



Zukunftsfähige Sicherheitstechnik für
den Schienenverkehr

Leitfaden



Dipl.-Ing. Sedat Sezgün, Head of Rail Segment, HIMA



Thomas Bell, Technology Development Manager Rail, HIMA

Warum sich der Einsatz von Commercial-off-the-Shelf-(COTS-)Steuerungen für
Zugsicherungs-, Zugsteuerungs-, Stellwerk- und Signalsysteme lohnt. →

Zusammenfassung

Heute dominiert proprietäre Sicherheitstechnik die Bahnindustrie. Doch die Zeichen stehen auf Wandel: Mehr und mehr Systemintegratoren, Rolling-Stock-Hersteller und Eisenbahnbetreiber weltweit setzen auf standardisierte Commercial-off-the-Shelf-(COTS-)Systeme. Dieser Leitfaden erklärt, warum COTS-Systeme die kosteneffizientere und zukunftsfähigere Lösung zur Sicherung von Stellwerken, Bahnübergängen, Signalanlagen und Schienenfahrzeugen sind. Dabei werden sowohl sozio-ökonomische Rahmenbedingungen als auch aktuelle Normung und technische Anforderungen beleuchtet. Außerdem gibt der Leitfaden Hilfestellung, worauf es bei der Auswahl des optimalen COTS-Systems für die eigene Anwendung ankommt.



Sedat Sezgün

Elektrotechnikstudium an der Hochschule Darmstadt bis 2006, seit 2006 bei HIMA für Bahnkunden zuständig, seit 2015 globale Leitung des Geschäftsbereichs Rail

E-Mail: s.sezguen@hima.com

Thomas Bell

Technology Development Manager Rail

E-Mail: t.bell@hima.com

Inhaltsverzeichnis

1. Sozio-ökonomische Rahmenbedingungen	4
1.1 Der globale Markt für Sicherheitstechnik in der Bahnindustrie	4
1.2 Die Anwendergruppen und ihre Bedürfnisse	5
1.3 Gesetzgebung, Normen und Zulassungsbehörden	5
1.4 Technische Rahmenbedingungen	6
2. COTS vs. proprietäre Sicherheitstechnik	8
2.1 Proprietär vs. standardisiert	9
2.2 Geschlossen vs. offen	9
2.3 Instandhaltung	9
2.4 Zukunftsfähigkeit	9
2.5 Wirtschaftlichkeit	10
3. COTS ist nicht gleich COTS	11
3.1 Zertifizierung	11
3.2 Skalierbarkeit	11
3.3 Neuartige Wartungskonzepte	11
3.4 Flexibilität	12
3.5 Schulungsbedarf	12
3.6 Interoperabilität	13
3.7 Cyber-Security	14
4. Fazit	15

1. Sozio-ökonomische Rahmenbedingungen

1.1 Der globale Markt für Sicherheitstechnik in der Bahnindustrie

Urbanisierung und ein wachsendes Umweltbewusstsein führen weltweit zu einer erhöhten Nachfrage nach zuverlässigen, umweltfreundlichen Transportmitteln. Dies gilt insbesondere für Ballungszentren, wo eine stetig wachsende Anzahl von Passagieren auf sichere, schnelle und komfortable Weise befördert werden muss. Die steigenden Passagierzahlen machen einen Ausbau der Netzkapazität unabdingbar. Der Schlüssel zu der benötigten Produktivitäts- und Effizienzsteigerung liegt im konsequenten Einsatz moderner Technologien. Häufig fehlt jedoch das Geld für notwendige Modernisierungsmaßnahmen und auch die Wartung wird nicht selten vernachlässigt, sodass Systeme oft auf Verschleiß gefahren werden. Dieser massive Modernisierungsrückstand in Kombination mit dem erhöhten Kostendruck durch sinkende Budgets hat den Bedarf an flexiblen, kosteneffizienten Steuerungslösungen in der Bahnindustrie weltweit erhöht.

Die Studie „Worldwide Rail Market Study – status quo and outlook 2016“ von Roland Berger zeigt, dass das Volumen des weltweiten Bahnmarktes auf ca. 101 Milliarden Euro geschätzt wird. Der Anteil der computergesteuerten Anwendungen lag 2015 bei 11,3 Milliarden Euro. Rund ein Drittel hiervon wird der Sicherheitselektronik zugeschrieben, also rund 3,7 Milliarden Euro.

Der Anteil von Safety-Steuerungen an der Sicherheitselektronik in der Bahnindustrie betrug 2015 etwa 253 Millionen Euro. Dabei wird der Markt derzeit noch klar von proprietärer Technik dominiert. Allerdings ist weltweit eine klare Tendenz hin zu Commercial-off-the-Shelf-(COTS-)Technologien erkennbar,

sodass damit zu rechnen ist, dass sich diese Statistik in den nächsten Jahren kontinuierlich umverteilen wird. Darauf deuten auch die Ergebnisse einer Unternehmensumfrage im Rahmen der Studie „Megatrends im europäischen Bahnmarkt“ des Beratungsunternehmens ASTRAN im August 2016 hin. Darin gaben 14 der 30 befragten Unternehmen an, „[...] zukünftig auf Standardindustriekomponenten im Sinne von Commercial-off-the-Shelf-(COTS-)Technologien setzen zu wollen [...]“.

Die Frage, ob proprietäre Sicherheitstechnologien oder standardisierte Commercial-off-the-Shelf-(COTS-)Lösungen zu bevorzugen sind, bewegt aktuell den Markt. In der oben genannten ASTRAN-Studie bewerteten die befragten Unternehmen unter den acht aufgeführten globalen Megatrends den Trend „Kundenspezifische Lösungen vs. Standardindustriekomponenten“ als den dringlichsten und nach der Digitalisierung zweitwichtigsten Trend der Branche.

Als COTS bezeichnet man seriengefertigte Steuerungen, die in großer Stückzahl als Standardkomponenten verkauft und in verschiedenen Industriezweigen eingesetzt werden. Diese Standardkomponenten sind deutlich kostengünstiger als proprietäre Systeme und erfüllen gleichzeitig alle wichtigen Sicherheitsstandards der Bahnindustrie. Man geht davon aus, dass der Anteil der COTS-Steuerungen am Weltmarkt für Sicherheitselektronik in der Bahnindustrie bis 2020 etwa 25 Prozent betragen wird.

Eine zentrale Herausforderung in der Bahnindustrie besteht darin, dass der globale Markt für Sicherheitstechnik extrem diversifiziert ist. Zumeist besteht aufgrund historisch gewachsener



Strukturen ein wahres Sammelsurium an heterogener Technik aus verschiedensten Jahrzehnten. Zusätzlich unterscheiden sich Bahninfrastruktur und Normen je nach Land. So gibt es international viele unterschiedliche Systeme, beispielsweise für Betriebsordnungen, Zugbeeinflussung, Signalisierung oder Stromversorgungen. Ein weiterer kritischer Punkt auf dem Weg hin zu mehr COTS besteht im unkalkulierbaren Einfluss der Politik, der aufgrund der oft staatlichen Bahnbetriebe und Zulassungsbehörden nicht zu unterschätzen ist.

Global gesehen wird vor diesem Hintergrund klar, dass das Level der Anforderungen an und die Verbreitung von Sicherheitselektronik je nach Land bzw. Region sehr unterschiedlich ausfällt. Unabhängig von den unterschiedlichen Rahmenbedingungen ist allen Märkten gemein, dass von der Sicherheitstechnik erwartet wird, dass sie ein entsprechendes Sicherheitsniveau (Freiheit von systematischen/zufälligen Fehlern) erfüllt. Dies ist eine Anforderung, die in vielen anderen Branchen ähnlich existiert und bereits durch COTS-Systeme erfüllt wird. Sehr viele Funktionen müssen dabei das höchste Sicherheitslevel – Safety Integrity Level 4 (SIL 4) – erfüllen.

1.2 Die Anwendergruppen und ihre Bedürfnisse

Zunächst gilt es, nach verschiedenen Anwendergruppen zu unterscheiden. Bahnbetreiber als Endanwender sind häufig in Staatsbesitz. Oft sind es politische Gremien wie kommunale oder regionale Regierungen, die Strategie und Konzepte der Bahnbetreiber stark beeinflussen. Durch diese politischen Abhängigkeiten können technische Zulassungsprozesse sehr aufwendig und langwierig sein. Bahnbetreiber sind daher eher zögerlich bei der Einführung neuer Technologie wie Commercial off-the-Shelf (COTS). Sind sie jedoch erst mal überzeugt, laufen Liefer- und Serviceverträge häufig jahrzehntelang. Um bei Bahnbetreibern direkt zum Einsatz zu kommen, muss Sicherheitstechnik daher höchsten Ansprüchen genügen und alle internationalen und nationalen Zertifizierungen vorweisen können. Bahnbetreiber legen bei der Sicherheitselektronik – neben Sicherheit und Zertifizierungen – vor allem Wert auf Dinge wie gute Handhabbarkeit, geringe Ausfallraten und schnelle Ersatzteillieferung.

