Praktische Beispiele für Security im kompletten OT-Lebenszyklus

Practical examples of security throughout the entire OT lifecycle

Martin Koop | Johannes Häring | Markus Heinrich

Der Beitrag beschreibt anhand praxisnaher Beispiele, wie Cybersecurity-Anforderungen bei Bahnanwendungen systematisch über den gesamten OT-Lebenszyklus umgesetzt werden. Von der Konzeptphase bis zur Außerbetriebnahme werden zentrale Methoden wie Risikoanalysen, Schwachstellenmanagement, Systemhärtung, Security-Tests und ein kontinuierliches Monitoring skizziert. Im Fokus steht ein strukturiertes, ganzheitliches Cybersecurity-Management nach aktuellen Normen und Gesetzen, das nur durch konsequente und fortlaufende Maßnahmen ein nachhaltiges Sicherheitsniveau für Bahn-OT-Systeme sicherstellen kann.

1 Einleitung

Die Entwicklung von Bahnanwendungen, die sowohl funktional als auch cybersicher sind, stellt eine erhebliche Herausforderung dar. Die CLC/TS 50701 und künftig die IEC 63452 bilden das Rahmenwerk für den sicheren (secure) Entwicklungslebenszyklus. Grundlage der Anwendung ist die Reihe der IEC 62443. Die Verbindung aus Industrienorm und Rail-Safety wird durch die Anlehnung an die zwölf Phasen des V-Modells der EN 50126 erreicht. Dieser Beitrag beleuchtet die wichtigsten Herausforderungen der Cybersecurity in allen Phasen und nennt praktische Beispiele für die erfolgreiche Entwicklung eines sicheren Systems.

2 Konzept bis Systemanforderungen (Phase 1, 2, 3, 4)

In Phase 1 wird der Cybersecuritymanagementplan (CSMP) erstellt, dieser dient dem Security-Manager als Planungsdokument, um die Rahmenbedingungen des Projektes sowie die Aktivitäten und zu erstellende Artefakte in allen durchzuführenden Lebenszyklusphasen zu beschreiben. Es empfiehlt, sich bereits hier den erwarteten Cybersecurity-Kontext und die Bedrohungsumgebung zu beschreiben, da diese Annahmen in den folgenden Phasen, insbesondere der (Cybersecurity-) Risikoanalyse, verwendet werden können. Bereits in der Konzeptphase sollte festgelegt werden, in welcher Form eine Zulassung für das Produkt erfolgen soll (z. B. GIuV). Diese projektweite Festlegung hat Auswirkungen auf die Cybersecurity, indem ggf. zusätzliche Nachweise zu erbringen sind. So kann die Besetzung der Rollen wie Verifizierer und Validierer sowie die Bestimmung eines Prüfsachverständigen (PSV) für IT-Security erforderlich werden. Die frühzeitige Einbindung des PSV ist für die erfolgreiche Begutachtung von Bedeutung, um etwaige Missstände nicht erst in der Integrationsphase durch Aufwände bzw. teure Kompensationsmaßnahmen beheben zu müssen.

This article uses practical examples to describe how cybersecurity requirements for railway applications are systematically implemented throughout the entire OT lifecycle. Key methods such as risk analysis, vulnerability management, system hardening, security testing and continuous monitoring are outlined from the concept phase to decommissioning. The focus is on structured, holistic cybersecurity management in accordance with current standards and laws, which can only ensure a sustainable level of security for railway OT systems through consistent and ongoing measures.

1 Introduction

The development of railway applications that are both functional and cybersecure poses a considerable challenge. The CLC/TS 50701 and, in future, the IEC 63452 form the framework for the secure development lifecycle. The IEC 62443 series is the basis for the application. The combination of industry standards and rail safety is achieved by following the twelve phases of the EN 50126 V-model. This article highlights the most important cybersecurity challenges in all the phases and provides practical examples for the successful development of a secure system.

2 Concept to system requirements (phases 1, 2, 3 and 4)

The cybersecurity management plan (CSMP) serves as a planning document for the security manager to describe the project's framework conditions, as well as the activities and artefacts to be created in all the lifecycle phases that are to be implemented. It is advisable to describe the expected cybersecurity context and threat environment at this stage, as these assumptions can be used in the following phases, particularly in the (cybersecurity) risk analysis. The form of approval for the product (e.g. GIuV) should be determined as early as the concept phase of development. This project-wide decision has implications for cybersecurity, as additional evidence may need to be provided. For example, it may be necessary to fill roles such as a verifier and validator and to appoint a test expert (PSV) for IT security. The early involvement of the PSV is important for a successful assessment so that any shortcomings do not have to be remedied during the integration phase by means of costly compensation measures.

