DIGITAL SAFETY AND SAFETY MANAGEMENT - CYBER SECURITY MANAGEMENT AND PERFORMANCE AT INFRASTRUCTURE MANAGER

Heidi Niemimuukko (Email: heidi.niemimuukko@vayla.fi, +358 29 534 3350[1]

[1] *Finnish Transport Infrastructure Agency, P.O. Box 33, 00521 Helsinki Finland.*

BACKGROUND

For an infrastructure manager, a lot of what is done is about data and information. Especially in the current global (business) environment cyber security and its management have become an almost paramount task in making sure the infrastructure is safe for customers to use.

A large part of safety management is about managing the risks of one's own operations. This means that while it's important to define processes critical to one's own operations, the same applies to digital services and information assets they require. Cyber security is an integral part of management system and operational safety culture.

OBJECTIVE

This presentation will show how digital safety and cyber security can be incorporated into an existing safety management system and how contingency planning is also a part of it. The item is discussed from three aspects: data, building a cyber security management system and examples of implementing it.

CURRENT STATE OF TRAFFIC AND ITS CYBER SECURITY

In today's world a key part of traffic is information. It's all about transfer of knowledge, collection of information and sharing of information. We hear about smart traffic and transport, and it could be argued that information and data are the so-called 5th transport mode. True enough, traffic would not be as efficient without data as it is today.

There are several sources of information for the infrastructure manager about situations on and of routes, either directly or indirectly

- Sensors in the infrastructure can provide a steady flow of data on the condition of road or track for maintenance
- Information on the use of the infrastructure for planning
- Information to and from traffic management and traffic management, like traffic lights, signals, automatic train protection, level crossing warning devices, beacons on the maritime side etc.

For infrastructure users, data and information on traffic is of course much more than that, such as

- Information for infrastructure users such as navigation, weather information, condition of the road and of course route planning
- Information for public transport passengers like passenger information, route information, location information
- Information between users for example adaptive speed
- Safety information on accidents and incidents
- Information on the situation in the logistic chain

As far as the Finnish Transport Infrastructure Agency is concerned, there are already a lot of things on the rail network that need a steady flow of information and data to make traffic run smooth. Information is collected and produced on both the condition of the rail network and traffic situation and traffic management. From the point of view of cyber security, we have to consider how well the technical solutions implemented in different eras respond to the cyber security climate created by the current geopolitical situation. Especially on the rail network, different solutions are very long-lasting. For example, the current train control was introduced almost 30 years ago, at a time when the Internet was still in its infancy and information was being sought in thick encyclopaedias. At that time, safety of transport and how safely some operating systems can be used were issues to which attention was being paid – as, of course, is still the case today. Cyber security or digital security were concepts that were not heard of or may not have been at the top of the priority list. The environment has naturally evolved over the years, but from the point of view of traffic management, we still have 60's technology in use on one section of the line and at the same time on another section state-of-the-art new technology, where ensuring cyber security has already been a requirement from the outset, is being used. Ensuring interoperability and overall safety of all this technology is a priority for us. This hardly needs justification. Just think of all that would be lost if we found that cyber risks are unbearable. In terms of development and, in fact, in enabling mobility, we would return to the distant past. To a situation where trains are controlled by hand and permits to move a train are given with ticket tags and where we hope that the train driver will notice the speed limits on the track side and all exceptional situations or that the track repair team will notice the arriving train on time. You could get from Madrid to Barcelona a couple of times a day, and to Seville maybe less often. Fortunately, however, in order to help ensure the safety of this current new and old technology, we have various requirements, recommendations and guidelines in place. In addition to risk management, ensuring safety is largely a question of preparedness and continuity management in general.