Die zweite Anwendergruppe von Sicherheitstechnik sind Hersteller von Schienenfahrzeugen (Rolling Stock). Die Kernkompetenz dieser Unternehmen liegt in der kompletten Entwicklung, Fertigung und Inbetriebnahme von Schienenfahrzeugen. Auf dem Gebiet der Sicherheitselektronik (Steuerungen, Sensoren, Aktoren) ist das Know-how in der Industrie (Maschinen- und Anlagenbau, Chemie, Kernkraftwerke) oder im Automotive-Bereich jedoch weiter entwickelt. Diese Branchen nutzen COTS, weil es die wirtschaftlichste Lösung darstellt. Basis hierfür sind die im Vergleich zur Bahnindustrie bzw. zu Herstellern von Schienenfahrzeugen um ein Vielfaches höheren Stückzahlen sowie die Tatsache, dass in diesen Branchen COTS als fortschrittlichste Lösung angesehen wird. Hier kann die Bahnindustrie sicher noch von anderen Industrien lernen. Herstellern von Schienenfahrzeu-

gen ist besonders wichtig, dass die eingesetzte Sicherheitselektronik den Ansprüchen und Anforderungen der Endkunden, also der Bahnbetreiber, entspricht. Höchste Sicherheit, Zuverlässigkeit und Langzeitverfügbarkeit sind hier nur einige der Punkte, auf die es bei der Sicherheitselektronik für Schienenfahrzeuge ankommt. Auch Zertifizierungen für die Akzeptanz der nationalen Zulassungsbehörden sind entscheidend.

Die dritte große Anwendergruppe sind die Systemintegratoren. Diese nutzen Sicherheitselektronik beispielsweise bei der Entwicklung eigener Stellwerk- und Bahnübergangslösungen, die häufig weltweit zum Einsatz kommen. Der Endkunde nimmt in diesen Fällen von der Art der Sicherheitselektronik, die dahinter steht, zunächst wenig Notiz, obwohl diese häufig den Kern der Lösungen bildet. Er sieht die Lösung eher als Gesamtpaket. Will ein Systemintegrator eine komplett neue Stellwerk- oder Bahnübergangslösung entwickeln, so muss er zunächst eine Menge Arbeit in Entwicklung und Zertifizierung stecken. Das heißt, die verwendete Sicherheitstechnik sollte im Idealfall bereits die nötigen Zertifizierungen mitbringen und möglichst flexibel programmierbar sein. Darüber hinaus erwarten Systemintegratoren von der Sicherheitstechnik, dass sie langzeitverfügbar und zukunftsicher ist, damit ihre entwickelte Lösung nicht in wenigen Jahren obsolet ist.

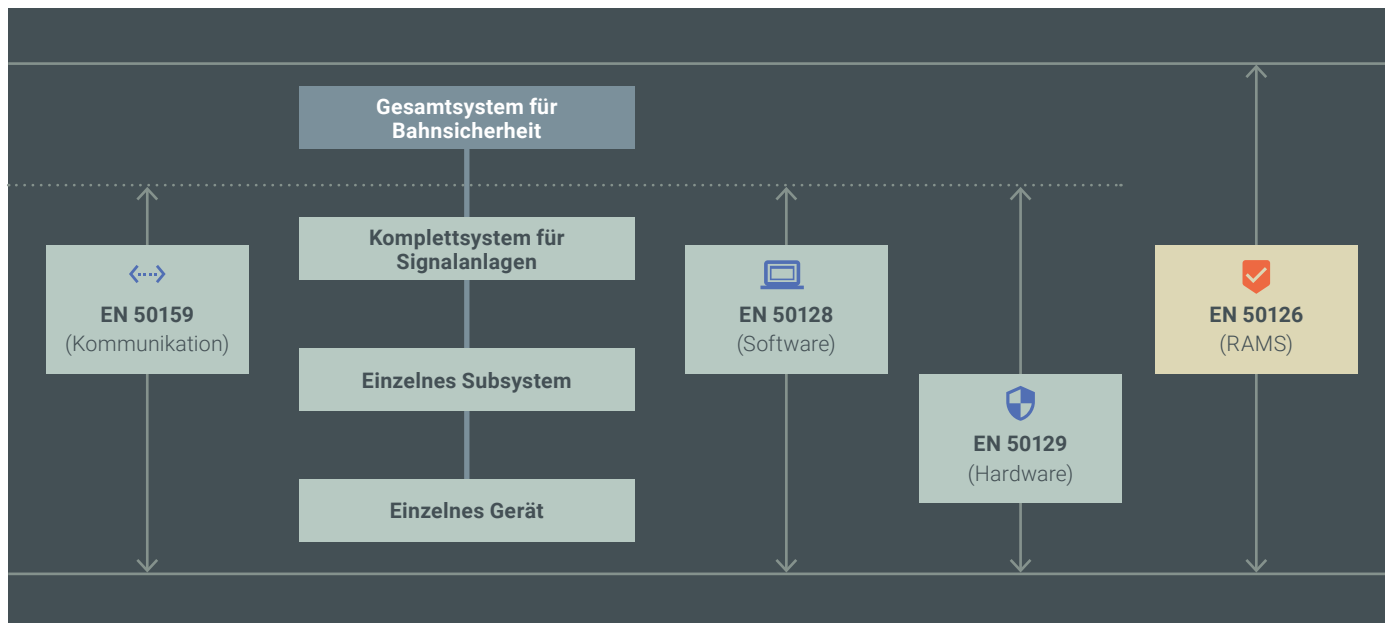
1.3 Gesetzgebung, Normen und Zulassungsbehörden

Der Bahnmarkt ist historisch bedingt und aufgrund der hohen Relevanz des Themas Sicherheit stark von Normen und Zulassungsbehörden geprägt. Generelle Safety-Standards in Europa, geregelt vom European Committee for Electrotechnical Standardization (CENELEC), sind auch weltweit akzeptiert. Das bedeutet, ein Sicherheitssystem, das nach CENELEC-Standards zertifiziert ist, kann weltweit in Bahnanwendungen eingesetzt werden. Zusätzlich zu diesen internationalen Standards gibt es eine Vielzahl von nationalen Regularien, die sich von Land zu Land deutlich unterscheiden können.

Die wichtigsten CENELEC-Normen, die im Zusammenhang mit Sicherheitselektronik zu nennen sind, sind:

- EN 50126: Legt den Rahmen für Safety fest, indem sie das Begriffspaket „Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit“ (im englischen RAMS, was als Abkürzung für „Reliability, Availability, Maintainability, Safety“ steht) definiert
- EN 50129: Regelt sicherheitselektronische Systeme für Signalanwendungen
- EN 50128: Bestimmt Anforderungen für Software von Steuerungen und Schutzeinrichtungen
- EN 50125-3: Regelt Umweltbedingungen für Betriebsmittel in Bahnanwendungen, Teil 3 behandelt speziell die Umweltbedingungen für Signal- und Telekommunikationseinrichtungen
- EN 50155: Regelt Umweltbedingungen für elektronische Einrichtungen auf Bahnfahrzeugen

Abbildung 1: Geltungsbereich der CENELEC-Standards



Zusätzlich zu diesen Standards gibt es noch zahlreiche gesetzliche Regelungen auf nationaler und regionaler Ebene (z. B. EU, Asien, Australien, Nord-/Südamerika). Fast alle Regionen haben als gesetzliche Grundlage die Anforderung, dass der Stand der Technik eingehalten wird. IEC und ISO als globale Standards sowie ihre auf EU und nationaler Ebene umgesetzten Regelwerke (Technische Spezifikationen für die Interoperabilität, TSI, und Normen der CENELEC, EN) bedienen und konkretisieren diese gesetzlichen Anforderungen. So definiert die europäische CSM-Verordnung (Common Safety Methods) beispielsweise eine Ausfallrate für Sicherheitssteuerungen von 10^{-9} .