ERORAT (the EULYNX EUG RCA OCORA Risk Assessment Tool) can be used both as a tool and for documentation in any risk analysis according to CLC/TS 50701[2, 3]. It uses the sam-

Für die Risikoanalyse nach CLC/TS 50701 kann ERORAT (EULYNX EUG RCA OCORA Risk Assessment Tool) als Werkzeug und zur Dokumentation verwendet werden [2, 3]. Es verwendet die Beispielrisikomatrix der CLC/TS 50701 sowie Exposition (EXP) und Verwundbarkeit (VUL) zur Bestimmung der Eintrittswahrscheinlichkeit (Likelihood), kann jedoch bei Bedarf auf anwenderspezifische Matrizen und Bewertungskriterien angepasst werden. Mit ERORAT können sowohl Security-Anforderungen für Neuentwicklungen abgeleitet werden als auch für bestehende Systeme, für die bisher noch keine Risikoanalyse durchgeführt wurde. Bereits umgesetzte Security-Anforderungen können hier bei der Bewertung des Risikos einfließen.

Zahlreiche Systeme im Eisenbahnumfeld sind auch Anlagen von Betreibern Kritischer Infrastrukturen, für die nach § 8a Abs. 1 BSI-Gesetz angemessene technische und organisatorische Vorkehrungen durch den Betreiber nachzuweisen sind, um ihre Funktionsfähigkeit zu schützen. Soweit es keinen anwendbaren branchenspezifischen Sicherheitsstandard (B3S) gibt, wie es für Vollbahnen bis heute der Fall ist, verwendet das BSI einen eigenen Katalog als Prüfgrundlage [1]. Daher sollte bereits frühzeitig im Entwicklungsprojekt geprüft werden, ob das System in seiner Betriebsphase einen Schwellwert gemäß Anhang 7 BSI-KritisV überschreiten wird.

Ein nach CLC/TS 50701 entwickeltes System implementiert Systemanforderungen der IEC 62443 3 3 und wird daher in seinen Security-Anforderungen bereits einen Großteil der technischen BSI-Anforderungen abdecken. Dennoch empfiehlt es sich, den BSI-Katalog in das Anforderungsmanagement aufzunehmen, um bereits im Entwicklungsprojekt die für ein Audit nach § 8a Abs. 4 BSI-Gesetz erforderlichen Nachweise zu erzeugen. Darüber hinaus enthält der BSI-Katalog auch Anforderungen, die nicht für ein einzelnes Produkt oder eine einzelne Anlage des Betreibers umgesetzt werden, sondern eine unternehmensweite Umsetzung erfordern. Hierunter fallen z. B. ein Informationssicherheitsmanagementsystem (ISMS), ein Asset Management sowie ein Kontinuitäts- und Notfallmanagement, welche ebenso nach den ISO 27001-Anforderungen zur Best Practice gehören und entsprechend frühzeitig betrachtet werden sollten.

3 Systemarchitektur bis Implementierung (Phase 5, 6, 7)

Die Hauptherausforderung in Phase 5, der Systemarchitektur, liegt in der korrekten Zuteilung von Systemanforderungen an die einzelnen Komponenten, was sich durch die Komplexität von Eisenbahnsystemen ergibt. Wesentlich ist dabei, auf das Defence-in-Depth-Prinzip zu achten, sodass Security-Anforderungen nicht nur an der Zonengrenze, sondern auf jeder relevanten Komponente umgesetzt sind. In der praktischen Umsetzung ist ein strukturierter Ansatz hilfreich, wodurch die Komponentenanforderungen mit den Systemanforderungen der Zone verknüpft werden, sodass verifiziert werden kann, dass alle nötigen Systemanforderungen von den Komponenten umgesetzt werden. Ein Beispiel der konsequenten Umsetzung dazu ist die EU Rail Secure Component Specification [7, 8].

Bei der Ableitung der Komponentenanforderungen muss zusätzlich darauf geachtet werden, welche Shared-Security-Services zur Umsetzung der Anforderungen notwendig sind. Dazu gehören beispielsweise eine PKI für digitale Zertifikate, IAM für die Authentifizierung und Autorisierung oder ein SOC für das Security Logging. Um Probleme in der Integration und dem Betrieb zu vermeiden, ist es wichtig, frühzeitig in die Kommunikation zwischen Hersteller, Integrator und Betreiber zu gehen und die nö-

ple risk matrix from CLC/TS 50701 as well as any exposure (EXP) and vulnerability (VUL) to determine the probability of occurrence (likelihood), but it can be adapted to user-specific matrices and evaluation criteria if necessary. ERORAT can be used to derive security requirements for new developments as well as for existing systems for which no risk analysis has yet been performed. Security requirements that have already been implemented can be included in the risk assessment.

Numerous systems in the railway environment also involve critical infrastructure operators' facilities, for which, according to Section 8a (1) of the BSI Act, the operator must demonstrate that the appropriate technical and organisational precautions have been taken so as to protect their functionality. If there is no applicable industry-specific security standard (B3S), as is still the case for mainline railways, the BSI uses its own catalogue as a basis for testing [1]. Therefore, it is recommended to check at an early stage of the development project whether the system will exceed a threshold value in accordance with Annex 7 BSI-KritisV during its operating phase.

A system developed in accordance with CLC/TS 50701 implements the system requirements of IEC 62443-3-3 and will therefore already cover most of the BSI technical requirements in its security requirements. Nevertheless, it is advisable to include the BSI catalogue in the requirement management so as to generate the evidence required for an audit in accordance with Section 8a (4) of the BSI Act during the development project. In addition, the BSI catalogue also contains requirements that are not implemented for a single product or a single system of the operator, but require company-wide implementation. These include, for example, an information security management system (ISMS), asset management and continuity and emergency management, which also constitute part of best practice according to the ISO 27001 requirements and should therefore be considered at an early stage.

