EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system work better for society.

Leitfaden

Anforderungen an das Sicherheitsmanagementsystem für die Sicherheitsbescheinigung oder die Sicherheitsgenehmigung

	Erstellt von	*Validiert von*	*Freigegeben von*
Name	S. D'ALBERTANSON C. LAGAIZE DAVOINE A. PATACCHINI	M. SCHITTEKATTE	B. ACCOU
Position	Projektleiter	Teamleiter	Referatsleiter
Datum	26.4.2021		
Unterschrift			

Dokumenthistorie

Version	*Datum*	*Anmerkungen*
1.0	29.6.2018	Für die Veröffentlichung bestimmte endgültige Fassung
1.1	10.7.2018	Abbildung 2 aktualisiert, Bildunterschrift zu Abbildung 3 hinzugefügt
1.2	4.9.2018	Abbildung 2 aktualisiert
1.3	26.4.2021	Durch die Anpassungen werden Änderungen der Bestimmungen der Verordnung (EU) 2019/779 (ECM-Verordnung) berücksichtigt, geeignete Verknüpfungen mit dem Modell der Agentur zur Sicherheitskultur im europäischen Eisenbahnverkehr und den Erfahrungen hergestellt sowie einige allgemeine Korrekturen am Text vorgenommen.

Das vorliegende Dokument ist eine rechtlich nicht bindende Leitlinie der Europäischen Eisenbahnagentur. Sie lässt die von der geltenden EU-Gesetzgebung vorgesehenen Entscheidungsfindungsprozesse unberührt. Zudem fällt eine bindende Interpretation des EU-Gesetzes unter die alleinige Zuständigkeit des Gerichtshofs der Europäischen Union.

0 Einleitung

Ein Antragsteller einer einheitlichen Sicherheitsbescheinigung oder einer Sicherheitsgenehmigung muss die Einhaltung der relevanten Anforderungen des Sicherheitsmanagementsystems nachweisen, die in der Verordnung (EU) 2018/762 festgelegt sind. Zu diesem Zweck muss er der nationalen Sicherheitsbehörde oder, wo zutreffend, der Eisenbahnagentur der Europäischen Union (im Folgenden auch „Agentur“ genannt) Belegdokumente vorlegen, aus denen hervorgeht, dass er ein eigenes Sicherheitsmanagementsystem (SMS) in Übereinstimmung mit Artikel 9 der Richtlinie (EU) 2016/798 eingeführt hat.

Das vorliegende Leitliniendokument ist ein fortschreibendes Dokument, das in Zusammenarbeit mit nationalen Sicherheitsbehörden und Vertretern des Sektors entwickelt wurde und das fortlaufend auf Basis der Rückmeldungen von Anwendern verbessert werden und die während der Umsetzung der Richtlinie (EU) 2016/798, der zugehörigen gemeinsamen Sicherheitsmethoden (CSM) und anderer relevanter EU-Verordnungen gewonnenen Erfahrungen berücksichtigen soll.

0.1 Zweck des Leitfadens

Das vorliegende Leitliniendokument soll Folgendes bereitstellen:

- *den Zweck hinter allen Bewertungsanforderungen in Anhang I und II der obigen CSM, die – wo erforderlich – durch Erläuterungen mit spezifischen Angaben zu bestimmten Begriffen oder Ideen in den Anforderungen ergänzt wurden;*
- *eine Angabe, welche Nachweise eine Organisation bereitstellen kann, um die von den obigen CSM geforderte Konformität zu belegen;*
- *eine veranschaulichende Liste mit Beispielen für Nachweise, die in Anträgen für eine einheitliche Sicherheitsbescheinigung oder Sicherheitsgenehmigung bei der Durchführung einer Bewertung beobachtet oder die vom Antragsteller als Referenzmaterial für seinen Antrag verwendet werden können;*
- *veranschaulichende Referenzen und Standards, die als Hilfsmittel bei der Bewertung, Entwicklung, Einführung oder kontinuierlichen Verbesserung eines Sicherheitsmanagementsystems verwendet werden können; und*
- *Angaben, welche Probleme eventuell von einer nationalen Sicherheitsbehörde bei der Aufsicht über ein Eisenbahnunternehmen oder einen Infrastrukturbetreiber berücksichtigt werden müssen.*

Bei der Beurteilung eines Antrags auf eine einheitliche Sicherheitsbescheinigung für die Beförderung gefährlicher Güter mit der Eisenbahn kann eine nationale Sicherheitsbehörde als zuständige Behörde direkte Verantwortung tragen, indem sie entsprechende Teile des Antrags beurteilt. Alternativ kann sie durch bedarfsweise Zusammenarbeit mit einer anderen für die Beförderung gefährlicher Güter zuständigen Behörde eine Koordinierungsrolle übernehmen, indem sie für die entsprechenden Teile des Antrags bei Bedarf ihren Rat einholt.

0.2 An wen richtet sich dieser Leitfaden?

Das vorliegende Dokument richtet sich an:

- *die nationalen Sicherheitsbehörden und die Eisenbahnagentur der Europäischen Union, wenn diese die Konformität des Sicherheitsmanagementsystems des Eisenbahnunternehmens mit den relevanten Anforderungen an das Sicherheitsmanagementsystem bewerten und wenn nationale Sicherheitsbehörden eine Aufsicht durchführen;*
- *die nationalen Sicherheitsbehörden, wenn diese die Konformität des Sicherheitsmanagementsystems des Infrastrukturbetreibers mit den relevanten Anforderungen an das Sicherheitsmanagementsystem bewerten und sie eine Aufsicht nach der Vergabe durchführen; und*
- *die Eisenbahnunternehmen und Infrastrukturbetreiber (im Folgenden auch „Antragsteller" genannt), um diese bei der Entwicklung, Einführung, Beibehaltung und kontinuierlichen Verbesserung ihres Sicherheitsmanagementsystems in Übereinstimmung mit den relevanten Anforderungen an das Sicherheitsmanagementsystem (und anderen anwendbaren Sicherheitsanforderungen) zu unterstützen und um in Erfahrung zu bringen, was während der Aufsicht erwartet werden kann.*

0.3 Geltungsbereich

Diese Leitlinien schreiben nicht vor, welche Nachweise ein Antragsteller vorlegen sollte. Der wesentliche Grund hierfür ist, dass das Sicherheitsmanagementsystem jeder Organisation auf die spezifischen Risiken zugeschnitten sein sollte, die Organisationen kontrollieren müssen. Daher ist jedes Sicherheitsmanagementsystem ein einzigartiges System dokumentierter Informationen, das Angaben zu den bestehenden spezifischen Risikokontrollmaßnahmen und Systemen innerhalb einer einzelnen Organisation bereitstellt und das sich mit dem Wandel der Organisation im Laufe der Zeit entwickelt. Es wäre demnach nicht richtig, eine verbindliche Liste mit Informationen zur Verfügung zu stellen, die ein Antragsteller bereitstellen sollte. Dies würde die Bewertung zwecklos machen, da alle Anträge gleich aussehen würden, obwohl die entsprechenden Sicherheitsmanagementsysteme unterschiedlich wären.