In road traffic, the current vehicle technology offers many items which increase safety. To some extent these marvels are normal in older cars as well. We have all sorts of abs, chips, hubs and bubs and even something as mundane as navigation. The newer cars truly have fantastic smart solutions. For example, the vehicle recognizes speed limits from a digital map download into the vehicle system or directly from cloud and at the same time monitors the restrictions along the road. Your car might assist you in keeping your lane, it might have forced braking, adaptive cruise controls, etc., not to mention various solutions related to securing the logistics chain and efficiency. On the infrastructure side, traffic control, changing speed limits or warnings to road users along the road, are currently the most visible signs of information on traffic. Thinking of cyber security again, as long as the driver is responsible for the safety of the vehicle, things are reasonably well. If my cruise control detects the wrong speed limit on the map template, it doesn't matter if it was put on there by accident or with bad intentions. I can adjust the speed myself to be safe. So far, the driver can influence how blindly he trusts the signals given by the vehicle or infrastructure. The driver is a road traffic risk and, at the same time, a means of risk management and mitigation.

In general, the current state of smart traffic and transport information, we are still innovating and experimenting. We talk about MAAS (mobility as a service) and its possibilities, and smart traffic is being promoted as a solution to climate issues. Knowledge of actual mobility enables understanding people's behaviour and perhaps in the future to assess the needs of the whole transport system and its needs for change in near real time. At the moment, digital transport services are not everyone's reality, and we can compare the current situation of smart traffic with e-commerce 15-20 years ago. It was emerging but the payment methods were clumsy and the selection of goods very limited. Cyber security was not a thing back then and to be honest cyber criminality wasn't booming either. It is today and will also be tomorrow. Today we have map services and route guides for traffic use and maybe in not-so-distant future my fridge reminds me that there seems to be no food for the rest of the week, suggest a meal plan and a shopping list based on the plan and remarks that since there is nothing on your calendar now, it might be worth going to the store now. Click ok and a free driverless car nearby will pick you up in a few minutes or maybe you would rather have your shopping brought home to your doorstep in the evening.

KEEPING US AND DATA SAFE

In terms of smart traffic and transport information use a lot exists already and a lot is in the experiment. The possibilities are almost endless. We live in a world we want everything right now, as easily as possible. We want open data to enable business cases for smart traffic, but at the same time we must think about what data must be open and what not. Data and knowledge risk management are key issues. We have to consider what could happen if someone would choose to use data for mischief. Until a few months ago this might not have been what we thought about. Now, however, cyber security and cyber risks are firmly taken into account in everything that is being done.

Challenges

Challenges related to cyber security on rail are a fact. The ENISA, the European Network and Information Security Agency, published a report on railway cyber security last year. The report described well the cyber challenges faced by railways today.

Low digital security awareness. Overall, the survey showed that awareness of cyber security is quite low, but it is increasing all the time. Fortunately or unfortunately, this learned the hard way. Cases like Wannacry and NotPetya, even though they did not directly target railways, show that cyber incidents targeting railways are increasing.

Difficulty in reconciling safety and cyber security worlds. On the railways, safety requirements have always been high and this has generally meant that traffic can move safely. Now that the systems are starting to ensure cyber security, it is still necessary to make sure that traditional security and safety are not compromised. This is slow and often expensive, and we often also come across competence challenges. Experts in traditional safety and security may not understand cyber security, and cyber experts may not understand the interconnectedness of everything in the railway system nor its safety requirement. These hurdles do not make discussion easier. In addition, in some countries it is difficult to meet the requirements of the safety and (data) security authorities at the same time. The demands are overwhelming or even contradictory. For example, at the same time, high SIL levels of traditional safety may be required for parts that from a cyber security point of view would just be better to remove. In other words, cyber security is not only about technology, but also about administrative matters and about coordinating many entities.

Digital transformation of railway core business. More and more functions of the railways are becoming electronic. This means connecting IT and different devices. These connections need to be well planned from procurement to taking into service. Network connected devices and software should be treated with the same diligence. In other words this electronification introduces new vulnerabilities and shows that we have reached a point where OT systems are required to have the same level of cyber security as IT systems.

Dependence on the supply chain for cyber security. Railways are forced to rely on different suppliers and service providers for both IT and OT systems. Each supplier may have its own ways of meeting functional requirements and its own level of competence or cyber awareness. Today this easily leads to different levels of cyber security and cyber security requirements for different systems. Not everything is standardized and that is probably not even appropriate. From a tendering process it is still a long way to deploying an IT system. All in all, discussion, standardization and guidance as well as long term coordination from the service buyer is required.

