Ministry of Infrastructure
and Water Management

> Return address Postbus 20901 2500 EX Den Haag

European Commission
Mrs V. Bulc
Rue de la Loi / Wetstraat 200
1049 Brussels, Belgium

Ministry of Infrastructure and Water Management

Rijnstraat 8
2515 XP Den Haag
Postbus 20901
2500 EX Den Haag

T 070-456 0000
F 070-456 1111

Reference number
IENW/BSK-2019/121327

Appendix
2

Date 14 June 2019
Subject Improving cybersecurity in ERTMS specifications

Dear Mrs. Bulc,

It is my pleasure to inform you that we are reaching a major milestone regarding the implementation of ERTMS in the Netherlands. Furthermore, I would like to emphasize the urgency for adding additional measures in the upcoming update of the ERTMS specifications to ensure a secure implementation of ERTMS.

After five years of careful, meticulous study and preparation for the implementation of ERTMS in the Netherlands in accordance with the ERTMS European Deployment Plan, the moment has arrived for the Dutch government to finalize decision-making on the issue of entering the execution phase. After which all parties involved can start their efforts regarding tendering the works necessary for implementing ERTMS in the infrastructure and rolling stock. Before reaching this decision, all relevant documentation was reviewed thoroughly and independently of the ERTMS programme and was subsequently improved upon. The national bureau of ICT reviews ("BIT") performed the final review, with a special focus on the ICT aspects of the programme. This was a mandatory review, reporting directly to parliament. The advice of the BIT bureau generally carries a lot of weight and I too have found their advice most valuable. The integral advice of the BIT bureau in the Dutch language is enclosed with this letter. An English translation of the part concerning cybersecurity has been added in appendix A.

As the main goal of the implementation of ERTMS in Europe is to improve interoperability, member states are dependent on each other for an adequate level of security in regards to international trains. Therefore, a common approach on cybersecurity is necessary. Regarding the cybersecurity aspects of the ERTMS system the BIT bureau has impressed upon me the need for more explicit attention in the technical requirements.

The BIT bureau has pointed out that the standard of encryption on GSM-R is rapidly becoming outdated and provides a less than desirable level of security for malicious practices such a hacking and spoofing. This is something that ERA in cooperation with ENISA should look into remedying in light of the upcoming improvement of the ERTMS specifications in 2022. Possible avenues could be updating the encryption standard, developing a system of monitoring measures or a faster upgrade path to the GSM-R successor, the Future Railway Mobile

Communication System (FRMCS). More secure software and hardware are of course only part of the solution. Therefor I also support new initiatives aimed at increasing cyber security awareness and cooperation, such as the establishment of an ENISA Working Group Cyber Security for the railways.

An important part of the ERTMS standard is securing the legitimate operation of rolling stock. This is dependent on having a valid ERTMS key for a specific train. The BIT bureau emphasizes the vital importance of secure storage and distribution of the keys. The specifications regarding key management have not been standardized as of yet, which means this could lead to weak controls being built.

Furthermore, the BIT bureau has stressed the need to issue specific rules and regulations to ERTMS-users regarding security measures, processes concerning updating security measures, the development of ERTMS-components and measures in regards to the monitoring, detection and response to threats. These rules and regulations would preferably be developed and maintained within a European body. In the meantime, I have agreed to the foundation of such an organization on a national level within the ERTMS programme in the Netherlands.

I realize that these desired improvements take time and that further development is needed. The participants in the ERTMS programme in the Netherlands and the staff at my ministry are very much motivated to work together with you and the other member states and associate countries in order to help make these improvements a reality and make the railway systems with ERTMS more secure.

Yours sincerely,

THE STATE SECRETARY FOR INFRASTRUCTURE AND WATER MANAGEMENT,

S. van Veldhoven - Van der Meer

Appendix A: Translation of BIT bureau advice regarding cybersecurity

The BIT bureau is of the opinion that the cybersecurity approach is underdeveloped and that additional measures are necessary to ensure a secure implementation of ERTMS in the Netherlands.

C. The cybersecurity approach is underdeveloped.
The digital ERTMS components and the GSM-R communications system are more susceptible to cybersecurity threats than the current [Dutch] analog system ATB. However, there is still little explicit attention to (technical) cybersecurity in the European ERTMS specifications:

- The communications system GSM-R has the same security weaknesses as GSM. In addition, the cryptographic standard for the communication of messages with the ERTMS components in the rolling stock is outdated. Therefor it appears to be possible to erase ERTMS messages without being detected and to send falsified warning messages.[1]
- The ERTMS specification does not require the use of specific cryptographic hardware, in contrast to comparable standards[2]. However, this is crucial for the secure storage of the secret keys which are necessary for the ERTMS system in the rolling stock to be able to ride on ERTMS tracks.

Even though the [Dutch ERTMS] programme acknowledges the necessity to reduce the cybersecurity risks – the programme also brings this to the attention on a European level – the current approach leaves the participants to much freedom in the interpretation. There are no specific requirements that ERTMS components and participants must meet. Also, there is no central organization that is responsible for the enforcement of the cybersecurity regulations, a so-called scheme provider. This is common practice among comparable implementations, such as the [Dutch] public transportation chip card. We see this as a risk, because security flaws within one ERTMS participant can have repercussions for another participant.

[1] A Formal Security Analysis of ERTMS Train to Trackside Protocols, Joeri de Ruiter et al, RSSRail 2016, Paris, France, June 28–30, 2016.

[2] For example: the standard regarding Intelligent Transport Systems voor transport by road: https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf.