Intrusion detection to protect the digital railway

Increasing reliance on digital technologies has made railways more vulnerable to cyber attacks. Intrusion Detection Systems can help to protect new and existing infrastructure and ensure availability.

Swantje Weiss
Product Manager,
Digital Services,
Siemens Mobility

Digitalisation is sweeping through the rail sector, and there are many different ways in which data are used as the basis for dependable, safe, sustainable, and economic railway operations.

One of the biggest promises from digitalisation is the prospect of increased system availability — potentially close to 100% — thanks to preventive and predictive maintenance. Condition, health and performance data from different assets can be analysed using an application such as the Siemens Mobility Railigent suite to assist operators and maintenance crews with decision making on whether to repair, continue using or replace components.

Meanwhile, in line with a more general move towards web-based connectivity, the closed or self-contained rail control and IT systems of yesterday are increasingly being replaced by connected systems, allowing remote access by authorised users from any location and a wide range of devices. But while connectedness offers countless benefits, it can also open the door for cyber criminals.

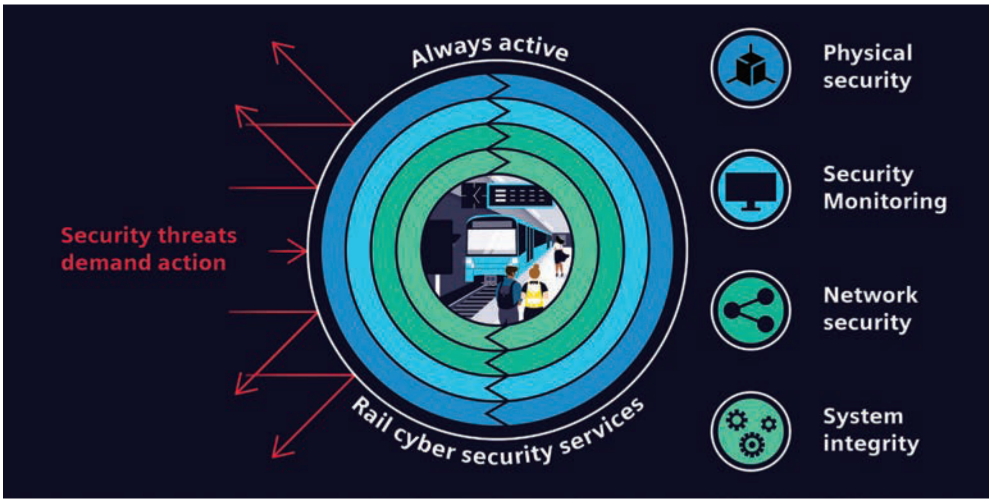
Defending rail systems against cyber threats is becoming increasingly important. Protected systems will allow railway digitalisation to progress further, as highlighted in the Unife Vision Paper on *Digital Trends in the Rail Sector*, published in April 2019. The recommended approach follows a ‘defence-in-depth’ concept, using several independent protection methods and layers (Fig 1). One part of this is the application of security monitoring to detect any anomalies and intrusions, combined with properly designed event management and incident response processes.

While cybersecurity monitoring systems are widely used in the IT world, for example in the finance sector, their implementation in the rail environment is still relatively new. As such, there is a lack of field experience for supporting railways in their selection of viable technologies and the design of system architectures. Siemens Mobility has been assisting its customers with the selection of proprietary or third-party systems, technical integration, configuration (baselining) and incident handling (Fig 2).

IDS

an Intrusion Detection System monitors network traffic for suspicious activity

Below: Fig 1. The defence in depth concept is built around several independent layers of protection.



Protecting against cyberattacks

Today’s railway environment is a complex mix of many IT and OT (operational technology) systems, sub-systems and components, embracing rolling stock, signalling, communication systems, power supplies and electrification, automatic fare collection, station or terminal systems and even platform screen doors.

Cyber attacks are nothing new for railway operators, and many security incidents have been reported over the years. Most have been in Europe, followed by North America, the Middle East, and the Asia Pacific region. The Enisa study *Railway Cybersecurity* in November 2020 found that in the majority of publicised cases it was the ‘visible’ systems that were being targeted, such as ticketing machines, passenger information systems, CCTV, and onboard wi-fi or entertainment systems.

However, it is highly probable that railway companies will also experience incidents targeting critical OT systems that are essential for the operation or the functional safety of their networks. An often underestimated source for potential attacks is insiders, who may inadvertently or even intentionally cause incidents.

