Security Lifecycle Management für bestehende ETCS-Produkte – ein Erfahrungsbericht

Security lifecycle management for existing ETCS products – a case study

Patric Birr | Stefan Karg | Christoph Ritschel

Seit Inkrafttreten des IT-Sicherheitsgesetzes [1] für den Sektor Transport & Verkehr ist die Integration der notwendigen Security-Aktivitäten in die für sicherheitsrelevante Systeme etablierten Prozesse eine der zentralen Herausforderungen für Security-Verantwortliche im Bahnbereich. Die ICS GmbH ist seit 2016 für Security Management in zahlreichen Bahnprojekten verantwortlich, insbesondere im Bereich ETCS (European Train Control System) und Retrofit. Ergänzend zum Beitrag über die Implementierung von Security in Bestandsfahrzeugen [2], beschreibt dieser Beitrag bewährte Ansätze für Security Management in ETCS-Projekten.

1 Motivation

Branchenübergreifend und international hat sich in den letzten Jahren die ISA/IEC 62443 [3] als State-of-the-Art-Standard für Security in industriellen Automatisierungssystemen (IACS) durchgesetzt. Auch CENELEC hat mithilfe der „TC9X Working Group 26" eine Adaption der ISA/IEC 62443 für den Bahnsektor als TS 50701 „Railway applications – Cybersecurity" realisiert [4] (Zusammenfassung siehe [5]).
In der TS 50701 ist der Integration von Security in Safety-Prozesse eine besondere Relevanz und folgerichtig ein eigenes Kapitel zugeteilt. Die „Lifecycle Sub-Group" hat, koordiniert durch Patric Birr, verbindliche Security-Aktivitäten festgelegt und den Weg geebnet für ein einheitliches Security Management für Bahnsysteme.
Mit einheitlichen normativen Festlegungen entstehen für Hersteller, Integratoren und Betreiber entsprechende Umsetzungszwänge, die durch die zuständigen Regulierungsbehörden auch verstärkt geprüft werden. Abseits der regulatorischen Vorgaben und obwohl das Thema in älteren Verträgen noch nicht immer verankert ist, wirkt sich die Security der Produkte auch positiv auf die internationale Wettbewerbsfähigkeit aus. Umso wichtiger wird für Security Manager in ETCS-Projekten, das Thema dem Stand der Technik entsprechend systematisch zu behandeln.
In der Praxis stehen die Verantwortlichen vor konkreten Herausforderungen, insbesondere im Zusammenhang mit nicht sicheren Bestandssystemen, Einschränkungen durch die ETCS-Spezifikation [6] und auch technisch oder finanziell begrenzte Handlungsspielräume. Das folgende Kapitel soll zeigen, wie unter diesen Rahmenbedingungen ein dem Stand der Technik entsprechendes Security Management möglich ist.

2 Security Lifecycle Management

Welche Security-Aktivitäten in der jeweiligen Lebenszyklusphase gemäß EN 50126-1 [7] durchzuführen sind, ist im Kapitel „Cyberse-

Since the IT Security Act [1] for the traffic and transport sector came into effect, one of the key challenges for security managers in the rail sector has been to integrate the necessary security activities into the processes established for security-relevant systems. ICS GmbH has been entrusted with security management in numerous rail projects since 2016, especially in the field of ETCS (European Train Control System) and retrofitting. In addition to the article on the implementation of legacy rolling stock security [2], this article describes proven approaches to security management in ETCS projects.

1 Motivation

In recent years, ISA/IEC 62443 [3] has been implemented as the state-of-the-art standard for security in the Industrial Automation and Control System (IACS). CENELEC has also instantiated the adaptation of ISA/IEC 62443 for the railway sector as the TS 50701 "Railway applications – Cybersecurity" with the help of the "TC9X Working Group 26" [4] (for a summary, refer [5]).
The integration of security into the safety processes is of particular relevance and consequently has its own dedicated chapter in TS 50701. The "Lifecycle Sub-Group", coordinated by Patric Birr, has defined a number of binding security activities and paved the way for uniform security management for railway systems.
Uniform standard specifications establish corresponding implementation obligations for manufacturers, integrators and operators, which are also increasingly being inspected by the responsible regulatory authorities. Despite the regulatory requirements and even though the topic has not always been included in older contracts, product security also has a positive effect on international competitiveness. Systematically addressing the scope of the state-of-the-art is becoming increasingly important for security managers in ETCS projects.
In practice, however, the responsible authorities face real challenges particularly related to existing unsafe systems, restrictions due to ETCS specifications [6] and technically or financially limited scope for action. The following chapter is intended to show how state-of-the-art security management is possible under these framework conditions.

2 Security lifecycle management

The security activities that have to be carried out in the respective lifecycle phases in accordance with EN 50126-1 [7] are de-

curity within a railway application lifecycle" der TS 50701 normativ erfasst. Bild 1 veranschaulicht die praktische Anwendung der ICS GmbH Projektteams in ETCS-Entwicklungsprojekten.
Die Security-Risikoanalyse ist sowohl in der Entwicklung als auch nach der Inbetriebnahme von besonderer Bedeutung, da sich aus vielen der folgenden Security-Aktivitäten Aktualisierungsbedarf in diesem Dokument ergeben kann. Darüber hinaus ist die nach dem Security und Penetration Testing aktualisierte Risikoanalyse ein wichtiges Eingangsdokument für die Security-Nachweisführung, den sog. „Security Case".

