SIL4-zertifizierte Sicherungsanlagenlösung mit flexiblen COTS

A SIL4 certified signalling solution with flexible COTS

Janne Sirilä

Das Stellwerkssystem der U-Bahn Helsinki und ihrer westlichen Verlängerung (2017) wurde mithilfe einer kommerziellen Standardplattform (COTS – Commercial Off The Shelf) implementiert. Das SIL4 HIMax-basierte Mipro-TCS-O Stellwerk steuert und überwacht seit fünf Jahren Hunderte von Strecken-Signalelementen und sicherheitskritische Zusatzkomponenten, wie z. B. Brandschutzrolltüren, mit hervorragender Verfügbarkeit und Sicherheit. Im Laufe der Jahre wurden dem System neue Funktionen und Elemente hinzugefügt. Dank der Struktur des Systems waren die Entwicklung und Erweiterung des bestehenden Systems ein unkomplizierter Prozess.

1 Vorteile der Verwendung kommerzieller Standardhardware

1.1 Verfügbarkeit und Sicherheit

In Eisenbahnsicherungsanlagen sind hohe Verfügbarkeit und Sicherheit ein Muss. Die gewählte Hardware und die Plattform spielen bei Systemlieferungen eine entscheidende Rolle. Der Systemlieferant muss sich darauf verlassen können, dass die verwendete Hardware den hohen Anforderungen der Branche gerecht wird. Der Systemlieferant muss auch darauf vertrauen können, dass der Lieferant die Hardware während der gesamten Lebensdauer des gelieferten Systems innerhalb kurzer Lieferzeit und wie vereinbart liefern kann. Bei der Verwendung von COTS-Hardware eines vertrauenswürdigen Anbieters verwendet der Lieferant der Sicherungsanlage Hardware, die sich im Einsatz bewährt hat – nicht nur in Schienenverkehr-Applikationen, sondern auch in verschiedenen anderen Branchen, die eine hohe Verfügbarkeit und Sicherheit erfordern, z. B. die Wasser-, Öl-, Gas- und Chemiebranche. Darüber hinaus erfüllen vorzertifizierte COTS-Plattformen nicht nur die relevanten Schienenverkehrs-Standards, sondern oft sind dieselben Plattformen auch nach anderen Branchenstandards zertifiziert. Diese beiden Tatsachen geben dem Systemanbieter ein sehr kräftiges Rückgrat, um die Anwendungen zu entwickeln, die eine hohe Verfügbarkeit und Sicherheit des Schienenverkehrs gewährleisten.

1.2 Kosten

Die Kosten für die Plattform und Hardware sind natürlich ein wesentlicher Faktor. Im Gegensatz zu proprietärer Hardware, die oft nur für einen Zweck und in kleineren Mengen hergestellt wird, wird COTS-Hardware, die mehrere Branchen bedient, in größeren Mengen hergestellt, wodurch die Kosten für die Hardware gesenkt werden können. Das bedeutet Einsparungen nicht nur bei der Anschaffung, sondern auch während des gesamten Lebenszyklus der Anlage. Anders als bei proprietären Systemen ist auch die Wiederverwendung von COTS-Hardware möglich. Dies bringt sowohl finanzielle als auch ökologische Einsparungen mit sich.

The interlocking system in Helsinki metro and its western extension (2017) has been implemented using a commercial off-the-shelf (COTS) platform. The SIL4 HIMax based Mipro TCS-O interlocking has been controlling and supervising hundreds of trackside signalling elements and auxiliary safety-critical components, such as rolling fire doors, for five years now with excellent availability and safety. New functions and elements have been added to the system over the years. The system structure enabled a straightforward development and expansion of the existing system.

1 The benefits of using COTS hardware

1.1 Availability and safety

High availability and safety are a must in railway signalling systems. The chosen hardware and the platform play a crucial role in system deliveries and the system supplier must be able to trust that the used hardware will meet the industry's high requirements. The system supplier also needs to be confident that the hardware supplier will be able to deliver the goods within a short delivery time and as agreed throughout the delivered system's entire lifetime. When using COTS hardware from a trusted vendor, the signalling system supplier is using hardware that has been proven for use not only in railway applications, but also in various other industrial fields that require high availability and safety, such as the water, oil, gas and chemical industries. In addition, pre-certified COTS platforms not only meet the relevant railway standards, but the same platforms are often also certified according to other industry standards. These two facts give the system vendor a very strong basis for building applications that ensure great availability and rail traffic safety.

