Vorgehensmodell zur IT-Sicherheitsanalyse für Bahnanwendungen

IT security risk analysis procedure for railway applications

Patric Birr

Der Artikel beleuchtet die Durchführung einer IT-Sicherheitsanalyse auf Basis der Normenreihe IEC 62443 [1] zum Schutz von industriellen Kommunikationsnetzen an einer Beispielarchitektur der Leit- und Sicherungstechnik. Das im bahnspezifischen Leitfaden DIN VDE V 0831-104 [2] beschriebene Vorgehen zur Anwendung der IEC 62443 wird dabei um eine mehrstufige qualitative Risikobetrachtung erweitert. Unter Anwendung bewährter „Bottom-Up"- und „Top-Down"-Analysetechniken werden iterativ die vorhandenen Schutzmechanismen bewertet und gegebenenfalls ergänzt.

1 Motivation

Mit dem Inkrafttreten des IT-Sicherheitsgesetzes in Deutschland im Juli 2015 entstehen den Betreibern Kritischer Infrastrukturen (KRITIS) im Sektor Transport und Verkehr neue Anforderungen an Organisation, Prozess, Technik und Nachweisführung. Die IT-Sicherheit rückt dabei in den Fokus des Compliance Managements als Motor zur Einhaltung von Vorschriften durch ein Unternehmen, seine Organisation und Mitarbeiter. Neben der Erfüllung von gesetzlichen und regulatorischen Vorgaben steht die Konformität mit Normen, Standards und Konventionen im Mittelpunkt. Entscheidungen müssen begründbar sein und dabei gilt, dass Informiertheit ein Maßstab für die Abgrenzung von Fahrlässigkeit im Schadensfall ist.

In der von Beständigkeit geprägten Domäne Bahn stellen die von kontinuierlicher Veränderung gekennzeichneten Problemstellungen der IT-Sicherheit die Hersteller und Betreiber vor neue Herausforderungen. Dazu gehören beispielsweise die Früherkennung bestandsgefährdender Risiken und deren fortlaufende Kontrollpflicht. Als präventive Maßnahme hat sich dabei die IT-Sicherheits-Risikoanalyse (nachfolgend IT-Sicherheitsanalyse) zur Überprüfung der Schutzziele etabliert, wobei Vertraulichkeit (engl. confidentiality) und Integrität (engl. integrity) der Daten sowie die Verfügbarkeit des Systems (engl. availability) maßgebliche Werte darstellen.

Die IT-Sicherheitszertifizierung eines Systems durch eine akkreditierte Stelle lässt sich in Neuzertifizierung sowie verschiedene Methoden der Aufrechterhaltung eines bestehenden Zertifikats unterteilen. Ein System bzw. Produkt wird nur zum Zeitpunkt der Ausstellung als IT-sicher bestätigt, weshalb die Gültigkeit des Zertifikats zeitlich befristet ist und zyklisch erneuert werden muss. Ein methodisch sauberes, systematisches Vorgehen zur Vorbereitung eines IT-Sicherheitsnachweises ist daher essentiell und soll im Folgenden an einem Vorgehensmodell für Bahnanwendungen dargestellt werden.

In this article, we present an IT security risk analysis procedure based on the IEC 62443 [1] series of standards on industrial automation and control system security. The German draft standard DIN VDE V 0831-104 [2] serves as a guideline for the application of IEC 62443 to railway systems. The initial set of requirements derived from this railway-specific approach is revised using a combination of bottom-up and top-down analysis techniques. The proposed procedure allows for iterative evaluation and possible extension of existing IT security measures within the system under consideration.

1 Motivation

Since the German IT Security Act came into effect in July 2015, operators of critical infrastructure in the transport sector have had the duty of fulfilling new requirements regarding their organisation, technology and certification process. Companies are now legally bound to include IT security in compliance management activities. Besides compliance with legal requirements, standards and guidelines have to be considered. Decisions must be well-founded and informed in order to avert allegations of negligence in the event of damage.

Threats to the IT security of a system change frequently and rapidly. That constitutes a new challenge for railway manufacturers and operators, since their technological environment is otherwise exceptionally stable. One such challenge is the obligation to implement measures for early detection and continuous monitoring of threats as well as a timely response to attacks.

Conducting an IT security risk analysis has proven to be an effective preventive measure, providing an initial definition and periodic revisions of protection goals. For IT systems especially, essential values to be protected include the confidentiality and integrity of data as well as the availability of a system. IT security certification of a system, performed by an accredited body, is achieved first by a new certification for initial system approval and thereafter through regular re-certification. A successful certification process confirms compliance at the time of the evaluation. Since certificate validity can be restricted to a limited period of time, the certification process needs to be repeated periodically. It is therefore essential to define a systematic and well-documented process, preparing a proof of IT security for the system under consideration. A proposal for such a procedure for railway applications is presented in the following sections, using a generic sample electric signalling system.

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

2 Vorgehensmodell Transportation

2.1 Einleitung

Bedrohungen im Sinne der IT-Sicherheit können zu Gefährdungen im Sinne der funktionalen Sicherheit (nachfolgend Safety genannt) führen, wenn beispielsweise die Schutzobjekte eines Systems dessen Sicherheitsfunktionen sind [3]. Bild 1 verdeutlicht die terminologischen Zusammenhänge im Fachbereich der IT-Sicherheit. Schwachstellen im Source Code führen zu Verwundbarkeiten in der Software, die ein Angreifer ausnutzen kann, um eine Bedrohung zu initiieren. Sind Sicherheitsfunktionen im Sinne der Safety betroffen, dann sollte der Sicherheitsnachweis hinreichende Maßnahmen zur Behandlung dieser Bedrohungen beschreiben [4].