3 System architecture to implementation (phases 5, 6 and 7)

The main challenge in phase 5 lies in the correct allocation of the system requirements to the individual components, which arises from the complexity of railway systems. It is essential to observe the defence-in-depth principle so that the security requirements are not only implemented at the zone boundary, but on every relevant component. A structured approach that links the component requirements to the zone's system requirements so that a check can be made to ensure that all the necessary system requirements have been implemented by the components is helpful in practical implementations. The EU Rail Secure Component Specification is an example of the consistent implementation of this [7, 8].

When deriving component requirements, additional attention must be paid to which shared security services are required for the implementation of said requirements. These include, for example, a PKI for digital certificates, an IAM for authentication and authorisation or an SOC for security logging. It is important to establish communication between the manufacturer, integrator and operator at an early stage and to specify the necessary interfaces to avoid any problems in integration and operations. One solution would be to use standardised interfaces, as is the case with EU Rail [6]. In addition, close consultation between the manufacturer, integrator and operator is necessary in order to discuss the necessary security-related application conditions (SecRACs) in time if a zone's components cannot implement

tigen Schnittstellen zu spezifizieren. Eine Lösung wäre z. B., standardisierte Schnittstellen, wie bei EU Rail, zu benutzen [6]. Zusätzlich ist eine enge Absprache zwischen Hersteller, Integrator und Betreiber notwendig, um rechtzeitig die notwendigen Security-related application conditions (SecRAC) zu besprechen, wenn die Komponenten einer Zone die Systemanforderungen nicht umsetzen können.

Im CENELEC-Sicherheitslebenszyklus markieren die Phasen 6 und 7 den Übergang von der dokumentierten Anforderung zur tatsächlichen Umsetzung. Während in Phase 6 der System- und Komponentenentwurf in die konkrete Umsetzung mündet, stehen in Phase 7 die Herstellung und der Einkauf dieser umgesetzten Bausteine im Vordergrund. Aus Cybersecurity-Sicht sind diese Abschnitte entscheidend, da in dieser Phase Sicherheitsanforderungen erstmals in lauffähige Systeme übersetzt werden – und damit der Grundstein für die Widerstandsfähigkeit im späteren Betrieb gelegt wird.

In Phase 6 geht es darum, die in den vorangegangenen Phasen erarbeiteten Sicherheitsmaßnahmen in der Systemarchitektur technisch zu realisieren. Eine entsprechende Expertise im Security Systems Engineering gewährleistet dabei eine konsistente Umsetzung. Das reicht von der Realisierung der Netzsegmentierung über die Integration kryptographischer Verfahren bis zur Implementierung von Authentifizierungs- und Autorisierungsmechanismen. Essenziell ist, dass Sicherheitsanforderungen nicht „auf den letzten Metern" hinzugefügt werden, sondern integraler Bestandteil der Systemanforderungen sind. Die Implementierung der SecRACs sollte dann in das Systemdesign einfließen.

In the CENELEC safety lifecycle, phases 6 and 7 mark the transition from documented requirements to actual implementation. While phase 6 sees the system and component design move into concrete implementation, phase 7 focuses on the manufacture and procurement of these implemented components. These sections are crucial from a cybersecurity perspective, as this is the phase in which the security requirements are first translated into executable systems, thereby laying the foundation for resilience in later operations.

Phase 6 is about technically implementing the security measures developed in the previous phases of the system architecture. Appropriate expertise in security systems engineering ensures consistent implementation. This ranges from the realisation of the network segmentation and the integration of the cryptographic procedures through to the implementation of the authentication and authorisation mechanisms. It is essential that the security requirements are not added "at the last minute", but are an integral part of the design. For an electronic interlocking (ESTW), for example, this means that the communication interfaces are encrypted from the outset and provided with role-based access control, instead of being "secured" retrospectively. The design must integrate security and safety functions in such a way that they also perform well under realistic operating conditions. For ESTW systems, this could mean optimising encrypted commu-

standteil des Designs sind. Für ein Elektronisches Stellwerk (ESTW) bedeutet dies beispielsweise, dass Kommunikationsschnittstellen per Design zu verschlüsseln und mit rollenbasierter Zugriffskontrolle zu versehen sind – statt sie nachträglich „abzusichern". Das Design muss Security- und Safety-Funktionen so integrieren, dass sie auch unter realistischen Betriebsbedingungen performant arbeiten. Für ESTW-Systeme könnte dies bedeuten, dass die verschlüsselte Kommunikation zwischen Stellwerk und Betriebszentrale so optimiert wird, dass Latenzzeiten im zulässigen Rahmen bleiben.