2.1 Security-Management-Plan

In der Praxis hat sich gezeigt, dass über den Lebenszyklus hinweg enge Abstimmungen zwischen den Security-Verantwortlichen und den ETCS-Produkt-Stakeholdern notwendig sind. Insbesondere für die Rollen RAMS, Verifikation und Validierung ist der Umgang mit Security-Themen erfahrungsgemäß noch eher unbekannt. Daher wird ein Security-Management-Plan erstellt. In der Praxis hat sich folgende Struktur in Anlehnung an die TS 50701 bewährt:

1. Zugrundeliegende normative Basis und Referenz auf das Unternehmens-ISMS nach [8]
2. High-level Darstellung der ETCS-Komponenten mit Verweis auf existierende Architektur- und Schnittstellendokumente
3. Produktorganisation, Rollen und Verantwortlichkeiten; Festlegung der Informationssicherheitsklassen, Datenmanagement und Referenz auf Kommunikationsplan
4. Tabellarische Darstellung des Security Lifecycle in Anlehnung an TS 50701, Tab. 1 [4]
5. Methodik des Security Risk Assessments in Anlehnung an TS 50701 und IEC/ISA 62443-3-2 [9], z. B. Angriffsbaumanalyse und toolgestützte detaillierte Risikoanalyse nach [10]
6. Werkzeuge für das Anforderungsmanagement und Umgang mit nicht vollständig umgesetzten Anforderungen. In der Praxis ergibt sich bei der erstmaligen Implementierung von Security-Maßnahmen in ETCS-Produkte oft ein Graubereich zwischen erfüllten und nicht-erfüllten Anforderungen, welcher zu regeln ist.
7. Schnittstellen zu Dritten, insbesondere RAMS, Verifikation und Validierung; Referenzen auf Security-Management-Pläne von Zulieferern

scribed in the "Cybersecurity within a railway application lifecycle" chapter of TS 50701. Fig. 1 illustrates the ICS GmbH project team's practical application in ETCS development projects.
The security risk analysis is of particular importance, both during development and after commissioning, because the subsequent security activities may necessitate this document being updated. In addition, the risk analysis that has been updated after security and penetration testing is an important input document for the "Security Case".

2.1 Security management plan

Experience has shown that close coordination between security managers and ETCS product stakeholders is necessary throughout the lifecycle. The empirical evidence suggests that the roles of RAMS, verification and validation are particularly still unfamiliar with security topics. Therefore, a security management plan will be drawn up. In practice, the following structure based on TS 50701 has proven effective:

1. The underlying normative basis and reference to the enterprise ISMS according to [8]
2. High-level representation of the ETCS components with reference to the existing architecture and interface documents
3. Product organisation, roles and responsibilities; the definition of the information security classes, data management and reference to communication plan.
4. Tabular representation of the security lifecycle based on TS 50701, tab. 1 [4].
5. A security risk assessment methodology according to TS 50701 and IEC/ISA 62443-3-2 [9], e.g., attack tree analysis and tool-based detailed risk analysis according to [10].
6. Tools for requirement management and the handling of partially implemented requirements. In practice, the initial implementation of security measures in ETCS products often results in a grey area between compliant and partially compliant requirements, which must be regulated.
7. Interfaces to third parties, particularly RAMS, verification and validation; references to suppliers' security management plans.
8. The procedure for creating and accepting the Security Case

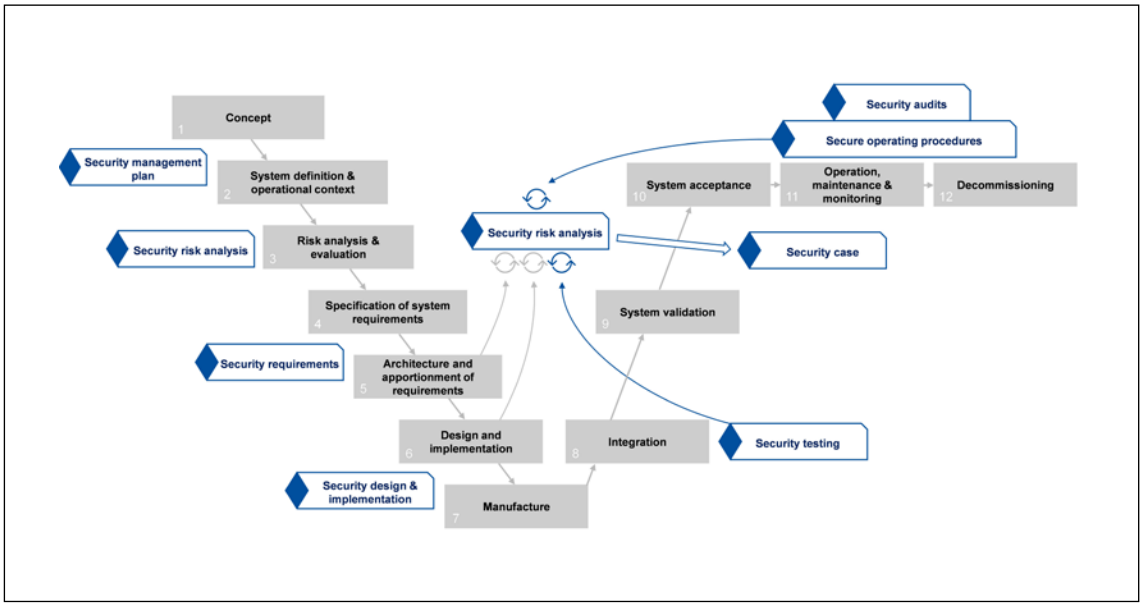

Bild 1: Security-Aktivitäten im V-Modell
Fig. 1: Security activities in the V-Model

8. Prozess zur Erstellung und Abnahme des Security Case
9. Sicherer Betrieb, Schwachstellenmanagement und Außerbetriebnahme.

