

Leistungsbeschreibung

Digital Freight Train Hub

Im Rahmen des CEF-Projektes
„CEF-Project 101233084 – 24-EU-TG-PioDAC / WP 6“

Inhalt

1 Projektbeschreibung	4
1.1 Projektziele	4
1.2 Beschreibung	4
1.3 Rahmenbedingungen	5
2 Leistungsbeschreibung.....	6
2.1 Funktionale Anforderungen:	6
2.1.1 Rollen- und Berechtigungskonzepte:	6
2.1.2 Verbindung und Datenkommunikation:	6
2.1.3 Sicherheit und Datenschutz	6
2.1.4 Verbindungsausfall:	7
2.1.5 Nichterreichbarkeit:	7
2.1.6 Standardisierte API:	7
2.1.7 Dashboard:	7
2.1.8 Administrationsoberfläche:	7
2.1.9 Session und Passwortregeln	7
2.2 nicht-funktionale Anforderungen (NFA)	8
2.2.1 Barrierefreiheit	8
2.2.2 Dokumentation	8
2.2.3 Erlernbarkeit	8
2.2.4 Bedienbarkeit	8
2.2.5 Feedback	8
2.2.6 Persönliche Konfigurierbarkeit	8
2.2.7 Support und Helpdesk	8
2.2.8 Authentifikation	8
2.2.9 Mehrsprachigkeit/Internationalisierbarkeit	9
2.2.10 Mandantenfähigkeit	9
2.2.11 Verantwortlichkeiten der Betriebsführung	9
2.2.12 Applikationsmanagement	9
2.2.13 Plattformbetriebsführung und Infrastrukturbetrieb	9
2.2.14 Protokollierung	9
2.2.15 Umgang des Systems mit sicherheitsrelevanten Ereignissen	9
2.2.16 Schutz vor Schadprogrammen	10
2.2.17 Portabilität/Anpassbarkeit	10
2.2.18 Browserversionen	10
2.2.19 Austauschbarkeit und Koexistenz	10
2.2.20 Umgang des Systems mit Fehlern	10
2.2.21 Anforderungen an Clusterfähigkeit	11
2.2.22 Betrieb und Wiederherstellbarkeit	11
2.2.23 Business Continuity Management	11
2.2.24 Performanz	12
2.2.25 Datenvolumen, Größe und Bestandsmengen fachlicher Objekte	12

2.2.26 Skalierbarkeit und Überlastverhalten	12
2.2.27 Accountverwaltung	12
2.2.28 Wartbarkeit und Instanzen	13
2.2.29 Systemstandort	13
2.2.30 Nachunternehmer	13
2.2.31 Ressourceneinsatz	13
3 Abkürzungsverzeichnis und Begriffserklärungen.....	14

Revision	Datum	Änderungsprotokoll	Status
0.1	05.04.2025	initial	
2.0	05.06.2025	Inkl. SBF Anforderungen	

1 Projektbeschreibung

1.1 Projektziele

Für die Testphase der Digitalen Automatischen Kupplung (im folgenden „DAK“ genannt, engl. „DAC“) werden ab vrs. 08/2027 sogenannte „Pioneer DAC Trains“ im Rahmen des CEF-Projektes „CEF-Project 101233084 – 24-EU-TG-PioDAC / WP 6“ in Betrieb gehen. Diese sollen unter realen/kommerziellen Einsatzbedingungen die Tauglichkeit des Konzepts unter Beweis stellen. Neben der mechanischen Kupplung gibt es auch eine Strom- und Datenleitung, welche die einzelnen Wagen und die Lok im Zug verbindet. Die Testphase dauert vsl. bis Ende 2028. Für diese Phase werden etwa 100 Fahrzeuge mit DAK und entsprechender IT Hardware auf den Fahrzeugen ausgerüstet.

