Sachstand IT-Security im Rahmen der Zulassungsbewertung

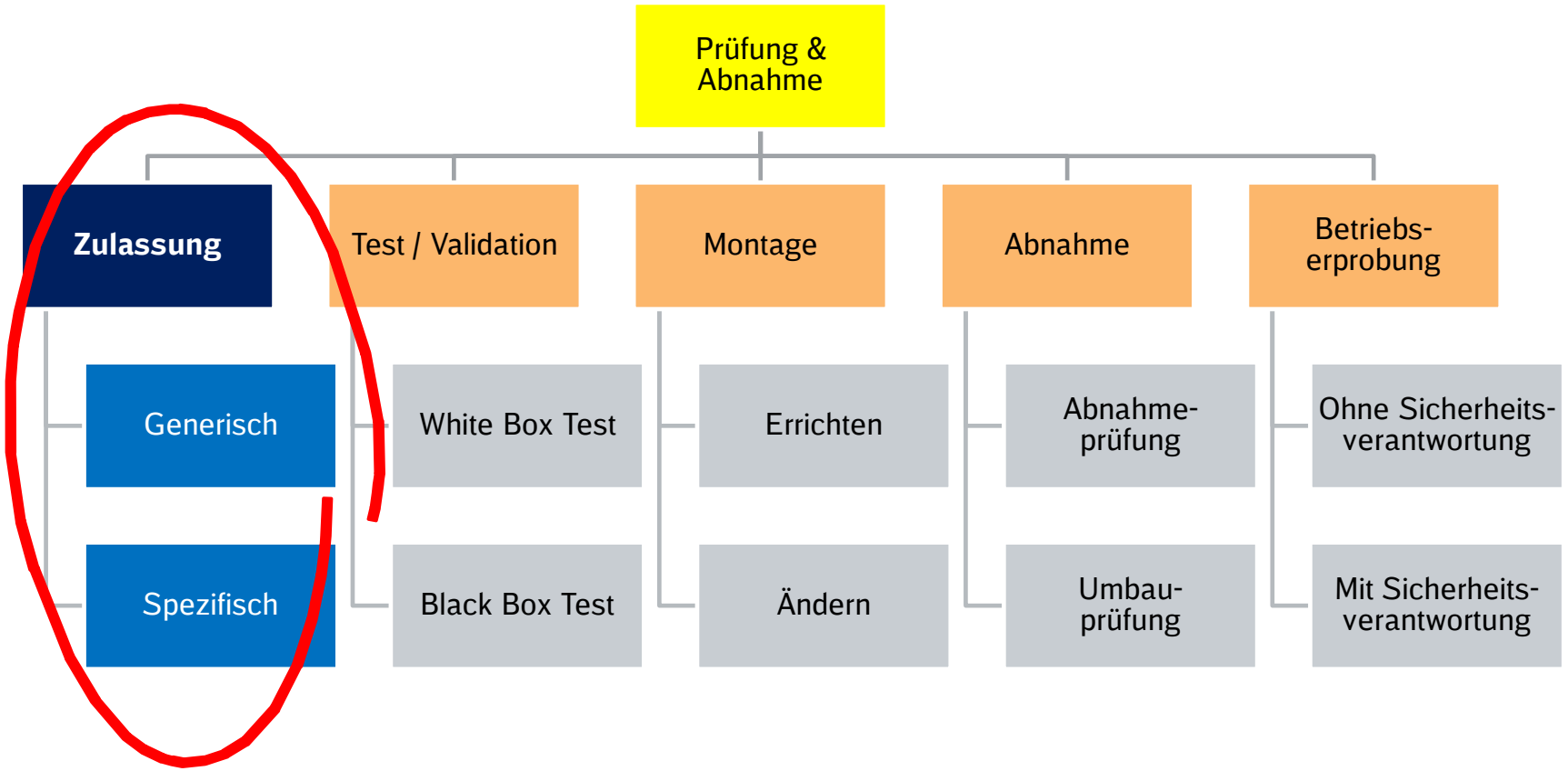
DRSS Digital Rail Summer School 2023

DB Netz AG | Dr. Matthias Drodt, Unabhängige Bewertungsstelle DB Netz | Jöhstadt | 19.09.2023