Die Basis der Systemzertifizierung bildet die Konformität zum Stand der Technik [5]. Das Ziel des Vorgehensmodells ist also die Bereitstellung und kontinuierliche Überprüfung eines hinreichenden Satzes an IT-Sicherheitsanforderungen. Wie in [6] beschrieben, rückt dabei die IEC-62443-Normenreihe in den Fokus, wobei ein funktionierendes Information Security Management System (ISMS) auf Grundlage der Norm ISO 27001 [7] gefordert wird. Der bahnspezifische Leitfaden DIN VDE V 0831-104 [2] für die IT-Sicherheit auf Grundlage der IEC 62443 schlägt einen integrierten Ansatz zur Einbettung der IT-Sicherheitsanalyse in die etablierten Vorgehensweisen gemäß EN 50129 [8] und EU VO 402/2013 [9] vor. Der Fokus liegt somit auf dem Schutz der Systemintegrität zur Wahrung der funktionalen Sicherheit.

Die hier vorgestellte Erweiterung des Ansatzes um eine detaillierte Risikoanalyse auf Basis des Leitfadens für IT-Sicherheitsanalysen NIST SP 800-30 [10] dient der Abschätzung von resultierenden Risiken durch erfolgreiche Angriffe von außen. In einer Kombination aus den bewährten Analysetechniken Security FMEA (engl. Failure Mode and Effects Analysis, „Bottom-Up"-Ansatz) und Angriffsbaumanalyse („Top-Down"-Ansatz) werden systematisch die organisatorischen und technischen Rahmenbedingungen den Bedrohungen gegenübergestellt und somit die Angreifbarkeit des Systems überprüft. Durch technologiespezifische Zuteilung nachweislich effektiver Schutzmaßnahmen können dann die Risiken verringert oder eliminiert werden.

2 Transport procedure

2.1 Introduction

IT security threats can lead to safety hazards if the assets of a system under consideration are its safety functions [3]. Figure 1 illustrates the key relationships of IT security terminology. Source code weaknesses can lead to software vulnerabilities, which can be exploited by an attacker to initiate a threat affecting the system assets. If safety functions are involved, the technical safety case must include the description of appropriate countermeasures [4].

The basis for system certification is the compliance with state-of-the-art requirements [5]. Therefore, the primary goal of such a procedure is to provide and continuously revise an appropriate set of IT security requirements using well-established engineering standards. As described in [6], the IEC 62443 series is widely accepted as well-suited for this purpose. As part of its application, an information security management system (ISMS) based on the ISO 27001 standard [7] is required. The railway-specific guideline for the application of IEC 62443 to electric signalling systems, DIN VDE V 0831-104 [2], proposes an integration of IT security assessments into the established procedures of EN 50129 [8] and EU Regulation no. 402/2013 [9]. The focus is therefore set on the protection of system integrity to maintain functional safety.

To evaluate the inherent risk of successful cyberattacks, this approach is extended by a detailed risk analysis based on the guideline for conducting risk assessments, NIST SP 800-30 [10]. Using a combination of bottom-up and top-down analysis techniques, each threat is evaluated within the organisational und technical framework of the system to assess its vulnerability. Through allocation of effective protection measures to the system architecture, existing risks can be reduced or eliminated.

The procedure presented here describes four stages (fig. 2) to define a specific set of state-of-the-art requirements, the implementation of which protects the system from all identified risks.

2.2 Railway-specific risk assessment (stage 1)

As already detailed in [6], the railway-specific risk assessment guideline DIN VDE 0831-104 [2] describes a simplified application of IEC 62443 in four steps:

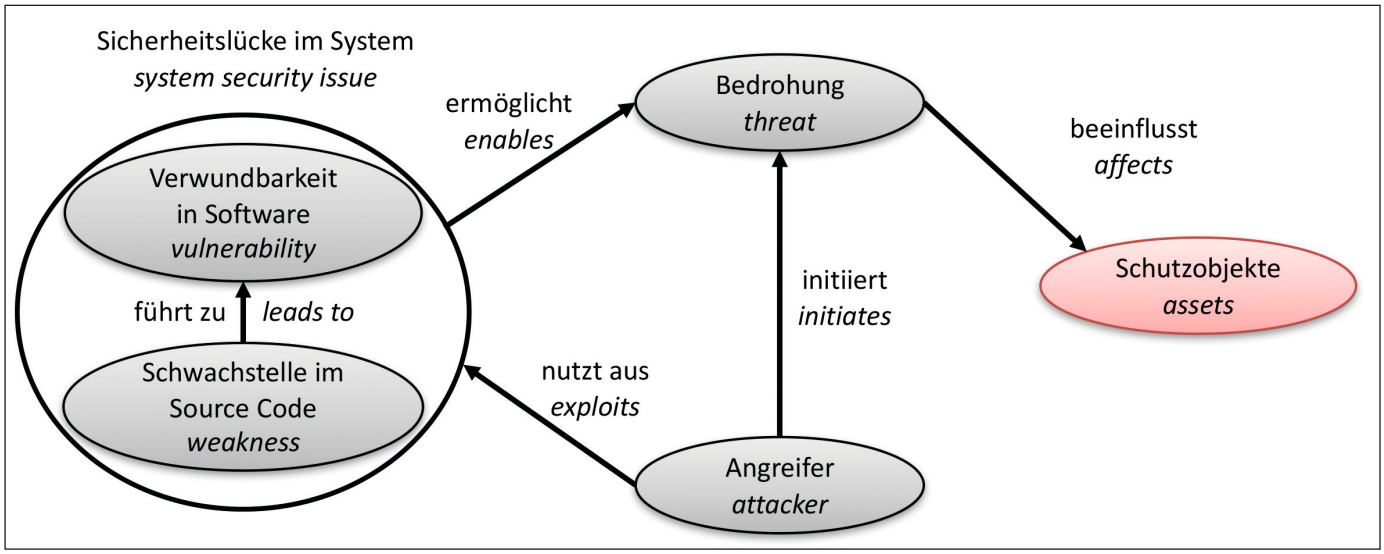

Bild 1: Zusammenhang zwischen Angreifer, Sicherheitslücke und Bedrohung für ein Schutzobjekt
Fig. 1: Relationship between attacker, security issue and threat affecting an asset

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

Das beschriebene Vorgehensmodell führt somit in vier Aktivitätsstufen (Bild 2) zu einem spezifischen, dem Stand der Technik entsprechenden Anforderungskatalog, durch dessen Umsetzung Risiken für das untersuchte System beherrscht werden können.