2.2 Security-Risikoanalyse

Als Security Manager in Entwicklungsprojekten mit international gültigen Rahmenbedingungen ist häufig ein Abwägen zwischen verschiedenen Schutzmaßnahmen erforderlich, sowohl durch technische als auch organisatorische oder finanzielle Restriktionen. Entscheidungen für oder gegen einzelne Schutzmaßnahmen, die dann auch eine Abweichung zum normativen Soll-Zustand darstellen können, müssen stets unter Berücksichtigung der Auswirkungen auf die Risikobewertung erfolgen. Ist beispielsweise durch den Einsatz von Bestandskomponenten die Verschlüsselung auf einzelnen Verbindungen technisch nicht umsetzbar, muss bewertet und dokumentiert werden, wie sich das Gesamtrisiko bei Verzicht auf diese Maßnahme oder durch eine Alternativlösung verändert.

Entscheidend für die Aussagekraft derartiger Bewertungen ist eine ganzheitliche Betrachtung der Systeme, also unter technischen, infrastrukturellen und auch organisatorischen Aspekten. Auch bei der Definition von Ausgleichsmaßnahmen (engl. „compensating countermeasures“) zu technisch nicht umsetzbaren Funktionen spielen die Umgebungsbedingungen eine besondere Rolle und müssen daher systematisch erfasst sein. Diese Ausgleichsmaßnahmen werden in der Regel als Security-Anwendungsbedingungen an den Kunden (Integrator oder Betreiber) übergeben und sollten mit diesem vor der Finalisierung des Dokuments hinsichtlich der Machbarkeit abgestimmt werden.

Für die systematische und ganzheitliche Identifikation von Bedrohungen und Schwachstellen empfiehlt sich die Durchführung einer Angriffsbaumanalyse, auf deren Basis dann je Bedrohung eine detaillierte Risikobewertung durchzuführen ist. Der Workflow für detaillierte Security-Risikoanalysen gemäß IEC 62443-3-2 [9] sieht auf Basis der Bewertungen je Zone und Conduit die Festlegung von Security Level Targets vor, an die jeweils Schutzmaßnahmen gekoppelt sind.

In der Praxis ist die vollständige Umsetzung dieser Anforderungen aufgrund der genannten Rahmenbedingungen selten machbar, und es muss stattdessen priorisiert werden, mit welchen Maßnahmen und Anwendungsbedingungen die größte Risikoreduktion erreicht werden kann. Dass ein System auch ohne vollständige Implementierung der vordefinierten Security Levels ausreichend sicher ist, muss sich aus dem Risikoanalysebericht ergeben, der neben allen Bedrohungen und Schwachstellen insbesondere auch die Restrisiken beinhalten muss. Bild 2 veranschaulicht, wie die ICS Projektteams die Teilschritte des normativen Workflows dokumentieren.

2.3 Security-Anforderungsspezifikation

Die Erstellung der Security-Anforderungsspezifikation geht Hand in Hand mit der Definition der Gegenmaßnahmen im Zuge der Risikoanalyse. Die aus den Maßnahmen abgeleiteten Anforderungen werden iterativ in der Spezifikation ergänzt, und es entsteht mit den Security-bezogenen Anwendungsbedingungen (SecRAC) eine vollständige Sammlung aller zur Umsetzung geplanten Maßnahmen.

In der Praxis zeigt sich hier vor allem die Schwierigkeit, dass bei bestehenden Produkten die Security nachträglich ins Produkt integriert werden muss. Normative Anforderungen oder Anforderungen von Kunden bezüglich Security betreffen Aspekte des Systems, die unter Umständen schon vor Jahren entworfen wurden

9. Safe operations, vulnerability management and decommissioning.

2.2 Security risk analysis

As a security manager in development projects with internationally valid framework conditions, it is often necessary to achieve a balance between various required countermeasures due to technical, organisational or financial restrictions. Decisions in favour of or against countermeasures, which may then also represent a deviation from the normative target status, must always be made with consideration of their effects on the risk assessment. For instance, if encryption is not technically feasible at individual connections due to the use of existing components, an evaluation must be undertaken and documented as to how the overall risk will change, if this measure is not implemented or an alternative solution is used.

A holistic view of the systems with regard to the technical, infrastructural and organisational aspects is decisive for the informative value of any such assessments. The environmental conditions also play a special role in defining the compensating countermeasures for functions that cannot be implemented technically and must therefore be recorded systematically. These compensating countermeasures are usually submitted to the customer (integrator or operator) as security-related application conditions and their feasibility should be coordinated with the customer before the document is finalised.

An attack tree analysis is recommended for the systematic and holistic identification of threats and vulnerabilities. A detailed risk assessment of each threat should then be performed on that basis. The workflow for the detailed security risk analyses in accordance with IEC 62443-3-2 [9] provides a definition of the security level targets based on the assessments for each zone and conduit, which are linked with protective measures of each case. The full implementation of these requirements is rarely feasible in practice due to the aforementioned framework conditions. As such, the measures and application conditions needed to achieve predominant risk reduction must be prioritised. The fact that a system is sufficiently secure even without the full implementation of the predefined security levels must be evident from the security risk analysis report, which must not only include all the threats and vulnerabilities, but particularly also the residual risks. Fig. 2 illustrates the approach of the ICS GmbH project teams towards documenting the sub-steps of the normative workflow.

