Sichere Softwareentwicklungspraktiken für Eisenbahnanwendungen gemäß IEC 62443

Secure software development practices for the compliance of railway applications with IEC 62443

Anssi Lampinen | Matti Laine | Viet Nguyen

Sicherheit in der Produktentwicklung kann nicht isoliert betrachtet werden – sie erfordert einen klar definierten Rahmen, bei dem alle Beteiligten effektiv zusammenarbeiten. Die Normenreihe IEC 62443 bietet einen strukturierten Ansatz, indem sie den Eigentümern von Anlagen, Integratoren und Produktentwicklern in betrieblichen Technologieumgebungen Rollen und Verantwortlichkeiten zuweist. Dieser Beitrag untersucht die wichtigsten Aspekte der Einbindung von Beteiligten, des Risikomanagements, der sicheren Programmierung sowie der DevSecOps-Praktiken (Development Security and Operation) und zeigt auf, wie die Einhaltung der IEC 62443 die Cybersicherheit, insbesondere in Eisenbahnsystemen, verbessert.

1 Die Rollen der Beteiligten im Rahmen der Produktentwicklung

Im Gegensatz zu Sicherheitsstandards, die von Unternehmen selbst definiert werden, ist die IEC 62443 eine etablierte Reihe von Normen, die darauf abzielen, Probleme des Sicherheitsmanagements in betrieblichen Umgebungen mit Technologien verschiedener Anbieter zu lösen. Sie definieren die Rollen und Verantwortlichkeiten des Betreibers des automatisierungstechnischen Steuerungssystems (engl. industrial automation and control system, IACS), des Integrators und des Entwicklers des verwendeten Produkts. In diesen Umgebungen verfügen Geräte und Software selten über die Hardware- oder Softwarefunktionen, die für aktuelle IT-Sicherheitsmaßnahmen erforderlich sind. Dennoch werden sie in Umgebungen eingesetzt, die zwar modernen IKT-Umgebungen ähneln, aber zusätzliche Sicherheitsmaßnahmen außerhalb der klassischen Industrieumgebungen erfordern. Nicht immer ist die Technologie die treibende Kraft. Geschäftsfälle von der Integration bis zur zentralen Verwaltung von Betriebs- und Hilfssystemen, Datenübertragungen, Aktualisierungen und Wartung können ebenfalls Auslöser sein. Normen ermöglichen es allen Beteiligten, ein Projekt mit einem gemeinsamen Rahmen und einem gemeinsamen Vokabular anzugehen, erfordern aber auch, dass sich alle Beteiligten daran halten, um eine erfolgreiche Umsetzung zu gewährleisten.

Zunächst möchte der Betreiber ein IACS einsetzen, das in sein Sicherheitsmanagementsystem (gemäß IEC 62443-2-1) integriert werden kann. Der Betreiber ist für die Sicherheit des Systems verantwortlich und definiert die Umgebung, die Sicherheits- und Geschäftsziele und -anforderungen sowie die im Projekt anzuwendenden Sicherheitsprozesse.

Der Betreiber verlangt vom Integrator, dass dieser das System gemäß seinen Vorgaben einsetzt, seine Sicherheitsanforderungen erfüllt und die erforderlichen Sicherheitsmaßnahmen umsetzt. Für den Integrator legt IEC 62443-2-4 die Anforderungen für die Bereitstellung von Sicherheitsmaßnahmen und die Integration des Systems in das Sicherheitsmanagement des IACS-Betreibers fest. IEC 62443-3-2 definiert den si-

Security in product development cannot be considered in isolation: it requires a well-defined framework where all the stakeholders collaborate effectively. The IEC 62443 series of standards provides a structured approach by assigning roles and responsibilities to the asset owners, integrators and product developers in technological operating environments. This article explores the key aspects of stakeholder involvement, risk management, secure coding and DevSecOps (Development Security and Operation) practices, thereby demonstrating how compliance with IEC 62443 strengthens cybersecurity, particularly in railway systems.

1 The stakeholders' roles in the framework

Unlike corporate security standards, IEC 62443 is a well-established series of standards aimed at solving the security management issues presented in multivendor technological operating environments. It defines the roles and responsibilities of the industrial automation control system's (referred to as IACS) owner, the integrator and the developer of the product being deployed. Devices and software in these environments rarely have the hardware or software capabilities that up-to-date security controls require. Yet, they are deployed in environments that resemble modern ICT environments and require additional security measures outside traditional industrial environments. The technology is not always the driving force; business cases ranging from integration to the centralised management of operations and auxiliary systems, data transfers, updates and maintenance warrant this. The standard allows all the stakeholders to engage in the project under the same framework and vocabulary, but it also requires all the parties to adhere to it for the deployment to succeed.

The asset owner is initially interested in deploying an IACS that is operable within its security management system (as defined in IEC 62443-2-1). The owner is accountable for the security of the entire system and defines the environment, security and business goals and the requirements, as well as the security processes applied in project.

The owner requires the integrator to ensure that the deployed system adheres to its policies, meets its security requirements and implements all the necessary controls. For the integrator, IEC 62443-2-4 sets out the required security measures and the integration of the system into the IACS owner's security management. IEC 62443-3-2 defines the secure design process, while IEC 62443-3-3 defines the kind of controls that the deployed system needs to demonstrate.