1.2 The cost

The cost of the platform and the hardware is naturally a significant factor. Unlike proprietary hardware which is often manufactured to serve only one purpose and therefore in smaller amounts, COTS hardware serves several industry sectors and is therefore manufactured in larger amounts, meaning that the hardware costs can be cut. This means savings not only at the time of acquisition, but also throughout the system's entire lifecycle. Unlike in proprietary systems, COTS hardware can also be reused. This brings both monetary and environmental savings.

1.3 Connectivity and interfaces

Now and in the future, a signalling system is not simply a separate, standalone system used to control traditional trackside sig-

1.3 Konnektivität und Schnittstellen

Heute und in Zukunft ist eine Sicherungsanlage nicht nur ein separates, eigenständiges System zur Steuerung der traditionellen Strecken-Signalelemente wie Signale, Weichen und Gleisfreimeldung. Der Kunde kann verschiedene Anforderungen haben, um Hilfssysteme an das zu steuernde und zu überwachende Stellwerk anzuschließen. Diese Hilfssysteme können beispielsweise Folgendes umfassen: Unterbrechungsfreie Stromversorgung (USV), Brandmeldesystem, Türsysteme, Einbruchmeldesysteme, automatisches Zugsicherungssystem, intelligente Weichenheizungen, intelligente Datenerfassung für Streckenelemente und Überwachungssysteme. E/A-Schnittstellen und Standard-Kommunikationsprotokolle wie Ethernet, TCP/UDP, RS232, RS422 und CAN sind normalerweise im Produkt verfügbar, und dank der Tatsache, dass COTS-Hardware in mehreren Branchensektoren verwendet wird, sind auch seltenere Protokolle verfügbar. Auch neue Schnittstellen können ohne allzu große Schwierigkeiten in die COTS-Plattform eingeführt werden. Beispielsweise hat Mipro ein RaSTA-Netzwerkprotokoll (Rail Safe Transport Application) implementiert, das in Mipros COTS-basiertem Stellwerk verwendet werden soll.

1.4 Langfristige Beziehung

1.4.1 Verfügbarkeit von Experten

Der Lebenszyklus von Eisenbahnsignalsystemen ist typischerweise sehr lang. Während der Lebensdauer des gelieferten Systems ist der Bedarf an Änderungen sehr wahrscheinlich. Gute COTS-basierte Systeme werden mithilfe von Tools entwickelt, die der Norm IEC 61131 entsprechen. Dadurch wird sichergestellt, dass im Laufe der Jahre neue Experten aus verschiedenen Generationen gefunden werden können und die Fähigkeit, eigene Systeme zu programmieren und einzurichten, nicht so umfangreich aufrechterhalten werden muss.

1.4.2 Verfügbarkeit von Komponenten und Herstellerunabhängigkeit

Systemkomponenten erreichen das Ende ihrer Lebensdauer, und der Support des Herstellers für sie läuft irgendwann aus. Eine Ersatzkomponente für ein proprietäres Produkt ist im schlimmsten Fall sehr schwer zu finden, während in der Welt von COTS eine Ersatzkomponente, die mehrere Branchenzweige bedient, schon Jahre vor dem Ende der Lebensdauer einer alten Komponente zur Verfügung gestellt werden kann. Es ist auch erwähnenswert, dass der Benutzer bei der Verwendung von COTS nicht vollständig an den ursprünglichen Systemanbieter gebunden ist, und aus diesem Grund haben einige Infrastruktureigentümer begonnen, COTS-Produkte zu bevorzugen.