2.3 Security requirement specification

The creation of a security requirement specification goes hand in hand with the definition of the countermeasures during the risk analysis. The requirements derived from the measures are iteratively added to the specification and a complete collection of all the planned measures for implementation is created along with the security-related application conditions (SecRAC).

In practice, the main challenge involves the retroactive integration of security into existing products. Normative or customer requirements regarding the security related system affect other system aspects that may have been designed years ago and are anchored in an architecture that has already been implemented in the hardware and software. This particularly applies to retrofit projects. The hardware and software platforms that have become established with rail manufacturers and been approved for safety applications also restrict the scope for patch management or the installation of additional libraries.

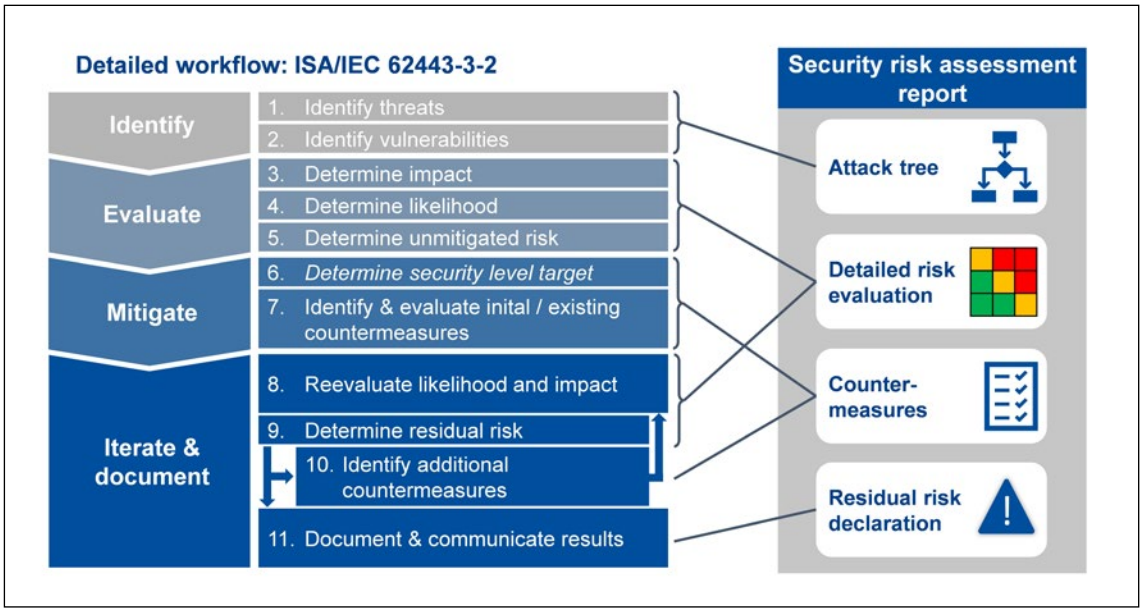

Bild 2: Dokumentation der Security-Risikoanalyse gemäß ISA / IEC 62443-3-2
Fig. 2: Security risk analysis documentation according to ISA / IEC 62443-3-2

und in einer Architektur verankert wurden, die bereits in Hard- und Software realisiert ist. Dies gilt insbesondere für Retrofit-Projekte. Auch bei Bahnherstellern etablierte, für Safety-Anwendungen zugelassene Hard- und Softwareplattformen schränken den Freiraum bezüglich der Durchführung des Patchmanagements oder Installation von zusätzlichen Bibliotheken ein.

Im Kontext von ETCS kommt bezüglich der Freiheitsgrade auch besonders das Thema der europäischen Standardisierung [6] ins Spiel. So wäre es beispielsweise aus Sicht der Security wünschenswert, dass Balisentelegramme mit einer kryptographischen Signatur versehen werden, um deren Authentizität beim Einlesen durch ein Fahrzeuggerät überprüfen zu können. Eine Umsetzung dieser Funktionalität würde allerdings zu einer nicht mit der europäischen Spezifikation von ETCS kompatiblen Umsetzung führen, da die Spezifikation eine solche Funktionalität nicht vorsieht [11].

Bei allen umgesetzten Security-Maßnahmen ist immer das Gesamtsystem zu betrachten. Welche Auswirkungen hat eine aus Security-Erwägungen getroffene Entscheidung auf die weiteren, bereits existierenden Systemkomponenten? Welche Auswirkungen hat sie auf die Wartung des Systems? Stehen die hierdurch entstehenden Mehrkosten noch im Verhältnis zum mitigierten Risiko? Hier muss eine sorgfältige Abwägung mit allen beteiligten Stakeholdern im Kontext des für Hersteller und Betreiber maximal akzeptablen Restrisikos getroffen werden.

2.4 Security Design und Implementierung

Ein in der TS 50701 ausgeklammerter Aspekt, der allerdings eine hohe Relevanz für die Praxis besitzt, ist das Begleiten der Implementierungsphase durch das für die Security zuständige Team. Es hat sich bewährt, im Rahmen dieser Begleitung ein sogenanntes Security-Design-Dokument zu erstellen. Dieses entsteht in enger Zusammenarbeit zwischen Security- und Entwicklungsteam und dokumentiert technische Entscheidungen und die bei Umsetzung der Security-Anforderungen angewandten Konzepte. Hierbei ist auf eine Nachverfolgbarkeit zwischen Anforderung und Beschreibung im Dokument zu achten.