Sachstand IT-Security im Rahmen der Zulassungsbewertung

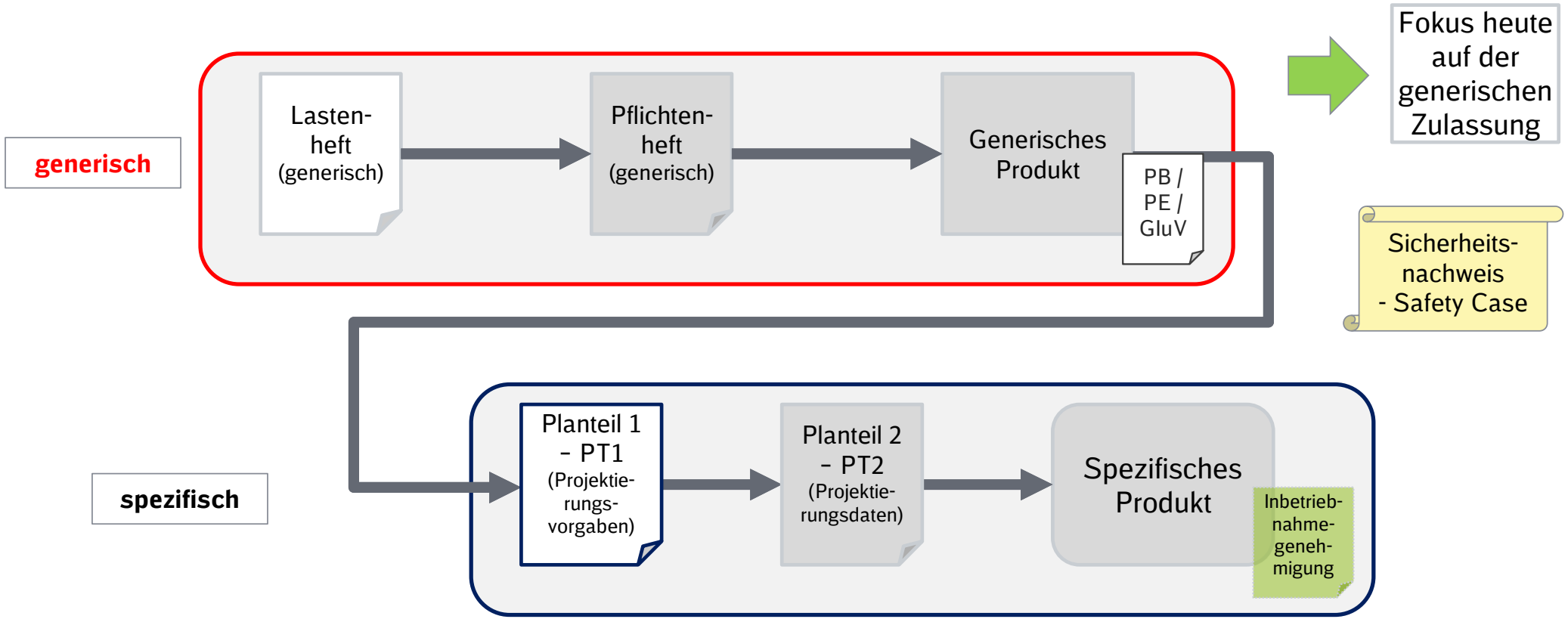
Prüfung und Abnahme von STE-Anlagen

Bestandteile und Aufgaben – Fokus auf Zulassung



Sachstand IT-Security im Rahmen der Zulassungsbewertung

Auf dem Weg zur Inbetriebnahme von STE-Anlagen: Generische und spezifische Zulassung (Bsp.: Signalanlagen)