In Phase 7 werden die Komponenten hergestellt oder eingekauft. Die Umsetzung der Sicherheitsanforderungen in den Komponenten muss auf die Anforderungen aus Phase 4 zurückführbar sein, beispielsweise mit DOORS (Dynamic Object Oriented Requirements System) oder Polarion. Das Vermeiden von Konflikten zwischen der Cybersecurity-Funktionalität und der funktionalen Architektur steht in dieser Phase im Vordergrund. Dies kann durch frühe Funktions- und Security-Tests erreicht werden. Dazu können z. B. automatisierte Schwachstellenscanner, wie trivy, genutzt werden. Das Risiko für die gefundenen Schwachstellen sollten dann zentral gemanaged werden, dazu bietet sich z. B. die Open-Source Software DefectDojo an.

Ebenfalls wertvoll sind Security-Funktionstests, wie sie auch im Fachartikel „Hinterfrage deine Annahmen: Praxiserfahrungen mit Testautomatisierung und Pentests" [5] beschrieben werden: Diese fokussieren sich gezielt auf die Wirksamkeit einzelner Sicherheitsmaßnahmen, etwa das Blockieren unerlaubter Zugriffe oder die korrekte Reaktion auf abgelaufene Zertifikate. Durch die frühe Identifikation von Abweichungen im Komponentenverhalten lassen sich kostspielige Nacharbeiten in späteren Phasen vermeiden. Eine typische Herausforderung bei Security-Funktionstests ist eine fehlende Testumgebung, die z. B. die Shared-Security-Services zur Verfügung stellt.

Wer in Phase 6 konsequent sichere Designprinzipien umsetzt und in Phase 7 die Umsetzung der Security-Funktionen sicherstellt, schafft eine robuste Basis für alle folgenden Lebenszyklusphasen. So wird Cybersecurity nicht zu einer nachträglichen Ergänzung, sondern zu einem integralen Qualitätsmerkmal des gesamten Systems – und das ist gerade im Bahnwesen mit seinen hohen Sicherheitsanforderungen unverzichtbar.

4 Integration bis Abnahme (Phase 8, 9, 10)

Ziel dieser Phase ist es, die auf Basis der Spezifikationen (Phasen 1–5) teilweise separat entwickelten oder beschafften Komponenten – beispielsweise Firewalls, Bedienrechner oder komplette LST-Systeme (Leit- und Sicherungstechnik) wie ein Radio Block Centre (RBC) und Digitale Stellwerk (DSTW) von verschiedenen Herstellern – zu einem Safety-konformen, cyberresilienten Gesamtsystem zu integrieren. Dabei geht es nicht nur um funktionales Zusammenspiel, sondern um die Nachweise, dass die Sicherheitsmaßnahmen wie spezifiziert im Systemverbund wirken. Während technische Funktionalität in der Bahntechnik vorausgesetzt wird, ist die wirksame Umsetzung der Cybersecurity-Maßnahmen im Systemverbund keineswegs trivial – und der Kern dieser Phase.

Typische Probleme während der Systemintegration zeigen sich, wenn Anforderungen unterschiedlich von Hersteller, Betreiber oder Integrator interpretiert wurden und in der Integration diese Unterschiede die Erfüllung der Anforderungen verhindern. Andererseits sind es nicht abgeschlossene Schnittstellenspezifikationen oder Anpassungen in „letzter Minute", welche die Konsistenz

nication between the signal box and the operations centre so that the latency times remain within acceptable limits.

In phase 7, the components are manufactured or purchased. The implementation of the security requirements in the components must be traceable to the requirements from phase 4. Tools such as Polarion or DOORS (Dynamic Object Oriented Requirements System) can be used for this. The focus in this phase is on avoiding any conflicts between the cybersecurity functionality and the functional architecture. This can be ruled out by early functional and security testing. The use of regression testing is recommended for security functionality at an early stage, especially in the case of in-house production. Automated vulnerability scanners such as trivy can be used for this purpose. The risk posed by the found vulnerabilities should then be managed centrally, for example using the open-source DefectDojo software. Security function tests, as described in the technical article "OT Security Pentest and Test Automation in Railway Systems" [5], are also valuable. These specifically focus on the effectiveness of individual security measures, such as blocking unauthorised access or responding correctly to expired certificates. The early identification of deviations in component behaviour can prevent costly reworking in later phases. A typical challenge in security function testing involves the lack of a test environment that provides shared security services, for example.

Those who consistently implement secure design principles in phase 6 and ensure the implementation of security functions in phase 7 create a robust basis for all the subsequent lifecycle phases. In this way, cybersecurity does not become an afterthought, but an integral quality feature of the entire system, i.e. something that is indispensable, especially in the railway industry with its high safety requirements.

4 Integration through to acceptance (phases 8, 9 and 10)

The aim of system integration is to integrate any components that have been developed or procured separately based on the specifications (phases 1–5), for example, firewalls, operating computers or complete LST (control and safety technology) systems such as a Radio Block Centre (RBC) or Digital Interlocking (DSTW) from different manufacturers, into a safety-compliant, cyber-resilient overall system. This is not just a matter of functional interaction, but also of providing integral evidence that the specified safety measures are fully or particularly effective in the system network. While technical functionality is a given in railway technology, the effective implementation of cybersecurity measures in the system network is by no means trivial and it is the real focus of this phase.