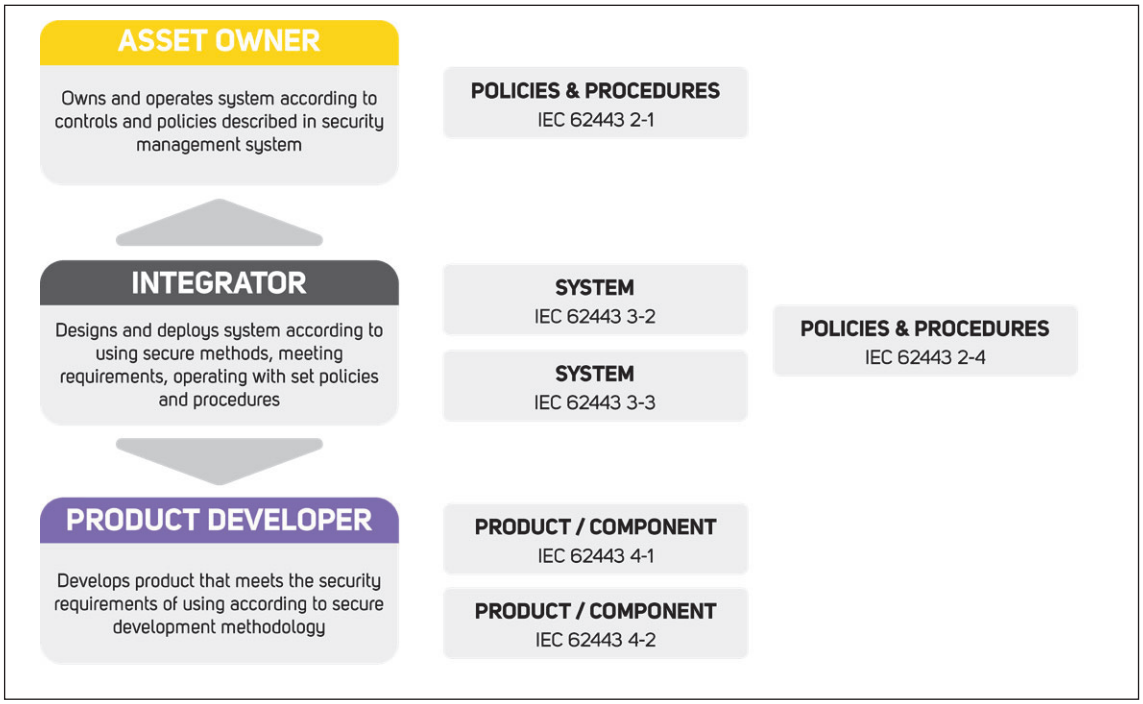

Bild 1: Rollen der Beteiligten und anwendbare Normen, auf die sich der Beitrag bezieht.
Fig. 1: The roles of the stakeholders and the applicable standards covered in the article.

cheren Entwicklungsprozess, und IEC 62443-3-3 definiert die Art der Sicherheitsmaßnahmen, die das betreffende System aufweisen muss.
Der Integrator muss in der Lage sein, die Sicherheit des Systems während seines gesamten Lebenszyklus zu gewährleisten. Dies ist eine große Herausforderung, wenn das Produkt nicht über die erforderlichen Sicherheitsfunktionen verfügt, keine Updates für neue Sicherheitsbedrohungen oder Sicherheitslücken während seines Lebenszyklus bereitstellt oder so entwickelt wurde, dass immer wieder neue Bedrohungen in das System gelangen. Dies wird durch zwei Normenteile abgedeckt: IEC 62443-4-1 und -4-2. Ersterer definiert den sicheren Entwicklungsprozess, Letzterer die Anforderungen an die Produktsicherheit.
In einem solchen Umfeld versteht der Betreiber die Umgebung, in der er arbeitet, und die Bedeutung des Systems für seinen Betrieb am besten. Er ist die primäre Autorität bei der Definition des Bedrohungsumfelds, der Sicherheitsziele, der Umgebung, der Managementprinzipien und der Kontinuitätsanforderungen an das System. Der Integrator wiederum verfügt über das beste technische Verständnis des Systems und der Produktentwickler über das beste Verständnis der Technologie. Diese beiden Parteien spielen eine entscheidende Rolle bei der Planung, dem Bedrohungsmanagement, der Risikobewertung, der Festlegung geeigneter Maßnahmen zur Risikominderung und der Umsetzung von Sicherheitsmaßnahmen. Der Prozess und die Kriterien werden jedoch vom Betreiber festgelegt, um sicherzustellen, dass die Ergebnisse in sein Sicherheitsmanagementsystem passen.

2 Bedrohungs- und Risikomanagement

Das Bedrohungs- und Risikomanagement ist ein wiederkehrender Prozess für alle Beteiligten – ein integraler Bestandteil sowohl des Systemdesigns als auch des Produktentwicklungsprozesses. Auch wenn die Produktentwicklung wahrscheinlich nicht in direkter Zusammenarbeit mit den Betreibern erfolgt, muss das Produkt dennoch für den vorgesehenen Verwendungszweck geeignet sein.
Die Norm IEC 62443-3-2 stellt eine Methodik zur Risikobewertung für den Systementwurf zur Verfügung, die auch das Bedrohungsmanagement umfasst. Das Bedrohungs- und Risikomanagement im Zusammenhang mit der Produktentwicklung wird im Folgenden näher be-

The integrator needs to prove its ability to maintain the system's security throughout its lifecycle. This is a major challenge if the product does not feature the required security features, fails to provide updates for any new security threats or vulnerabilities throughout the lifecycle or has been developed in a manner that continually introduces new threats to the system. This is covered by two standards: IEC 62443-4-1 and IEC 62443-4-2, the first of which defines the secure development process, while the latter defines the product security requirements.
In this kind of environment, the asset owner best understands the environment it is working in and the importance of the system to its operations. It is the primary authority in defining the threat environment, the security goals, the environment, the management principles and the continuity requirements for the system. On the other hand, the integrator has the best technical understanding of the system, while the product developer best understands the technology. These parties play an essential role in the design, threat management, risk assessment, designating the correct mitigating actions and implementing the controls. However, the process and criteria come from the asset owner in order to ensure that the results fit into their security management system.