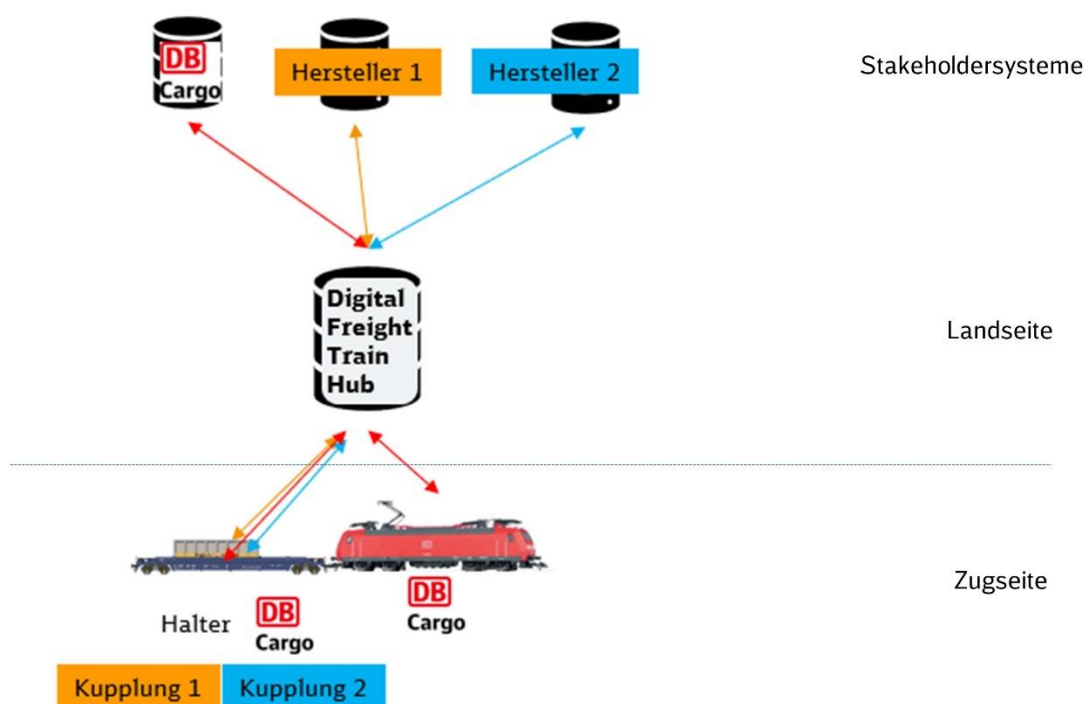
Um den Datenverkehr zwischen dem Zug und der sogenannten Landseite sicherzustellen, wird eine zentrale Datendrehscheibe benötigt, die alle Daten in Empfang nimmt und auf Basis festgelegter Verteilschlüssel die Daten an die korrekten Empfänger (siehe Grafik unten) weiterleitet. Optional sollen Steuerbefehle von den einzelnen Stakeholdern an die Wagen zurückgesendet werden können (ob diese Option genutzt wird, ist aktuell noch nicht entschieden).

Im Rahmen dieser Testphase soll die Datenkommunikation lediglich im Stand genutzt werden, während der Fahrt ist die Kommunikation deaktiviert.

1.2 Beschreibung

Für die o.g. Testphase „Pioneer DAC Trains“ möchte DB Cargo im Rahmen des europäischen CEF-Förderprojektes ein solches System als Proof of Concept aufsetzen und betreiben, um das Verhalten unter simulierten Einsatzbedingungen zu testen, Verbesserungsbedarfe zu identifizieren und Erfahrungen für den späteren Hochlauf zu sammeln. Für den weiteren Verlauf der Testphase besteht die Option, die IT auch auf dem fahrenden Zug zu testen (mindestens in einem Laborsetup – für den kommerziellen Betrieb ist die Zulassung vorausgesetzt).

Folgende Übersichtsskizze soll den geplanten Aufbau verdeutlichen:



Grafik 1: Darstellung Zugseite und Landseite

Je Fahrzeug (Lokomotiven und Wagen) gibt es ein Mobile Communication Gateway (MCG) mit Trusted Platform Module (TPM), welches Daten versenden und empfangen kann. Vom Zug in Richtung Landseite sollen im Zielzustand beispielsweise über das MCG folgende Daten versendet werden

Halterrelevante Daten (rote Pfeile in der Darstellung):

- Statusdaten für den Wagenhalter
- Standort für den Wagenhalter
- Performancedaten der Wagen

Kupplungsherstellerrelevante Daten (Pfeile in blau und orange in der Darstellung):

- Status- und Performancedaten der Kupplungen

Von der Landseite zum Zug sollen beispielsweise folgende Daten übertragen werden:

- Reihungsmeldung für die Lokomotive (Initialisierung vor Zugfahrt)
- Updates und Patches für die zentrale Steuereinheit auf den Fahrzeugen

Im Rahmen des geplanten PoC soll der Datenaustausch zwischen der Zug- und der Landseite erprobt werden. In erster Linie in Anlehnung an die Norm 61375-2-6 im Format json mit und ohne eingebetteten Inhalt.

