmes Department at IRT-SystemX.

Because the field is still relatively new, and because companies are often reluctant to reveal details of any attacks, insurers have limited historical data about cyber attacks, making it difficult for them to develop business models that can help protect the industry.

In a KPMG survey, 81% of respondents said that their companies had been compromised in the previous 24 months. At the same time, almost half (49%) said they had not invested in information security in the past 12 months.

> “We all collectively have to find counter measures, or we could face very big economic impacts.”
>
> Gilles Desoblin

For insurers to get an accurate picture of the cyber risks that the mobility sector faces, and how to price them so they can offer meaningful insurance products, they need data from companies that have faced attacks regarding the financial impact of those attacks, the time it took to recover from them and the best actions to take.

"The tricky point is to identify the role of each company in the value chain," he adds. "What is each interdependence between players and who is accountable for what? If a small or medium sized enterprise (SME) is providing digital PCs for Alstom that are integrated into a train, Alstom is accountable, but it has to be able to find out where the real weakness is."

SMEs are often targeted, not because they are a lucrative target, but because they offer an easier way into the systems of larger companies. Even if Alstom's cybersecurity awareness is mature, "in many SMEs there is basically no understanding of this kind of risk. SMEs are a weak point." A growing cyber risks insurance market would help to change this, Desoblin argues, with end-customers such as Alstom encouraging their SME suppliers to take out insurance, with premiums depending on the level of cyber maturity. "That could lead to cascading coverage throughout the value chain, which would help increase overall resilience to cyber attacks. Having insurance will make companies more aware of the risks and how to deal with them.

"With digital trains, the number of cyber attacks and their effectiveness will increase, so we all collectively have to find countermeasures, or we could face very big economic impacts. We have entered an era of collective intelligence – we can't fight cyber attacks without it," he adds. "Whatever your business model, you need to understand your vulnerabilities and weak points, identify the risks and cover them with insurance and make your suppliers more resilient."●

Operator Needs

For rail operators, the starting point for cybersecurity is a "secure by design" approach to the system's security architecture.

"The system must be resilient to malicious attacks but at the same time, legitimate users must be able to gain access easily," says Quentin Rivette, Industrial Information Security Officer at SNCF Voyageurs, Rolling Stock department. "Connections for on-board maintenance, communication between the train and trackside, and links between the train and passengers, are particularly important."

There must be a secure gateway between information technology and operating technology, adds Yseult Garnier, Industrial Information Security Officer at SNCF Réseau. At the same time, it is crucial to ensure that security measures do not compromise the efficient operation of the system.

Operators can prioritise their activities by taking a modular approach, splitting security systems and operational systems, and creating an inventory of cyber-critical assets, she says. Cyber-critical assets include equipment that links with devices or networks outside the system and those connected to the public.

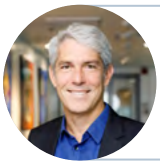
"These cyber-critical assets may have to be updated more regularly than trains or other equipment, so a strategy for doing that must be designed in from the start," Rivette adds.

While IoT technology is mostly used for collecting data from sensors at the moment, and cybersecurity needs are not often very high, in the future, more and more IoT will possess control and command characteristics so security will have to be increased, he points out.

Driverless trains will introduce new considerations, because the train's information systems will be making all the decisions with no human input. This introduces a new level of risk analysis and security that must be installed. The "attack surface" is bigger than before, Garnier says, as trains and infastructure systems have more IT components, and there are more interconnections between different networks to ensure that trains and systems run efficiently. "That creates more critical points that must be taken into account."

Joint visions for cybersecurity collaboration

Jean Thersiquel
Head of Product Security, Apsys-Airbus



Serge Van Themsche
VP Strategic Alliances, Cylus

Businesses across the mobility industry have the same objectives – to ensure their products are consistently fit for service and can safely transport goods and people from point A to point B.

When it comes to cybersecurity, it's key that businesses in the sector work closely not just with each other but with external experts, to ensure end-to-end protection against cyber risks. It only takes one weak link to open a door to networks and products, therefore it's imperative to share knowledge and expertise.

When Alstom began to put cybersecurity at the heart of its product development, it looked towards aerospace for guidance. Companies working in this sector have been dealing with high levels of automation and critical onboard electronic devices for many years now and it's become second nature to design aircraft with cybersecurity in mind. Alstom understood that it could learn much from the work already done in this sector and in 2017 it reached out to industry leader Airbus.

By taking on board the lessons Airbus had already learnt, the company was able to quickly develop products that were secure by design. This partnership was also beneficial for Airbus, as the company was able to benchmark its way of working by seeing its solutions implemented in a different environment.

"The objective was to put cybersecurity into the DNA of the company," says Jean Thersiquel, Head of the Product Security Business Unit at Apsys-Airbus. "We've worked closely with Alstom on risk analysis, developing key security objectives and system design. These are passed onto the suppliers and when the products are delivered, we worked together on auditing and penetration testing."

In order to lay the groundwork for strong cybersecurity, stakeholders must complement each other's core competencies. One actor cannot do everything; a full ecosystem is needed to design and deliver safety critical systems.

While Alstom is first and foremost a mobility company, it has also looked to collaborate with organisations that could bring different strengths to the table. Therefore, it joined forces with Israeli-based Cylus, experts in cybersecurity in the rail industry, to embed cybersecurity within its safety critical systems, such as signalling and control networks, both wayside and onboard.