Typical problems during system integration arise when requirements are interpreted differently by manufacturers, operators or integrators and these differences prevent the requirements from being met during integration or mean that the necessary evidence cannot be provided. On the other hand, it is unfinished interface specifications or last-minute adjustments that jeopardise the consistency of the overall system. Early conformity checks between the requirements specification, functional specification and product are recommended to avoid any undesirable developments.

Another aspect that is often underestimated is the systematic "hardening" of the built-in components. In practice, this means that every system component (operating systems, e.g. in the diagnostic computer, interfaces to the surrounding systems, network elements such as switches and firewalls or control units)

des Gesamtsystems gefährden. Um Fehlentwicklungen zu vermeiden, eignen sich frühzeitige Konformitätsprüfungen zwischen Lastenheft, Pflichtenheft und Produkt.
Ein oft unterschätzter Aspekt ist auch das systematische „Härten" (Hardening) der eingebauten Komponenten. In der Praxis bedeutet dies, dass jede Systemkomponente – Betriebssysteme z. B. des Diagnoserechners, Schnittstellen zu Umsystemen, Netzwerkelemente wie Switche und Firewalls oder Steuergeräte – so konfiguriert wird, dass nur die unbedingt benötigten Funktionen aktiv bleiben, potenzielle Angriffspunkte deaktiviert und alle sicherheitsrelevanten Einstellungen korrekt gesetzt sind. Dazu zählen u. a. das Deaktivieren ungenutzter Ports, das Entfernen von Default-Credentials, das Erzwingen starker Passwörter, die Absicherung von Remote-Access-Funktionen oder die Einschränkung von Admin-Rechten.
Ein bewährter Standard zur systematischen Härtung sind die CIS-Benchmarks (Center for Internet Security) [11], die für zahlreiche Plattformen (z. B. Windows Server, Linux, Netzwerkgeräte) konkrete Checklisten mit Bewertungsskalen bereitstellen. Diese Benchmarks lassen sich auch in Bahnanwendungen gut anpassen und automatisiert prüfen – insbesondere bei wiederkehrenden Konfigurationen wie in redundanten Steuergeräten.
Parallel zur Härtung ist in dieser Phase ausschlaggebend, dass alle Security-relevanten Funktionen des Systems gezielt getestet werden – nicht nur die Funktionalität im Safety-Kontext, sondern die konkrete Umsetzung der Cybersecurity-Anforderungen aus der Lastenheft- und Architekturphase (z. B. Zugriffsbeschränkungen, Verschlüsselungsfunktionen oder Kommunikationspfade) [5]. Anders als bei den bisherigen Systemen, muss die erfolgreiche (Teil)-Integration im Lebenszyklus durch Software- und Security-Patches regelmäßig wiederholt werden. Aus diesem Grund ist die Testautomatisierung, die bereits in Phase 7 angesprochen wurde, dringend zu empfehlen. Zwar ist es keine Grundvoraussetzung, um die initiale Systemintegration zu erreichen. Doch bereits zwischen der ersten Integration und der Inbetriebnahme können bereits Updates notwendig werden. Die manuelle Wiederholung aller notwendigen Tests erzeugt dann zwangsläufig Projektverzögerungen. Grundlage erfolgreicher Testautomatisierung sind die eingangs angesprochenen Testfallbeschreibungen. Diese müssen für das spezifisch entwickelte System angepasst werden, um tatsächlich eine Automatisierung zu erlauben.
Der Cybersecuritycase (CSC, Cybersecurity-Nachweis) ist das zentrale Dokument, um die IT-Sicherheit des Produktes zu dokumentieren. Die Validierung in Phase 9 arbeitet dem Nachweis zu, indem sie die Einhaltung des Entwicklungslebenszyklus prüft. Die Anforderungsvalidierung stellt sicher, dass die Systemanforderungen vollständig abgeleitet wurden und geeignet sind, ein sicheres (secure) Produkt zu entwickeln. Die Systemvalidierung prüft gestützt auf die durchgeführten Tests, ob die Anforderungen vollständig und wirksam im Produkt umgesetzt werden. In allen Lebenszyklusphase kann aus verschiedenen Gründen davon abgesehen werden, technisch erforderliche Security-Anforderungen umzusetzen. Um dennoch das Cybersecurity-Risiko auf ein akzeptables Niveau zu senken, können Auflagen an den Betrieb des Produktes durch IT-sicherheitsbezogene Anwendungsbedingungen (SecRAC) beschrieben werden. Der CSC sammelt die SecRAC über alle Phasen zusammen und bündelt alle Cybersecurity-relevanten Artefakte des Entwicklungslebenszyklus. Bei zusammengesetzten Systemen schließt dies die CSC von Teilsystemen ein, die in einem eigenen Projekt (z. B. durch Lieferanten) entwickelt wurden und daher einen eigenen CSC zuliefern, der in den CSC des integrier-