Decisions about where to deploy security monitoring tools depend on a careful assessment of the risk or likelihood of an attack, and the potential impact such an attack could have. The most obvious reason

Above: Digital technologies are now prevalent in many different aspects of railway operations, which all need to be protected.

to protect assets is to keep railway operations safe and secure at all times, and to ensure system availability, while avoiding bad publicity. In many cases, the use of a secure and hardened systems is required by laws, regulations and industry standards.

Security monitoring

By definition, cybersecurity requires the continuous monitoring of IT and OT systems. In the case of many legacy systems, where a complete redesign to a more secure architecture would take a tremendous effort, security monitoring offers a viable means to enhance protection. Ultimately, the goal is to detect any anomalies or suspicious events that could be an indication of a cyber attack. These events can then be evaluated and the results used to react appropriately, as well as designing suitable countermeasures.

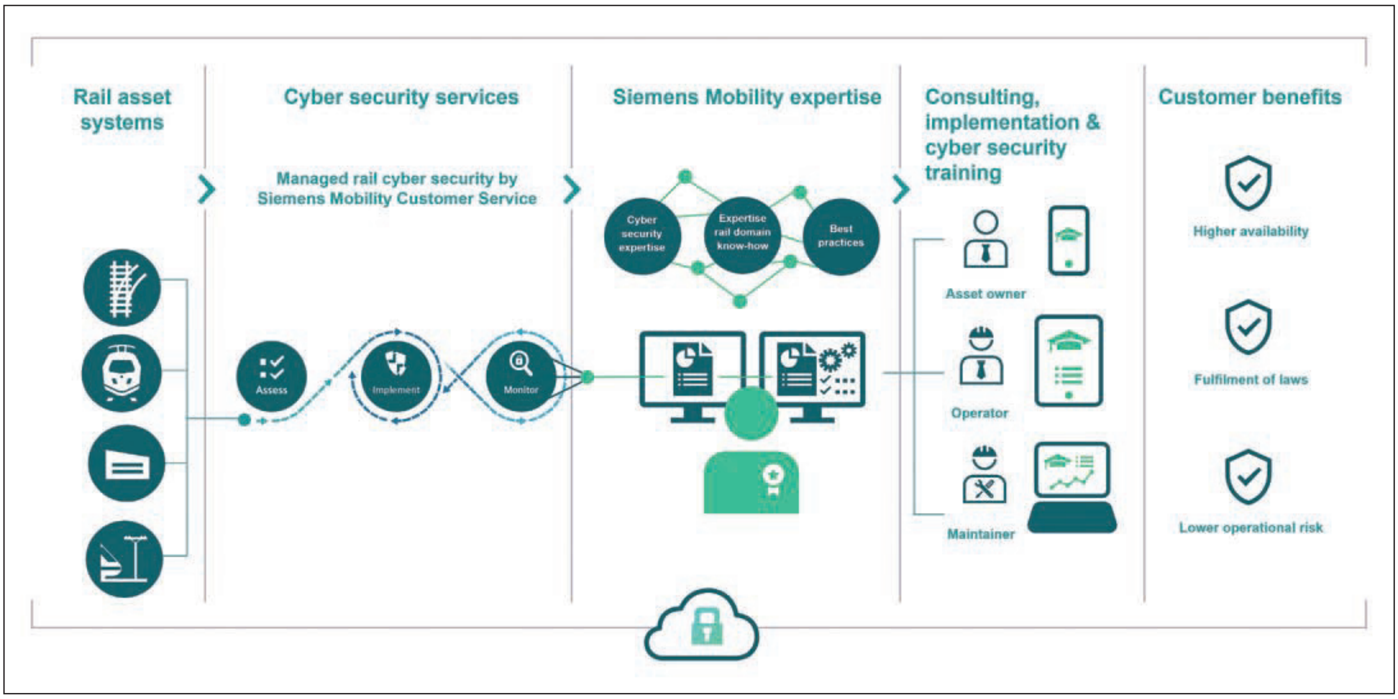
In simple terms, an Intrusion Detection System monitors network traffic for suspicious activity. More localised systems can also be deployed specifically to monitor particular components or subsystems, such as signalling systems or vehicles. A Network Intrusion System tracks unusual behaviour in a network, and a Host-based Intrusion Detection System that on the host servers.

The log files and data from all of these detection systems and other sources are collected, aggregated and evaluated using a Security Information & Event Management tool. The SIEM issues alerts about any suspected malicious behaviour to staff in the cybersecurity operations centre, who can then initiate the appropriate countermeasures.

Signature or AI-based?