"Real added value comes from understanding Alstom's specific protocols to find the best protection from cyber attacks. For proprietary technologies, working alone takes longer, uses more resources and would probably be less secure," says Serge Van Themsche, VP of Strategic Partnerships at Cylus. "Standardized technologies such as ERTMS or GSM-R are more straightforward, as our various deployments show."

Airbus and Alstom have now been working closely for several years and their shared vision has led to a variety of successful initiatives. Together they've defined the business' four security level requirements and created dedicated documents that are shared with suppliers, but a lot of work has also gone into bringing more partners to the table.

"We started with a one-to-one partnership, but now the objective is to get every mobility actor to the table – the big guys, but also the small, new players manufacturing UAVs, autonomous cars etc," says Thersiquel. "We've launched an initiative called Security for the Future. Our goal is to grow a diverse community of companies in the mobility industry that have a common commitment to protect their products against cybersecurity threats. This will enable collaboration and sharing of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all. There's no competition in cybersecurity – we all face the same threats."●

Part II

Develop & Deliver

From risk analysis to cybersecurity architecture

Serge Benoliel
Cybersecurity Management, Office Manager, Alstom

Jean-François Gillot
Cybersecurity Platform Manager, Alstom

Thierry Renouf
Cybersecurity Platform Manager, Alstom

Baptiste Fouques
Cyber Defense Expert for systems and core frameworks, Alstom

When it comes to developing new projects for railways, it is vital that cybersecurity is considered and integrated into the evolution of the design process from its conception, alongside the engineering aspects of a project.

This presents a number of challenges, not least because computer systems and railway systems are incompatible in several ways, starting with product lifetimes, which are three to five years for IT and 10 to 20 years for railway rolling stock and equipment. In addition, while cybersecurity measures can be constantly improved and upgraded, railway hardware cannot be easily altered, and since safety is the top priority, any changes must be exhaustively tested before introduction.

There also comes a point in the development process of railway projects when a "design freeze" is implemented. For the cybersecurity process, this is a key moment. Cyber-defence measures need to be built into the system as much as possible before this point because once the design freeze is in place, it is very difficult and extremely costly to make changes, and the client is liable for these expenses.

Due to this deadline, it is vital to start thinking about cybersecurity right at the start of the project. Every project, from building a new metro line to launching a new type of train or replacing out-dated signalling systems, has a cybersecurity manager who is the single point of contact for cybersecurity concerns. This manager ensures that everyone involved knows what the security requirements are for the project, which are defined in the cybersecurity management plan.

The first step to creating a cyber-secure railway system is to carry out a comprehensive risk analysis to identify the weaknesses in the system, how likely attacks are to occur and

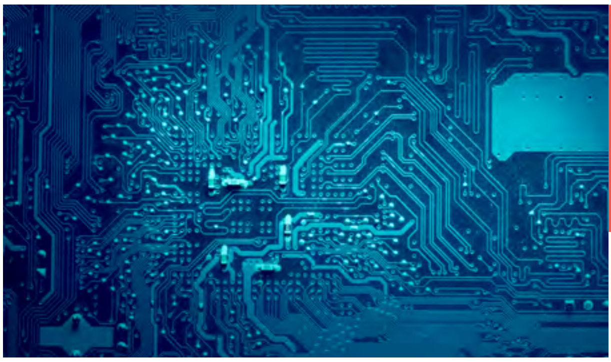
> "[The framework] enables us to demonstrate to our clients, through penetration tests, that we have installed measures that provide a certain level of resilience against agreed risks and carry out tests to show that these measures work"
>
> Serge Benoliel

how serious they will be if they do happen. The key risks are physical harm to people and the environment, and financial damages from services being brought to a standstill.

If the risk exceeds a certain threshold, then the cybersecurity team knows it must introduce defensive measures to limit the possibility of cyber attacks. These differ across the system – for metro system rolling stock, for example, it is very important to minimise the length of any disruption because so many people will be affected, while for a freight train on a single, long-distance line with few trains running, there is more time to deal with any problems that arise.

However, risk analysis is only the first step and it must be complemented by a robust cybersecurity architecture framework. For each risk, from building a new line to launching a new type of train or replacing old signalling systems, this architecture is defined by what you want to protect, the severity of the risks and where they come from – the internal system, inside the supply chain or from external threats.

The architecture framework helps to define all the cybersecurity measures that will be needed and how to install, operate and maintain a secure system – information that must be passed on to the customer and its employees through comprehensive training programmes.



“The framework also provides a benchmark against which the defences can be measured,” says Serge Benoliel, manager of the Cybersecurity Management Office. “It enables us to demonstrate to our clients, through penetration tests, that we have installed measures that provide a certain level of resilience against agreed risks and carry out tests to show that these measures work. Having done this, we present a Cybersecurity Accomplishment Summary.”

Since threats evolve continuously and very rapidly, it is important that the system can identify and stop future unfamiliar threats. This is done by constantly monitoring vulnerabilities, as cybersecurity is a permanent but continuous process, not a static task to be completed.●

Ensuring Product Resilience

“Our product portfolio encompasses everything from individual components to entire trains, and they all need to be resilient to cyber attacks,” says Thierry Renouf, Cybersecurity Platform Manager. Exactly how resilient depends on the product’s role in the system, but every component has some level of cybersecurity built in, from physical security, such as locks and cameras, to encryption, partitioning, backup and restoration strategies for critical data, he explains.