Geographic spread of railway infrastructure and the existence of legacy systems. Geographically railway infrastructure is by no means a small local thing. Even in Finland, there is almost 7000 km of infrastructure in very different environments. As for the existing technology, we have old and brand new. The service life of systems and solutions can reach tens of years. It has even been established in Europe that some existing systems simply cannot be upgraded to meet today's cyber requirements, because of their technical solutions in the hardware or just the fact that the manufacturers do not have technical skills to upgrade the product any longer.

The need to balance security, competitiveness and operational efficiency. Rail transport is a public service which needs to be affordable. Cyber security measures are often expensive, and these expenses cannot be covered by always rising either ticket prices, infrastructure charges or transport prices. Finding a balance between costs and efficiency of data flow and easily usable systems is not an easy task. This is a classic case of confrontation between business objectives and safety. It is often said that safety & security and business beat each other on the ears.

Complexity and lack of harmonization of regulations for cyber security. Cyber requirements are perceived as complex. Perhaps precisely because this is a new sector as a part of traditional safety and security. In many countries, there are heaps of other requirements in addition to the NIS Directive, which will add to the administrative burden. Hopefully, in the future, we will be able to harmonise this whole at least at EU level.

Good examples in success

One example is the Digirata project, which will take Finland towards a more efficient and smoother rail transport. The aim is to switch to pan-European radio-based train protection on the entire Finnish rail network. It is a significant investment in the future of Finnish rail transport and the impacts are also significant: more traffic and passengers on the tracks, better services and fewer disruptions and traffic emissions. The Digirata-project is an opportunity that unites the entire rail sector and will build a technological foundation for rail transport long into the future.

BUILDING A CYBER SECURITY AS PART OF MANAGEMENT

A management system or safety management is largely about managing the risks of one's own operations. Especially as an infrastructure manager, we at the Finnish Transport Infrastructure Agency are familiar with this. We are managing the above-mentioned challenges with a (safety) management system. A management system helps us to ensure the achievement of our goals and to do things better, in other words to continuously improve.

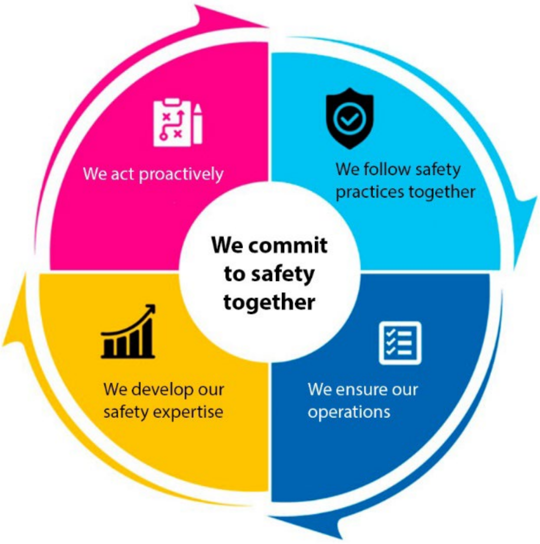
We act proactively
We follow safety practices together
We commit to safety together
We develop our safety expertise
We ensure our operations

Figure 1. Safety principles of Finnish Transport Infrastructure Agency

Figure 1 shows our safety principles in the form of the so-called Deming circle. The circle describes stages of continuous improvement. The same circle and principles can also be used to describe our cyber security principles and practices. Regarding cyber security, our goal could be, for example, that we want to improve digital security of our own operations and to ensure that what is already in place is sufficient. To do this, we naturally need to identify the risks of your own actions. Despite all the instructions, recommendations and even requirements, everything starts from assessing the situation and changes in the operating environment. An example of this could be the assessment of the fact that espionage and influence by state actors is on the increase globally and they might try to affect rail operations directly or indirectly here too.