Typically, an IDS employs either signature-based detection methods,

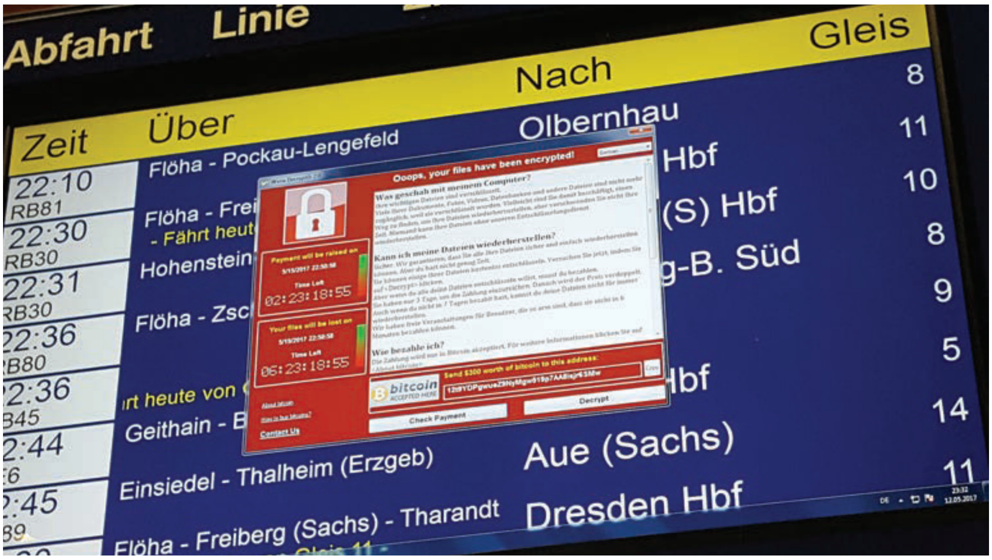
Below: Fig 2. Siemens Mobility Rail Services offers a range of managed cyber security options for the railway sector.



which rely heavily on expert configuration and maintenance, or AI-based methods, which are self-learning and can be considered almost 'zero-touch'.

A signature-based IDS is only as good as the number of patterns and protocols it supports, as well as the throughput. However, many of the protocols used in the rail environment are proprietary, and there is no public knowledge of the specifications. As a result, while most commercially available IDS can support common OT and IT protocols, it is rare that they are able to support such proprietary rail protocols.

AI-based detection systems, on the other hand, concentrate on behavioural data rather than signatures, and as such are potentially able to detect both known and unknown events. Rather than analysing packets in protocols, they look for abnormal behaviour as evidence of a potential attack.



Above: Deutsche Bahn was one of several railways affected by the Wannacry ransomware attack in May 2017.

Depth of traffic

In today's digital railway, a combination of both approaches is quite feasible, and often provides the best results. The protection is not only based on the location of the IDS within the whole system but also on the amount and depth of traffic being analysed.

Siemens Mobility deploys both types of systems in the rail environment depending on the specific requirements and levels of connectivity, building on experience from both testing and previous implementations.

The level of security that can be achieved is determined by the design, detection capabilities, and update frequency. Further aspects to factor in to the choice of approach are the requirements, use case and the specific application. For example, is the IDS intended to monitor rolling stock, signalling, or electrification control systems? Generally speaking, AI-based systems have lower maintenance requirements and offer the ability to detect unknown attacks. Regardless of the approach that is selected, installing an IDS can help railway companies achieve compliance in their next cyber audit.

Whether signature- or AI-based, a system should ideally detect anomalies as soon as they occur, while minimising the number of false positive alerts. An excess of false positives can increase the total cost of ownership for any cybersecurity solution by causing additional workload and costs. Other factors that must be taken into account include the need for on-site maintenance of the monitoring tools versus the scope for remote patching.

Technical considerations

From a technical perspective, several aspects must be considered. For example, it must be possible to integrate the IDS into safety-critical systems without impacting on their reliability or availability. This implies that active systems such as an Intrusion Prevention System may be unsuitable.

It must also be possible to update the IDS at any time to adapt to new threats and attack signatures, which means that it cannot be part of a safety-related system to comply with safety standards. As part of obsolescence management, railways should be able to exchange the IDS at any time without impacting on its safety-related aspects.

Railways also need to define clear processes for reacting to any potential or real incidents detected by their IDS. These processes must address the protection targets specific to rail systems, such as integrity and availability, whereas confidentiality is often the primary target for traditional IT protection systems.

By protecting systems and data against intrusion, railway companies can take advantage of the benefits of digitalisation without having to think constantly about cybersecurity. That makes it easier for them to focus on ensuring dependable, secure, sustainable and economic railway operations, for the benefit of their passengers and freight customers.

Below: Cyber attacks on public-facing systems such as passenger information displays are particularly visible, if less safety-critical.

www.mobility.siemens.com/global/en/portfolio/rail/services/digital-services/smart-security