Schließlich gibt es die nationalen Zulassungsbehörden (auch NSAs, National Safety Authorities genannt), die sicherstellen, dass alle geforderten Standards eingehalten werden. Die Zulassungsprozesse für Sicherheitselektronik in der Bahnindustrie sind hochkomplex und können teilweise Jahre dauern. Schienenfahrzeuge unterliegen in Europa einer ständigen Beobachtung durch die NSAs (EBA, BAV etc.). Sowohl Erstzulassung als auch Betrieb und spätere Veränderungen an Loks, Triebzügen etc. sind strengen Zulassungsverfahren unterworfen. Voraussetzung für eine erfolgreiche Zulassung eines Schienenfahrzeugs sind beispielsweise verschiedene Gutachten für Hardware und Software, funktionale Integrationsgutachten, entsprechende Zertifikate und zertifizierte Komponenten. Die Dokumentation gemäß den neuesten Standards ist mit einem großen Aufwand verbunden, da sich die nationalen und internationalen Normen häufig ändern. Gerade für Hersteller von Schienenfahrzeugen ist es daher nicht leicht, für jede eingesetzte Komponente alle Nachweise ständig auf dem neuesten Stand zu halten. Die heute sehr umfangreiche und zeitaufwendige Beschaffung und Pflege von Nachweisdokumenten lässt sich mit bereits zugelassenen, vorzertifizierten COTS-Komponenten deutlich reduzieren.

1.4 Technische Rahmenbedingungen

Moderne Sicherheitselektronik muss eine ganze Reihe von technischen Anforderungen erfüllen. Im Zuge der Digitalisierung, die auch in der Bahnindustrie Einzug hält, ergeben sich ständig neue Anwendungen, die es zu bedienen gilt. Hierzu zählen beispielsweise selbstfahrende Züge (Automatic Train Operation, ATO), Bahnsteigabfertigungsverfahren mit Kameras, Türsteuerungen, Antriebsstrangüberwachungen oder europaweite Zug-sicherungsfunktionen. All diese Funktionen lassen sich am günstigsten mit einem durchgängigen COTS-Zugsicherungs-system realisieren, da dieses verschiedenste I/O-Module, diverse Bussysteme und performante Prozessoren bietet.

Ein weiterer Aspekt, der mit der Digitalisierung der Bahntechnik zusammenhängt, ist das Thema IT-Sicherheit bzw. Cyber-Security. Denn immer mehr sicherheitsrelevante Steuerungsprozesse beruhen auf cloud- oder internetbasierten Lösungen. Auch im digitalen Zeitalter bilden Sicherheitssteuerungen die Basis für kritische Anwendungen wie Bahnübergänge, Schienenfahrzeuge oder Stellwerke. Immer wichtiger wird dabei das Zusammenspiel von Safety und Security.

Ein Zugsicherungssystem (Train Control Management System, TCMS), das komplette Züge in Mehrfachtraktion steuert – das heißt bis zu vier Loks zusammen bilden eine Einheit – erfordert nicht nur eine SIL 4-konforme Realisierung gegen innere systematische und zufällige Fehler, sondern auch eine hohe Verfügbarkeit der Fahrzeuge. Ausfälle der Elektronik bei millionenteuren Fahrzeugen werden seitens der Betreiber sehr ungern gesehen bzw. akzeptiert. Höchste Verfügbarkeit ist daher für moderne Zugsicherungssysteme eine ganz zentrale Anforderung. So gelten für Sicherheitssteuerungen in der Bahnindustrie dieselben

Anforderungen bezüglich der Ausfallwahrscheinlichkeit pro Stunde (Probability of Failure per Hour, PFH) gemäß SIL wie beispielsweise in der Prozessindustrie (siehe Abbildung 2).

Abbildung 2: Safety Integrity Level gemäß CENELEC

Tolerierbare Gefährdungsrate THR pro Stunde und pro Funktion	Safety Integrity Level (SIL)
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

Schienenfahrzeuge müssen notwendigerweise kontinuierlich gewartet werden, damit eine möglichst hohe Verfügbarkeit – und damit Pünktlichkeit für den Bahnkunden – erreicht wird. Zu Wartungsarbeiten müssen die Fahrzeuge in Depots. Bei bestimmten Wartungs- und Reparaturarbeiten muss hier die Leittechnik komplett heruntergefahren werden, damit die Gefahr von ungewollten Schaltungsvorgängen beseitigt wird. Mit Leittechniksystemen, die SIL 3 oder SIL 4 erfüllen, modulare und skalierbare Software-Algorithmen beinhalten sowie rückwirkungsfrei und unabhängig voneinander arbeiten, ist es möglich, viele Wartungsarbeiten auch bei eingeschalteter Leittechnik durchzuführen. Viele Arbeiten können so parallelisiert werden

(auch die Leittechnik-Wartung der Hard- und Software), was in Summe zu einer Reduzierung von Stillstandzeiten führt. Voraussetzung ist, dass sowohl das Gerätesystem als auch die Software-Tools die entsprechenden Möglichkeiten bieten.

Der typische Produktlebenszyklus in der Bahnindustrie stellt ganz besondere Anforderungen an die Sicherheitselektronik. Vom Wesen her sind Lokomotiven und Triebzüge sehr langlebige Produkte. 30 Jahre und mehr können und müssen diese kapitalintensiven Investitionsgüter in Betrieb bleiben. Eine Fahrzeugvariante bzw. Produktfamilie hat sogar 40 bis 50 Jahre Bestand. Dabei ist es unumgänglich, dass im Laufe der Lebenszeit dieser Fahrzeuge viele Wünsche seitens der Bahnbetreiber entstehen, die von den Schienenfahrzeugherstellern umgesetzt werden müssen. Auch spielt der Plattformgedanke bei den Herstellern eine große Rolle. So entstehen auf Basis einer ersten Fahrzeugentwicklung mitunter bis zu 20 Varianten. Das bedeutet, dass Sicherheitselektronik langzeitverfügbar sowie einfach und flexibel adaptierbar sein muss.

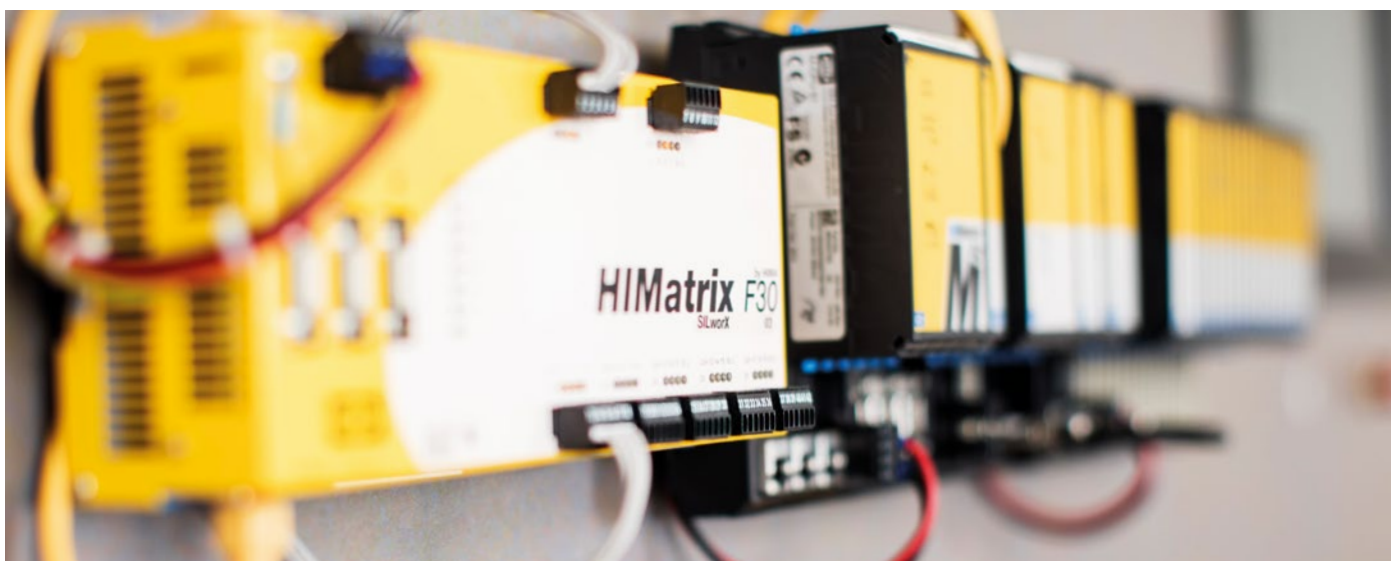


2. COTS vs. proprietäre Sicherheitstechnik

Bislang wird der Bahnmarkt noch von proprietären Sicherheitslösungen dominiert. Doch der Trend geht hin zu COTS. Vor einigen Jahren noch undenkbar, gibt es heute schon Anwendungen, bei denen die Nutzung von COTS explizit gefordert wird.