0.4 Struktur der Leitlinien

Das vorliegende Dokument ist Teil des Kompendiums der Leitlinien der Agentur, die Eisenbahnunternehmen, Infrastrukturbetreiber, nationale Sicherheitsbehörden und die Agentur bei der Erfüllung ihrer Rollen und der Durchführung ihrer Aufgaben gemäß der Richtlinie (EU) 2016/798 unterstützen.

Abbildung 1: Kompendium für die Leitlinien der Agentur

Die in diesem Leitfaden bereitgestellten Informationen müssen durch die Leitlinien spezifischer nationaler Sicherheitsbehörden, die die notifizierten nationalen Regeln beschreiben und erläutern, die für das vorgesehene geografische Tätigkeitsgebiet gelten, und die Dokumente, die im Antrag für eine einheitliche Sicherheitsbescheinigung zur Verfügung zu stellen sind, ergänzt werden, um den Bestimmungen von Artikel 10 Absatz 3 Buchstabe b und Artikel 10 Absatz 8 der Richtlinie (EU) 2016/798 zu entsprechen (siehe

ferner *Beantragungsleitfaden der Agentur zur Ausstellung einheitlicher Sicherheitsbescheinigungen*). Für Infrastrukturmanager gelten neben diesem Leitfaden auch die Leitlinien der nationalen Sicherheitsbehörden zu den Vorgaben für Sicherheitszulassungen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2016/798.

Notifizierte nationale Regeln sind nur diejenigen Regeln, die von einem Mitgliedstaat der Kommission mitgeteilt wurden. In Übereinstimmung mit Erwägungsgrund 12 der Richtlinie (EU) 2016/798 wird erwartet, dass die Anzahl der notifizierten nationalen Regeln mit der Zeit sinken wird. Diese werden entweder durch Maßnahmen in Technischen Spezifikationen für die Interoperabilität (TSI), andere EU-Verordnungen oder Unternehmensregeln ersetzt. Unternehmensregeln oder -standards werden wie jeweils anwendbar durch die Einhaltung der Technischen Spezifikationen für die Interoperabilität in Bezug auf das Teilsystem für das Betriebs- und Verkehrsmanagement des Eisenbahnnetzes der Europäischen Union bewertet (im Folgenden auch TSI OPE genannt), wie dies in den in diesem Leitfaden erläuterten Anforderungen an das Sicherheitsmanagementsystem zum Ausdruck kommt.

Die vorliegenden Leitlinien sind in Übereinstimmung mit den Anforderungen in Anhang I und Anhang II der Verordnung (EU) 2018/762 strukturiert. In den folgenden Abschnitten wird jede Anforderung zur besseren Übersicht in einem gelben Kasten dargestellt. Wo Unterschiede zwischen den geltenden Anforderungen für Eisenbahnunternehmen und den geltenden Anforderungen für Infrastrukturbetreiber bestehen, wird für letztere der relevante Text der Anforderungen in den gelben Kästen blau hervorgehoben.

Direkte Vergleiche oder Entsprechungstabellen zwischen den Bewertungskriterien der vorherigen Verordnungen (EU) Nr. 1158/2010 und (EU) Nr. 1169/2010 sowie den Anforderungen der Verordnung (EU) 2018/762 werden in Anhang 1 dieses Leitfadens bereitgestellt. Die Tabellen umfassen außerdem gegebenenfalls einen Querverweis zu den Klauseln der High Level Structure der ISO. Diese werden bereitgestellt, um Antragstellern beim Nachweis der Konformität ihres Sicherheitsmanagementsystems mit den neuen Anforderungen zu helfen, insbesondere in Fällen, in denen dem Antragsteller bereits eine Sicherheitsbescheinigung oder eine Sicherheitsgenehmigung gewährt wurde und/oder der Antragsteller bereits ein anderes ISO-Managementsystem (z. B. ISO 9001, 14001 oder 45001) betreibt (damit diese zusammen integriert werden können), oder der Antragsteller plant, anhand dieses Modells eines zu entwickeln. Die Verwendung dieser Tabelle bietet keine systematische Annahme der Konformität mit den Anforderungen in der Verordnung (EU) 2018/762 für Organisationen, die über eine ISO-Bescheinigung verfügen.

0.5 ISO-/IEC-Richtlinien Teil 1 und konsolidiertes ISO-Beiblatt

ISO hat offizielle Prüfungshandlungen entworfen, die beim Entwickeln und Pflegen einer internationalen Norm befolgt werden müssen. In Anhang SL Anlage 2 der ISO-/IEC-Richtlinien Teil 1 und dem konsolidierten ISO-Beiblatt wird eine High Level Structure (HLS) für die Verwendung von Kerntext in jeder Managementsystemnorm eingeführt.

Anhang I und Anhang II der Verordnung (EU) 2018/762 gewährleisten eine mit der ISO-HLS kohärente Struktur, welche die Integration verschiedener Managementsysteme, die über dieselben zentralen organisatorischen Grundsätze und Anforderungen verfügen, bei denen die rechtliche Konformität und die Risikobereiche jedoch für jede Disziplin spezifisch sind (z. B. Sicherheit am Arbeitsplatz, Umwelt, Qualität), wo möglich vereinfacht.

ISO-Normen und relevante Leitlinien können Eisenbahnunternehmen und Infrastrukturbetreibern dabei helfen, ihr Sicherheitsmanagementsystem zu entwickeln (z. B. ist ISO 31000 ein allgemeines Dokument zum besseren Verständnis des Risikomanagements, ISO 31010 bietet Informationen zur Auswahl und Anwendung von Risikobewertungstechniken wie die Ausfalleffekt- und Ausfallkritizitätsanalyse, die Schnellmaßnahme, ETA und HAZOP, ISO 55000 enthält Anforderungen für die Verwaltung von Sachanlagen). Diese können

jedoch nur ihren Beitrag leisten, wenn ein fundiertes Wissen bezüglich des Kontextes der auf die Eisenbahn bezogenen Risiken vorliegt.

Wenn die Anwendung der HLS Kohärenz gegenüber den ISO-Managementsystemnormen gewährleistet, muss hervorgehoben werden, dass es sich bei den obigen CSM um Vorschriften handelt, die hauptsächlich dem Zweck der nationalen Sicherheitsbehörden oder der Agentur beim Bewerten von Anträgen für die Erteilung von Sicherheitsbescheinigungen oder Sicherheitsgenehmigungen dienen. Als solches richten sich Bewertungen für einheitliche Sicherheitsbescheinigungen oder Sicherheitsgenehmigungen gegen die Anforderungen des Sicherheitsmanagementsystems und nicht die ISO-HLS an sich. Mit anderen Worten: Die ISO-Normen basieren auf einer freiwilligen Bescheinigung, aber manche Rechtsrahmen sehen diese vor, um eine Annahme der Konformität mit den geltenden Vorschriften, die einen spezifischen Bereich regeln, bereitzustellen. Es gibt keine Bestimmung, welche die Annahme der Konformität mit den Anforderungen in der Richtlinie (EU) 2016/798 oder mit der Verordnung (EU) 2018/762 auf die ISO-Normen überträgt.

Klauseln 4 bis 10.2 der ISO-/IEC-Richtlinien Teil 1 und des konsolidierten Beiblatts 2016, Anhang SL Anlage 2, wurden neu verfasst oder mit der Genehmigung der Internationalen Organisation für Normung (ISO) angepasst. Originaltext siehe Quelldokument. Dieses Dokument kann von der Website des ISO-Zentralsekretariats angefordert werden. Das Urheberrecht bleibt bei ISO.