2 Threat and risk management

Threat and risk management is a recurring process for all the stakeholders: an integral part of both the system design and the product development processes. Even though product development is not likely to work directly together with the asset owners, the product still needs to fit the intended use.
IEC 62443-3-2 includes a risk assessment methodology for system design, including threat management. The following includes a closer look at threat and risk management due to it being applied in product development, but skips the rest of the design process. In order to succeed in risk management, the asset owner or product owner must also fulfil some prerequisites that have not been defined in the standard:

trachtet, der Rest des Systementwurfs wird allerdings hier übersprungen. Für ein erfolgreiches Risikomanagement muss der Betreiber oder Produktverantwortliche einige Voraussetzungen erfüllen, die in der Norm nicht definiert sind:

- Definition der Bedrohungslandschaft. Die Bedrohungslandschaft ist eine ganzheitliche Bewertung des Zustands der Cybersicherheit auf globaler Ebene – dieses Makroumfeld umfasst aktuelle Trends, das Aufkommen neuer Technologien und wird von Politik, verfügbarer Technologie, gesellschaftlichen und gesetzlichen Vorgaben beeinflusst.
- Definition der Sicherheitsziele und -vorgaben für das System – wie das System gegen die Bedrohungslandschaft geschützt werden soll, um die Unternehmensziele zu erreichen. Ziele und Vorgaben können strategische Aussagen und die Umsetzung von Sicherheitsrichtlinien und -standards beinhalten.
- Definition der Bedrohungsumgebung – die konkreten Bedrohungen und Herausforderungen, denen das System in der Bedrohungslandschaft ausgesetzt ist. Häufig handelt es sich dabei um Bedrohungsszenarien, die in der Risikoanalyse auf das System angewendet werden können. Vorhandene Sicherheitsmaßnahmen, das Bewusstsein der Nutzer und Einschränkungen der Betriebsumgebung wirken sich auf die Fähigkeit aus, Bedrohungen abzuwehren.
- Festlegung einer Methodik zur Risikobewertung, um sicherzustellen, dass die Ergebnisse der Risikobewertung dem Risikomanagement des Unternehmens gerecht werden.
- Festlegung von Kriterien und Leitlinien für die Risikoakzeptanz.

Es ist eher unwahrscheinlich, dass der in der Norm beschriebene Prozess zur Bewertung von Sicherheitsrisiken von Unternehmen für die Risikobewertung verwendet wird. Daher wird dringend empfohlen, bestehende Prozesse zu verwenden, mit denen beide Parteien vertraut sind. Die gewählte Methode muss jedoch ausreichend detailliert sein und einige wichtige Einschränkungen berücksichtigen, die sich auf den Systementwurf auswirken. Der Grund dafür ist der Wunsch nach einer konsistenten und aussagekräftigen Risikoanalyse, die mit einem neuen Ansatz unter Umständen nicht möglich ist. Daher wird in diesem Beitrag nicht der Prozess selbst behandelt, sondern es wird erläutert, was der aktuelle Prozess beinhalten sollte und welche Ergebnisse erzielt werden sollten, um diesen bestehenden Prozess zu ändern.

- Identifizieren der Schutzobjekte – also das, was vor Bedrohungen geschützt werden soll. Ein System besteht aus Komponenten, wird von Menschen und Prozessen genutzt und an physischen und logischen Standorten gehostet. Es sind Prioritäten für die Schutzobjekte festzulegen und Verantwortliche für diese Schutzobjekte zu definieren, dies ist für das Risikomanagement erforderlich. Die Gruppierung von Schutzobjekten in logische Gruppen ist sinnvoll, da ähnliche Schutzobjekte mit ähnlichen Sicherheitsanforderungen und ähnlicher Nutzung auch ähnlichen Bedrohungen ausgesetzt sind.
- Identifizieren relevanter Bedrohungen – gängige Instrumente hierfür sind die Definition der Bedrohungsumgebung, historische Daten, Bedrohungsdatenbanken und spezialisierte Analysen. Anschließend erfolgt die Auswahl der für die betreffende Umgebung und Implementierung relevanten Bedrohungen.
- Bewerten der Wahrscheinlichkeit und der Auswirkungen der Bedrohung auf das Schutzobjekt, daraus ergibt sich das Risiko. Bis zu diesem Punkt wird nach Heuristiken gearbeitet, nach Prozessen, und es kann guter Fortschritt erzielt werden, wenn der betreffende Prozess einfach mit Informationen gefüttert wird. Die Wahl der Sicherheitsmaßnahmen und die Akzeptanz des Risikos sind mit einem hohen Maß an Abwägung und Unsicherheit verbunden.

Die unbefriedigende Wahrheit ist, dass der Betreiber, Integrator oder Produktlieferant mit begrenzten Ressourcen arbeitet – es gibt Budgets, Fristen und wenige Spezialisten, alle mit begrenzter Zeit. Der Fokus der

- The definition of the threat landscape: the threat landscape constitutes a holistic assessment of the state of the cybersecurity in global sense. This macro-scale environment includes current trends and the emergence of new technologies and is influenced by politics, available technology and societal constraints.
- The definition of the system's security goals and objectives: how the system will be protected against the threat landscape in order to fulfil its business objectives. The goals and objectives may include strategic statements, security regulations and the standards being implemented.
- The definition of the threat environment: the concrete threats and challenges the system faces from the landscape. This often takes the form of threat scenarios that can be applied to the system in the risk analysis. The existing controls, user awareness and operating environment constraints impact the ability to mitigate threats.
- The definition of the risk assessment methodology, so as to ensure that the results of the risk assessment are consistent with the corporate risk management.
- The definition of the risk acceptance criteria and policy.

The security risk assessment process described in the standard is highly unlikely to be applied for risk assessment by the undertakings and it is therefore strongly recommended that existing processes that are familiar to both parties are used. Still, the chosen method needs to be detailed enough and must take a few important constraints that impact the system design into account. The justification here is that consistent and meaningful risk analysis is necessary, i.e. something that a novel approach may not provide. Therefore, this article does not cover the process itself, but does cover what the process should contain and what outputs there should be in order to modify the existing process.

- Identify the assets – i.e. what needs to be protected from threats. The system consists of components, is used by people and processes and is hosted on physical and logical sites. Prioritising the assets and defining the asset owners is required in risk management. Grouping assets into logical groups helps, as similar assets that have similar security requirements and are operated similarly face similar threats.
- Identify the relevant threats – threat environment definition, history data, threat databases and specialist analysis are common tools. The relevant ones must be chosen for the environment and implementation and the relevant threats that apply to them.
- Assess the likelihood and impact the threat has on the asset, which dictates the risk. Up until this point, this has involved heuristics and processes and good progress can be made if the given process is fed with information. The choice of mitigating controls and risk acceptance involves a large degree of compromise and uncertainty.

