IT-Security – Hindernis oder Herausforderung für die Systemgenehmigung?

Durch das Verschwimmen der Grenzen zwischen der Safety und der Security entstehen enorme Herausforderungen für die Genehmigung von neuen Systemen. Das Safety-geprägte Eisenbahnumfeld mit seinen Genehmigungsprozessen steht vor der großen Herausforderung, die Sicherheit des Bahnbetriebs zu gewährleisten und gleichzeitig das Potential durch die Digitalisierung und Vernetzung der Systeme und damit der hohen Relevanz der Security schnell und effizient umsetzen zu können.

Einleitung

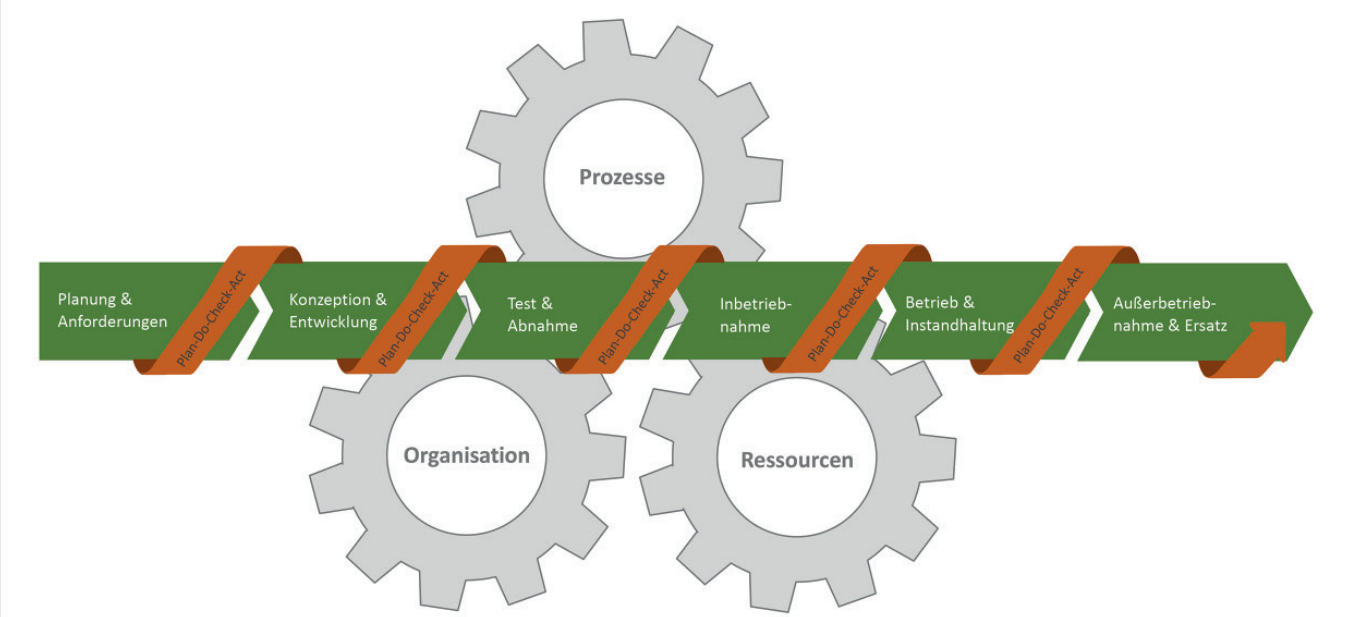
Im Eisenbahnumfeld ist IT-Sicherheit [1] kein Novum, gewinnt jedoch durch das enorme Entwicklungspotential im Kontext der Digitalisierung und Standardisierung zunehmend an Bedeutung. Durch Innovationsprogramme wie die „Digitale Schiene Deutschland" sollen die Kapazitäten und die Leistungsfähigkeit des Systems Bahn erhöht und die Effizienz gesteigert werden. Die hohe Komplexität von vernetzten Systemen schafft gleichzeitig eine enorme Angriffsfläche und eine zunehmende Skalierbarkeit der Angriffe, weshalb es gilt, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit […] [2]" zu treffen. Die sehr IT-lastigen Systeme und Anwendungen bedürfen eines immer schnelleren Entwicklungs- und Realisierungszyklus, um kurzfristig Sicherheitslücken zu schließen und grundsätzlich auf die sich verändernde Bedrohungslage zu reagieren. Gleichzeitig unterliegen diese Systeme langwierigen und komplexen Genehmigungsprozessen [3], die nur einen beschränkten Handlungsspielraum für stetige und zum Teil auch kurzfristige Anpassungen der IT-Security gewähren. Dieser Artikel beleuchtet das Spannungsfeld zwischen der schnelllebigen Security, der Einbettung dieser in die Systemgenehmigung und zeigt Handlungspotentiale auf.