1.3 Rahmenbedingungen

Datenhoheit bleibt unberührt. Daten zur Kupplung gehören den Kupplungsherstellern, Daten zum restlichen Fahrzeug dem jeweiligen Halter. Dies gilt auch für den PoC.

Der Proof of Concept soll erste Einblicke in das Zusammenspiel zwischen Fahrzeugen und Landseite geben. Er wird im Umfang aber nicht annähernd dem Zielzustand entsprechen. Dieser Zielzustand wird in mehreren Schritten in der Migrationsphase erreicht. Dabei steigen jeweils die Zahl der kommunizierenden Fahrzeuge/Assets sowie die Anforderungen an die Hardware und die Security kontinuierlich an.

Erwartet wird die Aufteilung in folgende Kosten/Aufwände:

- Kosten Entwicklung PoC
- Kosten laufender Betrieb PoC je Monat
- Kosten Weiterentwicklung und Betriebskosten bei Skalierung von 100 auf bis zu 60.000 Assets und Upgrade auf SIL4
- Kosten Weiterentwicklung und Betriebskosten bei Skalierung von 60.000 auf bis zu 800.000 Assets bei SIL4
- Für die beiden letztgenannten Szenarien zusätzlich bitte noch die Kosten für Übernahme der Rechte und Hardware (bzw. Betrieb auf eigener Hardware)

Um im Rahmen der Testphase unterschiedliche Szenarien simulieren zu können, soll für die im Folgenden beschriebenen Funktionen eine Möglichkeit (bspw. separate „Kommandozentrale“ im Adminbereich) vorhanden sein, diese separat zu deaktivieren bzw. wieder zu aktivieren.

2 Leistungsbeschreibung

2.1 Funktionale Anforderungen:

2.1.1 Rollen- und Berechtigungskonzepte:

In der Datendrehscheibe selbst (in der Darstellung „Digital Freight Train Hub“ - DFTH genannt) soll auf Basis eines Rollen- und Berechtigungskonzeptes sichergestellt werden, dass die Daten der Fahrzeuge nur bei den jeweiligen Fahrzeughaltern (den Eigentümern) ankommen und Daten der unterschiedlichen Kupplungshersteller auch nur dort ankommen. Für die jeweils anderen Stakeholder sollen die Daten nicht verfügbar sein. Die Zuordnung soll auf Basis einer Kennung im Header oder im Dateinamen erfolgen (**dies kann sich allerdings noch im Laufe der Diskussionen im Projekt ändern**).

Rollen:

- Administrator (je einer von DBC und von AN)
- Stakeholder (Sender bzw. Empfänger auf der Landseite, welcher i.d.R. EVU, Halter oder Industriepartner)

2.1.2 Verbindung und Datenkommunikation:

- Die Verbindung zwischen Zug und Datendrehscheibe sowie Datendrehscheibe und dem Gateway zu DB Cargo soll im Einklang mit den Vorgaben des „FDFT Link“ umgesetzt werden (siehe Anhang 1 „Auszug D3.3 FDFT Link Gateway“). Die genauen Spezifikationen zur Verbindung zu DB Cargo werden mit dem Auftraggeber abgestimmt.
- Die Verbindung soll für bidirektionalen Datenaustausch ausgelegt sein.
- Die Verbindung soll über das öffentliche Mobilfunknetz erfolgen.
- In Anlehnung an IEC 61375-2-6 sollen die Datenpakete in beide Richtungen im Format JSON versendet werden, individuell eingebetteter Content ist möglich.