It is therefore important to identify changes in the operating environment and threat scenarios. However, it is equally important to define the processes that are critical for one's own operations including all the digital services and information assets required for these operations. After all, these are just that kind of targets that are of interest to malicious attackers, who often take advantage of everyday security flaws. The Finnish Transport Infrastructure Agency believes that cyber security is an integral part of the agency's overall management system and safety culture of its operations. Cyber security may have its own goals and strategies, but it's good to keep them incorporated into other strategies and goals. This is one way of normalizing digital security and risk management, and this also shows that that there is nothing mysterious and miraculous about these or that only highly specialized experts can think about cyber security. We want every expert to consider it quite normal to think about and react to threats related to their own work. For example, this could be something as simple as thinking about what work to do in a local café.

After identifying and planning various items, it is time to do, in other words to ensure that important processes, services and information are safe and secure and that the information can be safely accessed too. Ensuring continuity can mean testing your own operations and security or auditing different IT and OT systems and processes. When something is done the results must also be observed and analysed and action must be taken based on these analyses.

Another integral part of the management system are matters related to competence. We have plenty of experts in their own field, but their cyber security expertise must also be taken care of. As an infrastructure manager, we also want to ensure that our service providers have sufficient cyber expertise. It is therefore important for us to have a joint debate on cyber security. In this way threats and risks will be sufficiently discussed and at the same time the know-how can also be disseminated more widely.

Building a cyber security management system might sound like rocket science, but it need not be if you have a solid base in a safety management system or any other management system. We have currently a management system and a safety management system (for rail). Having those separate is not an ideal situation, which is why we are integrating these into one management system. This will also make it easier to comply with ISO 27001 requirements on information security management.

IMPLEMENTING A CYBER SECURITY MANAGEMENT SYSTEM

A management system is not a book or a pile of documents. It's more about commonly agreed procedures that are described somehow and that fulfil mandatory requirements. The most important thing is to get your organisation into using and living those commonly agreed procedures. Here again everything should be done in such a way that the experts do not actually notice if they work according to a management system. Of course, they need to know it exists, but processes and procedures must describe real life.

What this means is, that a 'handbook' could be something as simple as a list proving conformity requirement by requirement.

The challenges described previously are real and have to be kept in mind when implementing and living according to a management system. A procedure might be easily described but making real life decisions is often far from that. It can be challenging to fulfil requirements one has set for oneself when there are conflicting interest like time, safety, security, money and efficiency.

Even if an organisation might not have a written and published cyber security management system yet, it doesn't mean that we cannot ensure and measure cyber security of our operations. One way to demonstrate capability of managing cyber risks is cyber preparedness and its performance. As the manager of critical infrastructure, the Finnish Transport Infrastructure Agency is prepared to have its operations running and continuing as smoothly as possible both in disruptions in normal conditions and in a state of emergency. Our contingency plan ensures that the Finnish Transport Infrastructure Agency has planned and prepared in advance the operating procedures to be followed in different situations. Especially in recent years, investments have been made in preparedness. The contingency plan covering the entire operations of the Finnish Transport Infrastructure Agency has been updated during 2021, and regular training has and will be carried out for various situations. For example, we participate in a nationwide information security exercise every year and work closely with key actors and authorities in the administrative branch. For years, the Finnish Transport Infrastructure Agency has been working to ensure that potential threats from internet are minimized and that disruptions caused by threats to critical systems are managed in all situations. For example, rail traffic control operates in a separate network and cannot be accessed without checks and verifications. A large part of our preparedness focuses on how to ensure our capability and procedures to provide a safe infrastructure for users – even if it might not meet the standards and conditions we usually expect from an infrastructure.

One measure of continuity management and preparedness is the rail network cyber security programme, which we launched almost two years ago. Its purpose is to further strengthen the reliability of the rail system as a whole and its various components through administrative, physical and IT measures.

In addition to a living management system, a comprehensive contingency plan and regular training are needed. All this should be done together with key stakeholders. At the same time audits, inspections, checks and surveys are being used to map current situation and performance. These give valuable feedback where risk based corrective measures are needed. Because of sometimes high costs of cyber security, it's important to find places where measures and development add most value to safety performance.

CONCLUSION

Cyber security isn't just about technology – Attempts to influence start with people and end with people. Therefore, we should never forget human and organisational factors. For digital safety it is us together who make our operations cyber secure!

Keywords: digital safety; cyber security; safety management; infrastructure manager; contingency