The unsatisfactory truth lies in the fact that the asset owner, integrator or product supplier work with limited resources, such as budgets, timetables, a lack of available specialists and even time constraints. It is necessary to be able to focus the efforts and resources on those things that have the largest impact and to sometimes choose controls that are not perfect, but are acceptable. When implementing new controls, it is necessary to consider whether the result is worth the effort.

- Assess whether the risk meets the acceptance criteria. If the threat poses an acceptable risk, it is possible to move on. If, however, the risk is not acceptable despite the built-in controls, countermeasures must be deployed to achieve risk tolerance.

Konzentration muss auf jenen Aufgaben und Ressourcen liegen, die die größte Wirkung haben, und manchmal müssen Kompromisse zugunsten Maßnahmen getroffen werden, die nicht perfekt, aber akzeptabel sind. Werden neue Sicherheitsmaßnahmen eingeführt, ist abzuwägen, ob das erzielbare Ergebnis den Aufwand wert ist.

- Prüfung, ob das Risiko die Akzeptanzkriterien erfüllt. Wenn es sich bei der Bedrohung um ein akzeptables Risiko handelt, kann fortgefahren werden. Wenn das Risiko jedoch trotz der eingebauten Sicherheitsmaßnahmen inakzeptabel ist, müssen weitere Gegenmaßnahmen ergriffen werden, bis die Risikotoleranz erreicht ist.

Es gibt verschiedene Methoden zur Auswahl wirksamer Sicherheitsmaßnahmen, die die Wahrscheinlichkeit oder die Auswirkungen durch technische Maßnahmen, Vermeidung, Begrenzung der Angriffsfläche, Begrenzung der Auswirkungen, Reduzierung der Auswirkungen oder sogar Aufteilung des Risikos verringern. Für die Risikobewertung und die Auswahl von Sicherheitsmaßnahmen zur Risikominderung sind Fachleute erforderlich, die sich mit der Umgebung und der Technologie auskennen und Teil der betreffenden Risikomanagementgruppe sind.

Wurde eine Maßnahme ausgewählt, ist das Risiko unter Berücksichtigung dieser Gegenmaßnahmen und Risikominderungsmaßnahmen erneut zu bewerten. Zusätzliche neue Sicherheitsmaßnahmen zur Verringerung des Risikos sind in Betracht zu ziehen, wenn das Risiko nach wie vor nicht akzeptabel ist. Die risikomindernden Maßnahmen sind als Anforderungen für den Entwurfsprozess zu protokollieren, um deren Umsetzung (und Überprüfung im Sicherheitsfall) zu gewährleisten.

- Dokumentieren der Ergebnisse. Die Ergebnisse der Risikobewertung müssen bekannt gemacht werden. Genehmigungen und Freigaben für die Risikoakzeptanz oder die Budgetierung der Maßnahmen sind einzuholen und nachfolgend als Anforderungen an die Implementierungsteams weiterzugeben. Manchmal erfordert Risikominderung auch Einschränkungen und Bedingungen für die Umsetzungsmaßnahmen.

Ein ähnliches Verfahren wird zur Analyse und Implementierung von Sicherheitsmerkmalen in der Produktsicherheit angewandt. Es gibt keine umgebungsspezifischen Beschränkungen und Eigenheiten, es müssen aber stattdessen Einschränkungen und Beschränkungen bei der Verwendung des Produkts in Kauf genommen und kommuniziert werden. Selbst wenn die Anforderungen der Normen erfüllt sind, kann die Produktsicherheit durch eine einzige improvisierte Funktion in der Umgebung oder durch eine nicht normgerechte Implementierung einer Schnittstelle gefährdet werden.

3 Sichere Programmierpraktiken

Bevor auf den Code Bezug genommen wird, noch einige Anmerkungen zum Systementwurf. Mit einem gut durchdachten System können Sicherheitsprobleme vermieden, Zeit und Geld gespart und Sicherheitsverstöße verhindert werden. Probleme, die in der Entwurfsphase auftreten, lassen sich später in der Umsetzung nur schwer oder gar nicht mehr beheben. Werden jedoch die Secure-by-Design-Prinzipien beachtet, ist die erste Grundlage für eine sichere Anwendung geschaffen.

Secure-by-Design-Prinzipien:

- Prinzip der geringsten Privilegien: Systeme sollten Benutzern und Komponenten nur jene Berechtigungen gewähren, die für deren Betrieb erforderlich sind.
- Gesicherter Ausfall (Fail Securely): Bei einem Ausfall muss das System in einen definierten, sicheren Zustand übergehen, keine (sensiblen) Informationen preisgeben und keine unbefugten Aktionen zulassen.
- Konzept der gestaffelten Verteidigung (Defence in Depth): Die Verwendung mehrerer Verteidigungsebenen (Authentifizierung, Verschlüsselung, Überwachung, Zonen), um die Wahrscheinlichkeit ei-

There are various methodologies for choosing effective controls that reduce the likelihood or impact by means of technical controls, avoidance, limiting the attack surface, limiting the impact, shortening the impact or even sharing the risk. Risk assessment and the choice of mitigation controls is the reason for employing specialists who understand the environment and technology as part of the risk management group.

After deciding on a control, the risk when using said countermeasures and mitigating controls must be reassessed. It is necessary to consider implementing new mitigating controls, if the risk remains unacceptable. These mitigating controls must the be logged as requirements for the design process in order to ensure their implementation (and verification in the security case).

- Document the results. It is necessary to communicate the results of the risk assessment. The approval and release of the risk acceptance or the budgeting of the measures must be acquired and then issued as requirements for the implementing teams. Sometimes, mitigation requires implementation restrictions and conditions.