2.1.3 Sicherheit und Datenschutz

Folgende Anforderungen hinsichtlich Security und Safety müssen erfüllt sein:

- Das System muss alle Anforderungen des IT-Sicherheitsgesetzes 3.0 erfüllen, insbesondere durch die Implementierung aktueller technischer und organisatorischer Maßnahmen zum Schutz vor Cyberangriffen sowie durch die regelmäßige Überprüfung und Protokollierung sicherheitsrelevanter Ereignisse.
- Für die Kommunikation soll eine End-to-End Verschlüsselung genutzt werden, das TPM im MCG dient als Speicherort für alle notwendigen Daten. Die Datenpakete sind verschlüsselt, die Verschlüsselung wird durch die zentrale Rechneinheit auf den Fahrzeugen selbst umgesetzt.
- Die Mindestanforderungen an kryptographische Verfahren sind gemäß DB-interner Vorgaben (siehe Anhang 2 Kryptografie) umzusetzen. Das genutzte Verfahren wird in Absprache mit dem Auftraggeber gewählt.
- Nutzung von IP/TCP/HTTPs/MQTT/SSL/TLS (wie in IEC 61375-2-6 beschrieben),

- SL3 (wie in IEC 62443-3-3 beschrieben)
- SIL2.

2.1.4 Verbindungsausfall:

Die Datenpakete sollen für den Fall eines Verbindungsausfalls zwischen Datendrehscheibe und Stakeholder auf der Landseite für 24h zwischengespeichert werden. Für den Fall, dass eine benötigte Information für den Zug (Use Case „Zugreihungsmeldung“) nicht von der Datendrehscheibe an den Zug weitergegeben werden kann, soll die Regelung von 2.1.5 in Kraft treten.

2.1.5 Nichterreichbarkeit:

Bei Nichterreichbarkeit (sowohl auf der Landseite wie auf der Zugseite) soll regelmäßig alle 2 Minuten ein Versuch zur Wiederherstellung der Verbindung gestartet werden.

2.1.6 Standardisierte API:

Die Anbindung der Stakeholder auf der Landseite an die Datendrehscheibe soll mittels standardisierter API erfolgen.

2.1.7 Dashboard:

Für den Zeitraum des Betriebs soll in einem für die Administratoren zugänglichen Dashboard eine graphische und statistische Aufbereitung folgender Informationen erfolgen:

- aktive Wagen
- inaktive Wagen
- verlorene Datenpakete
- Karte mit den Standorten der Wagen
- zurückgelegte Wegstrecke

2.1.8 Administrationsoberfläche:

- Für den Zeitraum des Betriebs soll es eine Administrationsoberfläche geben, über die von DB Cargo weitere Test Stakeholder für die Weiterleitung eingerichtet werden können.
- Die Adminoberfläche soll eine zentrale Verwaltung und Konfiguration aller angeschlossenen Geräte/Assets ermöglichen. In Absprache mit dem Auftragnehmer soll die Option bestehen, Geräte/Assets hinzufügen, bearbeiten, entfernen und deren Einstellungen komfortabel anpassen zu können.

2.1.9 Session und Passwortregeln

- Für Administrationsoberfläche und Dashboard soll jede Session nach 15 min. ohne Benutzeraktivität Status „Ausgeloggt“ bekommen.

Passwörter müssen bei technischen Konten/Servicekonten (bspw. Maschine zu Maschine) spätestens alle 12 Monate gewechselt werden. Die Komplexität von Passwörtern ist mindestens gemäß den folgenden Richtlinien zu gestalten:

- Mindestens 12 Zeichen
- Keine trivialen Passwörter
- Keine Passwörter, die den Anwendungsnamen enthalten
- Mindestens ein Großbuchstabe, ein Kleinbuchstabe, eine Zahl und ein Sonderzeichen
- Keine Doppelnutzung von Passwörtern

Die jeweils geltenden Vorgaben für sichere Passwörter und PINs werden systemseitig erzwungen.

- Die Zuteilung von Passwörtern an Benutzer erfolgt in einem geordneten Verfahren. Soweit diese initial vergeben werden, sind diese nur temporär, höchstens aber 14 Tage gültig. Benutzer werden ferner gezwungen, diese nach der ersten Verwendung zu ändern.

2.2 nicht-funktionale Anforderungen (NFA)

2.2.1 Barrierefreiheit

Da die Datendrehscheibe keine Interaktion mit Nutzern vorsieht, muss keine Barrierefreiheit berücksichtigt werden. Ausnahme: für den Adminzugang und die Bedienung der in der Leistungsbeschreibung unter 2.1.7 und 2.1.8 genannten Funktionen gilt WCAG 2.2 AA gemäß EU2019/882.