2.2 Bahnspezifische Risikobetrachtung (Stufe 1)

Wie bereits detailliert in Heft 10/2014 [6] beschrieben, sieht die bahnspezifische Risikobetrachtung gemäß DIN VDE V 0831-104 [2] ein schrittweises Vorgehen zur vereinfachten Anwendung der IEC 62443 vor:

- Einteilung des Systems in Zonen und Conduits (Kommunikationskanäle zwischen Zonen)
- Bedrohungsanalyse
- Bahnspezifische Risikoanalyse
- Zuteilung der IT-Sicherheitsanforderungen

Regelbasiert erfolgt eine Einteilung der Systemarchitektur in Zonen und Conduits. Dabei gilt es beispielsweise zu beachten, dass sicherheitsrelevante (Safety) Anwendungen und nicht-sicherheitsrelevante Anwendungen unterschiedlichen Zonen zugeteilt werden. Außerdem sollten mobile Endgeräte, denen temporärer Zugriff erlaubt werden soll, zonal separiert werden.

Die Bedrohungsanalyse erfolgt für jede Zone und jeden Conduit separat und kann beispielsweise auf Basis der negierten IT-Sicherheitsanforderungen gemäß IEC 62443-3-3 [11] durchgeführt werden. Bedrohungen mit ähnlichen Auswirkungen als Bedro-

- Separation of the system into zones and conduits (communication channels between zones)
- Threat analysis
- Railway-specific risk analysis
- Assignment of IT security requirements

Separation of the system into zones is to be done according to certain criteria based on, for example, functionality, safety relevance and the devices' modes of communication. Conduits represent connections between zones.

During the threat analysis, every zone and conduit must be considered separately. Threats can be derived from negated IT security requirements defined in IEC 62443-3-3 [11]. It is recommended that threats be grouped as threat classes based on similar effects on the system be grouped as threat classes to keep the analysis clear and simple. Building upon the results of the threat analysis, the railway-specific risk analysis is used to derive security level targets (SL-T) for every zone and conduit based on an estimate of realistic attacker characteristics. Taking into account some pre-defined railway-specific risk factors regarding location, traceability and potential severity of impact of a possible attack, the simplified analysis yields SL-T as a result. The security level of every zone defines the initial set of IT security requirements according to IEC 62443-3-3. The security levels determined for the sample system are mapped to its architecture in fig. 3.

A proof of completeness for the set of requirements defined must be based on existing threats and the corresponding tech-

We set priorities.
Together for safety.