A similar process is used to analyse and implement the security features in product security. There are no environment specific restrictions and quirks, but it is necessary to communicate the constraints and restrictions when using the product instead. Even if the standard's requirements are met, product security might be endangered by that one jury-rigged feature in the environment or non-standard implementation of an interface.

3 Secure coding practices

Before talking about the code, here are a few points about system design. A well-designed system can prevent any security issues moving forward, thereby saving time and money and preventing security breaches. Problems in the design can be difficult or impossible to fix later in the implementation. An adherence to secure design principles lays the groundwork for secure application.

Secure design principles:

- The Principle of Least Privilege: systems should only grant users and components the minimum permission they need to function.
- Fail Securely: in the event of a failure, the system should default to a secure state, thereby not exposing any sensitive information or allowing any unauthorised actions.
- Defence in Depth: the use of multiple defence layers (authentication, encryption, monitoring and zones) reduces the likelihood of a successful attack.
- Separation of Duties: the different roles within the system should be clearly defined and any actions that could cause significant harm should not be concentrated within a single person or module.
- Secure by Default: secure configuration should be the default, thereby minimising any risks from misconfigurations or user error.

When designing a system that complies with IEC 62443, as well as with the specific threats detected during the threat modelling, the system must also meet the cybersecurity technical requirements required by the standard. The standard defines four security levels, each with increasing requirements on top of the previous ones. The required level needs a separate assessment and the system can be divided into multiple zones, with each zone having a different target security level. As an example, we can pick level three for high cybersecurity: it aims to prevent an enti-

nes erfolgreichen Angriffs zu verringern, wird in dieser Strategie umgesetzt.
- Aufgabentrennung (Separation of Duties): Die verschiedenen Rollen innerhalb des Systems müssen klar definiert sein, und Handlungen, die zu erheblichen Schäden führen können, sollten nicht auf eine Person oder ein Modul konzentriert werden.
- Standardmäßig sicher (Secure by Default): Eine sichere Konfiguration sollte die Standardeinstellung sein, um Risiken durch Fehlkonfigurationen oder Benutzerfehler zu minimieren.

Bei der Entwicklung eines Systems, das der IEC 62443 entspricht, muss das System neben den spezifischen Bedrohungen, die bei der Bedrohungsmodellierung erkannt werden, auch die technischen Anforderungen der Norm bezüglich Cybersicherheit erfüllen. Die Norm definiert vier Security-Levels, wobei jedes Level strengere Anforderungen stellt als die vorhergehenden. Jedes erforderliche Level muss gesondert bewertet werden, und das System kann in mehrere Zonen unterteilt werden, wobei für jede Zone ein eigenes Security-Level festgelegt wird. Beispielsweise kann für eine hohe Cybersicherheit Level drei gewählt werden, das darauf abzielt, eine Entität daran zu hindern, aktiv nach Möglichkeiten zu suchen, das System zu kompromittieren, indem diese hochentwickelte Mittel mit mäßigen Ressourcen, bahnspezifischen Fähigkeiten und moderater Motivation einsetzt. Ein Beispiel für einen moderaten Akteur könnte ein Sicherheitsexperte sein, der Penetrationstests durchführt, über die entsprechenden Werkzeuge und Kenntnisse verfügt und bereit ist, etwas Zeit und Geld für den Erfolg zu investieren. Ein weiteres Problem, das nichts mit Sicherheitsstandards zu tun hat, sind Fehler im Entwurf, die ausgenutzt werden können. Wenn wir beispielsweise die Reservierung von Sitzplätzen in einem Zug für eine Gruppe ohne Anzahlung zulassen, könnte ein böswilliger Akteur alle Sitzplätze in einem Zug oder in mehreren Zügen reservieren. Dies könnte zu Gewinnverlusten und Reputationsschäden führen. Wenn es sich zudem um eine Kernfunktion handelt, bei der alle Ticketverkäufe die Gruppenbuchung nutzen, um den Sitzplatz bis zur Zahlung zu reservieren, kann die Lösung dieses Problems sehr zeit- und kostenaufwendig sein.

3.1 Umsetzung der Lösung

Selbst der beste Entwurf kann durch Fehler bei der Umsetzung zunichte gemacht werden. Daher ist bei der Umsetzung der Lösung Vorsicht geboten. Effektiv ist dies nur, wenn Programmierer über Kenntnisse und Ausbildung im Bereich der Cybersicherheit verfügen. Jemand anderes führt dann eine Sicherheitsprüfung des Codes (Secure-Code-Review) durch. Abschließend scannen Tools das Ergebnis. Wie beim Entwurf, wird auch hier die Grundlage durch die Einhaltung der Grundsätze der sicheren Programmierung geschaffen.

Sichere Programmierpraktiken:
- Validierung und Filterung von Benutzereingaben: Es ist sicherzustellen, dass alle eingegebenen Daten anhand der erwarteten Formate validiert werden, um Angriffe wie SQL-Injection zu verhindern. Benutzereingaben sind zu bereinigen, um potenziell schädliche Zeichen und Skripte zu entfernen.
- Verwendung von Richtlinien für die sichere Programmierung: Es ist die Verwendung von Richtlinien wie OWASP (Open Worldwide Application Security Project) einzuführen, um häufige Sicherheitslücken zu vermeiden.
- Sichere Bibliotheken und Frameworks: Es sind geprüfte Bibliotheken zu verwenden, um Sicherheitslücken zu minimieren, und es ist sicherzustellen, dass diese mit Sicherheitspatches auf dem neuesten Stand gehalten werden.
- Regelmäßige Code-Reviews und statische Analysen: Es sind Peer-Code-Reviews durchzuführen und statische Analyse-Tools in die

ty from actively searching for ways of compromising the system by using sophisticated means with moderate resources, railway system specific skills and moderate motivation. An example of a moderate actor could involve a security expert doing penetration testing, who has tools and knowledge and is willing to use some time and money to succeed.