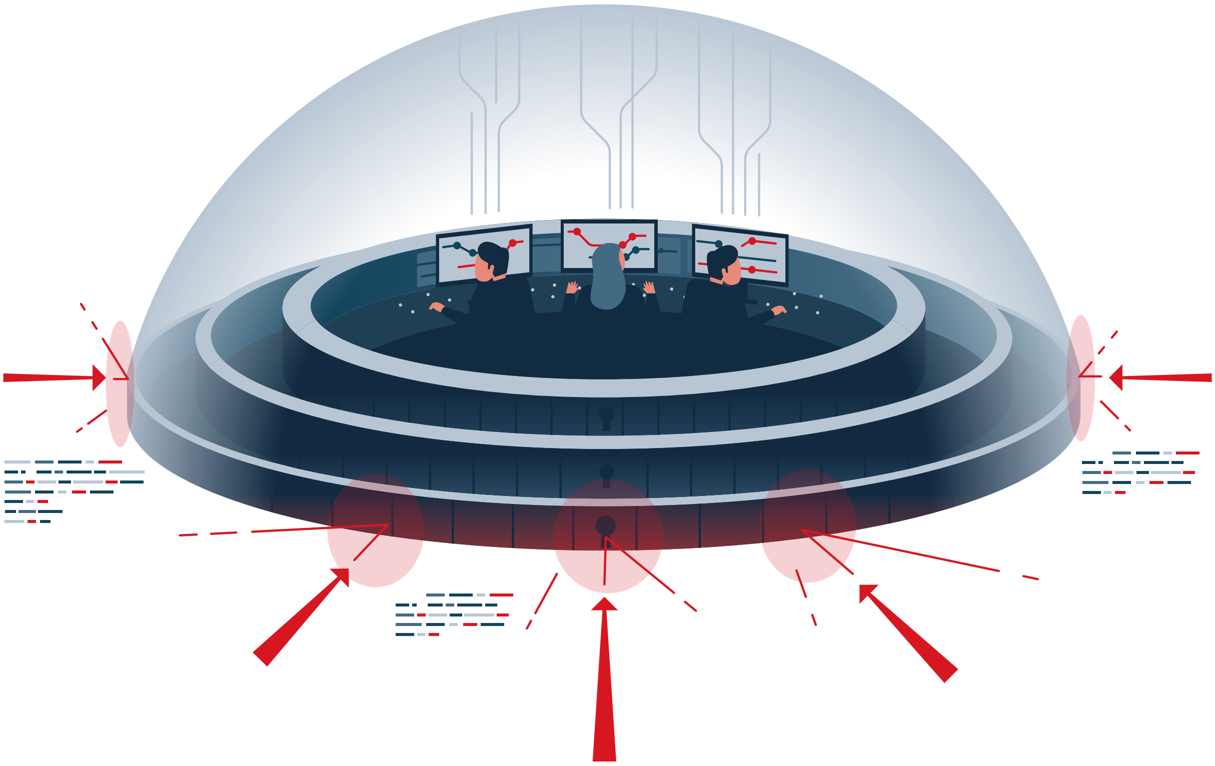
“The first step is to define the level of robustness required – a laptop can be very exposed to external threats, for example, while a signal line deep inside the system has several layers of protection surrounding it, including physical security, perimeter security, intranet security, host security, application security and data security,” he says. Targeted security measures are then created once the possible cyber attack scenarios have been defined.

There are two different approaches – one for legacy products designed years ago that were not built with external security threats in mind and where mitigation is key, and another for newer products designed with built-in cybersecurity measures.

The next step is to look at the component’s position within the system, adds Baptiste Fouques, Cyber Defense expert for systems and core frameworks. Components that are critical for and have a lot of communication with the system are extremely robust. “We are adding detection capabilities all the time and have reached a situation where each time a component is engaged, a signal is sent to the control centre so the operator knows what is happening on the system,” he says.

This improved resilience requires a change of mind-set for both buyers and final users. Aspects of the operating system that were transparent in the past must now be managed properly to ensure compliance with cybersecurity protocols.

The future proof solutions of secure railway technology



The future-proof pillars of a secure railway solution

The security architecture is based on the principle of defence in depth, similar to a fortified castle, with all solutions following a number of golden rules. "Cybersecurity architecture helps to ensure that protections are put in place at the most efficient locations, using dedicated, scaleable devices" says Jean-Francois Gillot, Cybersecurity Platform Manager.

The system has multiple layers of defence and the most critical assets – those most at risk of attack and those where an attack will have the biggest impact – are placed at the core of the system so there are several barriers between them and any potential attackers. If one part of the system is breached, the next layer creates time to perform any updates so the system remains resilient even if one layer of defence is broken, and the breach would be detected and recovered before any harm actually happens.

One key principle is to separate safety and security so that when cybersecurity measures are updated, which happens frequently, the impact on core safety devices is limited. As much as possible standard IT cybersecurity products should be used, because they are standard, proven technology.

The key is to minimise the impact on the company's operations and the cost required to defend against cyber attacks. Risk analysis helps to identify issues such as the difficulty of an attack, the window of opportunity, the knowledge and skills required and whether specific equipment is required.

The idea is not to create a vault for every electronic device but to limit cybersecurity to what is required. The more a product is exposed, the greater the level of robustness that is required. Each time a user enters a new protected zone, there are new barriers and scrutiny in place.

Safety and cybersecurity: orchestrating complementarity

Dr Leonardo J. Valdivia
Professor of Engineering,
Panamerican University
Zapopan, Jalisco, Mexico

Dr Leonardo J. Valdivia, a cybersecurity and safety expert in the Faculty of Engineering at the Panamerican University in Zapopan, Jalisco, Mexico, shares insight about how the synchronisation of safety and cybersecurity can help safeguard transport systems.