2.2.2 Dokumentation

Für die fachliche Betriebsführung sowie für Administratoren werden die notwendigen Informationen zusammengefasst zur Verfügung gestellt. Da es keine Enduser gibt, wird keine Dokumentation dafür benötigt. Die Dokumentation wird durch den Auftragnehmer erstellt und steht zur Inbetriebnahme zur Verfügung.

2.2.3 Erlernbarkeit

Es gibt keine Bedienung durch User, daher kein Aufwand an dieser Stelle. Aufwand für administrative Zwecke sollte die üblichen Anforderungen an eine/n Administrator/in nicht übersteigen. Für administrative Zwecke soll ein Tutorial erstellt werden, je nach Aufwand soll vom Auftragnehmer eine Einführungsveranstaltung organisiert werden.

2.2.4 Bedienbarkeit

Da keine Bedienung durch User erfolgen soll, gibt es keine Anforderungen an die Bedienbarkeit. Ausnahme: für die Aufgaben der Administration sollen die notwendigen Schritte zur Fehlersuche und -behebung möglichst einfach und intuitiv erfolgen können.

Die Bedienung der in der Leistungsbeschreibung unter 7) und 8) genannten Funktionen soll den gängigen Standards der einfachen und intuitiven Bedienung entsprechend implementiert werden.

2.2.5 Feedback

Es wird keine Feedbackfunktion zur Anpassung und zur Weiterentwicklung benötigt.

2.2.6 Persönliche Konfigurierbarkeit

Da es keine Enduser gibt, ist dieser Punkt nur für die Adminfunktion relevant. In Abstimmung mit dem AN kann dies umgesetzt werden.

2.2.7 Support und Helpdesk

Der Auftragnehmer stellt einen Support für den Zeitraum des Testbetriebs zur Verfügung. Die jeweiligen Zeitfenster werden in Abstimmung mit DB Cargo festgelegt und finden innerhalb der üblichen Arbeitszeiten zwischen 09:00 und 17:00 Uhr statt.

Der Auftragnehmer stellt die entsprechenden Kontaktdaten (Telefonnummer, E-Mailadresse) für die Notfallkommunikation zur Verfügung.

2.2.8 Authentifikation

Die Anmeldung und Authentifikation der Administratoren erfolgen direkt am System. Jeder Admin hat einen eigenen Account. Eine Zwei-Faktor-Authentifikation soll genutzt werden.

Die sichere Ablage der Autorisierungsdaten liegt in der Verantwortung des Auftragnehmers.

2.2.9 Mehrsprachigkeit/Internationalisierbarkeit

Die Benutzeroberfläche für den Adminzugang soll in Deutsch und in Englisch verfügbar sein. Für eine zukünftige Entwicklung sollen auch weitere Sprachen berücksichtigt werden (bspw. Französisch, Italienisch, Spanisch).

2.2.10 Mandantenfähigkeit

Wird benötigt – für die Testphase mindestens zwei Mandanten: DB Cargo und einen Dummystakeholder für Testzwecke. Weitere Mandanten sollen durch einen DB Cargo Admin angelegt werden können (Siehe auch 2.1.8).

2.2.11 Verantwortlichkeiten der Betriebsführung

- Die Fachliche Betriebsführung umfasst:
 - Das fachliche Benutzermanagement (Anlegen / Löschen von fachlichen Benutzern, Zuordnung von Rollen und Rechten)
 - Konfiguration fachlicher Parameter
 - Die Behandlung von besonderen fachlichen Fehlersituationen
 - Überwachung der fachlichen Logs
 - Anwenderunterstützung
- Die Fachliche Betriebsführung erfolgt durch den Auftragnehmer.

2.2.12 Applikationsmanagement

Es sollen keine zusätzlichen Applikationen auf der Datendrehscheibe installiert werden.

2.2.13 Plattformbetriebsführung und Infrastrukturbetrieb

Die Plattformbetriebsführung (Server und Datenbanken) sowie der Infrastrukturbetrieb liegen in der Verantwortung des Auftragnehmers. Server und Verarbeitung der Daten sollen in der EU verortet sein.