is configured in such a way that only the absolutely necessary functions remain active, any potential points of attack are deactivated and all the security-relevant settings have been set correctly. This includes deactivating any unused ports, removing the default credentials, enforcing strong passwords, securing remote access functions and restricting admin rights.
The CIS (Centre for Internet Security) benchmarks [11], which provide specific checklists with rating scales for numerous platforms (e.g. Windows Server, Linux, network devices), are a proven standard for systematic hardening. These benchmarks can also be easily adapted and automatically checked in railway applications, especially for recurring configurations such as in redundant control units.
In parallel with hardening, it is also crucial that all the system's security-relevant functions are specifically tested in this phase, i.e. not only the functionality within the safety context, but also the concrete implementation of the cybersecurity requirements from the requirements specification and architecture phase (e.g. access restrictions, encryption functions or communication paths) [5]. Unlike previous systems, successful (partial) integration must be repeated regularly throughout the lifecycle by means of software and security patches. For this reason, test automation is highly recommended. Although it is not a prerequisite for achieving initial system integration, updates may already be necessary between the first integration and commissioning. Manually repeating all the necessary tests inevitably leads to project delays. The basis for successful test automation involves the test case descriptions mentioned at the beginning. These must be adapted to the specifically developed system so as to allow automation.
The cybersecurity case (CSC, cybersecurity evidence) is the central document for documenting a product's IT security. Validation contributes to the evidence by checking compliance with the development lifecycle. Requirements validation ensures that the system requirements have been fully derived and are suitable for developing a secure product. System validation checks whether the requirements have been fully and effectively implemented in the product based on the performed tests. A decision may be reached not to implement any technically necessary security requirements for various reasons in all the lifecycle phases. The requirements for operating the product can be described by the IT SecRAC in order to reduce the cybersecurity risk to an acceptable level. The CSC collects the SecRACs across all the phases and bundles all the development lifecycle's cybersecurity-relevant artefacts. In the case of composite systems, this includes the CSCs of any subsystems that have been developed in a separate project (e.g. by suppliers) and therefore supply their own CSC, which must be integrated into the integrated product's CSC. The CSC also serves as a starting point for the PSV to assess cybersecurity [4].

5 Operations and decommissioning (phases 11 and 12)

The operation and maintenance phase is the longest and most critical phase in the railway system lifecycle. It becomes apparent during this time whether the security level achieved in development and integration has been maintained in the long term or gradually eroded. TS 50701 and IEC 62443 require operators to continuously monitor and maintain the security measures during operations and to adapt them to any changing threat situations. The CRA now also requires this by law for products from 11 December 2027 onwards.

ten Produktes integriert werden muss. Der CSC dient ebenso als Ausgangspunkt für den PSV, um die Cybersecurity gutachterlich zu bewerten [4].

5 Betrieb und Außerbetriebnahme (Phase 11 und 12)

Die Betriebs- und Wartungsphase ist die längste und zugleich kritischste Phase im Lebenszyklus bahntechnischer Systeme. In dieser Zeit stellt sich heraus, ob die in Entwicklung und Integration erzielte Sicherheitslage dauerhaft erhalten bleibt – oder schleichend erodiert. TS 50701 und IEC 62443 fordern, dass Betreiber Sicherheitsmaßnahmen im laufenden Betrieb kontinuierlich überwachen, pflegen und an geänderte Bedrohungslagen anpassen. Der CRA fordert dies nun auch gesetzlich für Produkte ab dem 11. Dezember 2027 ein.

Cybersecurity in dieser Phase bedeutet vor allem: fortlaufendes Schwachstellenmanagement, regelmäßige Systempflege und reaktionsfähige Überwachung durch ein aktives Security Operation Center (SOC). Dazu gehört auch das Prüfen aktueller Gefährdungsquellen – etwa anhand des BSI-Grundschutz – Elementary Threats [9] oder des jährlich erscheinenden ENISA Threat Landscape Report [10], der aktuelle Angriffstrends von Ransomware über Phishing bis zu Supply-Chain-Angriffen beschreibt. Die regelmäßige Auswertung solcher Quellen im Bahnbetrieb ermöglicht es, Schutzmaßnahmen gezielt zu priorisieren und rechtzeitig in die Safety- bzw. Zulassungsprozesse einzufügen.

Trotz klarer Normvorgaben stoßen Betreiber im Bahnumfeld immer wieder auf ähnliche Hürden:

- Konflikt zwischen Sicherheitsupdates und Betriebssicherheit: Notwendige Security-Patches müssen oft mit betrieblichen Sicherheitsanforderungen (Safety) abgestimmt werden, um Störungen zu vermeiden.
- Fehlende Ressourcen für kontinuierliches Monitoring: Personelle und technische Kapazitäten reichen nicht aus, um Bedrohungen proaktiv zu erkennen.
- Fehlende Meldewege: Es existieren keine klaren Kanäle oder Prozesse zur Meldung von Sicherheitsereignissen.

„Best Practice" ist dabei, quartalsweise alle eingesetzten Softwarekomponenten auf bekannte Schwachstellen (CVE-Datenbankabgleich) zu prüfen und erforderliche Patches zusammen mit dem Hersteller zu planen. Der Cyber Resilience Act (CRA) verpflichtet Hersteller dazu, dies für ihre Produkte proaktiv zu tun. Hier kommen zunehmend aktive Vulnerability Scanner zum Einsatz, nicht nur in der Produktionsumgebung, sondern auch in Entwicklungs- und Testsystemen, um Sicherheitslücken vor der Auslieferung zu erkennen. Ein praxisnahes Beispiel ist DefectDojo – eine Open-Source-Plattform zur zentralen Verwaltung von Scanergebnissen, die sich mit gängigen Scannern wie OpenVAS, Nessus oder Qualys koppeln lässt. Um die tatsächliche Widerstandsfähigkeit des Systems unter realistischen Angriffsbedingungen zu überprüfen, müssen regelmäßige Penetrationstests durchgeführt werden. Diese Tests helfen, Schwachstellen zu identifizieren, die im normalen Monitoring oder durch automatische Scanner nicht entdeckt werden [5].