Vor 10 bis 15 Jahren waren die Vorbehalte gegenüber COTS noch groß. Doch unter dem steigenden Kostendruck überlegten erste Bahnunternehmen Anfang der 2000er Jahre, ob diese bewährte Sicherheitstechnologie nicht auch im Schienenverkehr einsetzbar wäre. Um Sicherheitssteuerungen, die sich in ande-

ren sicherheitskritischen Industrien wie der Prozessindustrie bereits bewährt hatten, auch im Schienenverkehr einsetzen zu können, mussten COTS-Hersteller diese nach den Standards der CENELEC prüfen und zertifizieren lassen. Da sich die Sicherheitsanforderungen beispielsweise von Prozess- und Bahnindustrie überschneiden, können im Schienenverkehr exakt dieselbe Hardware und dasselbe Betriebssystem verwendet werden. Lediglich Berechnungen und Dokumentation müssen angepasst und das Steuerungskonzept auf die CENELEC-Philosophie übertragen werden.



Beispiele für COTS-Sicherheitssteuerungen, die sich bereits in zahlreichen sicherheitskritischen Anwendungen in der Prozessindustrie bewährt haben und jetzt im Schienenverkehr zum Einsatz kommen, sind HIMax (oben) und HIMatrix (unten).

Warum sich COTS zunehmend durchsetzt, wird deutlich, wenn man die wichtigsten Kriterien, die moderne Sicherheitslösungen laut übereinstimmender Expertenmeinung in der Bahnindustrie erfüllen sollten, ansieht und mit proprietären Systemen vergleicht.

2.1 Proprietär vs. standardisiert

Proprietäre Sicherheitssysteme sind nur für diesen Zweck entwickelt und werden in kleiner Stückzahl produziert. Das macht sie nicht nur teurer als COTS-Steuerungen, sondern schränkt auch die Flexibilität in der Anwendung ein. Anwender wie Bahnbetreiber sind nach der Erstausrüstung gezwungen, die Folgesysteme von ein und demselben Hersteller – häufig dem Leittechnik-Lieferanten – zu beziehen.

Bei COTS handelt es sich hingegen um standardisierte Systeme, die in hoher Stückzahl produziert werden und sich bereits in zahlreichen sicherheitskritischen Anwendungen außerhalb der Bahnindustrie bewährt haben. Durch Verwendung von Standardkomponenten sind Bahnbetreiber flexibel in der Auswahl der Lieferanten und können je nach Anwendung für sich die „Best of breed“-Lösung, z. B. in der Sicherheitstechnik, auswählen.

2.2 Geschlossen vs. offen

Entscheidende Voraussetzung für das digitale Bahnzeitalter ist die Vernetzung zahlreicher unterschiedlicher Systeme für den Datenaustausch. Auch hier sind COTS-Sicherheitssteuerungen gegenüber proprietären Lösungen im Vorteil. Denn bei herkömmlichen Systemen sind Schnittstellen nicht standardisiert. Die Integration solcher Lösungen in bestehende heterogene Automatisierungsarchitekturen kann daher schwierig sein. Aufgrund der proprietären Programmierung kann häufig nur der Steuerungshersteller Erweiterungen, Updates und Instandhaltung durchführen.

COTS-Steuerungen haben hingegen ein Betriebssystem, das auf weltweit verfügbaren Standard-Programmiersprachen gemäß IEC 61131 basiert. Zudem bieten sie Schnittstellen zu allen wichtigen Kommunikationsprotokollen wie Ethernet TCP/UDP, RS485, RS422, RS232 und CAN. Die Kommunikation erfolgt über gängige Industrieprotokolle.

2.3 Instandhaltung

Im Laufe der langen Lebenszeit einer Sicherheitssteuerung kommen viele Menschen mit ihr in Berührung. Hierzu zählen Hardware- und Software-Entwickler, Bediener wie Lokführer, Wartungspersonal, Gutachter, Prüfer von Zulassungsbehörden und Inbetriebnehmer. Deshalb gilt: Je transparenter und einfacher das System ist, desto besser. Denn allen Menschen, die

sich tagtäglich mit sicherheitskritischen Dingen beschäftigen, sollte es so einfach wie möglich gemacht werden, sehr komplexe Maschinen wie Schienenfahrzeuge sicher beherrschen zu können. Gerätesysteme, Sicherheitsarchitekturen und Werkzeuge, mit denen solche Systeme entwickelt und später gepflegt werden müssen, sollten einen möglichst geringen Komplexitätsgrad aufweisen. Speziell das immer mehr in den Fokus rückende Software-Engineering sollte global von möglichst vielen Software-Entwicklern in einheitlicher Weise beherrscht werden. Denn das erleichtert Handhabung, Wartung und Systemerweiterungen.

Darüber hinaus müssen diese sehr langlebigen Fahrzeuge von mehreren Generationen von Technikern, Ingenieuren und Behörden „verstanden“ werden. Und dies in vielen Regionen und Märkten dieser Erde. Auch der Aufwand für das Training der Service-Mitarbeiter reduziert sich, je weniger komplex die Sicherheitssysteme sind.

Derzeit ist es häufig so, dass bei Bahnanwendungen ein Sammelsurium an proprietärer Technik im Einsatz ist, oft bestehend aus mehreren Gerätegenerationen. Die fehlende Standardisierung und Modularisierung führt dazu, dass Wartung und Systemerweiterungen sehr aufwendig und kostspielig sind.

Standardisierung, weite Verbreitung und Verwendung von industriellen Programmiersprachen gemäß IEC 61131 machen COTS-Steuerungen deutlich einfacher in der Handhabung und Instandhaltung, sodass Betriebs- und Lebenszykluskosten bei gleichem Sicherheitslevel im Vergleich zu proprietärer Technik deutlich geringer ausfallen.

2.4 Zukunftsfähigkeit

Aufgrund der geforderten Langzeitverfügbarkeit von Sicherheitssteuerungen im Schienenverkehr, begründet unter anderem durch die langen Nutzungszeiten von Schienenfahrzeugen, ist Zukunftsfähigkeit ein ganz wichtiges Bewertungskriterium. Je schneller die Digitalisierung voranschreitet und sich die Innovationszyklen verkürzen, desto mehr nimmt dieser Aspekt noch an Bedeutung zu.

Die Herausforderung besteht darin, dass insbesondere die Software über 20 bis 30 Jahre immer auf dem neuesten Stand sein muss. Aber auch die Hardware muss sich flexibel erweitern und modernisieren lassen, möglichst ohne dass es zu Stillständen kommt.

Bei proprietärer Technik ist der Aufwand, die Lösungen auf dem neuesten Stand zu halten, aufgrund der geringen Stückzahlen verhältnismäßig hoch. Zudem besteht für Anwender das Risiko, dass das Produkt vielleicht bei der nächsten Anwendung nicht mehr verfügbar ist. Durch die Standardisierung und weite Verbreitung der COTS-Systeme geben diese dem Anwender mehr Planungssicherheit. Das gilt auch bezüglich

Ersatzteil-Verfügbarkeit oder Software-Updates. Dank modularem Aufbau und Standard-Kommunikationsschnittstellen lassen sich COTS-Systeme einfach an veränderte Bedürfnisse anpassen, wenn sich nach Jahren Änderungen im Projekt ergeben.

2.5 Wirtschaftlichkeit

Der Elektronikanteil nimmt in der Bahnindustrie stetig zu, gerade in dezentralen Anwendungen (z. B. auf Basis des European Train Control System, ETCS). Das hat eine massive Modernisierungswelle zur Folge. Um dabei den Spagat zwischen Kosten- und Modernisierungsdruck hinzubekommen, suchen Bahnunternehmen möglichst kosteneffiziente Steuerungslösungen.

Und genau hier liegen die Schwächen der bislang hauptsächlich verwendeten proprietären Sicherheitstechnik. Durch die hohen Entwicklungskosten für die kleinen Stückzahlen fallen die Kosten für die Bahnunternehmen ziemlich hoch aus und die Kosten für die Obsoleszenz werden auf den Anwender abgewälzt. Zudem verteuert und erschwert die proprietäre, nicht standardisierte Technik die Instandhaltung, egal ob beim Schienenfahrzeug oder bei Infrastruktur. Durch die Abhängigkeit bzw. Bindung an einen einzigen Anbieter in Sachen Erweiterungen, Wartung und Instandhaltung gibt es eigentlich nur bei der Erstausrüstung eine Wettbewerbssituation.