SCHALTBAU PINTSCH BAMAG
www.pintschbamag.de

SCHALTBAU PINTSCH ABEN
www.pintschaben.com

SCHALTBAU PINTSCH TIEFENBACH
www.pintschtiefenbach.de

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

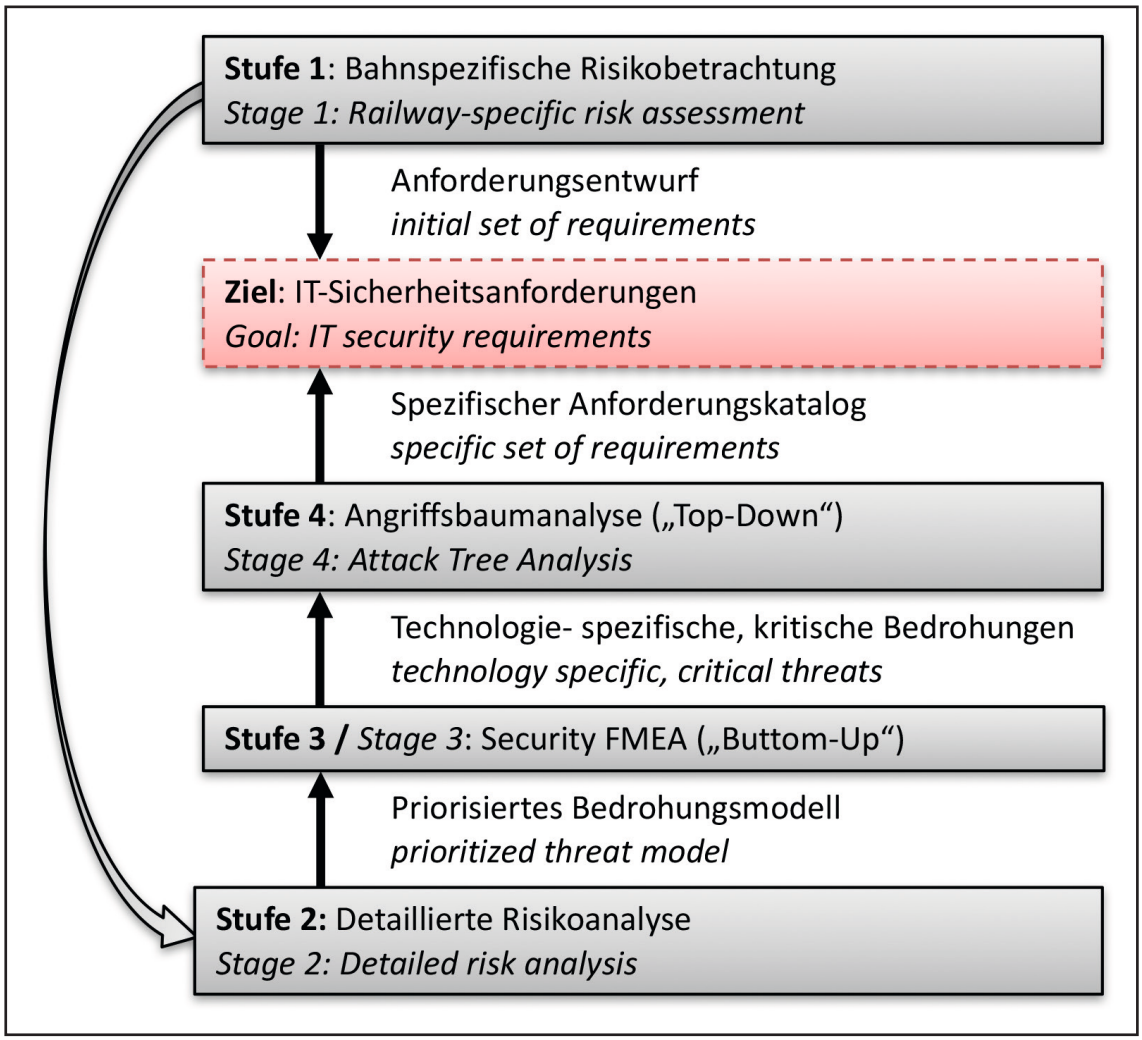

Bild 2: Stufen des Vorgehensmodells
Fig. 2: Stages of the proposed procedure

hungsklassen zu gruppieren, erleichtert die Umsetzung und verbessert die Übersicht im Laufe der Analyse.

Aufbauend auf den Erkenntnissen der Bedrohungsanalyse dient die vereinfachte Risikoanalyse der Ermittlung des Security Level Target (SL-T) für jede Zone und jeden Conduit. Maßgeblich dafür sind die Schätzung des realistisch anzunehmenden Angreifertyps und die Berücksichtigung der bahnspezifischen Risikofaktoren zu Ort, Nachverfolgbarkeit und Schadenspotenzial eines möglichen Angriffs. Der resultierende Security Level jeder Zone definiert für die untersuchte Systemarchitektur einen initialen Satz an IT-Sicherheitsanforderungen auf Basis der IEC 62443-3-3. Für die betrachtete Beispielarchitektur sind die in dieser Form ermittelten Security Levels in Bild 3 dargestellt.

Nun stellt sich jedoch die Frage nach der Vollständigkeit dieser Anforderungen, die sich an der aktuellen Bedrohungslage ausrichten soll. Besonderes Augenmerk wird dabei auf die technologie-spezifischen Risiken und ein Verständnis für die Angreifbarkeit der Systemkomponenten gelegt. Der beschriebene bahnspezifische Ansatz wird zu diesem Zweck um drei komplementäre Analyseschritte erweitert.

2.3 Detaillierte Risikoanalyse (Stufe 2)

Der aktuelle Entwurf der IEC 62443-3-2 [12] („IT-Sicherheits-Risikobetrachtung und Systemdesign“) definiert die geforderten Aktivitäten bei der Durchführung einer detaillierten IT-Sicherheitsanalyse. Gefordert werden unter anderem die Identifikation von

nology-specific risks to the system. The railway-specific approach introduced is therefore extended by a three-step detailed analysis.

2.3 Detailed risk analysis (stage 2)

The working draft of IEC 62443-3-2 [12], which focuses on security risk assessments and system design, defines activities required for a detailed risk assessment, including identification of threats and vulnerabilities as well as determining consequences and calculating risks to system assets. The procedure presented fulfils those requirements by extending the railway-specific approach with a more detailed assessment based on the system technology.

NIST SP 800-30 [10] is referred to as the benchmark for conducting IT security risk assessments in [2]. It defines the necessary steps to identify and evaluate the risks posed to IT systems. Every possible threat is prioritised on the basis of its attack method as well as consequences and likelihood of a successful attack. Figure 4 illustrates the corresponding relationships used to determine a risk posed to the system by a specific threat.

Working in cooperation with IT experts, a technology-specific threat model can be developed using detailed and extensive databases. When choosing such databases, the recommendations of the German Federal Office for Information Security (BSI) should be taken into account. The BSI itself provides

