THE AUTHOR
Jiri Petr
Head of Applications, CSA Engineering

Developing IoT applications with stringent safety requirements

In safety- and security-critical areas such as passenger transport, more stringent requirements with regard to fault resistance and reliability of communication software for IoT applications must be met. This also has a major impact on the development process.

IP technology is also increasingly finding its way into the rail industry and other areas in which operational safety and security, i.e. the protection of people and the environment, are paramount. This falls under the general umbrella of "safety", which supplements the security mechanisms of IT security and the compliance with which is exemplified by the development of the Rail Safe Transport Application (RaSTA) protocol. From a technical point of view, RaSTA enables the reliable transmission of data without the undetected loss of such by employing mechanisms such as Heartbeat for regular monitoring of connection quality, the use of redundant transport channels and strict time monitoring of data transmission. RaSTA is located at the interface between the application and transport layer and consists of two sub-layers: the safety and retransmission layer which, among other things, ensures the integrity and addressing of the transmitted data and provides the application layer with the functions necessary for implementing a RaSTA client, and the redundancy layer, which ensures the management of transport channels, which are executed via physically separate networks. The transport layer is made up of a UDP (User Datagram Protocol) or TCP (Transmission Control Protocol), whereby TCP increases the robustness of data transmission and thus of the solutions based on RaSTA. With these interfaces, RaSTA can be used on the Internet and thus also on all public networks – from Ethernet to 5G. Data transmission security, which is often indispensable, can thus be ensured with established encryption technologies such as TLS (Transport Layer Security).

Complex development processes

However, the development of safety applications does not end with the implementation of a safety protocol. In addition to selecting suitable hardware, the development processes also play a key role. These are defined in industry-specific standards, compliance with which must be verified by an independent body. EN 50128 and the associated CENELEC standards are relevant to railway technology. From the perspective of conventional application development, this results in modern development teams having to implement a variety of changes, such as using a V-model, which divides the development process into sequential phases and calls for a comprehensive set of coordinated documents to be drawn up before the first line of code is even written. As the documents have to be checked as part of formal reviews, this approach takes a considerable amount of time. Developers are also confronted with restrictions during implementation that force them to employ defensive programming and prohibit them from using middle methods common in “normal” software development such as pointers or dynamic memory allocation. Fortunately, this procedure is limited to the safety and retransmission layer of RaSTA, which is sufficient for the implementation of safety applications. The use of existing safety protocols should also be a worthwhile option in other cases. RaSTA is independent of the application protocol and can therefore help improve the reliability of all kinds of IoT applications in various areas of application.

The full article is available online at www.netzwoche.ch