0.6 Zweck des Sicherheitsmanagementsystems

Zweck des Sicherheitsmanagementsystems ist es zu gewährleisten, dass die Organisation auf sichere Weise Risiken kontrolliert, die sich aus ihren Geschäftszielen ergeben, und alle Sicherheitsverpflichtungen erfüllt, die dafür gelten.

Die Übernahme eines strukturierten Ansatzes ermöglicht die Identifikation von Gefahren und die kontinuierliche Verwaltung von Risiken in Bezug auf die Tätigkeiten einer Organisation mit dem Ziel, Unfälle zu verhindern. Dieser Ansatz berücksichtigt die geteilten Risiken an den Schnittstellen mit anderen Akteuren im Eisenbahnsystem (hauptsächlich Eisenbahnunternehmen, Infrastrukturbetreiber und Personen, die für die Instandhaltung zuständig sind, aber auch alle anderen Akteure, die den sicheren Betrieb des Eisenbahnsystems potenziell beeinflussen, wie beispielsweise Hersteller, für die Instandhaltung zuständige Stellen, Halter, Dienstleister, Auftraggeber, Beförderer, Absender, Empfänger, Verlader, Entlader, Schulungszentren, usw.). Die Einführung aller relevanten Elemente eines Sicherheitsmanagementsystems auf adäquate Weise kann einer Organisation das nötige Vertrauen geben, dass es alle Risiken in Verbindung mit ihren Tätigkeiten unter allen Bedingungen kontrolliert und kontrollieren wird.

Reife Organisationen erkennen, dass eine effiziente Risikokontrolle nur durch einen Prozess erzielt werden kann, der drei kritische Dimensionen zusammenbringt: eine technische Komponente mit den verwendeten Werkzeugen und Ausrüstungen, eine menschliche Komponente von auf vorderster Front tätigen Menschen mit ihren Fähigkeiten, ihrer Ausbildung und Motivierung sowie eine organisatorische Komponente, die aus Verfahren und Methoden besteht, welche die Beziehung zwischen den Aufgaben definieren.

Folglich hat ein adäquates Sicherheitsmanagementsystem bei der Überwachung und Verbesserung aller drei Dimensionen seiner Risikokontrollmaßnahmen Erfolg. Viele Funktionen des Eisenbahn-Sicherheitsmanagementsystems sind der Managementpraxis sehr ähnlich, die durch Verfechter von Qualität, Gesundheit und Sicherheit am Arbeitsplatz, Umweltschutz und Business Excellence vorgeschlagen wird. Deshalb können die Grundsätze des guten Managements einfacher als oben angegeben integriert werden. Hierfür wird eine CSM genutzt, die auf der ISO-HLS basiert und eventuell keine komplette Neugestaltung der Organisationen erfordert, die diese Systeme bereits eingeführt haben.

Anerkanntermaßen schaffen strukturierte Managementsysteme durch das effektive Management von Schnittstellen einen Mehrwert für Geschäfte. Dies hilft bei der Verbesserung der Gesamtleistung, der Einführung von Betriebseffizienzen, der Stärkung der Beziehungen mit Auftragnehmern und

Unterauftragnehmern, Kunden und Genehmigungsbehörden sowie beim Aufbau einer positiven Sicherheitskultur.

Ein Antragsteller muss sein Sicherheitsmanagementsystem so gestalten, dass es mit den Anforderungen in Artikel 9 der Richtlinie (EU) 2016/798 übereinstimmt, um das sichere Management seines Betriebs zu gewährleisten. Zu diesem Zweck muss er die Konformität mit den Anforderungen in Anhang I und II der Verordnung (EU) 2018/762 nachweisen. Diese Anforderungen sind so ausgelegt, dass sie ein vollständiges Bild des Sicherheitsmanagementsystems der Organisation vermitteln, das einen PDCA-Kreislauf (Plan, Do, Check, Act: Planen, Umsetzen, Überprüfen, Handeln) befolgt. Der Antragsteller muss jede einzelne Anforderung sowie die Art berücksichtigen, wie diese zusammenpassen, um ein kohärentes Sicherheitsmanagementsystem zu schaffen, das die relevanten Risiken kontrolliert.

0.7 Sicherheitsmanagementsystem und Prozessansatz

Ein SMS dient dazu, die verschiedenen Stränge zusammenzuführen, die nötig sind, um ein sicheres und erfolgreiches Unternehmen zu führen. Diese Elemente umfassen die vorhandenen Mechanismen zur Einhaltung internationaler und nationaler Vorschriften und Normen, die Vorgaben auf Branchen- und Geschäftsebene, die Ergebnisse einer Risikobewertung und Good Practice bei sämtlichen Tätigkeiten des Unternehmens. Daher sollte das Sicherheitsmanagementsystem in die Geschäftsprozesse der Organisation integriert werden, jedoch nicht zu einem papierbasierten System werden, das speziell für den Nachweis der Konformität mit dem Rechtsrahmen entwickelt wurde. Das Sicherheitsmanagementsystem sollte ein lebender Satz von Vorkehrungen sein, der zusammen mit der Organisation, der er dient, reift und sich entwickelt. Der Aufbau eines SMS verlangt von einer Organisation ein Verständnis der Risiken, die sie kontrollieren muss, des rechtlichen Rahmens, in dem sie tätig ist, sowie eine eindeutige Vorstellung davon, wie eine „gute“ Leistung aussieht. In diesem Leitfaden werden die Elemente des SMS angeführt, die erfüllt sein müssen, damit die Bewertungsbehörde eine einzelne Sicherheitsbescheinigung ausstellt. Dabei ist jedoch zu beachten, dass die Qualität des SMS mehr als die Summe seiner Teile ist. Das SMS muss auch als zusammenhängendes Ganzes funktionieren, bei dem die Konformität mit jedem Teil dafür sorgt, dass das gesamte System richtig funktioniert.

Die Anforderungen, anhand derer die Bewertung eines Sicherheitsmanagementsystems beurteilt werden kann, können durch einen dokumentierten Prozess (oder ein Verfahren, usw.) erfüllt werden, aber es sollte auch eine Integration in und zwischen den verschiedenen Geschäftsbereichen der Organisation stattfinden. Die nationale Sicherheitsbehörde kann beispielsweise überprüfen, ob eine Aussage zu den verfolgten Grundsätzen vorliegt, aber sie muss auch das Engagement der Organisation prüfen, diese anzuwenden. Eine praktische Art der Umsetzung ist, von der nationalen Sicherheitsbehörde prüfen zu lassen, wie das Sicherheitsmanagementsystem auf der oberen Führungsebene überwacht und überprüft wird, wie die Mitarbeiter daran beteiligt sind und wie ihnen die Ergebnisse mitgeteilt werden. Außerdem hat die Organisation eventuell kein(e) spezifisches/n Verfahren, um sicherheitsrelevante Informationen zu verwalten, muss aber beschreiben, wie die relevanten Geschäftsteile sie adäquat verwalten (z. B. Kommunikation von sicherheitsrelevanten Informationen an den Triebfahrzeugführer).