Eine Herausforderung in der Implementierungsphase ist das Aufbauen gegenseitigen Verständnisses und Vertrauen zwischen dem Securityteam und dem Entwicklungsteam. Je nach Produkt handelt es sich um seit langem eingespielte Teams, die die stark

The topic of European standardisation [6] also comes into play within the context of ETCS with regard to the degrees of freedom. For example, it would be desirable from the security point of view for balise telegrams to be signed with a cryptographic signature for authenticity verification while being read by a vehicle device. However, the implementation of this functionality would not be compatible with the European ETCS specification, because the specification does not provide for such a functionality [11].

The overall system must always be considered in relation to all the implemented security measures. What effects does a decision made for security reasons have on the other already existing system components? What impact will it have on system maintenance? Are the resulting additional costs still in proportion to the mitigated risk? All the involved stakeholders must give careful consideration within the context of the maximum acceptable residual risk for the manufacturer, integrator and operator.

2.4 Security design and implementation

One aspect that has been excluded from TS 50701, but is highly relevant in practice involves the team responsible for the security accompanying the implementation phase. It is best practice to create a Security Design Document during accompanied teamwork. This document is created in close cooperation between the security and development teams and documents the technical decisions, as well as the concepts used to implement the security requirements. Care must be taken to ensure the traceability between the requirement and the description in the document.

One challenge during the implementation phase involves building up mutual trust and understanding between the security team and the development team. Depending on the product, these are usually teams that have been working together for a long time and have successfully implemented the highly formalised processes surrounding a product's safety. The requirements and processes pertaining to security are now added to these established processes. Their implementation may complicate previously familiar means of information exchange or device access (for example, by deactivating development interfaces). It is quite comprehensible that this can lead to moderate enthusiasm on

formalisierten Prozesse rund um die Safety eines Produktes erfolgreich umsetzen. Nun kommen zu diesen etablierten Prozessen Anforderungen und Prozesse aus dem Umfeld der Security hinzu. Deren Umsetzung erschwert unter Umständen bisher gewohnte Möglichkeiten zum Informationsaustausch oder zum Zugriff auf Geräte (beispielsweise durch die Deaktivierung von Entwicklungsschnittstellen). Es ist nur verständlich, dass dies zu mäßiger Begeisterung des Entwicklungsteams führen kann, da das Securityteam dem Entwicklungsteam subjektiv erst einmal die tägliche Arbeit erschwert. Aus diesem Grund ist hier ein besonderes Augenmerk auf den Faktor Kommunikation zu legen. Im besten Fall steht das Securityteam dem Entwicklungsteam als ständiger, direkter Ansprechpartner mit technischer Kenntnis und eigener Entwicklungskompetenz zur Verfügung und kann bei Schwierigkeiten beraten und konkrete Lösungsvorschläge anbieten. Diese enge Zusammenarbeit fördert das gegenseitige Verständnis und hilft durch eine vertrauensvolle Basis bei der Verwirklichung von ganzheitlicher Security.

2.5 Security Testing

Von besonderer Relevanz für die spätere Nachweisführung sind die Testaktivitäten in Bezug auf Security.

Zu Beginn der Testaktivitäten steht der sogenannte Testplan. Unter einer vergleichbaren Bezeichnung gibt es einen solchen bereits in jedem Entwicklungsprojekt, insbesondere wenn dieses der funktionalen Sicherheit genügen muss. Der Testplan beschreibt anzuwendende Testmethoden und deren Durchführung. Im durch Security-Aspekte erweiterten Testplan wird beispielsweise festgelegt, auf welchem System die Security-Tests durchgeführt werden und welche Komponenten während des Tests real vorhanden sein müssen und welche simuliert werden dürfen.

Die TS 50701 definiert in Abschnitt 9.3.2 verschiedene Testarten:

- Tests der Security-Anforderungen
- Tests der Bedrohungsminderung
- Tests auf Schwachstellen
- Penetrationstest.

Die Spezifikation und Durchführung der Tests sollten so gut wie möglich in die etablierten V&V-Prozesse eingebettet und zeitlich zu einem mit funktionalen Tests vergleichbaren Zeitpunkt durchgeführt werden. Dies ermöglicht eine Verifikation der Testergebnisse durch den Verifizierer. Bezüglich der Validierung hat es sich bewährt, diese durch einen speziell für das Thema Security geschulten Validierer durchführen zu lassen, der sich auf dieses Thema fokussiert.

Tests zur Abdeckung von Security-Anforderungen sowie Schwachstellentests werden bei einer agilen Entwicklungsmethodik möglichst zeitnah zu einer erfolgten Entwicklung durchgeführt, um möglichst früh Ergebnisse zu erhalten.

Tests der Bedrohungsminderung können dagegen nur teilweise sinnvoll an einem nicht fertig entwickelten und integrierten System durchgeführt werden. Aus diesem Grund ist es sinnvoll, diese Tests im gleichen Zeitraum wie Systemtests stattfinden zu lassen. Zu diesem Zeitpunkt ist das System bereits fertig entwickelt, und ein stabiler, integrierter Versionsstand steht zur Verfügung. Andererseits ist dies noch früh genug im Prozess, um auf eventuelle negative Ergebnisse reagieren zu können.

Neben dem Nachweis der erfolgreichen Implementierung der in der Security-Anforderungsspezifikation definierten Anforderungen durch das Testen spielt insbesondere der sogenannte Penetrationstest eine wesentliche Rolle. Hierbei handelt es sich um eine Simulation eines Angriffs auf das System durch sogenannte „Ethical Hacker“ (auch „White Hat Hacker“). Entsprechend des TS 50701

the part of the development team, because the security team initially makes the development team's daily routine work subjectively more difficult. Special attention must therefore be given to the communication factor for this reason. In the best case, the security team is available to the development team as a permanent direct contact with technical knowledge and development expertise. The security team can advise on difficulties and offer concrete proposals for solutions as a result of this direct support. This close cooperation promotes mutual understanding and helps create a basis of trust for the realisation of holistic security.