Da viele Hersteller proprietärer Systeme von der Leittechnik her kommen, sind herkömmliche Sicherheitssteuerungen aufgrund der Fülle von Funktionen häufig überdimensioniert. Beispielsweise übernehmen heute elektronische Stellwerke auch Funktionen, die nicht sicherheitsrelevant sind, die aber Geld kosten. Die Kosten kommen dadurch zustande, dass diese Funktionen im Bereich der sicheren Funktionen entwickelt und getestet werden sowie bezüglich Rückwirkungsfreiheit auf die Sicherheit begutachtet werden müssen. So ist zum Beispiel in vielen Stellwerken die Steuerung der Fahrstraßen mit integriert. Will man eine neue Fahrstraße in den Prozess einbinden, muss man das ganze Stellwerk ändern und im schlimmsten Fall neu freigeben lassen, was mit hohen Kosten verbunden ist.

Aufgrund der Standardkomponenten und hohen Stückzahlen sind COTS-Steuerungen verständlicherweise deutlich günstiger in der Anschaffung. Aber hier hören die wirtschaftlichen Vorteile noch nicht auf: Erleichterte Inbetriebnahme und Instandhaltung, größere Freiheit bei der Lieferantenauswahl für den Endkunden, einfachere und zukunftssichere Programmierung, kurze Lieferzeiten und hohe Verfügbarkeit von Ersatzteilen sind nur einige der Gründe dafür, warum die Betriebs- und Lebenszykluskosten von COTS-Systemen im Vergleich zu herkömmlicher Sicherheitstechnik signifikant geringer ausfallen. Der Return on Investment (ROI) wird hier deutlich schneller erreicht.

3. COTS ist nicht gleich COTS

Nachdem wir ausführlich die Vorteile von COTS gegenüber proprietärer Sicherheitstechnik dargelegt haben, wollen wir nun erläutern, worauf es bei der Auswahl der COTS-Lösung ankommt. COTS-Systeme sind zwar standardisiert, unterscheiden sich aber im Detail.

3.1 Zertifizierung

Proprietäre Technik kann die ohnehin aufwendigen Zertifizierungs- und Zulassungsprozesse für Schienenfahrzeuge unnötig verkomplizieren. Für Systemintegratoren und Hersteller von Schienenfahrzeugen empfiehlt es sich, nur COTS-Systeme einzusetzen, bei denen Hard- und Software nachgewiesenermaßen SIL 4-Standards gemäß CENELEC erfüllen. In dem Fall ist das gesamte Gerätesystem bereits von den zuständigen Behörden akzeptiert und somit zugelassen für den Einsatz in jeglichen Schienenfahrzeugen sowie in Bahnübergängen und Stellwerken weltweit. Mit einer derartigen Lösung sinkt der Arbeitsaufwand für die Anwender deutlich (Zulassungs- und Zertifizierungsprozesse können ansonsten Monate, teilweise sogar Jahre dauern). Außerdem entstehen dem Anwender keine Zulassungskosten für Sub-Systeme. Nicht zuletzt ist das Risiko eines Projektverzugs – wenn z. B. Sicherheitsanforderungen nicht vollständig erfüllt werden bzw. Lücken entstehen – auf ein Minimum reduziert. Die vorzertifizierten Systeme ermöglichen Systemintegratoren, sich auf die jeweilige Applikation zu konzentrieren.

3.2 Skalierbarkeit

Schienenfahrzeuge und Anwendungen in der Bahninfrastruktur laufen in der Regel über Jahrzehnte. Produktfamilien von Schienenfahrzeugen werden regelmäßig um neue Varianten bzw. Fahrzeuggenerationen ergänzt. Sowohl für Hersteller von Schienenfahrzeugen als auch für Bahnbetreiber und Systemintegratoren sind Flexibilität und Modularität daher entscheidende Kriterien bei der Auswahl von Sicherheitssystemen. Mit COTS-Systemen lassen sich Modifikationen, Änderungen und Erweiterungen mit sehr viel geringerem Aufwand umzusetzen als mit proprietärer Technik. Das liegt vor allem daran, dass die Rückwirkungsfreiheit gegeben ist, das heißt dass bei Änderungen und Erweiterungen bzw. dem Hinzufügen neuer Funktionen nur diese betrachtet werden müssen und nicht das gesamte System erneut geprüft werden muss.

Hier ist es entscheidend, ein COTS-System auszuwählen, bei dem Hardware und Software optimal ineinandergreifen. Die

Software sollte auf offener Programmierung und industrieüblichen Programmiersprachen basieren. Handhabung und Programmierung der Steuerung sollten möglichst einfach und im Laufe eines Projekts auch ohne den Hersteller möglich sein. Wichtig sind in diesem Zusammenhang auch Aspekte wie Rückwärtskompatibilität von Software und Langzeitverfügbarkeit der Hardwarekomponenten. Verfügt das gewählte COTS-System über State-of-the-Art-Software-Tools, müssen jeweils nur diejenigen Teile wieder getestet werden, die tatsächlich geändert wurden, da zertifizierte Betriebssysteme und Software-Programmierung ein rückwirkungsfreies Engineering garantieren.

Darüber hinaus sollte die Systemarchitektur modular sein, damit sich die Steuerungen problemlos mit zusätzlichen I/Os erweitern lassen. Im Idealfall sind Gerätetausch und Erweiterungen sogar bei laufendem Betrieb möglich. Durch diese Flexibilität lassen sich Aufwand und Kosten in der Entwicklung und der Zulassung bei Änderungen bereits vorhandener Funktionen deutlich reduzieren. Somit können Systemintegratoren und Hersteller von Schienenfahrzeugen noch schneller auf sich verändernde Kundenwünsche seitens der Bahnbetreiber reagieren.

3.3 Neuartige Wartungskonzepte

Verfügbarkeit und die Reduzierung von Betriebskosten sind entscheidend für Bahnbetreiber, um dem wachsenden Kostendruck standzuhalten und die Profitabilität zu steigern. Eine wichtige Rolle spielt dabei die Wartung. Es gibt bereits erste COTS-Systeme auf dem Markt, z. B. die HIMax, die es Anwendern ermöglichen, neue Konzepte bezüglich Wartung und Service von Zugsicherungssystemen sowie anderen Subkomponenten zu realisieren. Grundlage hierfür sind bis zu vierfach redundante Prozessormodule sowie vollständig redundante Kommunikations- und I/O-Module. Parallelisierte Wartungs-/Austauschkonzepte bei laufendem Betrieb sind in diesem Fall teilweise konzeptionell bereits hinterlegt.

Dadurch dass in diesem Fall das Leitsystem bei Wartungsarbeiten an sicherheitskritischen Komponenten wie Leistungsschaltern, Brems Elektronik, Energieversorgung etc. nicht abgeschaltet werden muss (heute aus Sicherheitsgründen so noch gefordert) und darüber hinaus zeitgleich auch Wartungsarbeiten am Leitsystem selbst (Software-Updates, Modultausch oder Erweiterung etc.) möglich sind, könnten zukünftig die Stillstandzeiten von Fahrzeugen reduziert werden und Fahrzeuge länger im Dienst bleiben.

3.4 Flexibilität

Heute werden oft zwei Steuerungssysteme in Bahnanwendungen eingesetzt: eins für alle Standard-, nicht sicherheitskritischen Funktionen und ein zweites für die SIL>0-Funktionen. Wobei bei SIL 3 und SIL 4 zusätzliche Architekturelemente wie pneumatische und konventionelle Verdrahtungs- und Kanalredundanzen notwendig sind. Bei der Auswahl der COTS-Steuerung sollte darauf geachtet werden, dass die Lösung eine möglichst große Bandbreite von Anwendungen abdeckt. Eine HIMax erfüllt beispielsweise in einem System alle Anforderungen von SIL 0 bis SIL 4. Dies vereinfacht deutlich die Architektur des gesamten Zugsicherungssystems (TCMS). Durch die geringere Anzahl von Schnittstellen sinken Kosten und Zeitaufwand bei Systemänderungen bzw. -erweiterungen. Zudem entfällt die zeitaufwendige Analyse, welche Funktionen mit welchem System (SIL 1, 2, 3 oder 4) realisiert werden muss. So kann zum Beispiel eine HIMax-Steuerung sowohl Standard-I/O-Module als auch SIL 4-I/O-Baugruppen gleichzeitig tragen. Die „einfache“ Architektur und Transparenz führt zu größerer Akzeptanz und schnellerem Verständnis bei Behörden und Gutachtern, wodurch der Zeitaufwand für Zulassungsverfahren sinkt.

Durch den modularen Aufbau und die skalierbaren Gerätekonzepte von COTS-Steuerungen sind nahezu alle Funktionen im Bereich Schienenfahrzeuge realisierbar. Hierzu zählen Antriebsüberwachungsfunktionen, Zugsteuerung, Stillstands-, Geschwindigkeits- und Richtungsüberwachung. Aber auch Plausibilisierungen, Funktionsüberwachung und Fehlerdetektionsmechanismen sowie Steuerungsfunktionen und logische Verknüpfungen decken derartige COTS-Systeme ab. Teilweise können diese auch Kommunikationsaufgaben übernehmen.