Eine wichtige Entwicklung in Anhang I und Anhang II der Verordnung (EU) 2018/762 ist die Einführung eines Prozessansatzes. Dies wird auch in ISO-Managementsystemnormen gefördert, wobei die verschiedenen Prozesse des Managementsystems eng miteinander verbunden sind und ihr kohärenter Betrieb zum Erreichen der Ziele der Organisation beiträgt. Anhang I und Anhang II der Verordnung (EU) 2018/762 identifizieren wichtige Verbindungen zwischen Prozessen, um das Verständnis des Prozessansatzes zu erleichtern. Dies bedeutet aber nicht, dass es nur diese Verbindungen gibt oder dass sie zu Konformitätszwecken aufgezeigt werden sollen. Die Fähigkeit einer Organisation, zu zeigen, wie die Prozesse ihres Managementsystems miteinander verknüpft sind, ist ein guter Indikator für ihr Verständnis, wie ihr Managementsystem effektiv funktioniert.

Die Elemente des Sicherheitsmanagementsystems können beobachtet werden, um einen PDCA-Kreislauf anzuwenden (siehe Abbildung 2). Das PDCA-Konzept spiegelt die funktionalen Beziehungen zwischen den wichtigsten Elementen des Sicherheitsmanagementsystems wider:

- ***Planung**: Identifikation von Risiken und Chancen, Festlegen von Sicherheitszielen und Identifikation von Prozessen und Maßnahmen, die benötigt werden, um Ergebnisse gemäß der Sicherheitsordnung der Organisation zu liefern;*
- ***Betrieb**: Entwicklung, Einführung und Anwendung der Prozesse und Maßnahmen nach Plan;*
- ***Leistungsbewertung**: Überwachung und Bewertung der umgesetzten Leistung der eingeführten Prozesse und Maßnahmen hinsichtlich der Ziele und der Planung, anschließende Berichterstattung der Ergebnisse;*
- ***Verbesserung**: Ergreifen von Maßnahmen, um das Sicherheitsmanagementsystem und die Sicherheitsleistung kontinuierlich zu verbessern, um die vorgesehenen Ergebnisse zu erzielen.*

Dieser PDCA-Kernprozess wird von anderen Elementen des Sicherheitsmanagementsystems ergänzt:

- *„**Kontext der Organisation**“, der Angaben für die Planungsphase bereitstellt;*
- *„**Führung**“ als die treibende Kraft für den PDCA-Kreislauf;*
- *Verschiedene Funktionen zur „**Unterstützung**“, die sämtliche Elemente des Sicherheitsmanagementsystems stützen.*

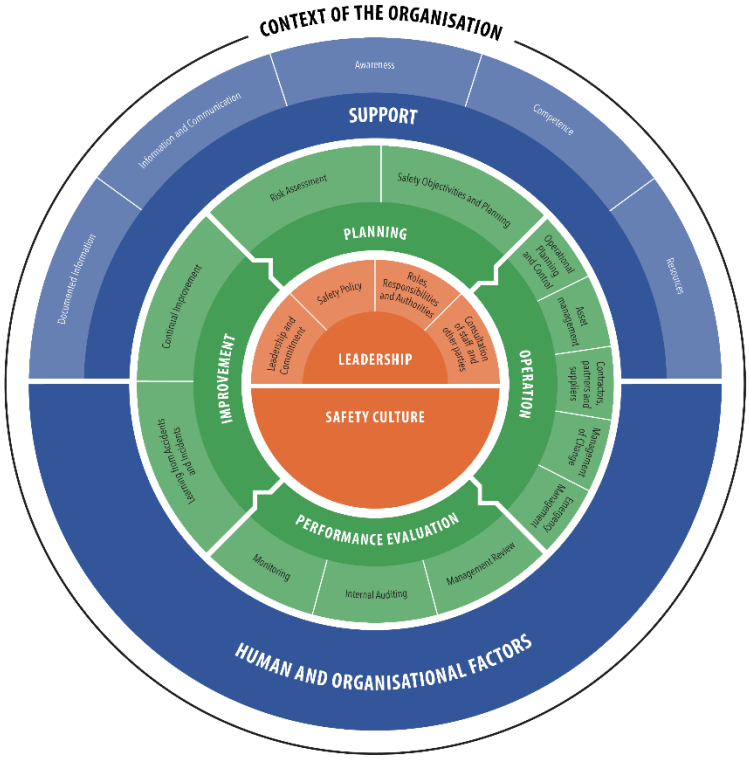

Abbildung 2: Sicherheitsmanagementsystem der Eisenbahn

0.8 Sicherheitsmanagementsystem, menschliche und organisatorische Faktoren sowie Sicherheitskultur

Menschliche und organisatorische Faktoren (Human and organisational factors – HOF) binden sozialwissenschaftliche Fachkenntnisse aus Bereichen wie Unternehmensführung, Psychologie, Soziologie, Designwissenschaft oder Politik ein, um den Studien- und Untersuchungsgegenstand zu erweitern und dabei organisatorischen, institutionellen, kulturellen oder politischen Faktoren Rechnung zu tragen, die die Sicherheit beeinflussen. Der International Ergonomics Association, dem internationalen Dachverband der Fachgesellschaften für Arbeitswissenschaft, zufolge ist Ergonomie (oder menschliche Faktoren) die wissenschaftliche Disziplin, die sich mit dem Verständnis von Interaktionen zwischen Menschen und anderen Elementen eines Systems befasst, und der Beruf, der Theorie, Grundsätze, Daten und andere Gestaltungsmethoden anwendet, um das menschliche Wohlbefinden und die allgemeine Systemleistung zu optimieren (siehe ferner die Definition in Artikel 6).

Der Begriff „organisatorisch“ wurde eingeführt, um die übergreifende organisatorische Analyseebene und nicht nur die individuelle Ebene hervorzuheben, obwohl sich Organisationen offenkundig aus Einzelpersonen zusammensetzen.

Die Untersuchung menschlicher und organisatorischer Faktoren ist Teil des Sicherheitsmanagementprozesses, wonach eine (positive) Sicherheitskultur Teil des Ergebnisses (oder Outputs) dieses Prozesses ist.

Die Sicherheitskultur ist ein Satz an Verhaltens- und Denkmustern, die größtenteils innerhalb einer Organisation hinsichtlich des Managements der Hauptrisiken in Verbindung mit ihren Tätigkeiten geteilt werden. Dies deutet natürlich darauf hin, dass innerhalb einer Organisation mehrere Kulturen beteiligt sein können, die auf Themen wie berufliche Rolle, Geografie oder anderen gemeinsamen Werten basieren. In diesem Sinne wird die Sicherheitskultur täglich durch die Interaktionen zwischen Akteuren im Zusammenhang mit einer Organisation entwickelt, die sich an ihre Umgebung anpassen muss (siehe ferner die Definition in Artikel 6).