The transport industry has been focused on safety for generations – the safety of passengers and staff, after all, is crucial to ensuring efficiency, profitability and reputational integrity. However, the shift to computer-based technologies means there is a need to refocus attention on both safety and cybersecurity, while ensuring that neither compromises the other.

Safety is the protection of passengers and systems from unintended harm, while security is the protection of people and infrastructure against intended harm. Safety and cybersecurity thus have different but inherently linked lifecycles. With safety, once something is proven, it's often unnecessary to change it. However, when it comes to cybersecurity, systems need to be updated regularly to take in corrective patches.

"Cybersecurity is relatively new compared with safety – this is why safety always takes centre stage," says Dr Valdivia. "However, more and more mechanical tasks are being replaced with computers and automatic systems. Railway infrastructure, for example, is broadly distributed and it is now largely based on computers."

There is a critical need to ensure transport operators, their staff and suppliers are aware of the relationship between safety and cybersecurity. "I think the first step is to educate people about the difference between safety and security," says Dr Valdivia. "It is amazing how many people working in the transport industry do not know the difference.

"Professionals who develop safety-critical modules are often not aware of security issues, so if security techniques are implemented, this is usually done after the development of the system or module. Instead, we need to create procedures to ensure security is included in the development cycle.

"If the same importance is given to cybersecurity as to safety, then the mind-set of transport professionals would change, and they would see cybersecurity as a necessity and not as an extra."

Developing standards and procedures

It is possible to apply pure safety or pure cybersecurity to a system, says Dr Valdivia, but the real issue concerns the interaction between the two. Manufacturers must apply for safety certification for each product so therefore they prioritize safety over security. "Each company defines the degree of security that it wants to implement. This is why a system that is safety certified can be considered safe but not secure. However, safety and security share the same objective of reducing and – if possible – eliminating risk, so they should work together."

> "Cybersecurity is relatively new compared with safety – this is why safety always takes centre stage."

The development of dual cybersecurity-safety standards in transport systems are in their infancy. The IEC 62443 Security for Industrial Automation and Control Systems standard is intended to ensure systems are designed to minimize cyber threats, but this general standard has not been designed for any particular industry.

"This standard is used in transport, but it does not take into consideration the entire transport infrastructure, which means it often leaves gaps," says Dr Valdivia. "Another issue is that solutions with generic standards are not very flexible – and it is very difficult to implement the same solution in different modules."

Whereas safety risks are systematic and can be statistically proven – for example, based on lives lost, efficiency or train delays – cybersecurity risks are less predictable. While it is possible to run risk analyses on existing threats and vulnerabilities, predicting future threats – and how they might impact safety – is more difficult. Having procedures in place that outline how to respond safely to the consequences of a cyber attack is therefore crucial.

It is also necessary to develop flexible systems that can be updated continuously when new threats arise. However, this in itself poses fresh challenges. "Any hardware or software that performs safety critical functions needs to be safety certified. If security and safety modules are integrated, it is very difficult to achieve that safety certification as security modules are not designed with respect to safety standards," says Dr Valdivia.

"Even if the safety certification is achieved for a solution that includes a security system, there is another issue in that new cyber threats appear daily. Security modules therefore need to be updated regularly to ensure protection. If any change is applied to a safety certified system, it must be certified again. Therefore, it is not feasible to certify for safety each time a security module is updated."

Even so, transport suppliers are starting to become more aware of security issues and are beginning to boost security in instances where a solution does not affect safety certification. However, as no regulation currently defines safety and security integration, most companies are implementing in-house solutions, generally in line with IEC 62443.

The issue of cyber patches again highlights one important difference between the demands of safety and cybersecurity. Patches – rarely used to ensure safety – are vital to cybersecurity.

Dr Valdivia says testing new patches and cyber solutions can be problematic – especially in systems that are already operational – because most transport networks are not designed with cybersecurity in mind. Again, this reiterates the need to change workflows to ensure both safety and security are addressed at the developmental stage of all new systems, software and equipment.

"Safety is a widespread and familiar topic in railways, but some organisations and governments remain unaware of the importance of improving security problems," says Dr Valdivia. "With the extensive use of communications in critical systems, security must be considered to reduce risks. If safety and security are considered together at the beginning of the development cycle, it is possible to identify the risks to which the system is exposed at an earlier stage. The protection priorities can then be defined to focus efforts in the most important areas."●

Case Study:
REM Montreal

Carlos Galan Arnillas
REM Project
Cybersecurity Manager,
Alstom

In April 2018, Alstom, in partnership with SNC-Lavalin, a Canadian company, won a €1.8bn contract to provide an automatic, driverless light metro system for the Réseau express métropolitain (REM) project in Montreal, Canada.

REM, a 67 km metro network with 26 stations, is due to open its first section by the end of 2021. The network will link a number of strategic locations in the city, including the central train station and, eventually, the Pierre Elliott Trudeau International Airport.

Due to the many technical services involved, it is one of Alstom's most ambitious projects according to Carlos Galan Arnillas, the project's cybersecurity manager. "The consortium is supplying the rolling stock, signalling equipment with the communications-based train control (CBTC) system, control centre solutions, platform screen doors and 30 years of operations and maintenance services. It will also be responsible for train and system integration tests and depot equipment supply for train maintenance."

Galan oversees the implementation of the cybersecurity processes and helps those in charge of the various systems to incorporate cybersecurity into their work. Being responsible for so many different aspects of the project has advantages and disadvantages, he says. "It means that we are the masters of our own cybersecurity and it enables us to take a holistic approach to the issue. Since they are all Alstom systems, it is easier to identify the points where we need more protection, and we have more freedom to implement our defence in depth."