2.5 Security testing

The test activities regarding security are of special relevance to the subsequent verification management. The so-called test plan is the initial document for any test activities. Such a plan already exists with a similar name in every development project, especially if it has to satisfy functional safety. The test plan describes the test methods that are to be used and their execution. The test plan expanded with the security aspects specifies, for example, which system the security tests will be performed on and which components must actually be available during the test and which may be simulated.

TS 50701 defines various types of tests in Section 9.3.2:

- security requirement tests
- threat mitigation tests
- vulnerability tests
- penetration tests.

The specification and execution of the tests should be embedded in the established V&V processes as much as possible and performed at a time comparable to the function tests. This enables the verifier to verify the test results. It is considered best practice to get validation by a validator who is specially trained and focussed on security topics.

Security requirement and vulnerability tests are carried out as soon as a development has been finalised in order to obtain results in an agile development methodology as early as possible.

Threat mitigation tests, on the other hand, can only be partially performed in a meaningful way on a system that has not yet been fully developed and integrated. For this reason, it makes sense to perform these tests during the same time period as system tests. At this point, the system is already fully developed and a stable, integrated version is available. It is also still early enough in the process to be able to react to any negative results.

The penetration test also plays a particularly essential role in addition to confirming the successful implementation of the requirements defined in the security requirement specification through testing. This involves a simulated attack on the system by so-called “Ethical Hackers” (also known as “White Hat Hackers”). According to TS 50701, this penetration test should be performed by independent testers (an independent department or organisation).

On the one hand, the penetration test aims to check the effectiveness of the selected measures against an attacker acting in the manner of a real attacker and, on the other hand, to confirm the completeness of the security risk analysis. Further vulnerabilities that were not detected during the security risk analysis despite the systematic approach may also be identified in this step. The independent point of view of a simulated attacker especially constitutes a control mechanism which completes the system assessment.

When communicating penetration test results to the development teams of internally or externally developed components, it is important to be careful that the developers do not feel that they

soll dieser Penetrationstest von unabhängigen Testern (unabhängige Abteilung oder Organisation) durchgeführt werden.
Ziel des Penetrationstests ist einerseits die Prüfung der Effektivität der gewählten Maßnahmen gegen einen Angreifer, der ähnlich einem echten Angreifer agiert, und andererseits das Bestätigen der Vollständigkeit der Security-Risikoanalyse. Gegebenenfalls werden in diesem Schritt weitere Schwachstellen erkannt, die trotz der systematischen Vorgehensweise bei der Security-Risikoanalyse nicht erkannt wurden. Dies führt, insbesondere durch den unabhängigen Blick auf das System durch die Augen eines simulierten Angreifers, zur Kontrolle und Vervollständigung des Bildes über das System.
Bei der Kommunikation von Penetrationstestergebnissen an Entwicklungsteams von intern oder extern entwickelten Komponenten ist es wichtig, darauf zu achten, dass Entwickler sich nicht bloßgestellt fühlen. Ein Penetrationstest ist ein wichtiges Werkzeug, um gemeinsam in enger Abstimmung eine Verbesserung der Security des Gesamtsystems zu erreichen.

2.6 Security-Nachweis

In DER EISENBAHNINGENIEUR 4/2022 wurde der „Security Case" bereits als *„zentrales Nachweisdokument für alle Phasen des Lebenszyklus"* und dessen *„zentrale Inhalte"* erörtert [12]. In der Praxis hat sich bei der Security-Case-Erstellung für ETCS-Produkte eine enge Abstimmung mit Safety und Validierung bewährt, da der Security Case zur Erfüllung der Security-Anforderungen der EN 50129:2019 [13] vom Safety Case referenziert werden muss. Generelle Auswirkungen des Security Case auf die Safety-Zulassung im Bahnbereich wurden von Okstad et al. [14] zusammengetragen.
In der Praxis hat sich folgende Nachweisstruktur in Anlehnung an die TS 50701 für ein ETCS-Produkt bewährt:

1. High-level-Darstellung der ETCS-Komponenten mit Verweis auf existierende Architektur- und Schnittstellendokumente
2. Nachweise der Umsetzung der Security-Management-Prozesse, siehe Abschnitt 2.1
3. Referenz auf die Security-Risikoanalyse, siehe Abschnitt 2.2
4. Referenz auf Security-Anforderungsspezifikation, siehe Abschnitt 2.3
5. Referenz auf Security-Testberichte, ETCS-Produkt-Verifikations- und -Validierungsbericht
6. Nachweis der Security-Anforderungen als tabellarische Übersicht mit Verweis auf Nachverfolgungsdokumente; Erörterung möglicher Abweichungen und Ausgleichsmaßnahmen
7. „Security Case"-Dokumente von Zulieferern und Subsystemen
8. Liste der Security Related Application Conditions („SecRACs")
9. Auflistung aller bekannter Restrisiken für das ETCS-Produkt
10. Abschließende Zusammenfassung und Fazit („Security Claim") des ETCS-Produktes.

Der ETCS-Produkt Security Case wird an den Systemintegrator übergeben und durch diesen abgenommen. Der Systemintegrator ist für die Erstellung des System Security Case verantwortlich, welcher den ETCS-Produkt Security Case referenziert.