Ein SIEM (Security Incident and Event Management)-System sammelt Logdaten zentral im SOC, während ein IDS (Intrusion Detection System) den Netzwerkverkehr – oft über eine Firewall-Funktion umgesetzt – auf verdächtige Muster hin überwacht. Für das zentrale Logmanagement eignen sich Lösungen wie Graylog, Splunk oder Elastic Stack (ELK).

Wer diese Maßnahmen konsequent umsetzt, stellt sicher, dass Cybersecurity im Bahnbetrieb nicht nur ein einmal erreichtes Ziel bleibt, sondern über die gesamte Betriebszeit hinweg wirksam fortgeführt wird.

Above all, the cybersecurity in this phase means ongoing vulnerability management, regular system maintenance and responsive monitoring by an active Security Operation Centre (SOC). This also includes checking any current sources of danger, for example, using the BSI's Elementary Threats [9] or the annual ENISA Threat Landscape Report [10], which describes current attack trends from ransomware to phishing to supply chain attacks. Regular evaluation of such sources in railway operations enables protective measures to be prioritised in a targeted manner and incorporated into the safety and approval processes in good time.

Despite clear standards, operators in the railway environment repeatedly encounter similar hurdles:

- conflicts between security updates and operating safety: necessary security patches often have to be coordinated with operating safety requirements in order to avoid disruptions.
- a lack of resources for continuous monitoring: human and technical capacities are insufficient to proactively detect threats.
- a lack of reporting channels: there are no clear channels or processes for reporting any security events.

It is best practice to check all the used software components for known vulnerabilities (a CVE database comparison) on a quarterly basis and to plan the necessary patches together with the manufacturer. The Cyber Resilience Act (CRA) obliges manufacturers to do this proactively for their products. Active vulnerability scanners are increasingly being used here, not only in the production environment, but also in development and test systems, to detect any security gaps before delivery. A practical example is DefectDojo, an open-source platform for the central management of scan results that can be linked to common scanners such as OpenVAS, Nessus or Qualys. Regular penetration tests must be carried out in order to check the actual resilience of the system under realistic attack conditions. These tests help identify any vulnerabilities that are not detected by normal monitoring or automatic scanners [5].

A SIEM (Security Incident and Event Management) system collects log data centrally in the SOC, while an IDS (Intrusion Detection System) monitors network traffic – often implemented via a firewall function – for suspicious patterns. Solutions such as Graylog, Splunk or Elastic Stack (ELK) are suitable for centralised log management.

Consistent implementation of these measures ensures that cybersecurity in railway operations is not just a one-time goal, but is effectively maintained throughout the entire operating period.

The decommissioning phase marks the end of a system's lifecycle, but from a cybersecurity perspective, it is by no means an uncritical conclusion. In the railway industry in particular, many systems contain sensitive operating or access data, cryptographic keys and configuration information such as IP addresses, which, if disposed of improperly, could fall into the wrong hands and be used for attacks. The TS 50701 (Section 10.4), IEC 62443-2-1 (Section 4.3.4.4.5) and IEC 62443-4-1 (DM-5) standards therefore emphasise that a structured, secure decommissioning process must be established that is synchronised with the safety requirements of EN 50126.

The safety focus in this phase is on three key points: the complete identification of all the safety-relevant data, the secure removal or destruction of this data or system components (hardware) and the prevention of any uncontrolled reuse. In practice, there is often a lack of centralised documentation for old systems: often no one knows exactly what data is stored on old

Die Phase der Außerbetriebnahme markiert das Ende des Lebenszyklus eines Systems, ist aber aus Cybersecurity-Sicht keineswegs ein unkritischer Abschluss. Gerade im Bahnwesen enthalten viele Systeme sensible Betriebs- oder Zugangsdaten, kryptografische Schlüssel und Konfigurationsinformationen wie IP-Adressen, die bei unsachgemäßer Entsorgung in falsche Hände geraten und für Angriffe genutzt werden können. Die Standards TS 50701 (§ 10.4), IEC 62443-2-1 (§ 4.3.4.4.5) und IEC 62443-4-1 (DM-5) betonen daher, dass ein strukturierter, sicherer Außerbetriebnahmeprozess etabliert werden muss, der mit den Safety-Anforderungen der EN 50126 synchronisiert ist.
Der Sicherheitsfokus liegt in dieser Phase auf drei Kernpunkten: der vollständigen Identifikation aller sicherheitsrelevanten Daten, der sicheren Entfernung oder Zerstörung dieser Daten bzw. Systemkomponenten (Hardware) und der Vermeidung einer unkontrollierten Wiederverwendung.
In der Praxis fehlt häufig eine zentrale Dokumentation alter Systeme – welche Daten liegen auf Alt-Hardware oder es gibt keine definierten Prozesse für sichere Entsorgung –, insbesondere bei dezentral verteilten Anlagen. Definition von Regelwerken oder Prozessen sowie Audits inaktiver Assets sorgen dafür, dass der Ablauf verbindlich geregelt ist und sensible Daten entfernt werden.