2.2.14 Protokollierung

Es findet eine Protokollierung folgender Daten statt:

- Performanz-, Durchsatz-, Fehler- und Überlast-Daten der Datendrehscheibe
- Anzahl übertragener Datenpakete
- Systemanomalien (bspw. untypisch hohes Übertragungsvolumen, massenhaft fehlerhafte Logins der Adminaccounts, sonstige DOS-ähnliche Attacken, etc.)
- Fehlerbehebungszeiten
- Fehlerdaten je Fahrzeug/Location

Es ist sichergestellt, dass Administratoren keine Befugnis erhalten, die Protokollierung ihrer eigenen Aktivitäten zu ändern oder zu löschen.

2.2.15 Umgang des Systems mit sicherheitsrelevanten Ereignissen

Sicherheitsrelevante Ereignisse, die die Anwendung beeinträchtigen können, werden protokolliert und an DB Cargo übermittelt.

Der Umgang mit Sicherheitsvorfällen bei der Anwendung ist definiert und dokumentiert. Der Ablauf der Dokumentation, das generelle Vorgehen bei Sicherheitsvorfällen und alle internen sowie externen Ansprechpartner sind den relevanten Personen bekannt.

Die Auslöser sowie die Behandlung des Sicherheitsvorfall werden dokumentiert. Alle relevanten Personen sowie eine zentrale Stelle werden über Sicherheitsvorfall informiert. Nach Bewertung und

Beseitigung des Sicherheitsvorfall werden Maßnahmen eingeleitet, um die Folgen zu beseitigen oder den Wiedereintritt des Sicherheitsvorfalls zu vermeiden.

Sicherheitsrelevante Ereignisse sind u. a.

- An- und Abmeldevorgänge
- Erstellung, Änderung oder Löschung von Benutzern und Erweiterung der Berechtigungen
- Verwendung, Erweiterung und Änderungen von privilegierten Zugriffsberechtigungen
- Nutzung von temporären Berechtigungen
- das Aktivieren, Stoppen und Pausieren der Protokollierung

2.2.16 Schutz vor Schadprogrammen

Es soll eine technische Lösung (bspw. Malware- /Virenschutz, Intrusion Detection System (IDS) Intrusion Prevention System (IPS)) zum Schutz von Schadprogrammen verwendet werden.

2.2.17 Portabilität/Anpassbarkeit

Es werden keine Anforderungen an Anpassbarkeit gestellt.

2.2.18 Browserversionen

Die GUI für den Adminzugang und das Dashboard soll für die jeweils aktuelle Version von MS Edge verfügbar sein.

2.2.19 Austauschbarkeit und Koexistenz

Es bestehen keine Anforderungen hinsichtlich Austauschbarkeit und Koexistenz.

2.2.20 Umgang des Systems mit Fehlern

- Es wird ein monatlicher Servicebericht erstellt und an DB Cargo versendet mit Auflistung aller Fehler/Vorfälle des vorherigen Monats.
- Fehler werden intern protokolliert und an den betroffenen Schnittstellen bekannt gegeben.
- Meldungen zu Fehlern müssen eindeutig auf den Fehler referenzieren (z.B. Benennung des Feldnamens).
- Meldungen zu Fehlern müssen Ursachen der Fehler angeben (z.B. Übertragungsfehler, falsches Format, Fehlerdiagnose für Telematikgeräte etc.)
- Die Datenkonsistenz wird beim Auftreten eines Fehlers durch die Standardmechanismen der verwendeten Referenzarchitektur / der Baupläne oder des Kaufprodukts sichergestellt.
- SLA-relevante Fehler, die z.B. durch Hardwareausfälle oder Fehler in lizenzierter Software (z.B. Oracle) auftreten, werden von der Betriebsführung erkannt, behoben und der fachlichen Betriebsführung per monatlichen Servicebericht berichtet.
- Fehler, auf die das System speziell reagieren muss:
 - Übertragungsfehler auf Grund von Netzwerkproblemen
 - Abgelehnte Übertragungen auf Grund von Format, Dateigröße etc.
 - untypisch hohes Übertragungsvolumen
 - massenhaft fehlerhafte Logins der Adminaccounts

- sonstige DOS-ähnliche Attacken
- Datenbankprobleme

2.2.21 Anforderungen an Clusterfähigkeit

Die Datendrehscheibe soll ein Clusterfähig sein, um die Funktionen wie:

- Lastverteilung: System soll automatisch regulieren
- Redundanz und Failover: für die Testphase der DAK nicht erforderlich, aber für einen späteren Zielzustand erforderlich.
- Fehlertoleranz soll durch geeignete Maßnahmen (beispielweise RAID System) gewährleistet werden.