2.7 Sicherer Betrieb

Die Security-Aktivitäten sind mit dem Security Case nicht abgeschlossen, da sich die Bedrohungslandschaft in ständigem Wandel befindet und neue Schwachstellen auftreten können. Das Schwachstellenmanagement umfasst das Identifizieren, Bewerten und Beheben von Schwachstellen. Zusätzlich muss das ETCS-Produktteam einen Prozess für die Meldung eines Security-Vorfalls durch den Betreiber einrichten. Dieser kann aus Erfahrung generell auf dem Prozess von Vorfällen der Safety aufgebaut werden.

have been denounced. Penetration tests are an important tool to enable closer work together and improved security in the overall system.

2.6 Security case

The security case and its central content has already been discussed in DER EISENBAHNINGENIEUR 4/2022 as the "*central verification document for all phases of the lifecycle*" [12]. In practice, close coordination with safety and validation during the creation of security cases for ETCS products has been proven to be of value. The security case must be referenced by the safety case in order to meet the security requirements of EN 50129:2019 [13]. The general implications of the security case for the safety approval in the railway sector has been compiled by Okstad et al. [14].
In practice, the following security case structure based on TS 50701 for an ETCS product has proven to be effective:

1. the high-level representation of the ETCS components with reference to the existing architecture and interface documents
2. evidence of the security management process implementation, see section 2.1
3. reference to the security risk analysis, see section 2.2
4. reference to the security requirement specification, see section 2.3
5. reference to the security test reports and the ETCS product verification and validation report
6. evidence of security requirements as a tabular overview with reference to tracking documents; a discussion of possible deviations and compensatory measures
7. security case documents from suppliers and subsystems
8. the list of security relevant application conditions (SECRACS)
9. the list of all the known residual risks for the ETCS product
10. the final summary and conclusion ("security claim") for the ETCS product.

The ETCS Product Security Case will be submitted to and accepted by the system integrator. The system integrator is responsible for creating a system security case that references the ETCS product security case.

2.7 Secure operating procedures

Security activities do not end with the security case, as the threat landscape is in constant flow and novel vulnerabilities may emerge. Vulnerability management includes identifying, assessing and rectifying any vulnerabilities. In addition, the ETCS product team must establish a process for the operator to report any security incidents. From experience, this can generally be built on the safety incident management process. The frequency of software updates is significantly higher for security than for safety. This circumstance, the associated problems and the proposed solutions have already been discussed generically in DER EISENBAHNINGENIEUR 4/2022 [12].
The management of the keys required for authentication between the EVC (European Vital Computer) and RBC (Radio Block Center) is an essential factor for ETCS products. A secure process must be defined for the complete lifecycle of the keys for this purpose.
In addition to the definition of the processes, another essential topic in secure operations involves the definition of the responsible roles by means of, for example, a RASCI matrix, so that immediate action can be taken in the event of any security incidents.
It has become evident that secure operations are rarely established in the existing contracts between ETCS product manufacturers, integrators and operators. Particularly during retrofits,

den. Im Unterschied zu Safety ist bei der Security die Frequenz der Software-Updates deutlich höher. Dieser Umstand, die damit verbundene Problematik und Lösungsvorschläge wurden bereits in DER EISENBAHNINGENIEUR 4/2022 im Allgemeinen erörtert [12]. Für ETCS-Produkte ist das Management der zur Authentifikation zwischen EVC (European Vital Computer) und RBC (Radio Block Center) benötigten Schlüssel zudem ein wesentlicher Faktor. Hierfür muss ein sicherer Prozess für den vollständigen Lebenszyklus der Schlüssel definiert werden.

Ein weiteres wesentliches Thema für den sicheren Betrieb ist neben der Definition der Prozesse die Festlegung der verantwortlichen Rollen durch beispielsweise eine RASCI-Matrix, damit bei Security-Vorfällen umgehend gehandelt werden kann.

In der Praxis hat sich gezeigt, dass der sichere Betrieb bisher selten in den bestehenden Verträgen zwischen Herstellern, Integratoren und Betreibern von ETCS-Produkten verankert ist. Insbesondere bei Retrofits müssen die Security-Verantwortlichen bei den beteiligten Parteien ein Verständnis für die zusätzlich erforderlichen Maßnahmen schaffen und bei den Verhandlungen über neue Verträge beraten. Dass die definierten Maßnahmen durch die Betreiber Kritischer Infrastrukturen auch umgesetzt sind, wird künftig in Übereinstimmung mit dem IT-Sicherheitsgesetz durch Regulierungsbehörden regelmäßig auditiert und sollte demnach jetzt schon vorbereitet werden.

3 Zusammenfassung

Security-Verantwortliche in ETCS-Projekten sehen sich mit vielfältigen Restriktionen und Abhängigkeiten konfrontiert, insbesondere in den zahlreichen Retrofit-Projekten, in denen bereits existierende Fahrzeuge um ETCS-Funktionalität erweitert werden sollen. Neben einem umfassenden Verständnis für das betrachtete System und für die relevanten Security-Standards, sehen wir vier besonders wichtige Aspekte, die für ein erfolgreiches und zielgerichtetes Security Lifecycle Management entscheidend sind.