1: Ganzheitliche Betrachtung der Security mit der Berücksichtigung von Prozessen, Ressourcen und der Organisation

Master of Science Brenda Reichert
Consultant
quattron management consulting gmbh
brenda.reichert@quattron.com

Berücksichtigung von Security-Anforderungen entlang des System-Lebenszyklus

Bei der Betrachtung von security-relevanten (IT-) Systemen besteht oftmals eine starke Technologiefokussierung, welche die Erfüllung der Sicherheitsanforderungen gewährleisten soll. Die eingesetzte Technologie sollte dabei jedoch nur als Mittel zum Zweck angesehen werden, die lediglich einen Teilbereich der Sicherheitsbetrachtung abdeckt. Mithilfe des Risikomanagementprozesses (an das Unternehmen angepasst, gemäß ISO 27005 [4]) werden Schwachstellen identifiziert und Risiken abgeleitet, die anschließend bewertet und in Form von Maßnahmen behandelt werden. Dieser Prozess sollte dabei nicht nur auf die Technologie angewendet werden, sondern darüber hinaus auf alle Facetten – Ressourcen, Prozesse und die Organisation selbst –, mit dem Ziel, das höchste Maß an Sicher-



2: Die Sicherheitsbetrachtungen mittels des Risikomanagementprozesses (orange) wird als ein kontinuierlicher Prozess betrachtet (Plan-Do-Check-Act), der entlang der Lebenszyklusphasen (grün) überprüft und integrativ auf die Bereiche Prozesse, Ressource und Organisation (grau) angewendet werden muss

heit zu erreichen (Bild 1). Hinsichtlich der Ressourcen sind neben den materiellen und immateriellen auch personelle zu berücksichtigen. Darüber hinaus sind bei den Prozessen Management-, Kern-, Unterstützungs- und Begleitprozesse zu unterscheiden und in der Organisation selbst u. a. die Organisationsformen zu betrachten. Ein Beispiel im Rahmen der personellen Ressourcen ist das häufig unterschätzte Thema des Risiko- und Sicherheitsbewusstseins im Management, bei Mitarbeitern und auch externen Dienstleistern. Durch die fehlende Definition von Sicherheitsschwerpunkten und -Zielen bzw. auch der Risikobereitschaft und Tragfähigkeit werden individuelle Lösungen aufgesetzt, die mit unterschiedlichen und oft unabgestimmten Sicherheitsniveaus verknüpft sind.