Another issue not related to security standards involves is design mistakes that can be exploited. For example, if seats can be booked on a train for a group without a deposit, this could allow malicious actors to reserve all the seats in a train or in multiple trains. This could lead to profit losses and reputational harm. In addition, if this is a core feature, all ticket sales will use the group booking to reserve a seat until the payment is completed, which can be very time and money consuming to remedy.

3.1 Implementing the solution

Even the best design can be foiled by faults in the implementation. Therefore, care needs to be taken when implementing the solution. An effective method involves having a programmer who is knowledgeable and trained in cybersecurity. Another person then does a secure code review of the code and tools are used to scan the final result. As in the case of design, adherence to the following secure coding principles lays the groundwork.

Secure coding principles:
- Input Validation and Sanitisation: ensure that all the data inputs have been validated against the expected formats in order to prevent any attacks such as SQL injection. Cleanse the inputs in order to remove any potentially malicious characters and scripts.
- Using Secure Coding Guidelines: implement the use of guidelines such as OWASP (Open Worldwide Application Security Project) to avoid any common vulnerabilities.
- Secure Libraries and Frameworks: utilise vetted libraries in order to minimise any vulnerabilities, while ensuring that they are up to date with security patches.
- Regular Code Reviews and Static Analysis: conduct peer code reviews and integrate static analysis tools into the CI/CD pipelines in order to detect any issues early. These tools help automate the detection of vulnerabilities.

A code review is a widespread practice used to improve code quality. A secure code review widens the focus to include security concerns. Together with static analysis, this is one of the most effective ways of identifying security bugs early in the system development lifecycle. The earlier vulnerabilities are detected, the faster and cheaper they are to fix.

OWASP is best-known for the OWASP Top Ten. This is a list of the most critical web application security risks. While it involves web application security risks, many of them also apply to embedded systems and railway control systems. This is good knowledge for both the programmer and the code reviewer. In addition, OWASP provides a code review guide that gives guidelines for a secure code review and contains technical references with examples of vulnerabilities. IEC 62443 also mentions OWASP as an example of a well-known guideline to use.

4 Enhancing railway cybersecurity through DevSecOps and IEC 62443 compliance

With over 45 years of experience in the railway industry, Mipro has invested substantial resources in software product development. By leveraging its modern and innovative DevSecOps pipeline, Mipro has effectively overcome the limitations of the

CI / CD-Pipelines zu integrieren, um Probleme frühzeitig zu erkennen. Diese Tools helfen, die Erkennung von Sicherheitslücken zu automatisieren.

Code-Reviews sind eine weit verbreitete Praxis zur Verbesserung der Code-Qualität. Secure-Code-Reviews erweitern den Fokus auf Sicherheitsaspekte. Zusammen mit der statischen Analyse stellen sie eine der effektivsten Methoden dar, um Sicherheitslücken in einem frühen Stadium des Systementwicklungszyklus aufzudecken. Je früher Sicherheitslücken entdeckt werden, desto schneller und kostengünstiger lassen sie sich beheben.

OWASP ist vor allem für die OWASP Top Ten bekannt. Dabei handelt es sich um eine Liste der kritischsten Sicherheitsrisiken in Web-Anwendungen. Obwohl der Schwerpunkt auf Web-Anwendungen liegt, gelten viele dieser Risiken auch für eingebettete Systeme und Eisenbahnsteuerungssysteme. Dies ist eine sowohl für Programmierer als auch für Code-Reviewer wertvolle Erkenntnis. Darüber hinaus stellt OWASP einen Leitfaden für das Code-Review zur Verfügung, der Richtlinien für Secure-Code-Reviews und technische Referenzen mit Beispielen für Sicherheitslücken enthält. Auch in der IEC 62443 wird OWASP als Beispiel für bekannte Richtlinien genannt, die zu verwenden sind.

4 Verbesserung der Cybersicherheit im Bahnwesen durch DevSecOps und Einhaltung der IEC 62443 bei Mipro

Mit mehr als 45 Jahren Erfahrung im Eisenbahnsektor hat Mipro Oy (Mipro) beträchtliche Ressourcen in die Entwicklung von Softwareprodukten investiert. Durch den Einsatz einer modernen und innovativen DevSecOps-Pipeline konnte Mipro die Beschränkungen des „magischen Dreiecks" effektiv überwinden. Durch die frühzeitige Integration von Sicherheitsaspekten in den Entwicklungszyklus und die Einhaltung der IEC 62443-Normengruppe verbessert Mipro die Ausfallsicherheit von Systemen, optimiert die Ressourcenzuweisung und gewährleistet die Einhaltung gesetzlicher Vorschriften.

Die IEC 62443 bietet einen strukturierten Rahmen für die Sicherung industrieller Automatisierungssysteme. Das Unternehmen setzt eine Kombination aus automatisierten Sicherheitstests, Risikobewertung und kontinuierlicher Überwachung ein, um die Anforderungen der Norm systematisch zu erfüllen. Die Integration von Tools wie Jenkins und GitLab erleichtert automatisierte CI / CD-Pipelines, in denen Sicherheitstests in jeder Phase der Softwareentwicklung und -bereitstellung integriert sind. Jira spielt eine entscheidende Rolle, wenn es darum geht, den Überblick über Sicherheitslücken zu behalten und sicherzustellen, dass Sicherheitsprobleme strukturiert und zeitnah angegangen werden.

Eine zentrale Anforderung der IEC 62443-3-3 und IEC 62443-4-2 ist die Sicherstellung der Software-Sicherheitsvalidierung. Um dieser Anforderung gerecht zu werden, setzt das Unternehmen SonarQube zur statischen Codeanalyse ein, um sichere Programmierpraktiken durchzusetzen und Schwachstellen frühzeitig zu erkennen. OWASP Dependency-Check wird zur Analyse von Bibliotheken von Drittanbietern verwendet, um die Einhaltung von Sicherheitsrichtlinien zu gewährleisten und das Risiko von Angriffen in der Lieferkette zu verringern. In containerisierten Umgebungen wird Trivy eingesetzt, um nach bekannten Sicherheitslücken zu suchen und die Integrität der eingesetzten Softwarekomponenten sicherzustellen.