The challenge, however, is the increase in follow-up and co-ordination required to align so many different aspects of the project. Since Alstom's cybersecurity strategy is based on thorough defence, it does not focus on a single main point of protection, he says. "We focus on different layers of defence and every layer has its own importance, from the process and policies to be applied to data protection technical measures, including the physical barriers that will be put in place."

He also highlights the importance of putting perimeter protection and network segregation in place, for instance through what is known in the cybersecurity world as a 'demilitarized zone' between internal and external networks. This protects industrial networks such as the CBTC system from attacks on administrative networks or through the passenger Wi-Fi system.

Alstom uses IEC 62443, a standard for the secure development of products used in industrial automation and control systems, as its preferred cybersecurity framework for rail applications. But when it comes to cybersecurity, "it's not all about full compliance to one set of standards, which is what happens in other areas," Galan says. "We know it's a moving scenario in cyber-protection, and at the same time the systems are going to be in operation for more than 30 years so we have to have the flexibility to adapt."

Since cybersecurity is a relatively new concern, it can be challenging to work quickly and maintain a firm schedule when there remains a lot of inertia in regard to old habits. Cybersecurity adds more procedures to already complicated projects, creating new challenges at every stage.

However, staff are keen to understand the issues of cybersecurity and are interested in learning how they can participate in its development. To encourage this engagement and facilitate cybersecurity adoption, Alstom provides internal training with the ultimate goal of making every project more cyber secure.●

Case Study:
Tel Aviv, a flagship cybersecurity project in Middle East Africa

Sangeeta Chomal
Cybersecurity Leader
MEA Region, Alstom

Cybersecurity has become of paramount importance to the Middle East due to the increase in cyber attacks on critical business infrastructure, as well as the region's geopolitical climate.

As the risk of cybercrime grew, many public and private sector entities began to include explicit cybersecurity requirements in their requests for tenders. It is unsurprising then that cybersecurity is at the heart of the Tel Aviv Red Line Project.

The Red Line will be the inaugural light rail line of the Tel Aviv Metropolitan Mass Transit System, which promises to transform the city by bringing an end to the chronic traffic congestion that plagues its roads. The Red Line is the first light rail line to be operated in the Tel Aviv metropolitan area and will operate as a high frequency rail transit system with a blend of street running Train Units at grade and underground metros. The first of three lines, the 24 km Red Line will be the backbone of the mass transit system with 34 stations. When opened, it is expected to transport approximately 200,000 passengers every day.

Due to tensions in the region, state-owned NTA believes this light rail network is at higher risk of cyber attacks than comparable rail operations in other countries and Israel's National Cybersecurity Directory (INCD) has classified it as critical infrastructure. To ensure its security, the project includes almost 600 individual cybersecurity requirements covering the entire cybersecurity gamut, from authentication, identification and network security through to data security, physical security and monitoring.

Alstom was awarded the contract to design the Red Line's Signalling and Train control and Shift Management systems. It has also been contracted to maintain these systems for a period of 10 years, with the option to extend for a further six. A key part of its cybersecurity remit was to ensure the integrity of the signalling communication network, which is the heart of the Signalling and Train control system. Considered a closed network on its own, for this project the signalling communication network needs to interface with several others, supplied by a variety of contractors. Because of their roles, many of these networks need to be open to communicate with external environments such as web applications, creating entry points that must be secured.

Alstom is implementing multi-layered and zone-based network architecture based on IEC 62443 to ensure strong separation of applicable core networks. Security zones are defined based on criticality and impact factors. The connections among the zones include strong security measures in order to control their access and prevent the spreading of attacks by acting as a shield for other systems in the network and protect the integrity and confidentiality of communications. One of these measures includes using physical unidirectional diodes. These types of perimeter security are more secure than many software solutions, where vulnerabilities can appear for hackers to exploit. The introduction of the diodes allows for data interchange to be restricted as necessary between the critical system and other networks with varying levels of security.

Alstom is working on the detailed design phase of the Red Line Project. At the time of testing and commissioning, the security of the system will be audited and face penetration tests by local cybersecurity companies and state agencies to ensure the network is fit for purpose.

Part III

Operate & Maintain

From awareness to expertise: cybersecurity, the other digital transformation

Christian Schlehuber
Head of IT Security,
DeutscheBahn Netz

When organisations talk about cybersecurity, they often focus on the technical and strategic aspects of ensuring systems are secure. But what about the human role?

The rail industry has always had a strong security culture. In the past, the focus was on the direct protection of passengers by following strict rules around the operation and maintenance of trains, stations and tracks. This of course is still key, but the arrival of the digital era has brought with it an increase in risks and threats from cyber attacks.

Thankfully this historical security ethos works to the sector's benefit. Rail industry professionals are already aware that systems and procedures are there to protect. Therefore, the groundwork is already in place to introduce staff to new cybersecurity-focused guidelines and processes.

Change is already underway. System architects, for example, must now consider cybersecurity from the start of every project. And these changes will have a domino effect throughout the industry, touching everyone from the operators through to the maintainers.

"Everyone is going to have to think about security more," says Christian Schlehuber, who's responsible for IT security of the operational technologies at Deutsche Bahn. "Operators won't be able to log into a workstation using a group password, for example. They'll have their own accounts and need to follow certain procedures. Maintainers will not only need to do functional checks of equipment, they'll also need to ensure systems have not been compromised or tampered with," he points out.