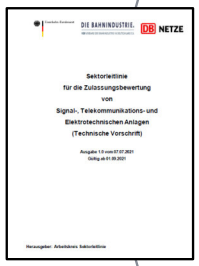


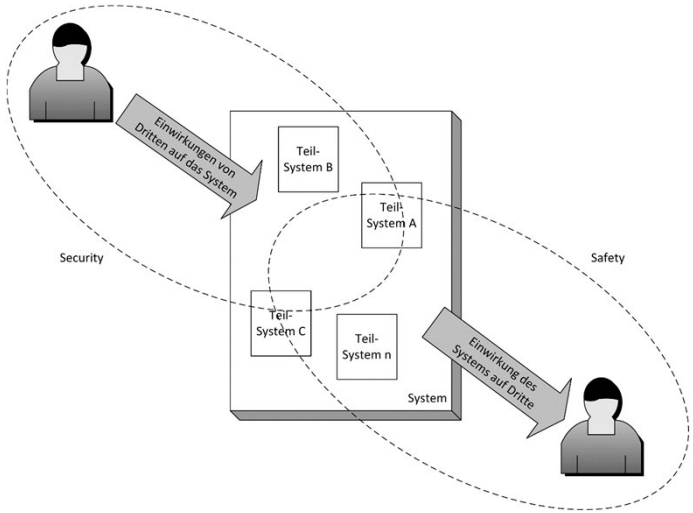
PB – Prüfbescheinigung
PE – Prüferklärung
GluV – Genehmigung zum Inverkehrbringen und Verwenden (gemäß §27 EIGV)

Sachstand IT-Security im Rahmen der Zulassungsbewertung

Notwendigkeit zur Berücksichtigung von IT-Security

- Sektorleitlinie für Zulassungsbewertung von S (Signal)-, T (Telekommunikations)- und E (Elektrotechnischen) ist seit 1.9.2021 in Kraft (Ablösung der VV-NTZ)
  - beschrieben sind generische Anforderungen an die Nachweisführung auf den Ebenen LH, PH und Produkt
  - Produktfreigaben bzw. IBN sind nachgelagert und werden von den Prozessen der SLL nicht berührt
  - Arbeitsgruppen EBA, VDB und DB





- Digitalisierung der Eisenbahn erfolgt zunehmend mittels IT vernetzter Betriebstechnik (OT)
- „Klassische“ Bahnsysteme
  - werden mittels aufwendiger Verfahren für mehrjährige Lebenszyklen zugelassen
  - fokussieren schwerpunktmäßig auf „Safety“
- Auswirkungen von IT-Security auf die funktionale Sicherheit (Safety) müssen ebenfalls betrachtet werden

Sachstand IT-Security im Rahmen der Zulassungsbewertung

Ein Blick in die relevanten Normen

IT-Security in Normen

- Die Normen für die Signaltechnik berücksichtigen im Wesentlichen Aspekte der funktionalen Sicherheit (Safety)
- Safety betrachtet nur systematische, zufällige Fehler sowie unabsichtliche Fehlhandlungen.
- Einwirkungen von „außen“/ Manipulationen, wie nicht autorisierte Zugriffe & Cyberangriffe, werden **nicht** betrachtet.
- In den RAMS-Normen der Safety (50126, …) kommt IT-Security praktisch nicht vor
- Zwei Ausnahmen:
  - **DIN EN 50129:** „… Bedrohungen der IT-Sicherheit müssen in den Prozessschritten Risikobewertung und Gefährdungs-beherrschung behandelt werden“. Maßnahmen zur Behandlung der IT-Sicherheit müssen im **Sicherheitsnachweis** … **oder** durch **Verweis** aufgeführt werden.
  - **DIN EN 50159:** Kryptographische Maßnahmen nötig für Netze der Kategorie 3 (offene Kommunikationsnetze)

Definitionen aus Norm 50126-1

Sicherheitsfunktion

- Eine Sicherheitsfunktion ist eine Funktion, deren alleiniger Zweck die **Sicherstellung der Sicherheit** ist; oder auch als funktionale Sicherheit oder Safety bezeichnet

Sicherheitsbezogene Funktion

- Ein System weist gemäß DIN EN 50126-1 eine sicherheitsbezogene Funktionen auf, wenn durch Ausfall oder Störung des Manipulationsschutzes der **sichere Bahnbetrieb gefährdet sein kann**

- IT-Security-Systeme und -Komponenten besitzen **keine** Sicherheitsfunktionen auf können aber **sicherheitsbezogene Funktionen** aufweisen (z.B. IT-Security Schwachstellen)

- Was ist regulatorisch notwendig?
  - **Kein** Sicherheitsnachweis für sicherheitsbezogene Funktionen
  - **Nachweis für IT-Security** gemäß DIN EN 50129
  - Berücksichtigung im Rahmen der **Gefährdungsbeherrschung**

Sachstand IT-Security im Rahmen der Zulassungsbewertung

Wie kann IT-Security angemessen berücksichtigt werden?