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

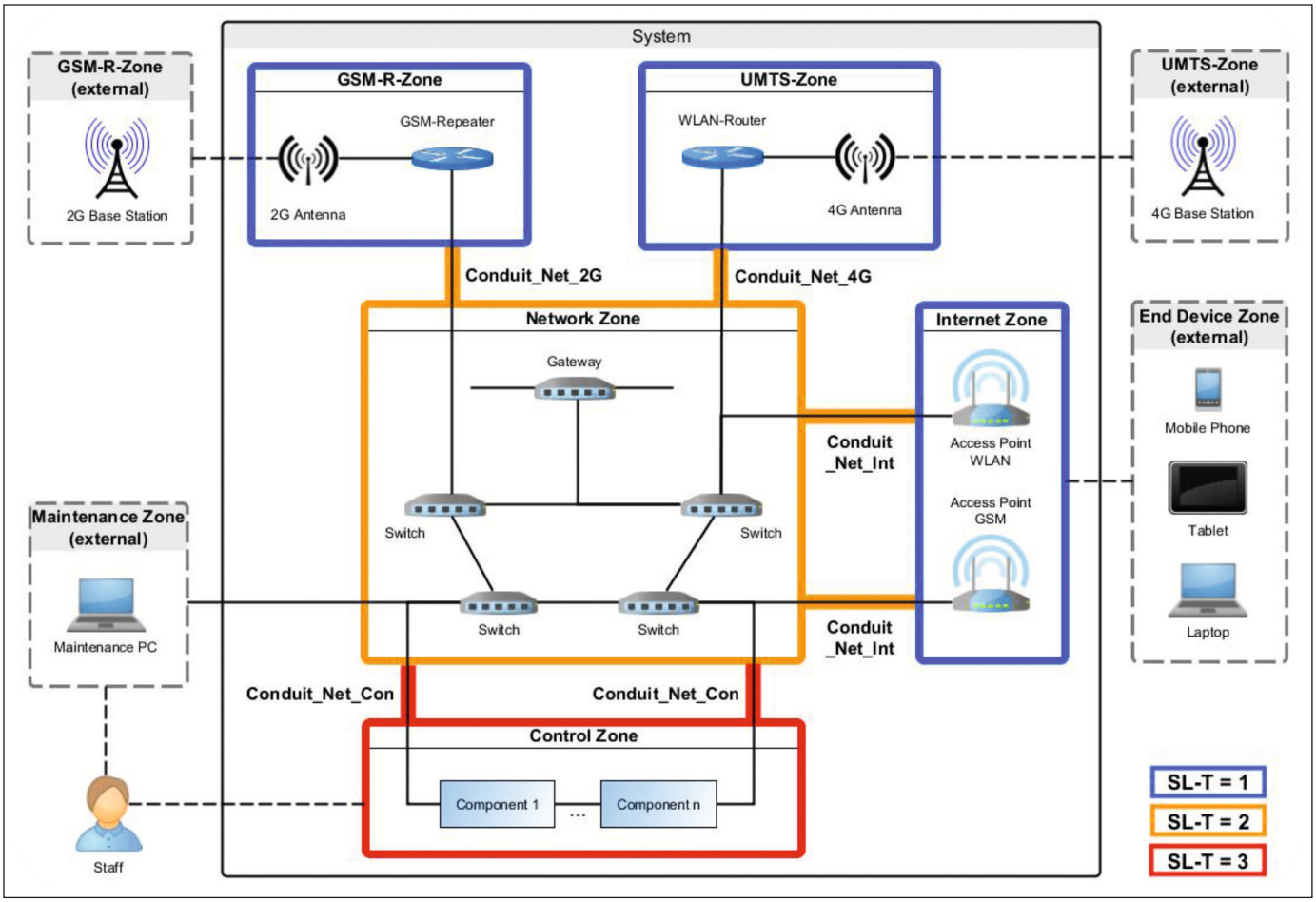

Bild 3: Einteilung einer Systemarchitektur in Zonen und Conduits
Fig. 3: System architecture segmentation into zones and conduits

Bedrohungen und Schwachstellen sowie die Bestimmung der Auswirkungen und Abschätzung der Risiken für die Schutzobjekte des Systems. Durch die Erweiterung des bahnspezifischen Vorgehens um eine technologie-spezifische und detaillierte Analyse wird diesen Anforderungen entsprochen.

Der gemäß [2] als Maßstab für die Durchführung von IT-Sicherheitsanalysen anzusehende Leitfaden NIST SP 800-30 [10] definiert die notwendigen Schritte zur Identifikation und Bewertung von Risiken bei der Verwendung von IT-Systemen. Im Mittelpunkt der Analyse steht die Bewertung aller möglichen Bedrohungen anhand ihrer Angriffsmethodik, der Auswirkungen auf das System und der Wahrscheinlichkeit eines erfolgreichen Angriffs. Die Zusammenhänge bei der Bestimmung des von jedem Angriffsmuster ausgehenden Risikos sind in Bild 4 dargestellt.

In Zusammenarbeit mit IT-Experten und auf Grundlage von etablierten sowie umfangreichen Datenbanken lässt sich somit, unter Berücksichtigung der Systemarchitektur, ein technologie-spezifisches Bedrohungsmodell entwickeln. Bei der Auswahl der zu verwendenden Datenbanken bietet sich an, Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu berücksichtigen. Das BSI selber stellt mit den IT-Grundschutzkatalogen (IT-GSK) [13] eine umfassende Datenbank an Gefährdungen und den entsprechenden Gegenmaßnahmen zur Verfügung, die zudem sogenannten „Bausteinen" als repräsentative Architekturkomponenten zugeordnet sind. International etabliert sind außerdem drei miteinander verknüpfte Datenbanken [14] zu Angriffsmustern, Schwachstellen und Verwundbarkeiten, die insbe-

a comprehensive database of threats and corresponding countermeasures, including mappings to typical architecture components [13]. Additionally, three internationally well-established databases [14] contain detailed descriptions of attack patterns, weaknesses and vulnerabilities. For systems with connections to untrusted networks especially, the detailed data should be used to identify and evaluate possible security issues and attack patterns. The 2016 issue of the yearly instalment, "The State of IT security in Germany" [15], published by the BSI, also lists one of these three databases as the only internationally accepted source of vulnerabilities.

NIST SP 800-30 defines a risk assessment procedure in five steps, starting with the identification of all threats to the technology in use and leading to the determination of risks to data confidentiality and integrity as well as system availability, respectively. All evaluated threats can then be prioritised on the basis of their risk values and merged into a technology-specific threat model. That allows for a comprehensive comparison with the technical and organisational framework of the system under consideration.

2.4 Security FMEA (stage 3)

In order to assess the vulnerability of the system analysed, we combine two techniques, which complement each other. A Security FMEA and an attack tree analysis are executed simultaneously in an iterative process to uncover security issues and define corresponding protection measures.