Then there's the very human dimension of cyber risks. Human error was the cause of roughly 90% of data breaches reported to the Information Commissioner's Office (ICO) between 2017 and 2018. Even with the best cybersecurity systems in place, it only takes one human mistake to open a system to attack. Therefore it's imperative that the industry implements a strong cybersecurity culture and training regime. "People are the weak link," Schlehuber says. "We can isolate systems as much as possible but if someone sees a USB port and just decides to charge their phone, then there's a risk.

"We once discovered a malware infection caused by someone simply deciding to bypass a firewall because it took too much time to set up new protocols! Training is needed to help people see the implications of their actions from a security standpoint."

This move towards a more cybersecurity-focused culture is already taking place – the 2019 Cybersecurity Breaches Survey reported that around three-quarters of businesses (78%) say that cybersecurity is a high priority for their organisation's senior management.

However, there's still much work to be done, as the report also highlighted that just 27% of businesses had staff attend internal or external training, including seminars or conferences on cybersecurity, in the previous 12 months.

"Basic cyber risk training is the first step, but organisations need to go further – people need to go for cybersecurity training several times a year," says Schlehuber. "As well as awareness, these courses need to cover current trends, so people know where the latest risks lie."

He adds that people also need to know where to go with their questions. "Communication is key. People need to know who is responsible for cybersecurity within the business so they can go to them with queries or report strange occurrences. On the flipside, cybersecurity teams need to ensure they respond to questions promptly and take every report seriously.

"A good way to bring a cybersecurity culture into an organisation is via the 'security ambassador' principle," he continues. "This is when every team and product has a security ambassador that gets specialised training. They are then the primary security contact for that team or product, meaning the barrier to contact is very low."●

Cybersecurity during maintenance of legacy railway systems

Jean-François Gillot
Cybersecurity
Platform Manager
Alstom

Unlike in the consumer market, where technology and devices become obsolete and need replacing regularly, transport systems are heavily dependent on legacy infrastructure that requires management over a long period of time.

Managing the cybersecurity of these legacy systems is a key challenge for transport operators. There are three ways operators can manage the cybersecurity of legacy systems:

1. Renew the entire system while integrating a brand new cyber-ready system
2. Upgrade the existing system to include more cybersecurity
3. If neither of the two ways apply, address cybersecurity during maintenance operations

Choosing the best approach for a system

When a new train system is designed, a thorough risk analysis is conducted. This paves the way for security controls to protect the system from cyber attacks across its lifecycle, including through upgrades and maintenance. The risk analysis allows robust architectures to be designed in line with best practices.

However, designing a new system from scratch is a rare luxury. As a result, networks comprise both ageing and new rolling stock, with control and signalling based on a broad range of solutions. This means older components may have been installed without security requirements.

“Nevertheless, threats to these systems remain and legacy systems must improve their defences accordingly by chosing the best protection”, says Jean-François Gillot, Cybersecurity Platform Manager at Alstom, because these infrastructures are critical.

The first step towards addressing cybersecurity in this case it to create an inventory of the system in its current condition, rather than what’s on record from commissioning. An analysis must then be conducted to identify the main risks and to implement security controls to reduce them.

“This is done by a ‘cybersecurity upgrade’ of the system,” says Mr Gillot. “These controls are similar to ones conducted on a new system – implementing technical, procedural or organisational controls – but they can often be less integrated and efficient for risk reduction because the controls are introduced into a system that was not designed to accommodate them.” Even so, a ‘cybersecurity upgrade’ is always possible and solutions exist to manage critical risks.

The decision to upgrade is the responsibility of the system owner, who may choose a step-by-step approach after a mandatory system risk analysis, says Mr Gillot. “Controls can be implemented progressively depending on operational and budget constraints.”

When the upgrade is not possible, a minimal approach has to be done. It focuses only on preserving the system’s cybersecurity and monitoring its ongoing health, through threat monitoring and vulnerability scan so the level of risk can be reduced.

The role of maintenance

Maintenance can handle several broad security operations. “First, we have all the activities for maintaining the system in operational conditions, such as daily maintenance for wear and tear, corrective and preventive maintenance, and maintenance after failures and accidents. There are also large and small overhauls conducted during the lifetime of rolling stock,” says Mr Gillot.

Secondly, maintenance often leads to small evolutions of a system. This may include replacing obsolete products,

integrating and deploying new versions of software. This includes software updates to remove vulnerabilities, antivirus database updates and the management of access rights.

Maintenance operations are critical for cybersecurity because they can be an entry point for cyber attacks. “It is very important to make sure that daily maintenance does not endanger the cybersecurity of the system – for example, by opening barriers or creating unsecured communication channels. Connections with compromised maintenance terminals can also risk infecting core devices with malwares,” says Mr Gillot.

Industrial maintenance means can be a major vector for train system contamination, with cyber attacks potentially freezing train maintenance depot operations. This can have a knock-on effect that results in fleet unavailability, which is key to maintenance operation security, especially on systems that have poor cyber defences.

Securing maintenance operations

“A risk analysis should be performed on maintenance activities by themselves in the context of the maintained system, with its weakness and its strengths,” says Mr Gillot. Adapted technical and organisational security controls can then be specially designed to manage maintenance activities without inadvertently having a detrimental effect on the maintained system. Although this approach isn’t fool-proof, it lays a foundation to ensure that maintenance operations do not contradictorily degrade the cybersecurity of their own systems. “It will also provide the opportunity to set up security supervision routines for the maintained system and allow it to better detect attacks, increasing the chances of containment,” says Mr Gillot.