- Für STE-Funktionen ist ein dedizierter **Sicherheitsnachweis** (Safety Case) notwendig
  - In diesem wird u.a. nachgewiesen, dass alle relevanten Anforderungen erfüllt sind und die Gefährdungen auf die funktionale Sicherheit (Safety) beherrscht werden
  - Dieser wird praktisch nie geändert im Rahmen des Lebenszyklus der (generischen) Anlage

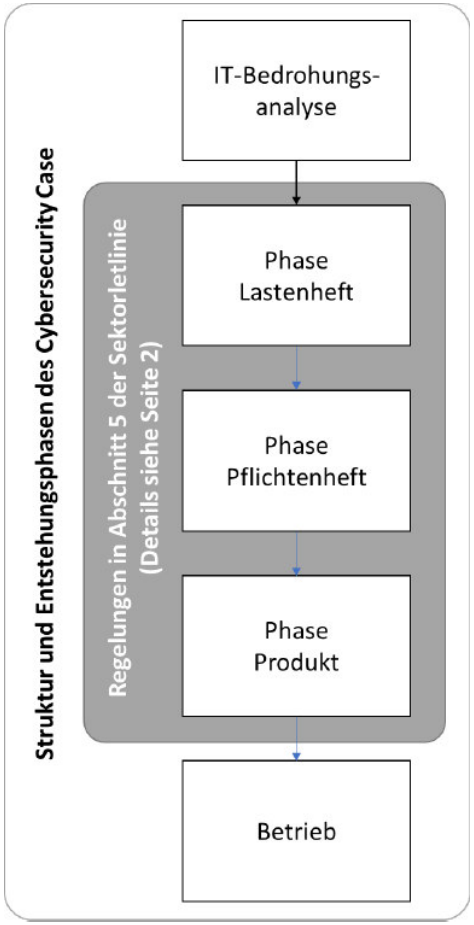
- Zur Berücksichtigung von IT-Security gibt es prinzipiell zwei Möglichkeiten
  1. Nachweisführung zusammen mit der Safety im Sicherheitsnachweis oder
  2. Eigener Nachweis für IT-Security

- **Gemeinsamer Sicherheitsnachweis**
  - **Vorteil:** Nur eine Nachweis ist erforderlich
  - **Nachteile:**
    - IT-Security bedingt stetige Anpassungen (Patches, Cyberbedrohungen, …), so dass der Sicherheitsnachweis häufig angepasst werden muss, bzw. Sonderregelungen notwendig sind
    - Know-how bzgl. IT-Security im Rahmen der Safety-Nachweisführung nicht vorhanden