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

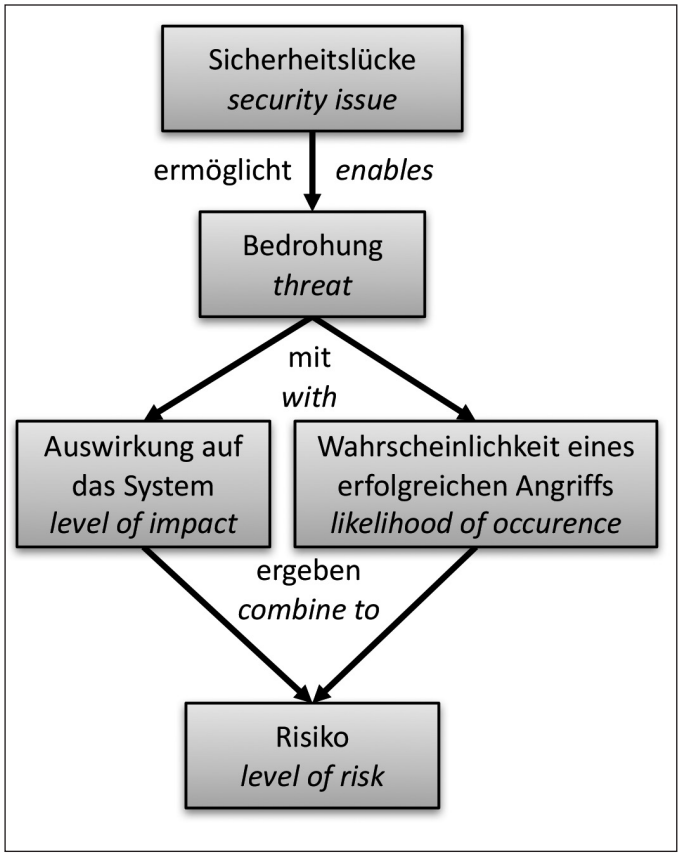

Bild 4: Risikobewertung gemäß NIST SP 800-30 [10]
Fig. 4: Risk evaluation according to NIST SP 800-30 [10]

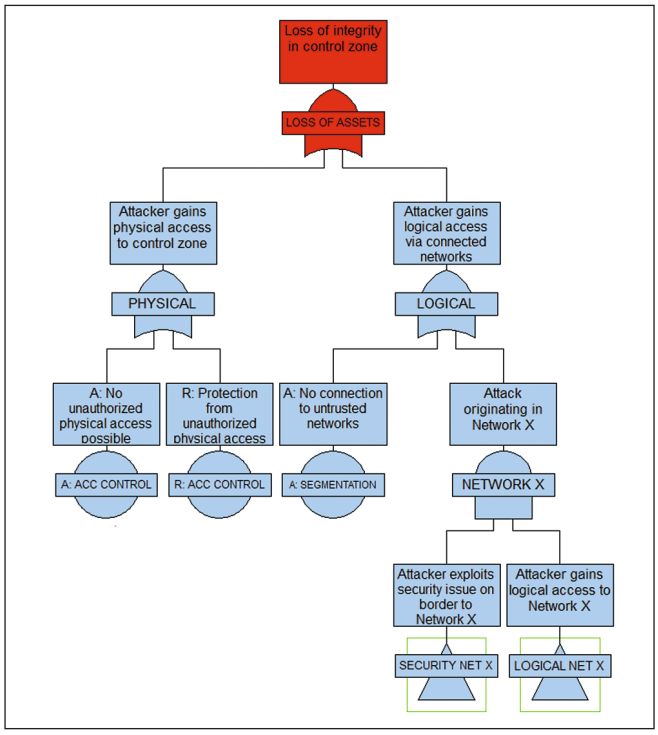

Bild 5: Vereinfachtes Beispiel einer Angriffsbaumanalyse
Fig. 5: Simplified example of an attack tree analysis

sondere bei Schnittstellen mit nicht vertrauenswürdigen Netzen zur Bewertung der Bedrohungslage herangezogen werden können. Auch das BSI verweist in seinem Ende 2016 veröffentlichten Bericht zur Lage der IT-Sicherheit in Deutschland [15] auf eine der drei Datenbanken als einzig weltweit anerkannte Quelle für Verwundbarkeiten.

Der fünfstufige Ansatz gemäß [10] führt von der Identifikation aller für die verwendete Technologie existierenden Bedrohungen bis zur Bestimmung des vom jeweiligen Angriff ausgehenden Risikos für die IT-Grundwerte des Systems: Integrität, Vertraulichkeit und Verfügbarkeit. Die Zusammenführung aller bewerteten Bedrohungen lässt sich zuletzt anhand dieser drei Risikowerte priorisieren und ermöglicht somit eine Gegenüberstellung mit den technischen und organisatorischen Rahmenbedingungen des betrachteten Systems.

2.4 Security FMEA (Stufe 3)

Zur Überprüfung der Angreifbarkeit des untersuchten Systems eignet sich eine Kombination aus zwei Analysetechniken, die sich durch entgegengesetzte Betrachtungsweisen ideal ergänzen. Die Security FMEA und die Angriffsbaumanalyse bilden bei paralleler Anwendung einen iterativen Prozess, anhand dessen Sicherheitslücken aufgedeckt und entsprechende Maßnahmen definiert werden können.

In der Security FMEA wird der sogenannte „Bottom-Up"-Ansatz verfolgt, der für jede Komponente des Systems alle in Stufe 2 identifizierten Bedrohungen hinsichtlich ihrer Kritikalität bewertet. Dabei werden jeweils die zuvor bestimmten Risikowerte den technologischen und organisatorischen Schutzmechanismen gegenübergestellt. Ergibt die Gegenüberstellung, dass Bedrohun-

The Security FMEA represents a bottom-up approach, evaluating the criticality of every threat identified (see stage 2) for every component in the system. The risk values determined previously are compared with the existing organisational and technological protection mechanisms. If the comparison shows that existing measures are insufficient to protect against a specific threat, additional requirements must be defined for the component examined. The databases [13, 14] mentioned in stage 2, offer guidance towards defining such additional requirements. To evaluate the effectiveness of measures against a certain attack pattern, extensive technical knowledge regarding attack patterns as well as the system technology is required.