Neben sicheren Programmierpraktiken sind die Erkennung von Bedrohungen und die Risikobewertung wesentliche Bestandteile der Sicherheitsstrategie von Mipro, die sich an der IEC 62443-3-2 orientiert. Nessus kommt zum Einsatz, um regelmäßige Schwachstellenanalysen durchzuführen, die Sicherheit des Systems zu bewerten und Fehlkonfigurationen zu erkennen, bevor sie zu einer ausnutzbaren Bedrohung werden. Das Robot Framework unterstützt dynamische Anwendungstests (Dynamic Application Security Testing, DAST), bei denen reale Angriffsszenarien simulieren, um Schwachstellen in laufenden Anwendungen zu identifizieren.

Mipro hat einen Defence-in-Depth-Ansatz implementiert, indem automatisierte Sicherheitsscans direkt in CI / CD-Workflows integriert wurden, um die kontinuierliche Einhaltung der IEC 62443-3-3 zu gewährleisten. Dieser Ansatz sorgt für mehrere Ebenen der Sicherheitsvalidierung und minimiert die Gefährdung durch potenzielle Angriffe. Durch die Implementierung automatisierter Überwachung und kontinuierlicher Sicherheitsbewertung stellt Mipro sicher, dass Eisenbahnsteuerungssysteme vor sich entwickelnden Cyberbedrohungen geschützt bleiben.

Das Unternehmen hat nicht nur seine Softwaresicherheit durch die Nutzung der DevSecOps-Tools in Übereinstimmung mit der IEC 62443 gestärkt, sondern auch seine Betriebseffizienz verbessert. Dieser proaktive Ansatz für Cybersicherheit fördert eine robuste Bedrohungserkennung, sichere Softwareentwicklung und widerstandsfähige Eisenbahninfrastruktur und gewährleistet letztendlich Sicherheit und Compliance in der Branche.

Während Sicherheitstools unverzichtbar sind, um sicherheitsrelevante Risiken zu identifizieren und zu mindern, hängt ihre Effektivität letztendlich von menschlicher Expertise ab. Automatisierte Tools können Schwachstellen hervorheben, aber die Umsetzung dieser Erkenntnisse in umsetzbare Sicherheitsverbesserungen erfordert die Zusammenarbeit mehrerer Teams. Bei Mipro arbeiten das Softwareentwicklungsteam, das Sicherheitsteam, das IT-Service-Management (ITSM) und das DevSecOps-Team zusammen, um Sicherheitsprobleme in einer strukturierten Weise zu bewerten, zu priorisieren und zu beheben.

Das Unternehmen hat ein spezielles DevSecOps-Steuerungsteam eingerichtet, um die Komplexität seiner Sicherheitsoperationen zu verwalten und die Übereinstimmung mit der IEC 62443 sicherzustellen. Dieses Team spielt eine entscheidende Rolle bei der Überwachung aller Aspekte der Sicherheitsintegration innerhalb des Entwicklungsprozesses und stellt sicher, dass Sicherheits- und Datenschutzüberlegungen nahtlos in Produktentwicklungen eingebettet werden.

triple constraint. Mipro Oy (Mipro) enhances system resilience, optimises resource allocation and ensures regulatory compliance by integrating security into the development lifecycle early on and adhering to IEC 62443 standards.

IEC 62443 provides a structured framework for securing industrial control systems. The company employs a combination of automated security testing, risk assessment and continuous monitoring to systematically fulfil the standard's requirements. The integration of tools such as Jenkins and GitLab facilitates automated CI / CD pipelines with embedded security checks at each stage of software development and deployment. Jira plays a critical role in tracking vulnerabilities and ensuring that security issues are addressed in a structured and timely manner.

Ensuring software security validation is a key requirement under IEC 62443-3-3 and IEC 62443-4-2. The company employs SonarQube for static code analysis in order to enforce secure coding practices and detect vulnerabilities at an early stage so as to meet these requirements. OWASP DependencyCheck is used to analyse any third-party libraries, thereby ensuring compliance with the security policies and reducing the risk of supply chain attacks. Trivy is implemented in containerised environments in order to scan for known vulnerabilities, thereby guaranteeing the integrity of the deployed software components.

In addition to secure coding practices, threat detection and risk assessment are also essential components of Mipro's security strategy, thereby aligning with IEC 62443-3-2. Nessus is utilised to conduct regular vulnerability assessments, evaluate system security posture and identify misconfigurations before they become exploitable threats. The Robot Framework supports dynamic application security testing (DAST), i.e. the simulation of real-world attack scenarios to validate the system's resilience against potential cyber threats.

The company has adopted a defence-in-depth strategy by integrating automated security scanning directly into CI / CD workflows in order to maintain its continuous compliance with IEC 62443-3-3. This approach ensures multiple layers of security validation and minimises exposure to any potential attacks. By implementing automated monitoring and continuous security assessment, Mipro ensures that railway control system applications remain protected against evolving cyber threats.

The company has not only strengthened its software security by leveraging the DevSecOps tools in alignment with IEC 62443, but it has also enhanced its operating efficiency. This proactive approach to cybersecurity fosters robust threat detection, secure software development and resilient railway infrastructure, thereby ultimately ensuring safety and compliance within the industry.

While security tools are invaluable in identifying and mitigating security-related risks, their effectiveness is ultimately dependent on human expertise. Automated tools can highlight vulnerabilities, but translating these findings into actionable security improvements requires collaboration across multiple teams. At Mipro, the software development team, security team, IT service management (ITSM) and DevSecOps team work together to assess, prioritise, and remediate any security issues in a structured manner.