3.5 Schulungsbedarf

Wichtig ist, dass sich die COTS-Software der gewählten Lösung vor allem auf nutzbringende und zwingend erforderliche Funktionen fokussiert. Der Aufwand für die Pflege von proprietären Zugsicherungssystemen entfällt in diesem Fall. Das bedeutet, dass Software-Abteilungen der Hersteller von Schienenfahrzeugen nicht mehr auf IT-Experten angewiesen sind, deren primäre Aufgabe es ist, das TCMS am Leben zu erhalten.

Ein weiterer wichtiger Aspekt bei der Kaufentscheidung sind die Folgekosten. Bei COTS-Systemen auf der Basis industriestandard Programmiersprachen wie HIMax lassen sich nahezu alle Automatisierungsaufgaben durch FUPla bzw. allgemein gemäß IEC1131 empfohlene Programmiersprachen realisieren. Das heißt zum einen, dass der Schulungsbedarf für das Service-Personal weltweit auf ein Minimum reduziert wird und dass potenziell mehr Programmierer zur Verfügung stehen (global geschätzte 500.000 Personen), die dieser Programmiersprachen mächtig sind. Gerade vor dem Hintergrund des in vielen Ländern bestehenden Mangels an Programmierern ist dies in der global tätigen Bahnindustrie ein wichtiges Argument in der Pflege und Instandhaltung von Schienenfahrzeugen und Bahninfrastruktur. Mit COTS ist eine optimale Betreuung der Fahrzeuge bezüglich der Software und dem Launch neuer Fahrzeuge global über den gesamten Software-Lebenszyklus in allen Regionen der Welt gesichert.

Abbildung 3: Ein Beispiel für die Funktionsvielfalt: Allgemeine Architektur von Antriebsüberwachungsfunktionen bei Power Drive Systemen

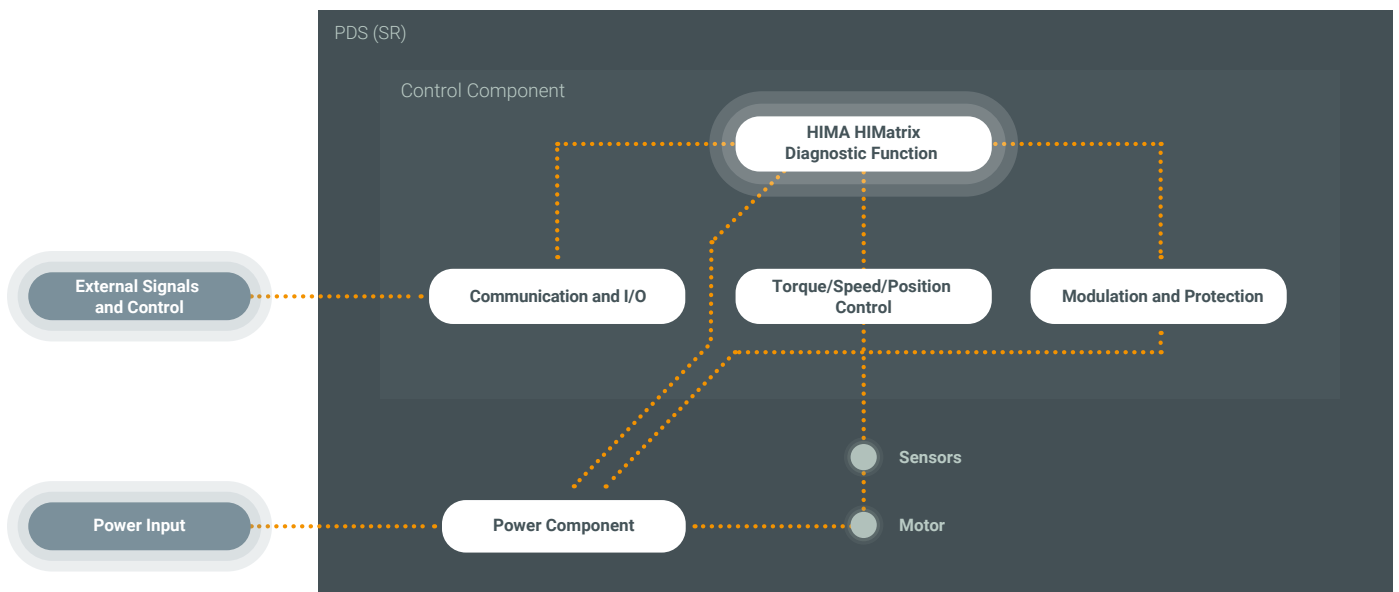
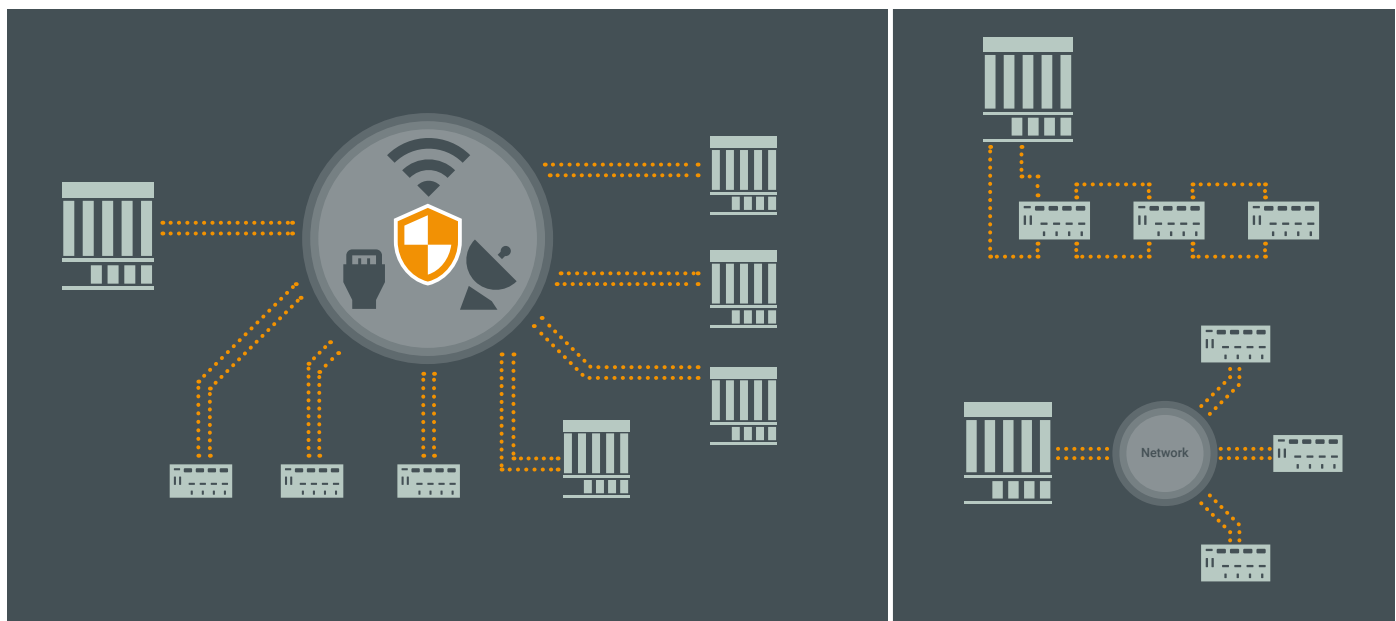


Abbildung 4: Vergleich von Systemarchitekturen – zentral, dezentral, redundant oder nicht redundant

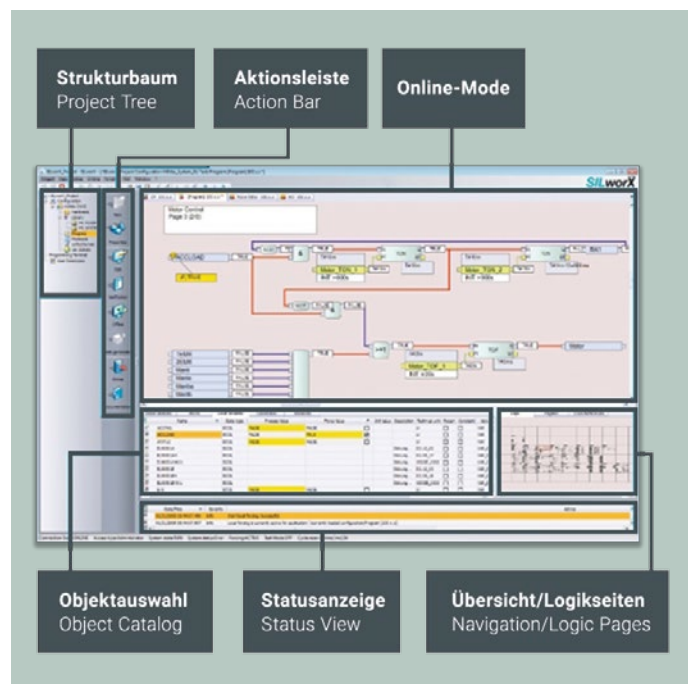


3.6 Interoperabilität

Gerade im Bereich der Stellwerk- und Signaltechnik sind Offenheit, Skalierbarkeit und Modularität ein wichtiger Faktor – Stichwort „Interoperabilität“. Eine zentrale Anforderung an das COTS-System sollte daher sein, dass es sich dank Standard-Betriebssystem und offener Schnittstellen bedarfsgerecht aufbauen lässt – als Einzelsteuerung, dezentral oder zentral. Denn dann lassen sich alle Anlagengrößen von Stellwerken und Anwendungen von der ortsbedienten Weiche über die Steuerung mit Remote-I/O-Modulen nahe der Feldelemente bis hin zu der zentralen Steuerung im redundanten Aufbau flexibel realisieren.