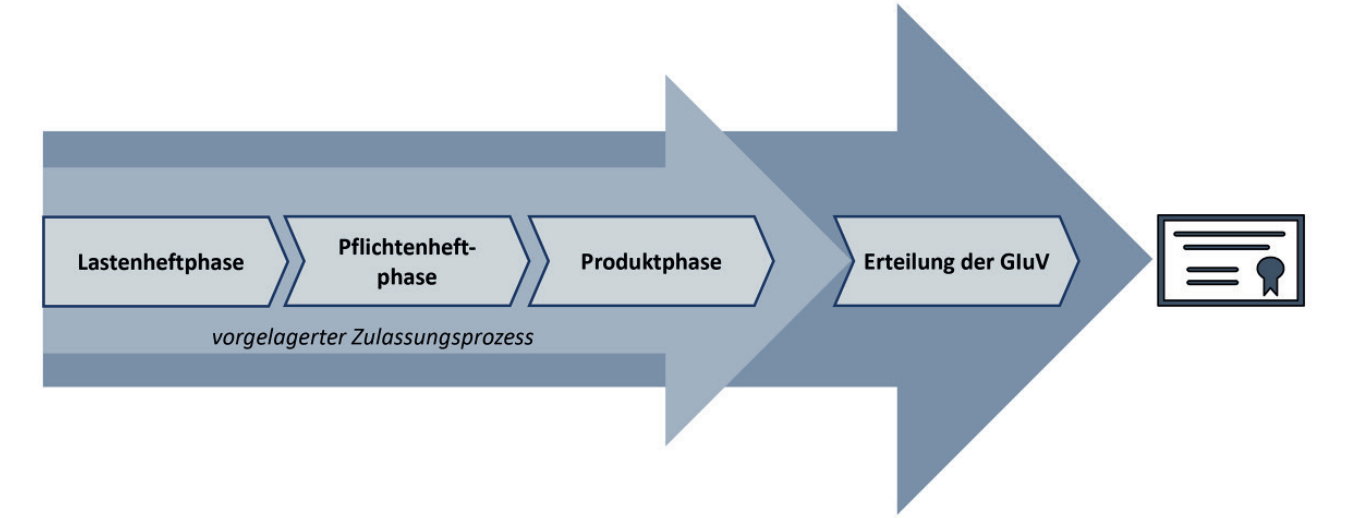
Neben der vollumfänglichen Betrachtung der beschriebenen Bereiche – Prozesse, Ressourcen und Organisation – spielt der Lebenszyklus von Systemen bei der Security-Betrachtung eine entscheidende Rolle. Anforderungen, Bedrohungen oder auch Schwachstellen können sich im Laufe des System-Lebenszyklus verändern. Eine nachträgliche Betrachtung der Risiko- bzw. Sicherheitsansätze kann durch die nur temporäre Abdeckung (bis zur finalen Lösung) von Risiken zu hohen Kosten führen, die darüber hinaus rückläufige Anpassungen, wie z. B. der Systemanforderungen, in allen Lebenszyklusphasen erfordern. Aus diesem Grund ist eine frühzeitige Implementierung der übergreifenden Security-Aspekte Voraussetzung für einen vollumfänglichen und integrativen Sicherheitsansatz. Dabei ist eine stetige Evaluierung (bspw. nach dem Deming- oder PDCA-Zyklus) der Inhalte des Risikomanagementprozesses unabdingbar, um Sicherheit (im Sinne der Security) jederzeit gewährleisten zu können (Bild 2).

Mit der in Kraft getretenen Eisenbahn-Inbetriebnahmegenehmigungsverordnung [5] (EIGV) wurden neue Regelungen für das Inverkehrbringen und Inbetriebnehmen von Bestandteilen des Eisenbahnsystems verbindlich. Zudem weisen erste Entwürfe der zukünftigen „Sektorleitlinie für die Zulassungsbewertung von Signal-, Telekommunikations- und Elektrotechnischen Anlagen“ [6] darauf hin, dass die Erteilung einer Genehmigung zum Inverkehrbringen und Verwenden (GluV) eine Zulassungsbewertung im Sinne der Entwicklungsphasen Lastenheft (LH), Pflichtenheft (PH) und Produkt voraussetzt (Bild 3). Die EIGV bzw. auch die „Verwaltungsvorschrift für die Neue Typzulassung von Signal-, Telekommunikations- und Elektrotechnischen Anlagen“ [7] (VV NTZ) behandeln die Bewertung der „Sicherheit im Eisenbahnsystem“ [8] im Sinne der Safety, wozu Systeme der Signal- und Telekommunikationstechnik einen maßgebenden Beitrag leisten.

Die Safety, die den sicheren Betrieb des Systems mit dem Schutz seiner Umgebung (Mensch, Umwelt) darstellt, ist klar von der Security zu unterscheiden, die im Bahnumfeld den Betrieb vor äußeren Einflüssen schützt, also das System vor der Umgebung schützt (z. B. durch bewusste Manipulation). Im Rahmen der Bewertung und Nachweisführung besteht grundsätzlich das Ziel, die Security von der Safety zu entkoppeln, da es Anforderungen bzw. Änderungen aus Sicht der Security gibt, die keinen Einfluss auf die Safety haben und damit nicht die Genehmigung des Gesamtsystems gefährden. Die Betrachtung von Security-relevanten Systemen ohne direkten Einfluss auf die Safety ist jedoch nicht unbedeutend und tritt insbesondere durch die Berücksichtigung der bestehenden komplexen Genehmigungsprozesse in den Fokus.