This analysis also provides the maintainer with knowledge of its own vulnerabilities that may affect its capacity to deliver fully operational trains on time.●

Checklist for Secure Maintenance

1. Ensure a maintenance team member is responsible for cybersecurity
2. Do an inventory of all computers used for maintenance, including terminals, industrial systems, test benches and maintenance tools
3. Raise awareness of security risk among operational teams and train teams in line with best practices
4. Undertake hardening of the maintenance organisation’s processes
5. Set up secure mobile media usage policies and procedures
6. Set up procedures to check software integrity before installation
7. Review physical security in the light of cybersecurity risk (set the level of protection of each area in line with associated cyber event impact)
8. Prepare and regularly test cyber incident management procedures
9. Undertake hardening of the maintenance organisation’s assets
10. Harden all maintenance terminals and keep them up to date
11. Map all maintenance networks and their connections with the ‘external world’. Secure all connections
12. Manage all access (logins/passwords) for assets used for maintenance
13. Do regular PenTests on the organisation’s assets
14. Insert cybersecurity management clauses into third party contracts
15. Set up business continuity plans in line with cyber risks on maintenance assets

Cybersecurity is an ongoing challenge for transport operators. Ideally, systems have to integrate it by design, or through cybersecurity upgrades. At minimum, with good management and robust cyber policies and procedures on maintenance, it is possible to bring a primary level of safeguards to train systems.

Cybersecurity is a continuous and permanent process

Christophe Ponchel
Technical Coordinator,
Innovation Products,
Airbus

Sebastien Rummelhardt
Head of Digital Security
Red and Blue Teams,
Airbus

Cybersecurity is not a one-off job that occurs at the start of a project – it is an ever-changing process because the technology that you want to protect is always evolving.

"A software system is not something that is static," says Christophe Ponchel, technical co-ordinator for innovation products at Airbus. "It evolves through the installation of upgrades and patches over its entire life cycle. It's a living product – the threats evolve, both because the system itself is evolving and because attackers find new ways to assault the system."

The starting point of the cybersecurity process is to carry out a risk analysis, he adds. "You have to know what services are crucial for your organisation and the risks those services face. You need to know what is inside your equipment and what role it plays in your system."

For a railway operator, because areas such as power control, level crossing automation and the signalling system are very important, the operator will take extra care to identify and seek to reduce any vulnerabilities. "If something goes wrong, you could lose money, you could lose customers but also, in a really serious incident there could be casualties, so it's really important that you know what to prioritise," he stresses.

Once you know the technical aspects that these services rely on, you need to determine your level of vulnerability. This "vulnerability watch" enables the organization to find out how secure its systems are. "You need to continuously assess the vulnerability of your systems every day. It is a huge and tedious task. You either have a team dedicated to this task or you hire in an external team. They won't have time to do anything else – it's a full-time job."

The first step involves the company sharing with the vulnerability watch service the list of technical assets whose vulnerability it wants to examine, along with their operating system, software layer, network architecture and asset dependencies. This is done annually or monthly depending on the company's requirements and capabilities.

Then the vulnerability watch team, on a daily basis, looks for issues relevant to the system being examined that have been identified by vulnerability bulletins.

Once a vulnerability is discovered, you need to assess what effect it will have on your system. Some vulnerabilities can destroy assets, some compromise the system, and some can result in lost information. Operators will want to take extra care with vulnerabilities that can be remotely accessed because of the damage that an attacker may cause from outside the system. The team then recommends actions to remediate the vulnerability.

But, says Ponchel, in most cases, the remedies are not that complicated. "There are three solutions that cover most eventualities," he explains. "You can apply patches to the

> "Sometimes you can't prevent an attack, but if you can detect it, you can either block the attack or cut communications to lock them out of the system."
>
> Christophe Ponchel

system, such as the latest OS or application version upgrade, or a dedicated bug fix patch. You can upgrade the configuration on areas such as servers and control systems to remove the vulnerability – for example change the default password to a more complex one – and you can simply warn users that there is a vulnerability in the system. Most of the time, that will be enough."

However, he adds: "You may find that the simple fix is refused by operational or business managers because it may affect sensitive or critical systems, making it difficult to apply a patch. You have to balance the risk of the attack against the risk of the solution."

Part of the development process for any product is to run basic automated tests every night on the system to check that it performs as expected. These procedures now need to include tests to prove that the system is resilient to cyber attacks.

These can include "black box" penetration tests, which examine the risks from an outside attacker who knows nothing about the system, and "white box" tests, which consider the dangers from insiders who know the system well. "Obviously, the better you know the system, the deeper you can go as an attacker," Ponchel points out. "Sometimes you can't prevent an attack, but if you can detect it, you can either block the attack or cut communications to lock them out of the system."

Another weapon is cyber threat intelligence, which is like a vulnerability watch but at a higher level. Carried out either in response to a specific attack such as Wannacry or periodically, it is about finding out what other relevant companies or assets have been targeted around the world. "Knowing what systems are being attacked elsewhere – on other railway systems, for example – helps you because you know you need to focus your defences on those systems."

Although the technical work of dealing with cyber threats is carried out by technical staff, when it comes to defining the acceptable level of risk, this is done by the company's management. "Managers have to balance the cost of countermeasures against the cost of the risk. Sometimes the countermeasure is to buy an insurance policy. The solution to technological risks is not always technological."●

Managing Crises —it's all about time

Cyber attacks are a fact of life for large multinational companies. "Some attackers are interested in intellectual property, others in commercial information such as prices, while some are looking to disrupt operations," explains Sebastien Rummelhardt, head of Airbus Digital Security Red and Blue teams.