Eine wichtige Rolle in Sachen Vernetzung und Interoperabilität spielt auch die COTS-Software. Idealerweise dient diese als vollintegriertes Konfigurations-, Programmier- und Diagnose-Tool und nutzt industrieeübliche Programmiersprachen gemäß DIN EN 61131. Neuere Software sollte durch Funktionsbaustein- und Ablaufsprache sowie C-Programmierung auch eine einfach nachvollziehbare Programmierung inklusive herstellerunabhängiger, offener Schnittstellenprogrammierung ermöglichen. In diesem Fall lassen sich validierte Funktionsbausteine oder ein generisches Programm erstellen, was dazu führt, dass Test- und Inbetriebnahmekosten sinken. Fremdkomponenten können in diesem Fall einfach eingebunden werden – ein wichtiger Punkt angesichts der heterogenen Technik in der Bahninfrastruktur.

Abbildung 5: Moderne COTS-Software (hier SILworX) sollte Konfigurations-, Programmier- und Diagnose-Funktionen in einer Lösung vereinen



3.7 Cyber-Security

Mit dem wachsenden Grad an Automatisierung und der zunehmenden Verlagerung von Funktionen in die Cloud steigt auch die Gefahr von Cyberattacken. Damit wird das Thema Cyber-Security in der Bahnsicherheitstechnik immer wichtiger. Sicherheitssteuerungen sind nicht nur ein sicherheitskritisches Ziel solcher Angriffe, sondern gleichzeitig ein effektiver Hebel, um Gefahren durch Cyberattacken für Mensch, Bahnfahrzeuge und -anlagen sowie Umwelt abzuwehren. Wichtige Maßnahmen zur Steigerung der Sicherheit sind in diesem Zusammenhang die Einschränkung menschlicher Zugriffsmöglichkeiten und das Aufsetzen eigenständiger, in sich geschlossener Sicherheitssysteme.

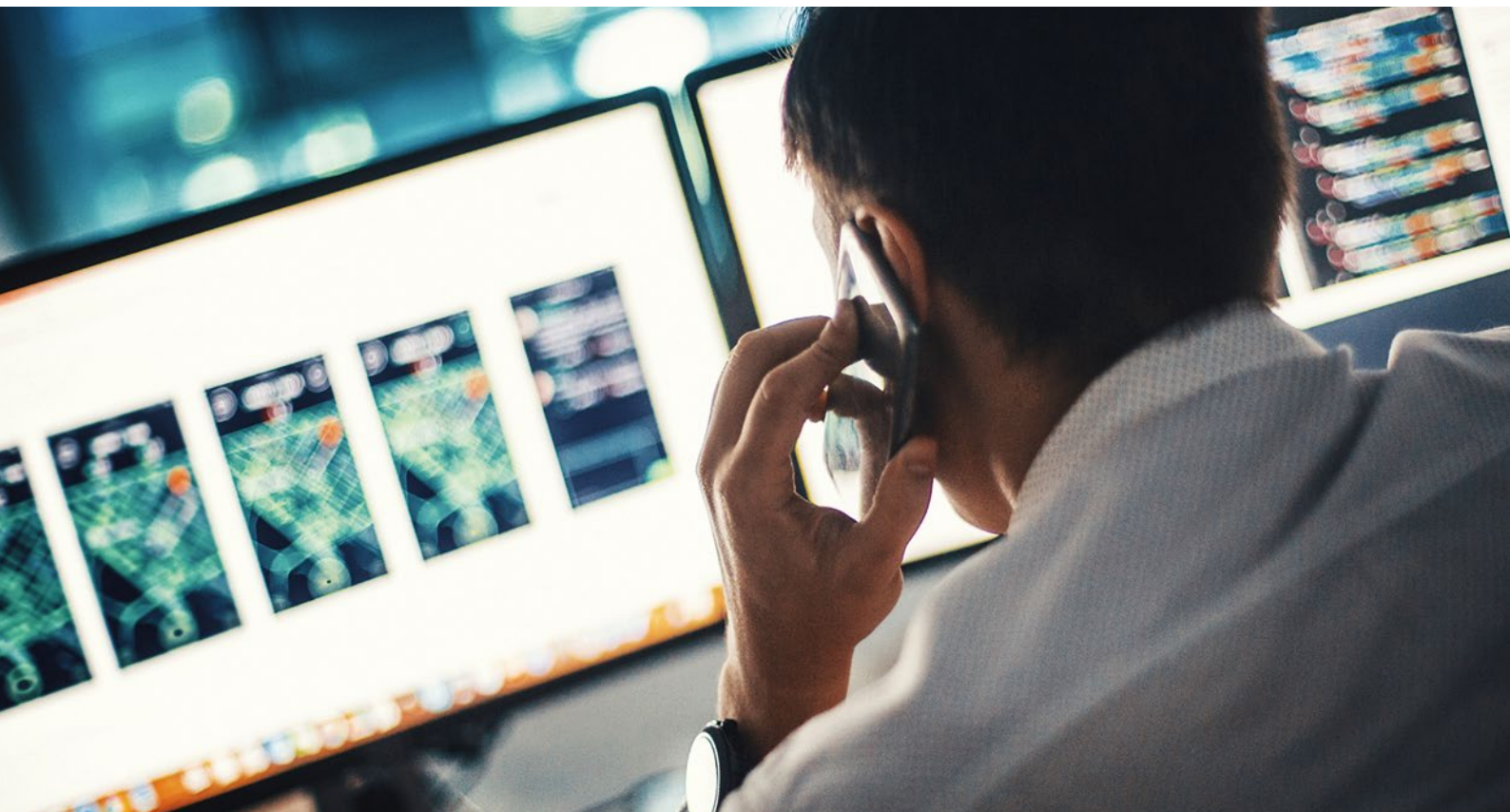
Eine COTS-Steuerung für den Einsatz im Schienenverkehr sollte daher optimalerweise ein Betriebssystem haben, das speziell für sicherheitsgerichtete Anwendungen entwickelt wurde. Gleichzeitig muss es aber – im Gegensatz zu proprietären Systemen – frei programmierbar sein. Ein derartiges Betriebssystem umfasst alle Funktionen einer Sicherheits-SPS, verzichtet aber darüber hinaus auf weitere Funktionen. Typische Attacken auf IT-Systeme sind in diesem Fall nicht erfolgreich.