6 Fazit

Die Herausforderungen jeder einzelnen Phase des Lebenszyklus unterstreichen die zentrale Bedeutung eines ganzheitlichen und praxisorientierten Cybersecurity-Managements. Nur wenn Security-Maßnahmen von der ersten Konzeption über Systemarchitektur, Integration und Validierung bis hin zu Betrieb und Außerbetriebnahme konsequent und strukturiert umgesetzt werden, kann langfristig ein hohes Schutzniveau erreicht und erhalten werden.
Praxisbeispiele zeigen, dass eine enge Verzahnung von Normen (IEC 62443, CLC/TS 50701), gesetzlichen Vorgaben (BSI-Gesetz, CRA) und erprobten Best-Practices – wie Schwachstellenmanagement, Testautomatisierung und regelmäßigen Penetrationstests – unabdingbar ist, um aktuellen und zukünftigen Bedrohungen wirksam begegnen zu können.
Besonders im Betrieb gilt: Sicherheitsmanagement ist kein einmaliges Projekt, sondern ein fortlaufender Prozess, der organisatorische wie technische Maßnahmen erfordert. Nur so kann gewährleistet werden, dass die Sicherheitseigenschaften der Bahn-OT-Systeme nicht nur einmalig erreicht, sondern über die komplette Lebensdauer hinweg wirksam erhalten bleiben. ■

AUTOREN | AUTHORS

Dr.-Ing. Martin Koop
Principal IT / OT Security Expert
Incyde GmbH
Anschrift / *Address:* Rheinstraße 16a, D-64283 Darmstadt
E-Mail: martin.koop@incyde.com

Dr.-Ing. Markus Heinrich
Senior IT / OT Security Expert
Incyde GmbH
Anschrift / *Address:* Rheinstraße 16a, D-64283 Darmstadt
E-Mail: markus.heinrich@incyde.com

Johannes Häring
IT / OT Security Expert
Incyde GmbH
Anschrift / *Address:* Münzgasse 1, D-04107 Leipzig
E-Mail: johannes.haering@incyde.com

hardware or there are no defined processes for secure disposal, especially in the case of decentralised systems.
In practice, there is often a lack of centralised documentation for old systems (which data is stored on old hardware or cases where there are no defined processes for secure disposal), especially in the case of decentralised systems. The definition of rules and regulations or processes, as well as audits of any inactive assets, ensure that the process is bindingly regulated and that any sensitive data is removed.

6 Conclusion

The challenges of each individual phase of the lifecycle underscore the central importance of holistic and practice-oriented cybersecurity management. Only if security measures are implemented consistently and in a structured manner, from the initial design to the system architecture, integration and validation and on to operations and decommissioning, can a high level of protection be achieved and maintained in the long term.
Practical examples have shown that the close integration of standards (IEC 62443, CLC/TS 50701), legal requirements (BSI Act, CRA) and proven best practices, such as vulnerability management, test automation and regular penetration tests, is essential in order to effectively counter any current and future threats. Particularly in operations, security management is not a one-off project, but an ongoing process that requires organisational and technical measures. This is the only way to ensure that the security features of railway OT systems are not only achieved once, but remain effective throughout their entire service lives. ■

LITERATUR | LITERATURE

[1] Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 und Absatz 1a BSIG umzusetzenden Maßnahmen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html
[2] Poschinger, R.; Jungo, C.; Kleine, E.; Espenschied, M.: Cyber-Security-Maßnahmen für ERTMS aus Sicht der Bahnbetreiber, SIGNAL+DRAHT (115) 9/2023
[3] Poschinger, R.; Sen, A.: EULYNX Security – Standardisierung für gemeinsamen Schutz, SIGNAL+DRAHT (114) 4/2022
[4] Katzenbeisser, S.; Wunderskirchner, M.: TS 50701 – Cybersicherheit aus Sicht der Begutachtung, SIGNAL+DRAHT (114) 4/2022
[5] Koop, M.; Hagemann, L.; Kaffo, A.: Hinterfrage deine Annahmen: Praxiserfahrungen mit Testautomatisierung und Pentests, SIGNAL+DRAHT (116) 9/2024
[6] Europe's Rail System Pillar Publication: Shared Cybersecurity Services Specification, SP-SEC-ServSpec, v1.0, 2/2025
[7] Europe's Rail System Pillar Publication: Secure Component Specification, SP-SEC-CompSec, v1.0, 2/2025
[8] Knapp, O.; Poschinger; R., Weller, M.; Wischy, M.: EU-Rail veröffentlicht Cybersecurity-Spezifikation, SIGNAL+DRAHT (117) 5/2025
[9] BSI IT-Grundschutz-Compendium Edition 2022, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf
[10] Threat Landscape, https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape
[11] CIS-Benchmarks, https://www.cisecurity.org/cis-benchmarks