1.5 COTS in der Welt der Telekommunikation

Es gibt Ähnlichkeiten zwischen der Welt der Telekommunikation und der Welt der Eisenbahnsicherungsanlagen. Die Systeme sind für eine lange Nutzungsdauer ausgelegt, und es dauert Jahre, bis die neue Technologie entwickelt ist und der Markt sie adaptiert. Wie das Eisenbahn-Sicherungsanlagengeschäft wurde auch das Telekommunikationsgeschäft zuvor von proprietären Systemen einiger weniger großer Unternehmen beherrscht. Vor etwa zehn Jahren traten neue Unternehmen mit COTS in den Telekommunikationsmarkt ein. Die Migration zu COTS hat zu schnelleren Designzyklen und reduzierten Wartungs- und Hardwarekosten geführt. Der Einsatz von COTS ebnete zudem den Weg für die Server-Virtualisierung, die auch im Eisenbahngeschäft Einzug hält.

nalling elements such as signals and points and for track vacancy detection. The customer may need to connect various auxiliary systems to the interlocking so that they are controlled and supervised. These auxiliary systems can include for example: a UPS, a fire alarm system, door systems, intrusion detection systems, automatic train protection (ATP), intelligent point heating systems, intelligent trackside element data collection and monitoring systems. I/O-interfaces and standard communication protocols such as the Ethernet, TCP/UDP, RS232, RS422 & CAN are usually readily available in the products and the fact that COTS hardware is used in multiple industry sectors means that rarer protocols are also available. New interfaces can also be introduced to a COTS platform without too much pain. For example, Mipro has implemented a Rail Safe Transport (RaSTA) network protocol to be used in Mipro's COTS based interlocking.

1.4 The long-term relationship

1.4.1 The availability of experts

A rail signalling system's lifecycle is typically very long. The need for changes will likely ensue throughout the delivered system's lifetime. Good COTS based systems are developed using tools that comply with the IEC 61131 standard. This ensures that new experts can be found from different generations over the years and it is not so necessary to maintain the capability to program and set up proprietary systems.

1.4.2 The availability of components and vendor locking

The system components will eventually reach the end of their lifetime and the manufacturer's support for them will run out. A replacement component for a proprietary product is, at worst, very difficult to find, while a replacement component that is simultaneously serving several industrial sectors can be made available in the world of COTS even years before the end of the old component's life. It is also worth noting that the user is not completely locked into the original system supplier when using COTS and for this reason some infrastructure owners have started to prefer COTS products.

1.5 The use of COTS in the world of telecommunications

There are similarities between the world of telecommunications and that of railway signalling. The systems are built for long use and it takes years for new technology to be developed and for the market to adapt it. Like the railway signalling business, the telecommunications industry was previously ruled by proprietary systems supplied by a few big companies. New companies entered the telecom market using COTS around ten years ago. The migration to COTS has brought about faster design cycles and reduced maintenance and hardware costs. The use of COTS has also smoothed the way to server virtualisation, which is also taking place in the rail industry.

2 Securing the world's northernmost metro

2.1 The Helsinki Capital Area Metro

The Helsinki metro opened in 1982 and it has been extended several times throughout its history. The biggest change occurred in 2017 when the metro tracks crossed the Helsinki city limits for the first time and extended to the city of Espoo. The West Metro Project brought eight new stations to the metro network. Another big project, the West Metro Extension, is currently on the verge of completion (fig. 1).