The Security FMEA allows for a prioritisation of threats for every component, taking protection measures into account. Threats with an assigned risk value above a pre-defined threshold are considered critical and are examined further in the attack tree analysis.

2.5 Attack tree analysis (stage 4)

Representing a top-down approach, an attack tree analysis (ATA) completes the combination. In such an analysis, all possible penetration paths are developed systematically, starting from a loss of assets as the top event to be prevented. The results of the threat analysis and Security FMEA are thus mapped onto the architecture of the system under consideration. Within the ATA, technological barriers as well as operational and organisational assumptions that rule out certain attacks need to be taken into account. If a certain attack pattern requires physical access to closed areas, for instance, references to specific procedures limiting area entrance can be used to eliminate the corresponding penetration path.

The ATA may either reveal security issues to be fixed through requirements of additional protection measures or it may be used to verify that no critical penetration paths remain, given

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

gen durch bereits vorhandene Maßnahmen nicht abgewehrt werden können, sind zusätzliche Anforderungen an die jeweilige Komponente zu definieren. Einen Anhaltspunkt zu dieser Ergänzung des initialen Satzes an IT-Sicherheitsanforderungen liefern die in Stufe 2 beschriebenen Datenbanken [13, 14]. Für eine fundierte Bewertung der Effektivität von Schutzmaßnahmen zur Abwehr der einzelnen Angriffe ist sowohl bezüglich des Systems als auch der Angriffsziele und -muster ein umfassendes technisches Verständnis essentiell.

In Zusammenarbeit mit IT-Experten lassen sich somit in der Security FMEA für jede Komponente Bedrohungen unter Berücksichtigung der Schutzmaßnahmen über einen Risikowert priorisieren. Jene Bedrohungen, deren resultierende Risikowerte oberhalb eines betrieblich zu definierenden Schwellwertes liegen, werden dann als kritische Angriffe in der Angriffsbaumanalyse berücksichtigt.

2.5 Angriffsbaumanalyse (Stufe 4)

Als zweite Analysetechnik der vorgestellten Kombination repräsentiert die Angriffsbaumanalyse den „Top-Down"-Ansatz. Der Verlust oder die Beeinträchtigung der Schutzobjekte ist dabei das abzuwehrende Ereignis, dem systematisch alle möglichen Angriffspfade zugeordnet werden. Die Angriffsbaumanalyse bildet dadurch die Ergebnisse der Bedrohungsanalyse und Security FMEA auf die untersuchte Systemarchitektur ab. Berücksichtigt werden sollen hier neben technologischen Barrieren auch sämtliche Annahmen zu Betrieb und Organisation, die zum Ausschluss von Angriffen führen können. Erfordert beispielsweise ein Angriff den physikalischen Zutritt zu geschlossenen Räumlichkeiten, so kann durch einen Verweis auf entsprechende zutrittsbeschränkende Verfahren der dazugehörige Angriffspfad abgeschlossen werden.

Die Angriffsbaumanalyse offenbart entweder Sicherheitslücken im System, für die zusätzliche Schutzmaßnahmen gefordert werden können. Oder sie führt abschließend zum Nachweis, dass unter Berücksichtigung eines bestimmten Katalogs an betrieblichen, organisatorischen und technischen Annahmen keine kritischen Angriffspfade verbleiben. Die Verantwortung dafür, dass die getroffenen Annahmen auch Gültigkeiten haben und behalten, liegt dabei beim Betreiber bzw. Hersteller des untersuchten Systems. So muss beispielsweise ein Unternehmen entweder sicherstellen, dass der unerlaubte Zutritt zu geschlossenen Räumlichkeiten nachweislich effektiv unterbunden wird. Oder es ist als Ergebnis der Analyse zu fordern, dass zusätzliche Maßnahmen der Zutrittsbeschränkung eingeführt werden.

Bild 5 veranschaulicht an einem vereinfachten Beispiel die beschriebene Methodik im Verlauf der Analyse. Ausgehend vom abzuwehrenden Ereignis, das hier generisch als Integritätsverlust in der Steuerungszone des untersuchten Systems definiert ist, werden die möglichen Angriffspfade untersucht. Über logische UND- bzw. ODER-Gatter ist abzubilden, wie ein Angreifer den Verlust der Schutzobjekte herbeiführen kann. Am Beispiel des physikalischen Zutritts (Gatter „PHYSICAL") ist dargestellt, wie zur Handhabung des entsprechenden Angriffspfades entweder betriebliche Annahmen (Markierung „A:") herangezogen werden können oder stattdessen zusätzliche Anforderungen (Markierung „R:") zu definieren sind. In der finalen Version des Baumes ist dann in Abhängigkeit von der Bewertung der Annahme nur noch einer der beiden Einträge vorhanden.

Demselben Prinzip folgend, offenbart das Gatter „LOGICAL", dass sich durch Anbindung der Steuerungszone an Netzwerke neue, potenziell umfangreiche „Äste" des Angriffsbaumes ergeben.

a specific set of valid assumptions on technology, operation and organisation. The operator of the system under consideration is responsible for the validity of such assumptions. For instance, a company must ensure and prove that unauthorised physical access to closed areas is prevented effectively. Otherwise, additional requirements of access control need to be defined as a result of the ATA.

Fig. 5 illustrates this method, using a simplified example. Starting from a generic top event "Loss of integrity in control zone", each penetration path is investigated. All possible ways for the attacker to cause a loss of assets within the system need to be mapped to the ATA using Boolean logic along the paths. Examining the paths leading to physical access (gate PHYSICAL), we can see how assumptions (label "A:") on safe operation can be placed within the tree. If there is no valid assumption to be used, an additional requirement (label "R:") must be defined instead. Depending on the evaluation of this assumption on access control, only one of the two inputs for gate PHYSICAL can remain as a result of the ATA.