- **Idee** eines eigenes Nachweisdokumentes für IT-Security

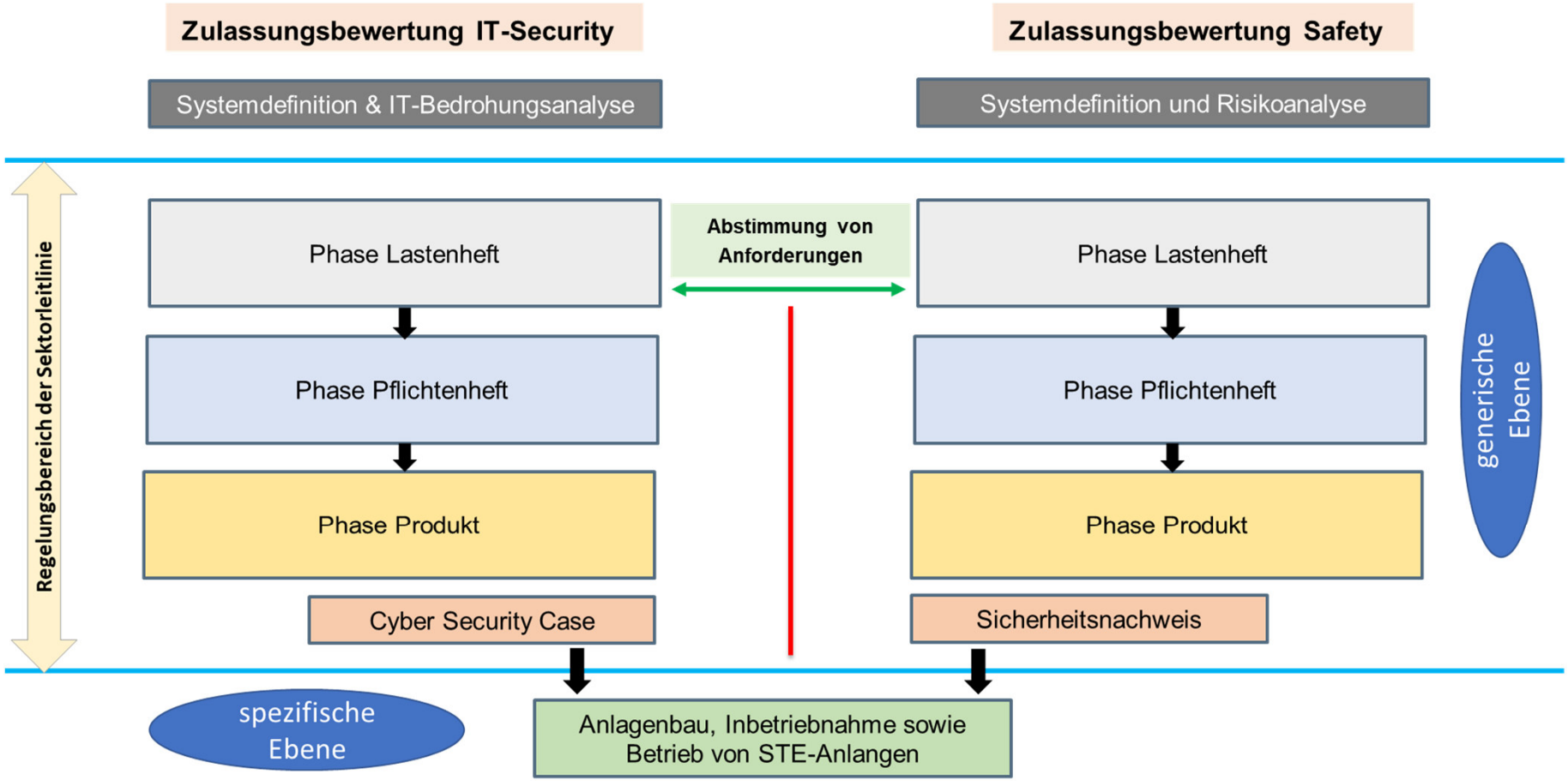
Sachstand IT-Security im Rahmen der Zulassungsbewertung
Grundsätze

- **Getrennte Nachweisführung** (IT-Security/ Safety)
  - Um in einem Gesamtsystem eine schnelle Reaktion auf IT-Security-Änderungen zu möglichen, ohne dass erstellte Sicherheitsnachweise ihre Gültigkeit verlieren
  - Prozessuale und technische (logische!) Trennung von IT-Security und Safety
- **Drei-Phasen-Modell (LH, PH, Produkt)** für IT-Security
- **Cybersecurity Case (CSC)** (Nachweis IT-Security gem. DIN CLC/TS 50701)
  - erstreckt sich über den gesamten Lebenszyklus des Betrachtungsgegenstands und
  - Nachweisführung
    - der Gefährdungsbeherrschung & Rückwirkungsfreiheit IT-Security → Safety und
    - dass alle Anforderungen der IT-Security umgesetzt sind (Schutzfunktion; „Schalenmodell“)
- **„Stand der Technik“** vs. „Anerkannte Regeln der Technik“
  - sowie Nutzung bestehender Prozesse (z.B. Schutzbedarf, IT-Risk Assessment, ISMS)



Sachstand IT-Security im Rahmen der Zulassungsbewertung

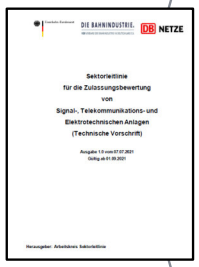
Zusammenhang Zulassungsprozesse IT-Security und Safety



Sachstand IT-Security im Rahmen der Zulassungsbewertung
Prozess für Security-Patching

