SECURING COMMUNICATIONS
BETWEEN WIRELESS REMOTE SENSORS, ONBOARD IOT GATEWAYS AND BACK OFFICE RAIL SYSTEMS

CLOUD CONNECTIVITY ENABLES SECURE CONNECTIONS

by Valentin Scinteie, Transportation Business Development Manager, Kontron

Network security is becoming increasingly important for transit systems to ensure reliable operation of ever more connected devices and applications that make up the rail ecosystem. Securing vital infrastructure, system functionality and even passenger personal data is essential to prevent system disruption, downtime and malicious information hacking. But achieving reliable data transmission between fast-moving rail cars and ground stations is a technical challenge made more difficult when implementing security.

Helping to meet these network and communication security needs is the LoRaWAN™, a low power wide area network protocol specification developed by the LoRa Alliance. It uses an unlicensed radio spectrum for wireless battery operated devices to enable secure communication between remote sensors and gateways connected to the network. This standards-based approach allows for quick set up of safe public or private networks anywhere.

LoRa-based networks feature layers of encryption that ensure end-to-end network and application security. A benefit to transit agencies in adopting platforms that support LoRaWAN is that they satisfy several key requirements of Internet of Things (IoT) and smart transportation connectivity such as secure bi-directional communication, mobility, interoperability and accurate localization services. Plus, seamless interoperability between smart devices is achieved without the need for rail operators to install complex local systems allowing them to more quickly realize the real-time data and remote monitoring advantages of IoT.

Secure Communications

An example of a successful IoT gateway is one that gives rail operators a secure LoRa solution while also providing the ability to transform messages to Message Queue Telemetry Transport (MQTT) streams. When coupled with cloud connectivity services, this type of all-in-one secure IoT gateway supports continuous communications from LoRa-based devices to a Cloud server for highly-secure data collection and remote analysis. In this way, operators have a private local LoRaWAN network infrastructure reserved for intra-vehicle communication so that installed LoRa end-devices, which are typically sensors, can communicate to the gateway. The security benefit is that all LoRa™ messages that belong to this private network are secured and restricted to registered sensors. The connection to the cloud server is secured by TLS connection using private keys used on both sides.

Figure 1: Kontron **TRACe™ LoRa-MQTT** is an EN50155(*) fanless solution ready platform offering LoRa™ local network and transforming messages to MQTT streams

Ensuring Digital Security

Digital security is of tremendous importance for all transit systems, especially the expanding number of deployed autonomous devices. Without the monitoring of an operator, these devices are vulnerable to threats. And, many of these devices will run without supervision for either a part or all of their many-year lifespan. The main digital security threats are linked to confidentiality, integrity and availability. Confidential data must be restricted to assigned users. Likewise, the integrity of important data cannot be compromised, have malicious data injected into an application or have its execution code altered to change the application's behavior. Transit systems, either the software application or the devices within the network are at risk of being cloned without authorization.

Protecting rail applications from these risks is the **Kontron APPROTECT** hardware and software solution that delivers the security of a dedicated hardware secure element located on all Kontron boards and modules. It combines an embedded hardware security module

and a software framework that provides a comprehensive range of protection capabilities that include IP and integrity protection, license creation, management and tracking, license model implementation as well as the assignment of privileges and access levels.

These types of digital security solutions ensure that all or part of the application execution code is encrypted on a storage device, and will only be decrypted in memory in the presence of the keys stored inside its secure element. At run time, the integrity of the application in memory is also permanently checked. The application can be fully encrypted as a whole with no modification, or only critical sections encrypted by using a dedicated API.

Additional digital security can be satisfied with hardware enforced root of trust (secure elements), and software techniques such as Trusted Boot to protect system software during boot with a Trusted Platform Module (TPM) secure element. Authentication with TPM is necessary to secure network protocols. For transit systems to establish a secure network connection such as https, a private key is, at the very least, required on the server side. It is also recommended on the client side for embedded computing since no operator is present to enter a password. It is often not a good idea to store the private key on the disk, even encrypted, because at some point, it will be decrypted in memory and CPU registers when used at the beginning of a network session. With the TPM authentication, the private key will be stored and used under the hardware protection of the TPM, so that it is never exposed. Without this hardware protection, the risk exists of having the private key stolen, which would allow the duplication of a compromised server or client machine, or a "man in the middle" attack where the hacker has access to the communication.

Kontron's SEC-Line (Secure Embedded Computing) modules and services use these advanced security technologies to provide state-of-the-art protection for embedded systems. The SEC-Line offers Trusted and Secure Boot, Trusted Modules, advanced authentication and application binary encryption that meets rail operation data goals of enhanced availability, integrity and confidentiality.

Although, safeguarding systems is no easy task as new threats arise on a regular basis. There are, thankfully, transit system security solutions available that are proven effective in protecting the expanding number of rail devices. With rock-solid security as confidence, operators can take full advantage of all the benefits the connected train has to offer.