2.2.22 Betrieb und Wiederherstellbarkeit

- Betriebszeit: 24/7
- Entstörung: 9/5
- Maximale Reaktionszeit: innerhalb von 60 min
- Verfügbarkeit/Kalenderjahr: mindestens 99,9%
- RTO (recovery time objective, maximale Störfallzeit): 4 Stunden
- RPO (recovery point objective, maximal akzeptierter Datenverlust): 5 Stunden
- Daten sollen für einen Zeitraum von 24 Stunden zwischengespeichert werden, um Probleme bei der Verbindung ausgleichen zu können. Einen Datenverlust durch Ausfall der Datendrehscheibe entsteht insofern, als dass dann keine Informationen zwischen den Zügen und der Landseite ausgetauscht werden können. Diese Verbindung muss nach Wiederherstellung der Datendrehscheibe wieder hergestellt werden.
- Aufgelaufene Daten müssen dann sequenziell abgearbeitet werden.
- Seitens des Auftragnehmers wird ein detaillierter Plan zum Wiederanlauf aufgestellt und mit dem Auftraggeber besprochen.
- Die Durchführung von Datensicherungen erfolgt mindestens einmal wöchentlich, wird überwacht und ist zusammen mit der Wiederherstellung dokumentiert. Der Zugriff auf die Datensicherung ist auf autorisiertes Personal beschränkt. Sicherungsdatenträger und Wiederherstellungsverfahren werden regelmäßig geprüft. Die regelmäßige Datensicherung umfasst mindestens die folgenden Elemente:
 - Liste der zugelassenen Sender (sowohl von der Landseite wie auch von der Zugseite)
 - Liste der zugelassenen Empfänger (sowohl auf der Landseite wie auch auf der Zugseite)
 - Verbindungsdaten
 - Nutzerkonten
 - Konfiguration

Weitere werden in Abstimmung zwischen Auftragnehmer und DB Cargo aufgenommen.

2.2.23 Business Continuity Management

Es soll ein Notfallplan aufgestellt werden, welcher die festgelegten Schritte im Falle eines Ausfalls bis zum Wiederanlauf darstellt.

Notfallpläne werden regelmäßig (mindestens jährlich) oder nach wesentlichen organisatorischen oder umgebungsbedingten Veränderungen überprüft, aktualisiert und getestet.

Der angestrebte Wiederanlauf nach Ausfall soll nach spätestens 4 Stunden abgeschlossen sein. Ein manueller Notbetrieb ist möglich, führt aber zu einem unerwünschten manuellen Mehraufwand, welcher den Fahrplan der betroffenen Züge massiv gefährdet.

2.2.24 Performanz

Relevante Aktionen

Login Admin	< 1 sec
Logout Admin	< 1 sec
Empfängerermittlung Datenpaket Zug -> Land	< 1 sec
Empfängerermittlung Datenpaket Land -> Zug	< 1 sec

2.2.25 Datenvolumen, Größe und Bestandsmengen fachlicher Objekte

Die geschätzte Datenmenge im Regelbetrieb (d.h. keine Updatepakete oder Patches) sind 20MB pro Stunde.

2.2.26 Skalierbarkeit und Überlastverhalten

Das System soll dynamisch skalieren und bei drohender Überlast selbstständig zusätzliche Ressourcen aktivieren. Bei einer festgelegten Grenze von 500% soll der Prozess gestoppt werden, um ungebremste Skalierung zu vermeiden.

2.2.27 Accountverwaltung

Die Verwaltung der Accounts (im Falle der Datendrehscheibe lediglich Adminzugänge) obliegt dem Auftragnehmer und hat nach den aktuell gängigen Standards der Informationssicherheit (ISO 27001) zu erfolgen.

Die Vergabe, Änderung, und der Entzug von Konten und Berechtigungen erfolgt im Vier-Augen-Prinzip unter Sicherstellung einer Funktionstrennung zwischen Antragsteller und Führungskraft.