Herausforderungen der Schnelllebigkeit der Security im Kontext der Systemgenehmigung

Im Gegensatz zur Safety ist die IT-Sicherheit geprägt von einer dynamischen Entwicklung, da sich risikospezifische Annahmen, Bedrohungen und Schwachstellen



3: Genehmigung zum Inverkehrbringen und Verwenden (GluV) gem. EIGV mit vorgelagerter Zulassung

kontinuierlich verändern. Im Kontext der Digitalisierung und übergreifenden Vernetzung von Systemen (z. B. digitale Stellwerke) erhält die Security als inhärenter Systembestandteil einen neuen Stellenwert, auch unter der Annahme, dass Teile des Gesamtsystems selbst nicht Safety-relevant sind. Die bisherigen Zulassungs- und Genehmigungsverfahren – die fast ausschließlich die Safety betrachten – bieten einen nur beschränkten Handlungsspielraum zur Anpassung des Systems im Hinblick auf die Schnelllebigkeit der Security, die darüber hinaus mit einem hohen ressourcenbezogenen Aufwand verbunden ist. Anhand der folgenden exemplarischen Herausforderungen wird das Spannungsfeld zwischen schnelllebigen Security-Anforderungen und der Integration dieser in die Systemgenehmigung beschrieben.

Kurzfristiges Schließen von Sicherheitslücken

Schnelllebige sich verändernde Annahmen zu getroffenen Risiken und den daraus resultierenden Maßnahmen können dazu führen, dass sich Änderungen ergeben, die auf den Genehmigungsprozess wirken. Dabei ist zu unterscheiden, ob es sich um eine genehmigungspflichtige Änderung handelt, die mit einer neuen GluV einhergeht, oder um eine nicht genehmigungspflichtige Änderung, womit die bestehende GluV gültig bleibt [5].

Je größer die Deltabetrachtung im Rahmen der Änderungen und damit der erforderlichen Genehmigung ist, desto schwieriger kann die Durchführung einer kurzfristigen Maßnahme bspw. zur Behebung der Sicherheitslücke durch Patchen der Komponente, sein. Für Betreiber, Hersteller, Behörden und Gutachter bedeutet dies einen sehr ressourcenaufwendigen Prozess zur Berücksichtigung der Änderung, der darüber hinaus eine Vielzahl von notwendigen Begleitprozessen (z. B. Auswirkungsanalysen) auslöst. Resultierend hieraus werden bspw. Patches gesammelt mit dem Ziel, diese konsolidiert genehmigen zu lassen und den Prozess effizienter zu halten. Darüber hinaus kann je nach Sicherheitslücke eine verzögerte Behebung zur Beeinflussung des Gesamtsystems führen, bspw. durch Beeinträchtigung der Verfügbarkeit. Dementsprechend gestaltet sich eine Konsolidierung bei z. B. Emergency Patches schwieriger, die ein kurzfristiges Schließen einer Sicherheitslücke erfordern. Dem statischen Vorgehen im Rahmen der Genehmigung und der daraus resultierenden langen Zeitspanne bis zur Erlangung dieser, steht ein erforderlicher Handlungsspielraum zur kontinuierlichen Anpassung des Systems und der Minimierung der Risiken entgegen.

Berücksichtigung der Security im Laufe der Genehmigung

Eine weitere Herausforderung zwischen den sich wandelnden Sicherheitsbetrachtungen und der Genehmigung stellt die Berücksichtigung der Security über den gesamten Zulassungsprozess – Lastenheft, Pflichtenheft und Produkt – dar.