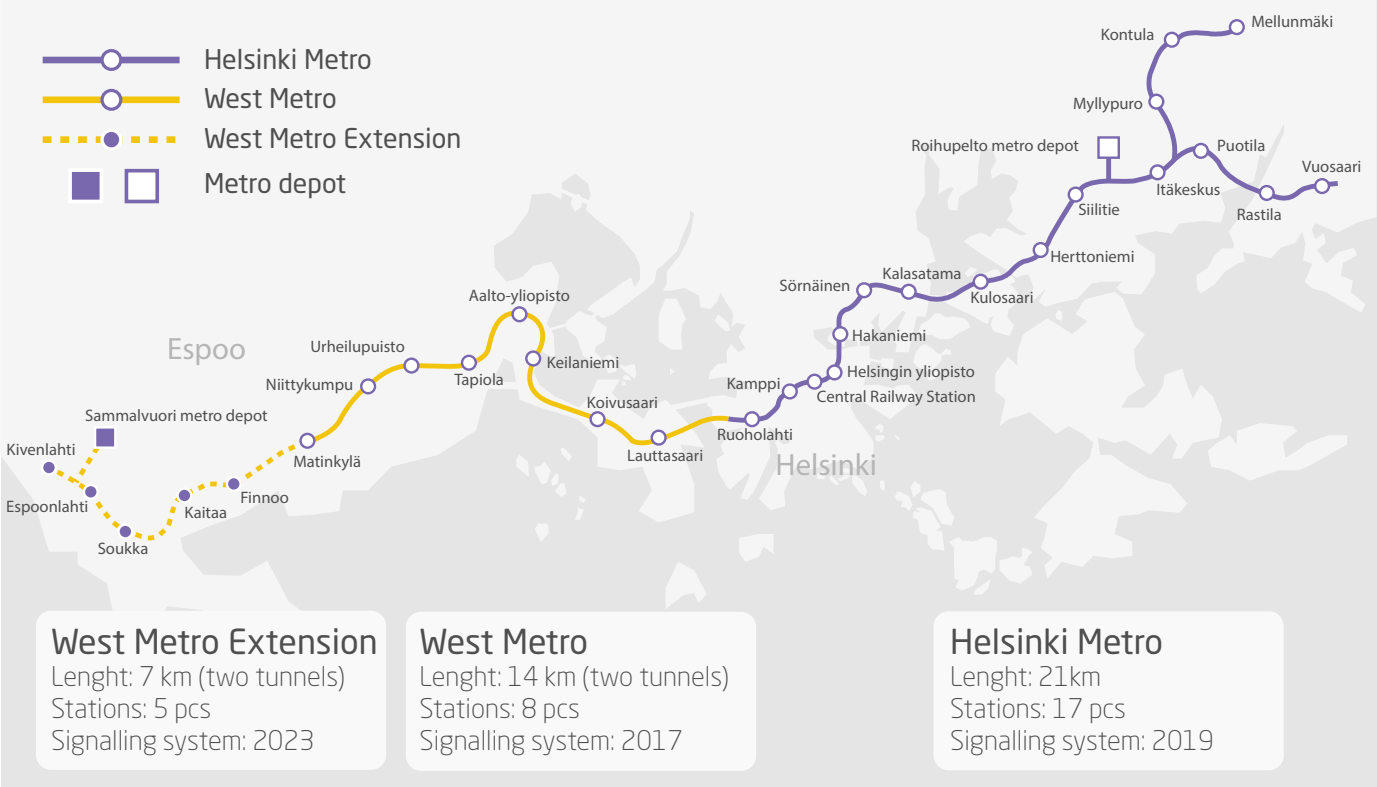

Bild 1: U-Bahn-Netz im Großraum Helsinki
Fig. 1: The Helsinki Capital Area Metro network

2 Sicherung der nördlichsten U-Bahn der Welt

2.1 U-Bahn im Großraum Helsinki

Die U-Bahn von Helsinki wurde 1982 eröffnet und im Laufe ihrer Geschichte mehrmals erweitert. Die größte Veränderung gab es 2017, als die U-Bahn-Gleise zum ersten Mal die Stadtgrenzen von Helsinki überquerten und bis nach Espoo verlängert wurden. Das U-Bahn-West-Projekt brachte acht neue Stationen in das Metronetz. Derzeit steht ein weiteres Großprojekt, die Verlängerung der U-Bahn West, kurz vor der Fertigstellung (Bild 1).

2.2 Kritische Beschaffung in der Vorentwurfsphase

Der ursprüngliche Plan sah vor, die Sicherungsanlage der U-Bahn West mit CBTC-Technologie (Communication Based Train Control) zu realisieren und im vollautomatischen GOA 4-Betrieb (Grade of Automation 4) zu betreiben. Dieser Plan wurde jedoch Anfang 2015 aufgegeben, und die Sicherungsanlage musste kurzfristig neu ausgeschrieben und neu beschafft werden. Als Mipro 2015 mit der Lieferung des Stellwerks und des Verkehrsleitsystems für die U-Bahn-Verlängerung beauftragt wurde, war keine Zeit zu verlieren. Dank der modularen COTS-Lösung war die Entwicklung der richtigen Ausrüstungskonfigurationen für jede Station ein schneller Prozess, und bereits in der Vorentwurfsphase konnte mit dem Kauf der Ausrüstung begonnen werden. Obwohl bei der endgültigen Planung noch einige zusätzliche Anforderungen berücksichtigt werden konnten, wäre die Erweiterung des Systems aufgrund der modularen Architektur immer noch möglich gewesen. Die Lieferzeiten des COTS-Plattformanbieters unterstützten ebenfalls den schnellen Projektstart.