Eine direkte Art, die Sicherheitskultur zu beschreiben, ist jedoch, sich die Faktoren anzusehen, die zu dem Verhalten beitragen. Das Sicherheitsmanagementsystem stellt die Grundlage bereit: Durch die Definition der angenommenen Arbeitsbedingungen und des erwarteten Ergebnisses definiert eine Organisation eine bevorzugte Arbeitsweise und die technischen Mittel, um die Tätigkeit zu unterstützen. Um sicher zu arbeiten, wird eine Organisation nachteilige Situationen frühzeitig erkennen und Regeln sowie Mittel einführen, um mit diesen umzugehen. Darüber hinaus gibt es die „menschliche Welt“ der Organisation: Eigenschaften, Gefühle, Bedeutungen und die Beziehungen, die Interaktionsmuster zwischen Personen in der Organisation so bedingen, dass diese ihr Denken und Handeln beeinträchtigen. Diese kulturelle Seite bezieht sich hauptsächlich auf „ungeschriebene Regeln, die das Verhalten und die Entscheidungen einer Gruppe von Personen lenken“. Zusammen erleichtern (oder hemmen) der strukturelle und kulturelle Teil der Organisation die organisatorische Leistung.

Es besteht jedoch ein hohes Risiko, dass ein allzu bürokratischer Ansatz des Sicherheitsmanagements der betrieblichen Realität widerspricht und dazu führt, dass das Sicherheitsmanagementsystem ein Eigenleben entwickelt, d. h. es werden sämtliche Bemühungen für die Entwicklung, die Pflege und sogar die Bereitstellung von Nachweisen für ein dokumentiertes System aufgewendet und dabei die betrieblichen Vorgaben ignoriert, die erforderlich sind, damit es wie vorgesehen funktioniert, sodass gravierende Inkohärenzen zwischen der „gewünschten Arbeit“ und der „geleisteten Arbeit“ entstehen.

Auf der anderen Seite besteht die Möglichkeit, das Sicherheitsmanagementsystem als Instrument einzusetzen, um einen positiven Einfluss auf die Sicherheitskultur einer Organisation auszuüben und die physische Umgebung sowie das Verhalten der Mitarbeiter auf eine Weise zu beeinflussen, welche die Sicherheit fördert und erleichtert. Es ist die Übereinstimmung zwischen dem strukturellen und dem kulturellen Teil der Organisation, die schließlich Sicherheit schafft. In diesem Kontext sollten menschliche und

organisatorische Faktoren eine wichtige Rolle spielen. Um Personen beim Ausführen ihrer Aufgaben zu helfen, muss eine Organisation verstehen, wie Menschen (mit ihren Fähigkeiten und Einschränkungen) Sachanlagen (z. B Ausrüstung des Fahrerhauses des Triebfahrzeugführers oder eine Mensch-Maschine-Schnittstelle) und Spezifikationen nutzen, um Probleme zu lösen, und dieses Wissen anschließend bei der Konzeption der Arbeitsumgebung berücksichtigen. Dasselbe gilt für Regeln und Vorschriften: Solange die Arbeiter, die diese umsetzen, bei der Entwicklung der Arbeitsverfahren nicht berücksichtigt werden, werden sie gezwungen sein, Regeln zu brechen, um ihrer Arbeit nachzugehen, wenn Widersprüche oder Konflikte auftreten.

Die Agentur hat gemeinsam mit Vertretern des Sektors das Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr (ERSCM), das in Anhang 4 dargestellt ist, entwickelt (Übersetzungen der Leitlinien zum ERSCM sind in allen EU-Sprachen auf der Website der Europäischen Eisenbahnagentur zu finden, deren Link in Anhang 4 zu finden ist). Im gesamten Dokument werden nach Bedarf die menschlichen und organisatorischen Faktoren sowie die Grundeigenschaften erläutert, die bekanntermaßen zu einer positiven Sicherheitskultur beitragen. Zudem stellen Anhang 4 und Anhang 5 dem Leser weitere nützliche Informationen bereit, damit die Organisation ihre eigenen Strategien entwickeln kann. Die Leser werden daran erinnert, dass es ihnen freisteht, ihre eigenen Modelle zur Sicherheitskultur zu nutzen, um ihren rechtlichen Verpflichtungen gerecht zu werden.

0.9 Sachdienliche Nachweise und dokumentierte Informationen

Das vorliegende Dokument enthält Angaben zu den Nachweisen, die der Antragsteller (d. h. das Eisenbahnunternehmen oder der Infrastrukturbetreiber) bei der Beantragung einer Sicherheitsbescheinigung oder Sicherheitsgenehmigung bereitstellen muss; hierbei wird aus den oben genannten Gründen nicht spezifiziert, was genau vorgelegt werden muss. Für jede Anforderung wird zusammen mit dem angemessenen Verweis auf die Anforderung eine Angabe zu den Nachweisen gemacht, die der Antragsteller bereitstellen soll. Im Folgenden werden Beispiele aufgeführt, wie diese Nachweise in der Praxis aussehen können. Es sollte anerkannt werden, dass die Beispiele als Verständnishilfe angegeben werden, nicht die einzigen Mittel zum Nachweis der Konformität sind und keine komplette Liste der möglichen Alternativen darstellen. Darüber hinaus muss verstanden werden, dass der Antragsteller bei der Beantragung beschreiben muss, wie er jede der Anforderungen erfüllt. Der Sachverständige oder der Antragsteller kann nach der Art der vorgeschlagenen Informationen zur Klärung oder Bekräftigung, wie diese erfüllt werden, fragen oder diese als Nachweis bereitstellen. Für den Antragsteller und den Sachverständigen ist der wichtigste Punkt für jede Anforderung, sicherzustellen, dass die Aussagen zur Konformität mit Referenzen verknüpft sind, die erläutern, wo weitere Nachweise gefunden werden können, welche die getroffenen Aussagen unterstützen. In dem Abschnitt mit Beispielen für jede der Anforderungen wird versucht, anzugeben, wie dieses referenzierte Material aussehen könnte.

Referenzen, die für Antragsteller bei der Vorbereitung ihrer Anträge nützlich sein sollten, werden im Anschluss an diesen Abschnitt aufgeführt. Im letzten Abschnitt unter jedem Element wird schließlich versucht, die nötige Verbindung zur Aufsicht herzustellen. Hier wird eine Angabe zu Problemen gemacht, die ein Sachverständiger eventuell für die Aufsichtsteams der nationalen Sicherheitsbehörden als Bereiche von Interesse, die zur Prüfung der Vollständigkeit des Sicherheitsmanagementsystems verwendet werden können, hervorheben möchte.

Gleichermaßen wird in dem in ISO-Managementsystemnormen sowie in Anhang I und Anhang II der Verordnung (EU) 2018/762 aufgeführten Ansatz außer in bestimmten Fällen nicht die Art der Nachweise (z. B. Verfahren) vorgeschrieben, die vom Antragsteller erwartet werden. Die dem Antragsteller überlassene Flexibilität zielt darauf ab, es der Organisation zu ermöglichen, die Vorkehrungen ihres Sicherheitsmanagementsystems auf eine Weise zu präsentieren, die der Art des Geschäfts entspricht und für seine Größe angemessen ist. Darüber hinaus wird dabei geholfen, von einem papierbasierten

Konformitätstest zu einer Bewertung eines lebenden, sich entwickelnden Systems überzugehen, welches die Sicherheitsmanagementvorkehrungen eines Unternehmens so widerspiegelt, wie sie in der Praxis bestehen.