Die Einbettung der Security in die Zulassungsphasen eines Systems muss sich grundsätzlich von der Vorgehensweise im Rahmen der Safety unterscheiden. Die für die Safety im Bahnwesen relevante DIN EN 50126 [9] sieht eine Risikoanalyse auf Basis der Systemdefinition vor. Aus Sicht der Safety wird eine nahezu statische Umwelt für Systeme angenommen, die durch abgeleitete Risiken und Maßnahmen zu Beginn abgedeckt werden müssen, um die Umweltrisiken in der Spezifikation des jeweiligen Systems zu berücksichtigen. Aus Sicht der Security stellt sich die Umwelt jedoch als hoch volatil dar, weshalb eine frühzeitige Risikoanalyse unzureichend ist. Die Herausforderung besteht darin, dass zu einer frühen Phase der Anforderungsspezifikation (LH) oftmals noch keine vollumfängliche Systemspezifikation existiert, sondern der Ansatz verfolgt wird, die Funktionalität des Systems und die für die Integration notwendigen Schnittstellen zu beschreiben. Durch den noch offenen Lösungsraum, aufgrund beispielsweise noch nicht bekannter Anforderungen einer zukünftigen Anwendung des Systems, ist es nur schwer möglich eine vollständige Risikobetrachtung für die Security in dieser Phase durchzuführen. Daraus resultiert, dass eine vollumfängliche Security-Risikobetrachtung erst zu einer späteren Zulassungsphase sinnvoll umsetzbar ist und sich dadurch wiederum Änderungen am Design oder gar der Anforderungen ergeben können, die einen erneuten Durchlauf

des Zulassungsprozesses im Rahmen der Genehmigung unabdingbar macht.

Berücksichtigung der Security entlang des Lebenszyklus von Systemen

Um die sichere Funktionstüchtigkeit eines Systems zu bewahren, muss dieses kontinuierlich hinsichtlich der Security evaluiert werden, um die sich verändernden politischen, wirtschaftlichen und technologischen Rahmenbedingungen zu berücksichtigen. Der über die Zulassungsphasen hinausgehende Lebenszyklus von Systemen – der bspw. die Phasen des nachgelagerten Betriebs beinhaltet – muss durch Security-Betrachtungen dementsprechend fortlaufend vollständig abgedeckt werden können. Diese Abdeckung kann nur erreicht werden, wenn es nach der Genehmigung des Systems möglich ist, notwendige Änderungen (z. B. zur Anpassung der bestehenden Security-Maßnahmen) durchzuführen, die nicht gleichzeitig die Genehmigung gefährden und dadurch eine Genehmigungslücke des in Betrieb befindlichen Systems erzeugen. Daraus folgt, dass zur Inbetriebnahme des Systems das Ziel angestrebt werden muss, eine soweit vollumfängliche Genehmigung zu erwirken, welche die Durchführung von definierten Änderungen oder Erweiterungen und somit sich ändernden Security-Anforderungen erlaubt, ohne die Systemgenehmigung zu gefährden.

Handlungspotentiale zur Einbettung der Security in die Systemgenehmigung

Es ist also zu prüfen, wie die Genehmigung und vorgelagerte Zulassungsprozesse einen flexibleren Handlungsspielraum für Änderungen und Neubewertungen der Security an Systemen zulassen, ohne die Systemgenehmigung zu gefährden.

Ein Handlungsfeld ist, die Genehmigung durch neue Methoden zu flexibilisieren. Durch die Integration von Konzepten im Rahmen der vorgelagerten Zulassung können definierte Änderungen und Erweiterungen am System und damit auch eine kontinuierliche Evaluierung und Anpassung der Security erfolgen, ohne die bestehende Genehmigung zu gefährden. Dieses Vorgehen setzt voraus, dass zu jedem Zeitpunkt die Rückwirkungsfreiheit gewährleistet ist. Resultierend daraus können auch Veränderungen im System-Lebenszyklus berücksichtigt werden, die über die Zulassungsphasen hinausgehen und sich zudem auf die Prozesse, die Organisation und die Ressourcen auswirken.

Des Weiteren ist zu prüfen, inwiefern detaillierte Ergebnisdokumente aus der Security-Risikobetrachtung in die Genehmigung von Systemen einfließen sollten. Basierend darauf ist die Prüftiefe dieser Dokumente zu definieren. Möglicherweise können generische Vorgehensweisen hinsichtlich der Sicherheitsbetrachtung (Security) bewertet werden, während detaillierte Analysen (bspw. hinsichtlich dedizierter Komponenten) außerhalb der Genehmigung durch einen Security-Gutachter geprüft werden. Diese können den Behörden informativ angezeigt werden, sollen jedoch nicht direkter Bestandteil der Systemgenehmigung sein. Durch die Trennung der Security von den Zulassungsbestandteilen kann eine zeitliche Entkopplung bei Änderungen der Bedrohungslage bzw. Maßnahmen und dem kurzfristigen Schließen von Sicherheitslücken erreicht werden.