2.3 Spezielle Schnittstellen und Funktionen

Da es sich bei der neuen Linie um eine Verlängerung der bestehenden U-Bahn-Linie handelte, wurde eine Schnittstelle zum vor-

2.2 Critical procurement in the preliminary design phase

The original plan was to implement the West Metro signalling using CBTC technology to be operated in fully automatic GOA 4 (Grade of Automation 4) operations. However, this plan was cancelled in early 2015 and the signalling system had to be re-tendered and re-procured on a fast schedule. When Mipro was selected to deliver the interlocking and traffic control system for the metro extension in 2015, there was no time to be wasted. Thanks to the used modular COTS solution, designing the right equipment configurations for each station was a quick process and equipment purchases were able to be started well in advance, already in the preliminary design phase. Even though some additional needs still had to be taken into account during the final design, the expansion of the system would still have been possible due to its modular architecture. The COTS platform supplier's delivery times also supported the fast pace of the project start-up.

2.3 Special interfaces and functions

As the new line involved an extension to the existing operating metro line, an interface to that system was needed. The project organisation could not find an economically and technically sensible way of making the changes to the existing metro line's signalling system. For this reason, the interface was not built in the usual way where two signalling systems communicate together and thus jointly protect any train movements between the systems. In co-operation with the customer and the project safety organisation, Mipro designed and built a special interface, where the two systems' control and supervision areas overlapped to ensure safe traffic at the border of the two systems. The new metro section has a total of 52 different technical systems to ensure passenger safety and a smooth travel experi-

handenen System benötigt. Die Projektorganisation konnte keine wirtschaftlich und technisch sinnvolle Möglichkeit finden, Änderungen an der Sicherungsanlage der bestehenden U-Bahn-Linie vorzunehmen. Aus diesem Grund wurde die Schnittstelle nicht wie herkömmlich so gestaltet, dass die beiden Sicherungssysteme miteinander kommunizieren und so gemeinsam die Zugbewegungen zwischen den Systemen absichern. In Zusammenarbeit mit dem Kunden und der Sicherheitsorganisation des Projekts entwarf und entwickelte Mipro eine spezielle Schnittstelle, an der sich die Kontroll- und Überwachungsbereiche der beiden Systeme überschnitten, um einen sicheren Verkehr im Grenzbereich der beiden Systeme zu gewährleisten. Die neue U-Bahn-Strecke verfügt über insgesamt 52 verschiedene technische Systeme, um die Sicherheit der Fahrgäste und eine reibungslose Fahrt zu gewährleisten. Einige dieser Systeme sind auch mit dem Sicherungssystem verbunden. Natürlich reicht allein die Schnittstelle für die Datenübertragung nicht aus, sondern es müssen auch Funktionen geplant und in die Systeme implementiert werden. Die Flexibilität der modularen COTS-Plattform und die Architektur von Mipro ermöglichten ungewöhnliche Schnittstellen und Funktionen, ohne dass das Basisprodukt selbst stark angepasst werden musste.