Der Begriff „dokumentierte Informationen“ wurde als Teil der ISO-HLS und der gängigen Begriffe für Managementsystemnormen eingeführt. Die Definition von „dokumentierten Informationen“ befindet sich in *ISO 9000 Abschnitt 3.8*. Dokumentierte Informationen können verwendet werden, um Nachrichten zu übermitteln, Nachweise für Pläne und tatsächliche Handlungen zu erbringen oder Wissen zu teilen. Sie umfassen insbesondere Dokumente und Aufzeichnungen, wie beispielsweise Verfahren, Sitzungsprotokolle, Berichte, förmliche Mitteilungen von Zielen, Ergebnisse, Vereinbarungen, Verträge, usw. Weitere Erläuterungen finden sich in den *Leitlinien zu den Anforderungen an dokumentierte Informationen der ISO 9001:2015*, die auf der ISO-Webseite verfügbar sind.

Der Begriff „Verfahren“ sollte nicht auf das Vorhandensein eines eigenständigen Dokuments hindeuten, das die Verwaltung eines einzelnen Elements des Sicherheitsmanagementsystems exklusiv und umfassend behandelt, oder die Entwicklung eines spezifischen Satzes neuer Dokumente anfordern. Wenn in diesem Dokument auf ein Verfahren Bezug genommen wird, bedeutet dies dokumentierte Informationen (z. B. Papierdokumente), in denen der anzuwendende Prozess festgelegt ist. Wenn auf einen Prozess Bezug genommen wird, bezieht sich dies auf die Mittel zur Durchführung von Aufgaben oder zum Erreichen von Zielen, die eventuell in einem Verfahren festgelegt sind oder nicht.

0.10 Querverweise auf andere EU-Verordnungen und geltende gesetzliche Anforderungen

Verweise auf andere EU-Verordnungen stärken die Einheitlichkeit zwischen den verschiedenen Rechtstexten, während sie die Zusammenhänge zwischen ihnen bestätigen. Die Vorkehrungen des Sicherheitsmanagementsystems sollten, sofern nicht anderweitig angegeben (z. B. spezifische Übergangsbestimmungen, verzögerte Beantragung), stets mit den geltenden Rechtstexten übereinstimmen. Wenn eine EU-Verordnung aufgehoben wird, werden normalerweise sämtliche Verweise als Verweise auf die neue Verordnung angesehen (wenn diese dort angegeben wird).

Alle Eisenbahnunternehmen und Infrastrukturbetreiber müssen eine Reihe von Verpflichtungen erfüllen, die über diejenigen hinausgehen, die sich ausschließlich mit Sicherheitsangelegenheiten befassen. Einige dieser anderen Verpflichtungen werden einen direkten oder indirekten Einfluss darauf haben, wie die Organisation ihren Sicherheitsverantwortlichkeiten durch ihr Sicherheitsmanagementsystem gerecht wird, wie beispielsweise der Einhaltung der Gesetzgebung, die sich aus der Richtlinie (EU) 2016/797 (Interoperabilitätsrichtlinie) ergibt, oder der Sicherheitsrelevanz der von den Infrastrukturbetreibern im Rahmen der Richtlinie (EU) 2012/34 für die Eisenbahnunternehmen bereitgestellten Dienstleistung. Deshalb muss das Sicherheitsmanagementsystem, das die Eisenbahnunternehmen und die Infrastrukturbetreiber verwenden, um Sicherheitsrisiken Rechnung zu tragen, so organisiert sein, dass die Einhaltung solcher anderer rechtlicher Verpflichtungen gegebenenfalls gewährleistet ist.

Inhaltsverzeichnis

1 Kontext der Organisation

1.1 Regulatorische Anforderung

1.1 Die Organisation muss:

(a) die Art, den Umfang und den Bereich ihrer Tätigkeiten beschreiben;

(b) ernste Sicherheitsrisiken ihres Eisenbahnbetriebs ermitteln, unabhängig davon, ob er von der Organisation selbst oder von Auftragnehmern, Partnern oder Zulieferern unter ihrer Kontrolle durchgeführt wird;

(c) Beteiligte – auch außerhalb des Eisenbahnsystems – ermitteln (z. B. Regulierungsstellen, Behörden, Eisenbahnunternehmen, Infrastrukturbetreiber, Auftragnehmer, Zulieferer, Partner), die für das Sicherheitsmanagementsystem relevant sind;

(d) rechtliche und sonstige Anforderungen in Bezug auf die Sicherheit der unter Buchstabe c genannten Beteiligten ermitteln und aufrechterhalten;

(e) sicherstellen, dass die Anforderungen gemäß Buchstabe d bei der Entwicklung, Umsetzung und Aufrechterhaltung des Sicherheitsmanagementsystems berücksichtigt werden;

(f) den Anwendungsbereich des Sicherheitsmanagementsystems beschreiben, wobei die betroffenen bzw. nicht betroffenen Geschäftsbereiche anzugeben und die Anforderungen gemäß Buchstabe d zu berücksichtigen sind.

1.2 Für die Zwecke dieses Anhangs bezeichnet der Begriff

(a) „Art“ in Bezug auf den Eisenbahnbetrieb von Infrastrukturbetreibern die Charakterisierung des Betriebs anhand seines Anwendungsbereichs, einschließlich Entwurf und Bau der Infrastruktur, Infrastrukturinstandhaltung, Verkehrsplanung, Verkehrsmanagement und Verkehrssteuerung, sowie anhand der Nutzung der Eisenbahninfrastruktur, einschließlich konventioneller und/oder Hochgeschwindigkeitsstrecken, Personen- und/oder Güterbeförderung;

(b) „Umfang“ in Bezug auf den Eisenbahnbetrieb von Infrastrukturbetreibern den Umfang des Betriebs, der durch die Länge der Eisenbahnstrecken und die überschlägige Größe des Infrastrukturbetreibers hinsichtlich der Zahl der im Eisenbahnbereich tätigen Mitarbeiter gekennzeichnet ist.

1.2 Zweck

Der Antragsteller sollte gegenüber der Behörde so genau wie möglich nachweisen, dass sein Sicherheitsmanagementsystem seinen gesamten Betrieb abdeckt. Die bewertende Behörde sollte eindeutig erkennen können, um welche Art von Betrieb es sich handelt und wie die Verwaltung durch das Sicherheitsmanagementsystem erfolgt. Der Antragsteller sollte zeigen, dass er ein klares Verständnis dafür besitzt, welche Beziehungen er mit interessierten Parteien hat sowie für die schwerwiegenden Risiken, mit denen er konfrontiert ist, wer betroffen ist und wie diesen Angelegenheiten im Sicherheitsmanagementsystem Rechnung getragen wird.

1.3 Erläuterungen

In Nummer 1.1 des vorstehenden Rechtstextes wird in der englischen Fassung bei der Anforderung an Infrastrukturbetreiber „type“ durch „character“ ersetzt (diese Änderung betrifft nicht die deutsche Fassung, da darin beide Begriffe mit „Art“ übersetzt sind); darüber hinaus wird der Begriff „Bereich“ gestrichen.