Ein weiteres Handlungspotential liegt in der Auflösung der starren Genehmigungsphasen hin zu einem agileren und iterativeren Ansatz, der zum Beispiel anhand von Entwicklungsstufen zum einen die Abstufung von Anforderungen und deren schrittweiser Umsetzung als auch die Berücksichtigung von neuen kurzfristig auftretenden Risiken ermöglicht. Dieses abgestufte Vorgehen könnte eine Erhöhung der Flexibilität in der Umsetzung und Erweiterung von Anwendungen ermöglichen und den Handlungsspielraum für Anpassungen der Security vergrößern. Hieraus resultierend könnten wesentlich schnellere Umsetzungszyklen erreicht werden, da nicht die gesamthafte Umsetzung und Inbetriebnahme von Systemen notwendig ist, sondern nur einzelne Systembestandteile schrittweise entwickelt und (in Verbindung mit Nachweisen der Rückwirkungsfreiheit) genehmigt würden. ●

Summary

IT-Security – obstacle or challenge for system approval?

Looking at the aspects of security of systems, a holistic approach is to consider which not only integrates the actual technology but also processes, resources and the organization itself. Furthermore, risk-relating requirements, threats and applied measures have constantly to be reviewed and revalued along the system life-cycle. The safety procedure within the system approval process is not transferable to security as the requirements differ significantly due to the environment and thus with regard to external influencing factors. The embedding of security requests into actual approval processes have to be designed suchlike that alterations of the threat level – along the system life-cycle and by considering resources, processes and the organization – are feasibly at short notice without endangering the system approval.

Literatur

[1] Unter „Security" wird bei einem System die IT-bezogene Sicherheit verstanden (Schutz der Daten). In Abgrenzung zielt die „Safety" auf die Betriebssicherheit (Sicherheit des Bahnbetriebs) bzw. die funktionale Sicherheit ab.
[2] IT-Sicherheitsgesetz, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015. Online unter: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf, letzter Zugriff 23.11.2020 14:35 Uhr.
[3] In diesem Artikel wird gemäß den ersten Entwürfen der Sektorleitlinie unter der (System-) Genehmigung die Genehmigung zum Inverkehrbringen und Verwenden (GluV) gemäß EIGV verstanden, die eine vorgelagerte Zulassungsbewertung im Sinne der Phasen Lastenheft Pflichtenheft und Produkt voraussetzt. Die Phasen und Inhalte sind angelehnt an die Verwaltungsvorschrift Neue Typzulassung Stufe 2 Übergangsregelung. Damit inkludiert die Genehmigung die vorgelagerte Zulassung des Systems.
[4] DIN EN ISO/IEC 27005:2018, Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheitsrisikomanagement, Beuth Verlag, Juni 2018.
[5] Verordnung über die Erteilung von Inbetriebnahmegenehmigungen für das Eisenbahnsystem (Eisenbahn-Inbetriebnahmegenehmigungsverordnung – EIGV), 26.07.2018. Online unter: http://www.gesetze-im-internet.de/eigv/, letzter Zugriff 23.11.2020 15:20 Uhr
[6] Sektorleitlinie für die Zulassungsbewertung von Signal-, Telekommunikations- und Elektrotechnischen Anlagen (Nationale Technische Vorschrift), 16.04.2020. Online unter: https://www.eba.bund.de/SharedDocs/Fachmitteilungen/DE/2020/13_2020_Pilotierung_erster_Teile_der_zukuenftigen_Sektorleitlinie_fuer_die_Zulassungsbewertung_von_STE-Anlagen.html, letzter Zugriff 23.11.2020 14:54 Uhr
[7] Verwaltungsvorschrift für die Neue Typzulassung (NTZ) von Signal-, Telekommunikations- und Elektrotechnischen Anlagen (Stufe 2: Übergangsregelung für Signalanlagen zur Anwendung bei den Infrastrukturen der Eisenbahnen des Bundes), Ausgabe 1.0, Bonn, 02.09.2013.
[8] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV), 22.04.2016, Online unter: https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf, letzter Zugriff 24.11.2020 11:37 Uhr
[9] DIN EN 50126-1:2018-10, Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS-Prozess, Beuth Verlag, Oktober 2018.