2.4 Vorzertifizierte Plattform, um Zeit und Geld zu sparen

Bei Schienenverkehrsprojekten ist die Erlangung der SIL4-Genehmigung des endgültigen Ergebnisses der Lieferung ein großer und wichtiger Prozess. Die Eignung des gelieferten Systems für die vorgesehene Umgebung und Anwendung muss nachweisbar sein. Bei allen drei U-Bahn-Projekten von Mipro wurde eine vorzertifizierte COTS-Plattform verwendet. Die verwendete Plattform wurde gemäß den Standards der Eisenbahnsicherungsanlagen entworfen und implementiert. Der Einsatz einer vorzertifizierten Plattform reduzierte die Beweislast gegenüber dem unabhängigen Sicherheitsbewerter (EN ISA) während des Projektentwurfs und der Implementierung, und als Systemlieferant konnte sich Mipro auf seine eigenen Kernkompetenzen und den Nachweis der Eignung der Anwendung selbst konzentrieren. Der Hersteller der COTS-Plattform hat bereits dafür gesorgt, dass die relevanten Standards eingehalten werden und dass die plattformbezogene Hardware, Software, Programmiertools, Kommunikationsprotokolle und die zugehörige Dokumentation den erforderlichen Bewertungen unterzogen wurden. Dies bedeutet, dass die vorzertifizierte Plattform in SIL4-Anwendungen eingesetzt werden kann, sofern der Systemlieferant die vom COTS-Hersteller festgelegten sicherheitsbezogenen Anwendungsbedingungen (SRAC) kontrolliert und die spezifische Anwendung in kontrollierter Weise für die vorgesehene Umgebung konzipiert und implementiert.

3 U-Bahn im Großraum Helsinki heute

Die U-Bahn West ist seit 2017 im Fahrgastbetrieb. Nach dem U-Bahn-West-Projekt hat Mipro den Zuschlag für zwei weitere U-Bahn-Projekte im Großraum Helsinki erhalten: zum einen der Austausch der Sicherungsanlage des alten Teils der U-Bahn Helsinki (2017–2019) und zum zweiten die Errichtung der Sicherungsanlage für die zweite westliche Verlängerung (2020–2022), die die U-Bahn-Strecke noch weiter bis zur Stadt Espoo verlängert und das Netz um fünf neue Stationen und ein unterirdisches U-Bahn-Depot erweitert. Zum jetzigen Zeitpunkt steht das Sicherungsanlagenprojekt für die zweite Verlängerung kurz vor dem Abschluss, und die Fahrerschulung auf dem neuen Streckenabschnitt läuft derzeit, gesichert und gesteuert durch das neue System. ■

ence. Some of these systems also interface with the signalling system. Of course, the interface alone is not enough for the data transmission, so functions have also had to be planned and implemented in the systems. The flexibility of the modular COTS platform and Mipro's architecture have enabled unusual interfaces and functions without any heavy adaptation of the base product itself.

2.4 A pre-certified platform to save time and money

Getting the SIL4 approval of the final output of a delivery in rail transport projects is a big and important process. The delivered system's suitability for its intended environment and application must be demonstrable. All three Mipro metro projects have used a pre-certified COTS platform. The used platform has been designed and implemented according to the railway signalling standards. The use of a pre-certified platform has reduced the burden of proof in relation to the independent safety assessor (EN ISA) during the project design and implementation and, in its capacity as the system supplier, Mipro was able to focus on its own core competencies and prove the suitability of the application itself. The COTS platform's manufacturer has already taken care of the compliance with the relevant standards and ensured that the platform-related hardware, software, programming tools, communication protocols and related documentation have undergone the necessary assessments. This means that the pre-certified platform is capable of being used in SIL4 applications, provided the system supplier controls the safety related application conditions (SRAC) set by the COTS manufacturer and designs and implements each specific application in a controlled manner for the intended environment.

3 The Helsinki Capital Area Metro today

The West Metro has been in passenger operation since 2017. After the West Metro project, Mipro was awarded two other projects in the capital area metro: the re-signalling of the old part of the Helsinki Metro (2017–2019) and the signalling for the second western extension (2020–2022) which extends the metro tracks even further to the city of Espoo and adds five new stations and an underground metro depot to the network. At the time of writing, the signalling project for the second extension is nearing its completion and driver training on the new line section that is secured and controlled by the new system is currently underway. ■

LITERATUR | LITERATURE

[1] https://doyleresearch.wordpress.com/2012/07/26/why-cots-is-important-to-the-network-and-telecom-industry-2/ 16.6.2022

AUTOR | AUTHOR

Janne Siirilä
Account Manager, B.Sc.
Mipro Oy
Anschrift / *Address*: Bertel Jungin aukio 1, FI-02600 Espoo
E-Mail: janne.siirila@mipro.fi