Die Anforderung „Organisation“, ihr Kontext und der Anwendungsbereich des Sicherheitsmanagementsystems **(1.1)** zielen auf ein besseres Verständnis des Geschäfts der Organisation, der Erwartungen der Interessengruppen und der Umgebung, in der die Organisation arbeitet, aus Sicht der Sachverständigen ab. Die Art der Organisation ist der Ausgangspunkt für die Bewertung; wenn diese Information am Anfang des Antrags steht, kann ein Antragsteller beschreiben, was er tut und wie seine Organisation strukturiert ist, was dem Sachverständigen wiederum Entscheidungen zur Planung seiner Bewertung ermöglicht. Wenn die Organisation beispielsweise zentralisiert ist oder verschiedene Betriebe mit weitreichender lokaler Selbstständigkeit hinsichtlich der Planung und Gestaltung ihrer Tätigkeiten umfasst oder wenn die Organisation mehr oder weniger Auftragnehmer beschäftigt, gibt es eine entsprechende Erwartung, dass die Organisation des Antragstellers und sein Sicherheitsmanagementsystem so strukturiert sind, dass die entstehenden Probleme bewältigt werden. Die Organisation sollte klar erläutern, wer ihre Auftragnehmer sind, welchen Überwachungsmaßnahmen sie unterzogen werden (siehe ferner Abschnitt 6.1) und wie die Verantwortlichkeiten für die verschiedenen Aspekte des Betriebs vom Antragsteller geregelt werden. Es sollte zudem klar sein, wie die Verantwortlichkeiten zwischen dem Sicherheitsmanagementsystem des Antragstellers und den Systemen anderer Organisationen aufgeteilt sind, zu denen es Schnittstellen gibt. Die Erläuterung des Gesamtkontextes der Organisation kann auch Aufschluss darüber geben, wie menschliche und organisatorische Faktoren verwaltet werden. Die Struktur in Abschnitt 4 der High Level Structure der ISO kann dabei helfen, die Vorbereitungsarbeit zu verstehen, die vor der Einführung des Sicherheitsmanagementsystems nötig ist. Es ist ausschlaggebend, dass der Sachverständige den Anwendungsbereich des Betriebs versteht, wenn er eine ordnungsgemäße Bewertung durchführen soll.

Die Betriebsart **(1.1. Buchstabe a)** deckt per Definition die Beförderung von Fahrgästen (mit oder ohne Hochgeschwindigkeitsverkehr) und Gütern (mit oder ohne gefährliche Güter) sowie Rangierdienste ab. Sie kann auch andere besondere Betriebsarten umfassen, wie beispielsweise das Prüfen von Fahrzeugen, den Betrieb von Fahrzeugen für die Instandhaltung der Eisenbahninfrastruktur oder den Betrieb auf Anschlussgleisen im Privatbesitz. Weitere Informationen zu Betriebsart, Betriebsumfang und geografisches Tätigkeitsgebiet finden sich im *Beantragungsleitfaden der Agentur zur Ausstellung einheitlicher Sicherheitsbescheinigungen*. Weitere Informationen zum Betrieb auf Anschlussgleisen können Anhang 3entnommen werden.

Für einen Infrastrukturbetreiber sind die Art und der Umfang **(1.2)** des Geschäfts sowie dessen geographische Größe und Komplexität wichtig. Die Art bezieht sich darauf, welche Infrastruktur verwendet wird, wie modern diese ist, ob es sich um Hochgeschwindigkeits- oder konventionelle Infrastruktur oder beides handelt, während der Umfang darauf abstellt, welches Geschäft geführt wird.

Die Ermittlung schwerwiegender Risiken bedeutet in diesem Fall, dass der Antragsteller zeigen sollte, dass er sich basierend auf seiner Analyse der wichtigsten Risiken, mit denen er konfrontiert ist, bewusst ist. Die Ermittlung schwerwiegender Risiken bedeutet auch, dass der Antragsteller ein Risikomanagementsystem eingerichtet hat (oder dessen Einrichtung vorbereitet), mit dem er:

- *gefährliche Ereignisse analysieren und Risiken bewerten kann,*
- *auf die wichtigsten Risiken (in Bezug auf Konsequenzen und Häufigkeit) aufmerksam gemacht werden kann und*
- *Maßnahmen zur Vorbeugung von Unfällen Priorität einräumen kann **(1.1 Buchstabe b)**.*

Dies hilft dabei, den Kontext der Organisation festzulegen und zeigt der bewertenden Behörde, dass der Antragsteller die Umgebung, in der er tätig ist, versteht. Die Tätigkeiten anderer Akteure oder Parteien, die nicht zum Eisenbahnnetz gehören (1.1 Buchstabe c), können die Sicherheit des Betriebs beeinträchtigen und

müssen somit bei der Risikobewertung ebenfalls berücksichtigt werden. Weitere Informationen zu vertraglichen Vereinbarungen und Partnerschaften sind Anhang 3zu entnehmen.

Der Antragsteller sollte auch ausreichende Informationen vorlegen, damit die Sicherheitsbescheinigungsstelle verstehen kann, welche Art von Betrieb das Unternehmen durchführt und wo; z. B. die Fracht, die das Unternehmen befördert, beispielsweise Holz, Container, kombinierter Verkehr, Sattelanhänger in Taschenwagen, Güter in geschlossen oder offenen Waggons usw. sowie die abgedeckten Strecken angeben. Für verschiedene Arten von Waren muss das Unternehmen möglicherweise über verschiedene Arten von Managementregelungen verfügen, auf die im SMS Bezug genommen wird (Beladung, Schulung usw.).

Der Kontext der Organisation muss auch beschreiben, wie das Eisenbahnunternehmen oder der Infrastrukturbetreiber die Instandhaltung aller von ihm eingesetzten Fahrzeuge zu organisieren gedenkt. Wird die Organisation beispielsweise im Rahmen des SMS eine zertifizierte für die Instandhaltung zuständige Stelle (ECM) nutzen oder möchte die Organisation eine für die Instandhaltung zuständige Stelle werden und Fahrzeuge instand halten, die ausschließlich für ihren eigenen Betrieb eingesetzt werden, und selbst die einschlägigen Anforderungen an für die Instandhaltung zuständige Stellen erfüllen (siehe Anhang II der Verordnung (EU) 2019/779 und den zugehörigen Leitfaden)? Der Antragsteller muss das Verhältnis zwischen verschiedenen für die Instandhaltung zuständigen Vertragsparteien angeben: Wenn z. B. das Eisenbahnunternehmen Fahrzeuge mietet, die von einer dritten für die Instandhaltung zuständigen Stelle gewartet werden, sollte dies angegeben werden. Weitere Informationen über das Management der Instandhaltungstätigkeiten sind dem ERA-Leitfaden zu den für die Instandhaltung zuständigen Stellen zu entnehmen.

Die Ermittlung geltender Anforderungen in Bezug auf die Sicherheit **(1.1 Buchstabe d)** erstreckt sich von den Bestimmungen geltender EU-Vorschriften (z. B. relevante CSM zu Sicherheitsmanagementsystemen und insbesondere Anhang I und Anhang II, CSM für die Evaluierung und Bewertung von Risiken, CSM für die Kontrolle, relevante TSI, der Durchführungsrechtsakt zu praktischen Vereinbarungen für die Sicherheitsbescheinigung und gegebenenfalls der Durchführungsrechtsakt zu praktischen Vereinbarungen für die Fahrzeugzulassung und die Verordnung über die für Instandhaltung zuständigen Stellen) über die nationale Gesetzgebung (z. B. notifizierte nationale Vorschriften, nationales Gesetz) bis hin zu allen anderen Anforderungen, zu deren Erfüllung sich die Organisation freiwillig verpflichtet (z. B. Regeln auf Sektor- oder Branchenebene für Zugbetrieb oder Managementsystem- und technische Normen wie ISO, CEN/CENELEC, UIC).