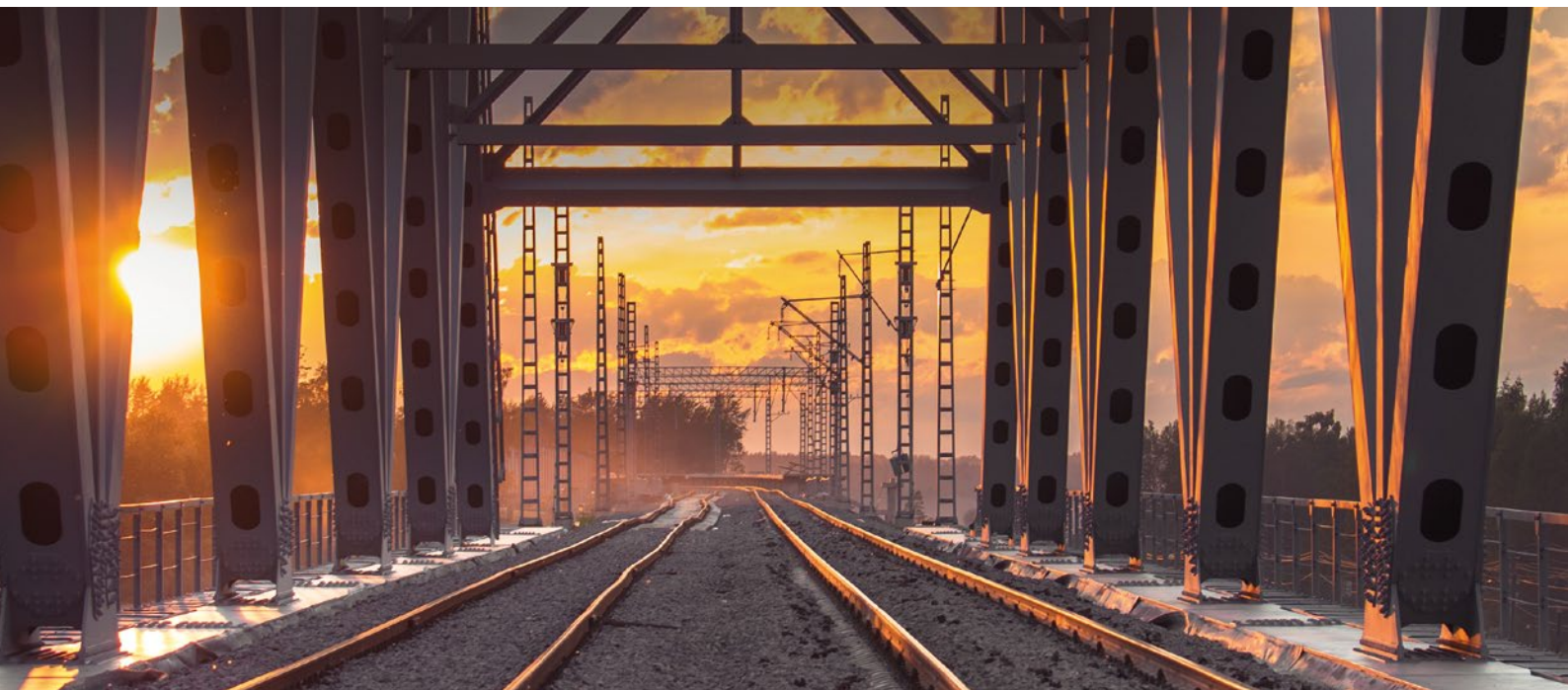
Für besonders effektiven Schutz sollte die IT-Sicherheit bereits in die Betriebssysteme der COTS-Steuerungen integriert sein. HIMatrix und HIMax werden beispielsweise bereits in ihrer Entwicklung auf ihre Widerstandsfähigkeit gegenüber Cyberattacken getestet. Wer dagegen mit herkömmlichen, PC-basierten SPS-Systemen operiert, muss theoretisch ständig die Betriebs-

software dieser PCs aktualisieren, um sich effektiv vor Angriffen zu schützen. Durch eine Aktualisierung der Betriebssoftware setzen Betreiber jedes Mal den Sicherheitsnachweis bzw. die Zulassung aufs Spiel.

System- und Kommunikationsprozessor sollten bei COTS-Steuerungen im Idealfall getrennt voneinander sein. Dies gewährleistet eine hohe Betriebssicherheit, selbst im Falle einer Cyberattacke auf den Kommunikationsprozessor. Darüber hinaus ist so der Betrieb verschiedener, physikalisch getrennter Netzwerke auf nur einem Kommunikationsprozessor oder einem Prozessormodul möglich. Im Sinne der Cyber-Security ist es auch sinnvoll, wenn sich ungenutzte Schnittstellen einzeln deaktivieren lassen, was die Sicherheitssteuerungen auf die Kommunikationsfunktionen limitiert, die wirklich benötigt werden.

COTS-Software sollte über ein mehrstufiges Nutzer-Management verfügen, über das sich die Zugriffsrechte individuell einstellen lassen, sodass sowohl die Anwendung als auch das Sicherheitssystem optimal geschützt werden. So muss beispielsweise bei einer Passwortänderung kein neuer Patch erstellt werden und die Anlage nicht neu zertifiziert werden.





Leitfaden

4. Fazit

Derzeit wird die Bahnindustrie noch von proprietärer Sicherheitselektronik dominiert. Aber es ist klar zu erkennen, dass COTS-Steuerungen sich aufgrund der vielfältigen Einsatzmöglichkeiten und ihrer deutlich geringeren Investitions- und Lebenszykluskosten im Vergleich zu proprietärer Technik zum Standard entwickeln. Die Gegenüberstellung der wichtigsten Anforderungen und Eigenschaften moderner Sicherheitssteuerungen vor dem Hintergrund der aktuellen Normung und sozio-ökonomischer Rahmenbedingungen hat gezeigt, dass Bahnbetreiber, Hersteller von Schienenfahrzeugen und Systemintegratoren beim Einsatz von COTS-Systemen von erhöhter Flexibilität und Zukunftsfähigkeit, vereinfachter Instandhaltung und optimierter Wirtschaftlichkeit profitieren – und zwar über die gesamte Lebensdauer von Schienenfahrzeugen oder Infrastruktur-Anwendungen.

Die Unterschiede bei COTS-Systemen liegen im Detail. Wichtige Aspekte, die Bahnbetreiber, Hersteller von Schienenfahrzeugen und Systemintegratoren bei ihrer Kaufentscheidung berücksichtigen sollten, sind Zertifizierung (sind Steuerungen nach CENELEC zertifiziert und welches SIL-Level bieten sie?), Skalierbarkeit, Flexibilität, Interoperabilität, einfache Wartung und Handhabbarkeit der Software. Gerade vor dem Hintergrund zunehmender Cyberattacken und einem wachsenden Grad an Vernetzung sollten Anwender außerdem immer hinterfragen, was die jeweilige COTS-Lösung bietet, um die eigene Anwendung effektiv gegen solche Angriffe zu schützen.

Neben den technischen Aspekten ist es für die global tätige Bahnindustrie ebenfalls entscheidend, dass der COTS-Lieferant nicht nur Hardware, Software und Tools liefert, sondern auch weltweiten Support. Er muss Ersatz und Retrofit über Zeiträume von 30 Jahren und mehr garantieren können.

COTS-Systeme stellen die Zukunft der Bahntechnik dar: Sie sind skalierbar, modular und leicht zu adaptieren. Selbst neue Funktionen lassen sich in der Regel problemlos integrieren. Das heißt, sie wachsen mit der Infrastruktur bzw. Automatisierungsarchitektur. Aus diesem Grund lassen sich langlebige Schienenfahrzeuge mit vielen Updates und diversen Fahrzeugvarianten mithilfe von COTS-Lösungen einfach und wirtschaftlich umsetzen. Hinzu kommt, dass eine größere Freiheit bei der Wahl der Komponenten-Lieferanten besteht. Darüber hinaus sind Ersatzteile weltweit kurzfristig verfügbar und lassen sich einfach installieren. All das führt dazu, dass mehr und mehr wichtige Player der Bahnindustrie auf COTS-Lösungen setzen.


Sie möchten mehr erfahren? Kontaktieren Sie uns:

HIMA Rail Segment Team

Telefon: +49 6202 709-411

E-Mail: rail@hima.com

Oder gehen Sie online:

 www.hima.com/de/branchen-loesungen/bahn

Die in diesem Whitepaper enthaltenen Inhalte dienen reinen Informationszwecken und stellen keine Beratung oder Leistung technischer oder sonstiger professioneller Art dar. Aufgrund von besonderen Umständen des Einzelfalls und den standortspezifischen Gegebenheiten sollte jede Verwendung der in diesem Whitepaper enthaltenen Informationen nur in Absprache mit einem qualifizierten Fachmann erfolgen, der alle relevanten Faktoren und die gewünschten Ergebnisse berücksichtigen kann. Dieses White Paper wurde mit angemessener Sorgfalt und Aufmerksamkeit erstellt. Dennoch ist es möglich, dass einige in diesem Whitepaper enthaltene Informationen unvollständig, inkorrekt oder im Einzelfall nicht anwendbar sind. Weder HIMA noch die mit HIMA verbundenen Unternehmen, Geschäftsführer, leitende Angestellte oder Mitarbeiter noch irgendeine andere Person haften für Schäden, die sich aus der Verwendung oder im Zusammenhang mit der Benutzung des Inhalts des Whitepapers oder im Vertrauen auf einen solchen Inhalt ergeben oder in sonstiger Weise im Zusammenhang mit diesem Whitepaper entstehen. Eine inhaltliche Änderung, die Vervielfältigung oder der Nachdruck des Whitepapers sowie deren Weitergabe an Dritte – auch auszugsweise – ist nur mit der ausdrücklichen Zustimmung von HIMA zulässig.