Following the same concept, the inputs to gate LOGICAL show that allowing a connection between the control zone and untrusted networks can lead to additional, potentially extensive branches that would have to be examined. If there is no such connection, the section below gate NETWORK X can be removed, precluding logical access to the control zone in this simplified example.

Using this method, the final ATA must only contain basic events that represent either an assumption on safe operation or an ad-

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017

Besteht keine Verbindung, kann der Abschnitt ab einschließlich „NETWORK X" entfernt und der logische Zugang zur Steuerungszone in diesem vereinfachten Beispiel ausgeschlossen werden.
Der beschriebenen Systematik folgend ist sicherzustellen, dass entlang jedes Angriffspfades das jeweils letzte Element eine Annahme zum sicheren Betrieb oder eine zusätzliche Anforderung repräsentiert. Die Ergebnisse der Stufen 2 und 3 werden somit abschließend zu einem Nachweis der Vollständigkeit zusammengeführt und alle zusätzlich definierten IT-Sicherheitsanforderungen im initialen Entwurf der bahnspezifischen Risikobetrachtung ergänzt.

3 Zusammenfassung

Die Anwendung des bahnspezifischen Vorgehens gemäß DIN VDE V 0831-104 [2] liefert einen initialen Satz von IT-Sicherheitsanforderungen gemäß IEC 62443-3-3 [11] für alle Zonen und Conduits des untersuchten Systems. Durch die Erweiterung des Vorgehens um eine mehrstufige qualitative Risikobewertung kann dieser initiale Satz auf Vollständigkeit überprüft und ergänzt werden. Durch die Analyse real existierender Bedrohungen und ihrer Auswirkungen auf das System sowie die iterative Überprüfung und Ergänzung von Schutzmaßnahmen wird den Anforderungen gemäß IEC 62443-3-2 [12] entsprochen.
Die Verwendung aktueller und etablierter Datenbanken sowie die Zusammenarbeit mit IT-Experten gewährleisten, dass der spezifische Anforderungskatalog dem Stand der Technik entspricht und definierte Maßnahmen zur Reduktion bestehender Risiken geeignet sind. Durch Umsetzung der IT-Sicherheitsanforderungen im System und den entsprechenden Nachweis ist dem IT-Sicherheitsgesetz entsprechend die Grundlage für eine erfolgreiche Systemzertifizierung geschaffen. ■

ditional requirement. Hence, the results of stages 2 and 3 are consolidated to a proof of completeness for the system's protection measures. All additional requirements are then added to the initial set as defined in the railway-specific risk assessment to obtain a complete and technology-specific set.

3 Summary

The application of the railway-specific procedure according to DIN VDE 0831-104 [2] yields an initial set of IT security requirements defined by IEC 62443-3-3 [11] for all zones and conduits of the system under consideration. This initial set can be tested for completeness and extended where required, by an additional multi-stage qualitative risk assessment. Thus, the procedure presented helps fulfil the detailed requirements on threat identification and evaluation as well as an iterative revision and extension of countermeasures as defined in IEC 62443-3-2 [12].
Through cooperation with IT experts and use of well-established, up-to-date databases, the procedure presented ensures that the resulting set of requirements is state-of-the-art and all defined measures are effective in risk reduction.
Implementation of the entire set of requirements in the system and the corresponding proof can serve as a basis for a system certification as required by the IT Security Act. ■

LITERATUR | LITERATURE

[1] IEC 62443, "Industrial communication networks – Network and system security", Series of 13 Standards on Industrial Automation and Control System Security
[2] DIN VDE 0831-104, "Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443", May 2015
[3] pr EN 50129:2016, Section 6.4: "There is no doubt that IT-Security can affect not only the service but also functional safety of a signalling system."
[4] Braband, J.: „Safety trifft Security: Sicherheitsnachweis und Begutachtungsstrategien" / „Safety meets security: safety case and assessment strategies", SIGNAL+DRAHT, Heft 4/2016
[5] 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."
[6] Störtkuhl, T.: „IT-Sicherheit auf Basis IEC 62443 für elektrische Signalanlagen" / „IT safety based on IEC 62443 for electrical signalling systems", SIGNAL+DRAHT, Heft 10/2014
[7] ISO/IEC 27001: 2013, "Information technology – Security techniques – Information security management systems – Requirements", October 2013
[8] EN 50129:2003, "Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling", December 2003
[9] EU 402/2013, "EU Regulation 402/2013 on the Common Safety Methods (CSM) for risk assessment and repealing Regulation 352/2009", in effect since May 2015
[10] NIST Special Publication 800-30 Revision 1, "Information Security - Guide for Conducting Risk Assessments", September 2012
[11] IEC 62443-3-3, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels", August 2013
[12] IEC 62443-3-2 Working Draft, "Industrial communication networks – Network and system security – Part 3-2: Security risk assessment and system design", August 5 2015
[13] BSI IT-Grundschutz-Kataloge: https://www.bsi.bund.de/DE/Themen/ITGrundschutz, 04.01.2017 um 13:08
[14] MITRE Corporation Datenbanken/databases: capec.mitre.org, cwe.mitre.org, cve.mitre.org, 04.01.2017 um 13:08
[15] Bundesamt für Sicherheit in der Informationstechnik, „Bericht zur Lage der IT-Sicherheit in Deutschland 2016"/„The state of IT security in Germany 2016", https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html, 10.01.2017 um 12:53

AUTOR | AUTHOR

M.Sc. Patric Birr
RAMS Engineer
ICS AG
Anschrift / *Address:* Alt-Moabit 73, D-10555 Berlin
E-Mail: patric.birr@ics-ag.de

Homepageveröffentlichung unbefristet genehmigt für www.ics-ag.de
DVV Media Group 2017