Konten werden nach Ablauf ihrer Gültigkeit oder bei begründetem Verdacht auf missbräuchliche Nutzung umgehend gesperrt.

Beim Wechsel oder der Beendigung des Arbeitsverhältnisses werden Berechtigungen innerhalb der Anwendung entzogen bzw. angepasst.

Bei Anwendungen mit hohem Schutzbedarf werden Konten, welche länger als drei Monate nicht genutzt wurden, gesperrt. Die Sperrung ist zu dokumentieren.

Bei Änderungen im Beschäftigungsverhältnis eines Mitarbeiters (Kündigung, Versetzung, längerer Abwesenheit/Sabbatical/Elternzeit) wird Berechtigungen zeitnah, spätestens aber 10 Tage nach Inkrafttreten entzogen bzw. deaktiviert.

Der Zeitpunkt und der Grund der Entsperrung des Kontos sind nachvollziehbar dokumentiert.

Es wurde definiert und dokumentiert, welche Berechtigungen und Rollen der Anwendung nicht gemeinsame vergeben werden dürfen. Weiterhin wird organisatorisch oder technisch unterbunden, dass diese Rollen und Berechtigungen gemeinsam vergeben werden. Segregation of Duties (SoD), auch bekannt als „Prinzip der Funktionstrennung“ soll auch für die Adminkonten gelten.

Privilegierte Berechtigungen sind von nicht-privilegierte Berechtigungen organisatorisch sowie technisch zu trennen.

Durch die Vergabe von privilegierten Berechtigungen dürfen keine ungewollten, kritischen Kombinationen, die gegen das Prinzip der Funktionstrennung verstoßen (z. B. Zuweisen von Berechtigungen zur Administration der Datenbank wie auch des Betriebssystems), entstehen.

Im Berechtigungskonzept ist die Verwendung und Zuordnung von privilegierten Berechtigungen beschrieben, begründet und dokumentiert.

Privilegierte Berechtigungen sind entsprechend gekennzeichnet.

Administratoren sollen nicht in der Lage sein, ihre in den Logdateien gespeicherten Vorgänge und Aktionen zu löschen.

Es sind in Absprache mit DB Cargo geeignete Vertreterregelungen sowie erforderliche Qualifikationen für Nutzer mit privilegierten Rechten festgelegt.

2.2.28 Wartbarkeit und Instanzen

- Um Mängel und Ursachen von Ausfällen ermitteln zu können, sollen Logdateien angefertigt und über einen Zeitraum von zwei Wochen gespeichert werden und einsehbar sein.
- Für die Pflege und Weiterentwicklung des Systems sollen in regelmäßigen Abständen Wartungsdokumentationen erstellt werden.
- Zur regelmäßigen Überprüfung des Sicherheitsstatus soll ein Penetrationstest mindestens 1x jährlich durchgeführt werden.
- Produktiv- und Nicht-Produktiv- (Test-, Entwicklung-, Schulungs- etc.) Umgebungen sind voneinander getrennt.

2.2.29 Systemstandort

Der/Die Server sollen in der EU stehen und die Daten sollen ebenfalls nur in der EU verarbeitet werden.

2.2.30 Nachunternehmer

Etwaige Nachunternehmer in der Erbringung der Leistung sind vom Dienstleister benannt. Die Anteile von Services oder Produkten, die durch Nachunternehmer erbracht oder hergestellt werden, sind definiert.

2.2.31 Ressourceneinsatz

Es sind ausreichend personelle wie auch technische Ressourcen für den sicheren Betrieb der Anwendung eingeplant und verfügbar.

3 Abkürzungsverzeichnis und Begriffserklärungen

AN	Auftragnehmer
DAK	Digitale Automatische Kupplung
DAC	Digital Automatic Coupling/Coupler
FDFT	Full Digital Freight Train
FDFT Link	Verbindung zwischen dem FDFT und der Datendrehscheibe
HTTPS	Hypertext Transfer Protocol Secure
MCG	Mobile Communication Gateway
Pioneer DAC Train	Testverkehr mit DAK unter realen Bedingungen im kommerziellen Betrieb
TPM	Trusted Platform Module
CEF	Connecting Europe Facility