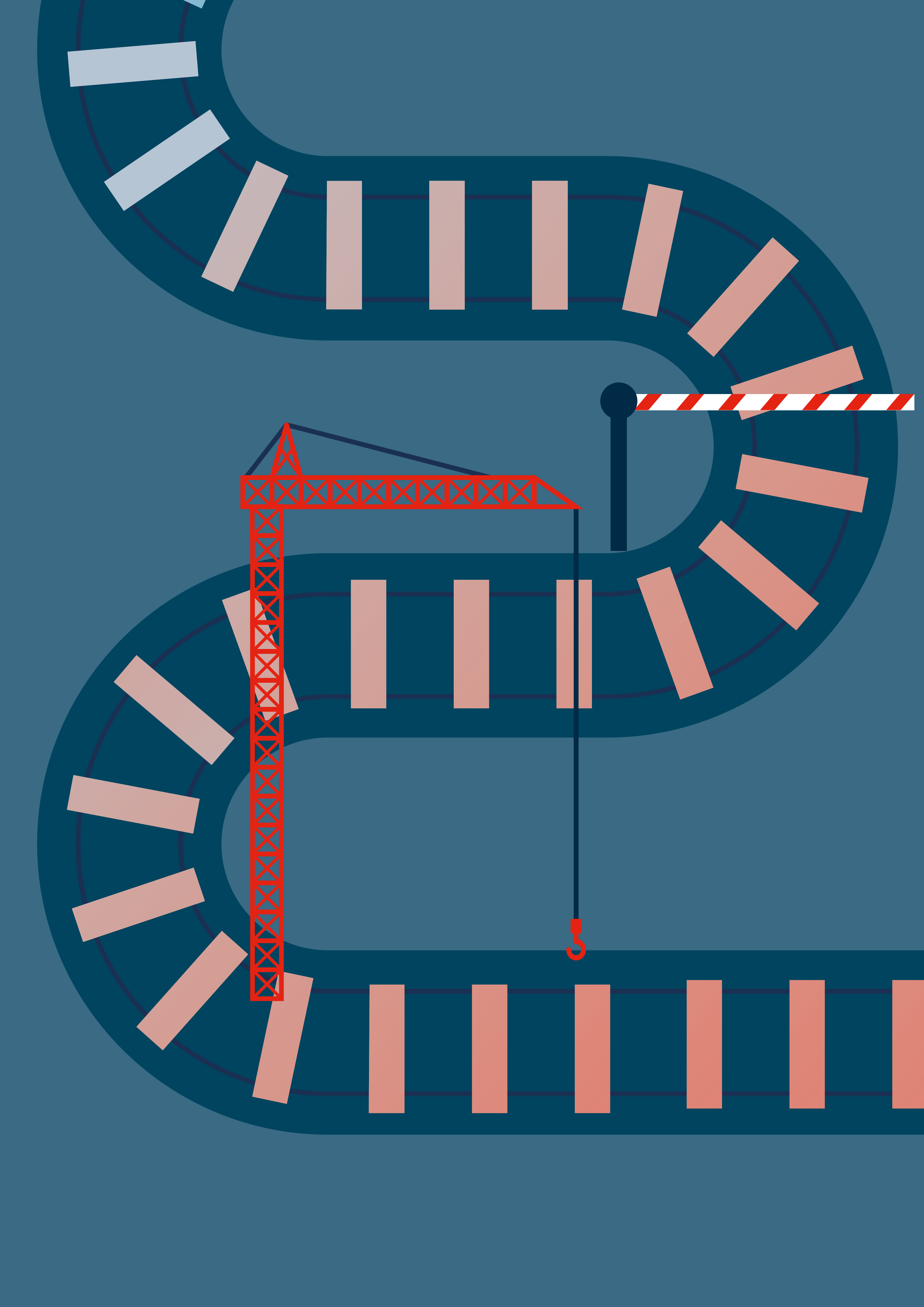
There are two ways the company discovers an attack has occurred, he says, either from external sources such as a national security agency or partner, or internally, when the Security Operating Centre notifies the team of suspicious activity.

"When we receive a notification, if it's a crisis, we jump into 'restricted crisis' mode. At some point we have to decide whether others apart from the IT department need to be involved," he says.

"If necessary, we launch a crisis management team. Once the investigations team have told us how, when and what happened, the workload gradually shifts to mitigation and remediation. If the attack came through a channel that was easy to penetrate, we prepare countermeasures – limiting opportunities to enter the system or the amount of information that can be removed," Rummelhardt adds.

Rummelhardt runs Airbus's Red and Blue teams – the Red team is 'offensive', looking for weaknesses in cyber defences, while the Blue team is on the defence, looking to repel cyber attacks.

"Although similar skills are required, daily life is extremely different for the two teams. There is a sense of urgency in Blue because they need to be on alert 24/7, while Red might be mimicking a skilled attack, impersonating a specific attacker and developing attacks aimed at training and improving the detection capabilities of Blue."



Alstom
48, rue Albert Dhalenne
93 482 Saint-Ouen-sur-Seine Cedex – France
Telephone: +33 1 57 06 90 00

www.alstom.com

ALSTOM
• mobility by nature •

Design-Production: Photo credits: ©Alstom/Identity, ©Alstom/Michael Wittwer, ©Alstom/Gé Dubbelman ©iStock/baranozdemir, ©iStock/ipopba, ©iStock/Elen11, ©iStock/Dance60, ©iStock/buzbuzzer, ©iStock/santofilme, ©iStock/matejmo, ©iStock/Chainarong Prasertthai.