Die Entwicklung von IoT-Anwendungen mit hohen Sicherheitsanforderungen

In sicherheitskritischen Bereichen wie dem Personentransport müssen erhöhte Anforderungen hinsichtlich Fehlerresistenz und Zuverlässigkeit von Kommunikationssoftware für IoT-Anwendungen erfüllt werden. Dies hat auch grossen Einfluss auf den Entwicklungsprozess.

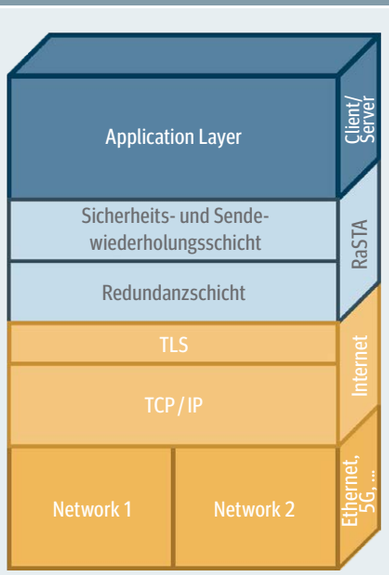
DER AUTOR

Jiri Petr
Bereichsleiter Applications, CSA Engineering

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Die IP-Technologie hält immer mehr auch Einzug ins Bahnwesen und andere Gebiete, bei denen die Betriebssicherheit, also der Schutz von Mensch und Umwelt, im Vordergrund steht. In diesem Fall spricht man von Safety, welche die Sicherheitsmechanismen der IT-Security ergänzt und deren Einhaltung bei der Entwicklung des RaSTA-Protokolls (Rail Safe Transport Application) beispielhaft ist. Aus technischer Sicht ermöglicht RaSTA eine verlässliche Datenübertragung ohne unbemerkten Datenverlust mithilfe von Mechanismen wie Heartbeat zur regelmässigen Überwachung der Verbindungsqualität, dem Einsatz von redundanten Transportkanälen sowie einer strikten Zeitüberwachung der Datenübertragung. RaSTA ist zwischen der Applikations- und Transportschicht anzusiedeln und besteht aus zwei Teilschichten: aus der Sicherheits- und Sendewiederholungsschicht, die unter anderem für die Integrität und die Adressierung der übertragenen Daten sorgt und der Applikationsschicht Funktionen zur Verfügung stellt, die für die Implementierung eines RaSTA-Client notwendig sind. Die Redundanzschicht wiederum sorgt für die Bewirtschaftung von Transportkanälen, die über physisch getrennte Netzwerke realisiert werden. Als Transportschicht ist UDP (User Datagram Protocol) oder TCP (Transmission Control Protocol) vorgesehen, wobei TCP die Robustheit der Datenübertragung und somit der auf RaSTA basierenden Lösungen erhöht. Mit diesen Schnittstellen kann RaSTA im Internet und damit auch in allen öffentlichen Netzen eingesetzt werden – von Ethernet bis zu 5G. Die oft unabdingbare Datenübertragungssicherheit (Security) kann wiederum mit etablierten Verschlüsselungstechnologien wie TLS (Transport Layer Security) gewährleistet werden.

RASTA IM KONTEXT DES SCHICHTENMODELLS



Aufwendige Entwicklungsprozesse

Die Entwicklung von Safety-Applikationen endet aber nicht mit dem Einsatz eines Sicherheitsprotokolls. Nebst der Auswahl einer geeigneten Hardware spielen auch die Entwicklungsprozesse eine wesentliche Rolle. Diese sind in branchenspezifischen Normen definiert, deren Einhaltung durch ein unabhängiges Gremium überprüft werden muss. Für die Bahntechnik sind EN 50128 und die dazugehörigen CENELEC-Normen massgebend. Aus Sicht der herkömmlichen Applikationsentwicklung bedeutet dies für ein zeitgemäss arbeitendes Entwicklungsteam einige Änderungen wie etwa den Einsatz eines V-Modells, das die Entwicklung in sequenzielle Phasen unterteilt und das einen umfangreichen Satz an sich abgestimmten Dokumenten vorsieht, bevor überhaupt die erste Zeile Code geschrieben wird. Da die Dokumente durch formelle Reviews zu prüfen sind, ist der Zeitaufwand erheblich. Ebenfalls sind die Entwickler bei der Implementierung mit Restriktionen konfrontiert, die eine defensive Programmierung erzwingen und in der «normalen» Softwareentwicklung gängige Mitte wie die Verwendung von Pointern oder die dynamische Speicherallokation verbieten. Glücklicherweise beschränkt sich dieses Verfahren auf die Sicherheits- und Sendewiederholungsschicht des RaSTA, was für die Implementierung von Safety-Applikationen genügt.

Der Einsatz von bereits vorhandenen Safety-Protokollen dürfte auch in anderen Fällen eine lohnenswerte Option sein. RaSTA ist unabhängig vom Applikationsprotokoll und kann deshalb in verschiedenen Einsatzbereichen die Zuverlässigkeit von IoT-Anwendungen aller Art verbessern helfen.

www.netzwoche.ch © netzmedien ag