1. Kommunikation: Eine enge Abstimmung mit allen Nachbargewerken, Zulieferern von Komponenten und auch den Integratoren oder Betreibern, die zum Abschluss des Entwicklungsprojektes das Zielsystem und insbesondere dessen Anwendungsbedingungen übernehmen, ist essenziell. Nur durch abgestimmte, für alle beteiligten Parteien realisierbare Maßnahmen wird das angestrebte Security-Niveau auch im Betrieb erreicht.
2. Risikozentrierung: Die Risikoanalyse muss im Projekt als das zentrale Werkzeug, insbesondere bei Abweichungen von generischen Vorgaben, verstanden werden. Alle Entscheidungen im Projekt müssen risikobasiert erfolgen.
3. Lösungsorientierung: In der Implementierung von technischen Schutzmaßnahmen sind Abweichungen von den Standards in begründeten Fällen notwendig und sinnvoll. Entscheidend ist bei derartigen Abweichungen die vollständige und systematische Dokumentation aller Konsequenzen, insbesondere der Restrisiken.
4. Pragmatismus und Flexibilität: Erfolgreiches Security Lifecycle Management erfordert ein umfassendes Verständnis für die projektspezifischen Rahmenbedingungen technischer und ökonomischer Natur, auch bei den Partnern, Kunden und Zulieferern. Zielstellung sollte stets sein, mit den vorhandenen Ressourcen das höchste realistisch erreichbare Security-Niveau für das Zielsystem zu verwirklichen, u. a. auch durch Ausgleichsmaßnahmen und Anwendungsbedingungen. ■

those responsible for security must create an understanding of the additional required measures among all the involved parties and advise them during the negotiation of the new support contracts. In the future, the implementation of defined measures by critical infrastructure operators will be regularly audited by regulatory authorities in accordance with the IT Security Act and should therefore be prepared accordingly.

3 Summary

Security managers and the personnel responsible for security in ETCS projects are facing a wide range of restrictions and dependencies, especially in the numerous retrofit projects where existing vehicles have to be expanded to include ETCS functionality. In addition to a comprehensive understanding of the system under consideration and the relevant security standards, we see four crucial aspects for successful and goal-oriented security lifecycle management.

1. Communication: Close coordination with all the related disciplines, component suppliers and the integrators or operators who take over the target system and in particular its application conditions at the end of the development project is essential. The targeted security level in operations can only be achieved through coordinated measures that are feasible for all the involved parties.
2. Risk orientation: Risk analysis must be understood as the central tool in the project, especially in the case of any deviations from the generic specifications. All the decisions in the project must be risk-based.
3. Solution orientation: Deviations from the standards for the implementation of technical countermeasures in justified cases are necessary and appropriate. The decisive factor in such deviations involves the complete and systematic documentation of all the consequences especially including the residual risks.
4. Pragmatism and flexibility: Successful security lifecycle management requires a comprehensive understanding of the project-specific technical and economic framework conditions, including those of the partners, customers and suppliers. The objective should always be to achieve the highest realistically attainable security level for the target system with the available resources, including by means of compensatory measures and application conditions. ■

LITERATUR | LITERATURE

[1] IT-Sicherheitsgesetz, § 8a: „Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten […] angemessene organisatorische und technische Vorkehrungen […] zu treffen. Dabei soll der Stand der Technik eingehalten werden."

[2] Jaeggi, D.; Cavalcanti, R. S.; Cowan, A.: Fahrzeug-Cybersecurity – Erfahrungen bei der Implementierung in Bestandsfahrzeugen, SIGNAL+DRAHT, 4/2022

[3] IEC 62443, "Industrial communication networks – Network and system security", Series of 13 Standards on Industrial Automation and Control System Security

[4] CENELEC CLC/TS 50701:2021 "Railway applications – Cybersecurity"

[5] Röhrig, R.: Zunehmende Bedeutung von Security für Bahnanwendungen – der neue Standard TS 507", SIGNAL+DRAHT, 4/2022

[6] ERA * UNISIG * EEIG ERTMS USERS GROUP, "System Requirements Specification Chapter 7 ERTMS/ETCS language SUBSET-026-7, 3.6.0", https://www.era.europa.eu/sites/default/files/filesystem/ertms/ccs_tsi_annex_a_-_mandatory_specifications/set_of_specifications_3_etcs_b3_r2_gsm-r_b1/index004_-_subset-026_v360.zip, 03.05.2022 um 17:23

[7] EN 50126-1:2018-10, "Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS-Prozess"

[8] ISO/IEC 27001:2013, "Information technology – Security techniques – Information security management systems – Requirements", October 2013

[9] DIN EN IEC 62443-3-2:2021-12, "IT-Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung"

[10] Birr, P.: Vorgehensmodell zur IT-Sicherheitsanalyse für Bahnanwendungen, SIGNAL+DRAHT, 4/2017

[11] European Railway Agency, "Set of specifications 3 (ETCS B3 R2 GSM-R B1)", https://www.era.europa.eu/content/set-specifications-3-etcs-b3-r2-gsm-r-b1, 03.05.2022 um 17:16

[12] Katzenberger, S.; Wunderskirchner, M.: TS 50701 – Cybersicherheit aus Sicht der Begutachtung, SIGNAL+DRAHT, 4/2022

[13] EN 50129:2019, "Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling", 06-2019

[14] Okstad, E. H.; Bains, R.; Myklebust, T.; Jaatun, M. G.: Implications of Cyber Security to Safety Approval in Railway, 2021

AUTOREN | AUTHORS

M.Sc. Patric Birr, CISSP
Head of Business Center Security
ICS GmbH
Anschrift / *Address*: Wallstraße 27, D-10179 Berlin
E-Mail: patric.birr@ics-gmbh.de

M.Sc. Stefan Karg, CISSP
Lead Security Consultant
ICS GmbH
Anschrift / *Address*: Sonnenbergstraße 13, D-70184 Stuttgart
E-Mail: stefan.karg@ics-gmbh.de

M.Sc. Christoph Ritschel, COSP
Senior Security Consultant
ICS GmbH
Anschrift / *Address*: Wallstraße 27, D-10179 Berlin
E-Mail: christoph.ritschel@ics-gmbh.de