- Anforderungen an einen Patch-Prozess, sodass bei einer Software-Aktualisierung (z.B. Security-Patches) **keine** neuen Nachweise, weder für IT-Security und schon gar nicht für Safety, erforderlich sind
  - Ein solcher Prozess ist Bestandteil der Zulassungsbewertung, wird durch den **Prüfsachverständigen IT-Security** geprüft und im Cybersecurity Case dokumentiert
  - Unabhängig von der Zulassungsbewertung ist ein Patching (z.B. für die Beseitigung von Schwachstellen in IT-Security Systemen und Produkten) vorzusehen; das Patching selbst benötigt **keine** Zulassungsbewertung
  - Die Freigabe für einen Patch ist damit wesentlich **kurzfristiger** möglich als die Erstellung einer PB/ PE für eine Produkt- oder Systemänderung
  - Mit der geplanten Vorgehensweise ist nicht nur ein Patch relativ schnell freigebbar, der Patch ist auch schnell auf den entsprechenden Anlagen implementierbar (**kein** Bauprozess, **kein** Abnahmeprüfer erforderlich)

Sachstand IT-Security im Rahmen der Zulassungsbewertung
Plan- und Abnahmeprüfungen



- Die nachfolgenden Bauprozesse können unverändert beibehalten werden
- Eine hinreichende Qualität der Unterlagen ist durch den **Prüfsachverständigen IT-Security (ZP),** der die Zulassungsbewertung prüft, sicherzustellen
  - Die betreffenden Unterlagen für die IT-Security (Planungs-, Projektierungs-, Prüfunterlagen, etc.) werden dahingehend geprüft und sind so gestaltet, dass diese ausreichen, um bisherige Plan- und Abnahmeprüfer **ohne IT-Security-spezifische Anerkennung** für eine Anlage einsetzen zu können
  - Vom PSV IT-Security geprüft werden die Eingangsdokumente des Cybersecurity Cases (z.B. LH, Patch-Prozess), aber **nicht** der Cybersecurity Case selbst („lebendes“ stetig zu aktualisierendes Dokument)
- Damit ist der Einsatz der aktuell anerkannten Plan- und Abnahmeprüfer weiterhin möglich
  - Ohne eine dedizierte Anerkennung für IT-Security
  - Ggf. Qualifizierung bzgl. IT-Security erforderlich

Sachstand IT-Security im Rahmen der Zulassungsbewertung

Zusammenfassung

(1) IT-Security muss im Rahmen der Zulassungsbewertung berücksichtigt werden

(2) Erweiterung der Sektorleitlinie für Zulassungsbewertung für S, T und E um IT-Security

(3) Prozessmethodik / Lösungsansätze zur Integration und Aktualisierung von IT-Security-Funktionen in zuzulassenden Bahnsystemen ohne Anpassung der Safety-bezogenen Sicherheitsnachweise

(4) Prozessuale und technische (logische!) Trennung von IT-Security und Safety

(5) Fokus auf Begutachtung von Prozessen (z.B. Patch-Prozess) und weniger Einzelmaßnahmen

(6) Review-Prozess ist abgeschlossen (finale Abstimmung ausstehend)

(7) Ansätze sollten in Anwendungsprojekten verprobt werden, um ihre Praxistauglichkeit nachzuweisen

(8) Gewährleistung der Rechtssicherheit bzgl. IT-Security bei zukünftigen Inbetriebnahmen

Sachstand IT-Security im Rahmen der Zulassungsbewertung

IT-Security im Rahmen der Zulassung betrifft nicht nur den Bahnsektor
→ „Typgenehmigung“ am Beispiel der Automobilbranche

Quelle: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/230901_Branchenlagebild-Automotive.html

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.html?nn=520690

… Die Zukunft der gesamten Mobilität hängt maßgeblich von der **Cybersicherheit** ab …

… Wenn Fahrzeuge mit komplexer IT-Hard- und Software ausgestattet und **durchgehend online** sind, dann sind sie auch **anfällig für Cyberangriffe**. …

… Die Cybersicherheit ist eine wesentliche Voraussetzung für die weitere **Digitalisierung** im Straßenverkehr. Hersteller sind gemäß Vorgaben für die **Typgenehmigung** verpflichtet, die **Cybersicherheit** in der Entwicklung **zu berücksichtigen** und die Sicherheitslage für ihre Produkte fortlaufend zu beobachten.

Fragen & offene Diskussion

Vielen Dank für Ihre Aufmerksamkeit

Dipl.-Physiker
Dr. Matthias Drodt

Unabhängige Bewertungsstelle
DB Netz; I.NVS 22

Tel. +49 (0)69-265-17502
Mobil +49 (0)160-97866610
matthias.drodt@deutschebahn.com

DB Netz AG
Adam-Riese-Straße 11-13
60327 Frankfurt/ Main
www.deutschebahn.com

Fragen … ?