The organisation has established a dedicated DevSecOps steering team to manage the complexity of its security operations and ensure alignment with IEC 62443. This team plays a crucial role in overseeing all the aspects of security integration within the development process, thereby ensuring that security and privacy considerations are embedded seamlessly into product develop-

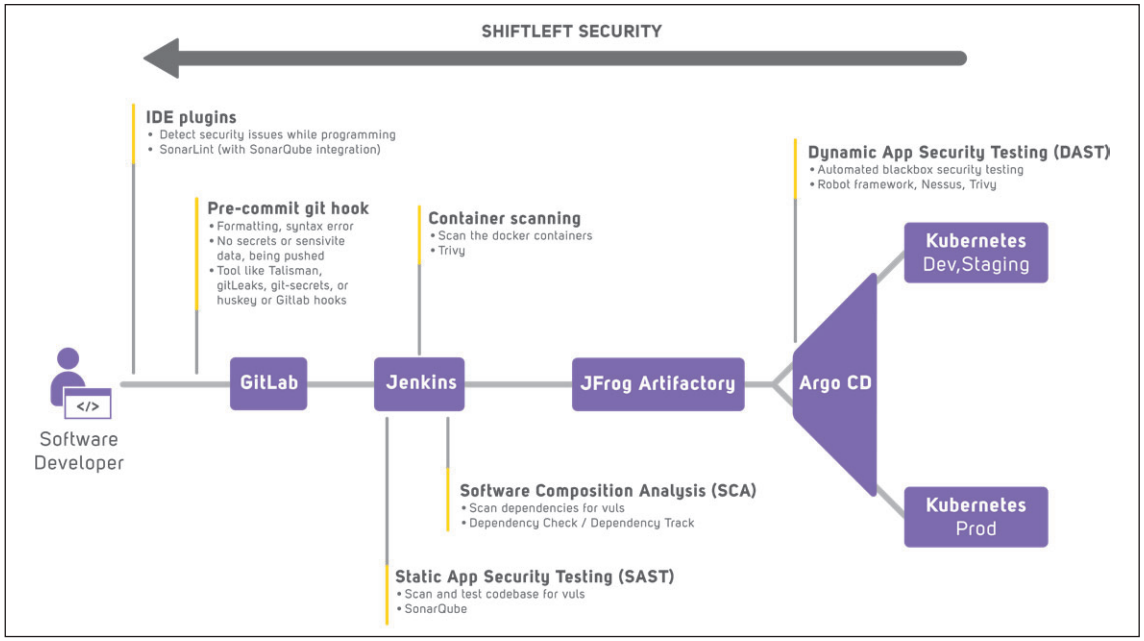

Bild 2: Die DevSecOps-Pipeline von Mipro
Fig. 2: Mipro's DevSecOps pipeline

muliert werden, um die Widerstandsfähigkeit von Systemen gegen potenzielle Cyberbedrohungen zu überprüfen.

Um die kontinuierliche Einhaltung der IEC 62443-3-3 zu gewährleisten, verfolgt das Unternehmen eine Defense-in-Depth-Strategie, indem automatisierte Sicherheitsscans direkt in die CI/CD-Workflows integriert werden. Dieser Ansatz gewährleistet eine mehrschichtige Sicherheitsvalidierung und minimiert die Anfälligkeit für potenzielle Angriffe. Durch die Implementierung von automatischer Überwachung und kontinuierlicher Sicherheitsbewertung stellt Mipro sicher, dass die Anwendungen von Bahnsteuerungssystemen vor sich entwickelnden Cyberbedrohungen geschützt bleiben.

Durch den Einsatz von DevSecOps-Tools gemäß IEC 62443 erhöht das Unternehmen nicht nur die Softwaresicherheit, sondern steigert auch die betriebliche Effizienz. Diese proaktive Herangehensweise an die Cybersicherheit fördert eine zuverlässige Erkennung von Bedrohungen, eine sichere Softwareentwicklung und eine widerstandsfähige Eisenbahninfrastruktur, die letztlich die Sicherheit und die Einhaltung von Vorschriften in der Branche gewährleistet.

Sicherheitstools sind zwar von unschätzbarem Wert, wenn es darum geht, sicherheitsrelevante Risiken zu erkennen und zu mindern, ihre Wirksamkeit hängt jedoch letztlich von der menschlichen Kompetenz ab. Automatisierte Tools können Sicherheitslücken aufdecken, aber die Umsetzung dieser Erkenntnisse in praktikable Sicherheitsverbesserungen erfordert die Zusammenarbeit mehrerer Teams. Bei Mipro arbeiten das Softwareentwicklungsteam, das Sicherheitsteam, das IT Service Management (ITSM) und das DevSecOps-Team Hand in Hand, um Sicherheitsprobleme strukturiert zu bewerten, zu priorisieren und zu beheben. Um die Komplexität der Sicherheitsprozesse zu bewältigen und die Einhaltung der IEC 62443 zu gewährleisten, hat das Unternehmen ein spezielles DevSecOps-Lenkungsteam eingerichtet. Dieses Team spielt eine entscheidende Rolle bei der Überwachung aller Aspekte der Sicherheitsintegration während des Entwicklungsprozesses und stellt sicher, dass Sicherheits- und Datenschutzaspekte nahtlos in die Produktentwicklung integriert werden. Durch die Förderung der funktionsübergreifenden Zusammenarbeit und der strategischen Aufsicht ermöglicht das DevSecOps-Lenkungsteam dem Unternehmen, eine proaktive Sicherheitshaltung beizubehalten, die die Einhaltung von Industriestandards gewährleistet und gleichzeitig qualitativ hochwertige, sichere und effiziente Eisenbahnsoftwarelösungen bereitstellt. ■

ment. By fostering cross-functional collaboration and strategic oversight, the DevSecOps steering team enables the organisation to maintain a proactive security posture and ensures compliance with the industry standards, while delivering high-quality, secure and efficient railway software solutions. ■

AUTOREN | AUTHORS

Anssi Lampinen
Software Architect
E-Mail: anssi.lampinen@mipro.fi

Matti Laine
ICT&M Director
E-Mail: matti.laine@mipro.fi

Viet Nguyen
PhD student, Industrial Engineering and Management at Tampere University of Technology, and System Manager
E-Mail: viet.nguyen@mipro.fi

Alle Autoren / *all authors*:
Mipro Oy
Anschrift / *Address*: Kunnanmäki 9, FI-50600 Mikkeli