In diesem Abschnitt identifiziert die Organisation diejenigen Rechtsvorschriften, die sie einhalten muss, sowie die sektorspezifischen und sonstigen Anforderungen, die sie erfüllen muss, um den Zugverkehr sicher zu betreiben. Es kann unterschiedliche Anforderungen in den einzelnen Mitgliedstaaten geben, und das SMS muss in der Lage sein, etwaige Konflikte zwischen diesen Anforderungen und dem Rechtsrahmen zu lösen. Weitere Informationen, die für diese Anforderungen relevant sind, sind unter Umständen Dokumenten wie den Schienennetz-Nutzungsbedingungen zu entnehmen.

Wenn das Eisenbahnunternehmen beabsichtigt, gefährliche Güter zu befördern, oder der Infrastrukturbetreiber plant, die Beförderung gefährlicher Güter auf seiner Infrastruktur zuzulassen, müssen beide die besonderen Anforderungen der Ordnung für die internationale Eisenbahnbeförderung gefährlicher Güter (RID) sowie alle geltenden nationalen Vorschriften erfüllen. Die RID enthält spezifische Anforderungen an die Ausbildung von Personal, das an der Beförderung gefährlicher Güter beteiligt ist, wie z. B. den Sicherheitsberater, sowie Beispielanforderungen an Notfallpläne, die im SMS abgedeckt werden sollten (siehe ferner UIC – IRS 40471-3).

Für die Zwecke dieses Dokuments haben die Begriffe „Personal“, „Mitarbeiter“ und „Arbeiter“ dieselbe Bedeutung, nämlich eine Person, die unter der direkten Leitung der Organisation des Antragstellers arbeitet.

1.4 Nachweise

- *Für Eisenbahnunternehmen: Informationen über die Art des Betriebs, z. B. Fahrgäste und/oder Güter, Beförderung gefährlicher Güter, geografische Abdeckung (durch Einfügen einer Karte oder eines Streckenplans) und Skalierung des Betriebs, Einsatz von Unterauftragnehmern, Partnerschaften mit anderen Betreibern (Name), die verschiedenen beteiligten Akteure (Name und Art des Akteurs), die gewählte zertifizierte für die Instandhaltung zuständige Stelle mit einer Kopie der gültigen Bescheinigung. Ferner sollten die Arten von Schienenfahrzeugen und die Anzahl der direkt beschäftigten Mitarbeiter angegeben werden und darüber hinaus, woher zusätzliches Personal rekrutiert wird und, sofern es sich bei dem Antrag um eine Verlängerung einer Bescheinigung handelt, etwaige Änderungen seit der letzten Bewertung;* ***(1.1 Buchstabe a)***
- *Für Infrastrukturbetreiber: Informationen über die Art des geführten Betriebs, z. B. Güter und/oder Fahrgäste, Rangier- oder andere infrastrukturelle Dienstleistungen (auf die in Anhang II der Richtlinie 2012/34/EU Bezug genommen wird), die einen Einfluss auf die Eisenbahnsicherheit haben, geografische Abdeckung (durch Einfügen einer Karte oder eines Streckenplans) und Skalierung des Betriebs der Eisenbahnunternehmen, der im Netz stattfindet. Der Infrastrukturbetreiber sollte außerdem Informationen zum Einsatz von Unterauftragnehmern (Name), zu Partnerschaften mit anderen Betreibern (Name), verschiedenen beteiligten Akteuren (Name und Art des Akteurs) und der gewählten zertifizierten für die Instandhaltung zuständigen Stelle mit einer Kopie der gültigen Bescheinigung bereitstellen. Er sollte zudem Informationen zu Schienenfahrzeugen (einschließlich Anlagen zur Infrastrukturwartung oder Messung), die er unter Umständen betreibt, sowie die Anzahl der von ihm beschäftigten Mitarbeiter sowie bei Verlängerungen Änderungen der Regelungen für die Personalausstattung seit der letzten Bewertung angeben;* ***(1.1 Buchstabe a)***
- *Der Antragsteller muss angeben, welches die schwerwiegendsten Sicherheitsrisiken sind, die sein Geschäft beeinträchtigen;* ***(1.1. Buchstabe b)***
- *Die Person, die eine Sicherheitsbescheinigung oder eine Sicherheitsgenehmigung beantragt, muss zeigen, wie sie die relevanten regulatorischen Anforderungen, z. B. die Anforderungen an die CSM-Bewertung, die Technischen Spezifikationen für die Interoperabilität, insbesondere diejenige in Bezug auf das Teilsystem für das Betriebs- und Verkehrsmanagement (TPI OPE), die geltenden nationalen Vorschriften und sonstigen Anforderungen (sektorspezifische und weitere Vorschriften), die sie befolgen muss, um den Zugverkehr sicher zu betreiben, ermittelt hat und wie sie diese einhält (die Prozesse des Sicherheitsmanagementsystems, welche die Konformität unterstützen);* ***(1.1 Buchstaben c und d)***
- *Der Antragsteller muss die Interessengruppen identifizieren, die für die erfolgreiche Einführung seines Sicherheitsmanagementsystems relevant sind (d. h. deren Tätigkeiten eine Wirkung oder mögliche Wirkung auf das SMS haben, z. B. Auftragnehmer oder Partner) und angeben, warum diese für den erfolgreichen Betrieb des SMS gebraucht werden;* ***(1.1 Buchstaben c und d)***
- *Für beide: Der Antragsteller sollte angeben, wo in der Dokumentation seines Sicherheitsmanagementsystems jede der Anforderungen an das Sicherheitsmanagementsystem, einschließlich der einschlägigen Anforderungen an die geltenden Technischen Spezifikationen für die Interoperabilität, insbesondere die TSI OPE, sowie relevante notifizierte nationale Vorschriften und sonstige Anforderungen erfüllt werden;* ***(1.1 Buchstabe e)***
- *Der Antragsteller muss Informationen hinsichtlich des Anwendungsbereichs des Sicherheitsmanagementsystems bereitstellen (einschließlich der Frage, wo die Grenzen zu anderen Teilen des Geschäfts wie der Instandhaltung von Fahrzeugen verlaufen);* ***(1.1 Buchstabe f)***

1.5 Beispiele für Nachweise

Eine Karte, die das geografische Tätigkeitsgebiet zeigt. Informationen zu den für den Betrieb zugelassenen Schienenfahrzeugen (gegebenenfalls einschließlich vorgeschlagener Schienenfahrzeuge, deren Betrieb während der Gültigkeitsdauer der Bescheinigung oder der Genehmigung vorgeschlagen wird, sowie Einschränkungen des Einsatzbereichs). Informationen zu den Arten von Dienstleistungen, die angeboten werden sollen (Fahrgäste und/oder Güter), sind enthalten.

Wenn der Antragsteller ein Infrastrukturbetreiber ist, kann diese Information durch einen Verweis bereitgestellt werden, zum Beispiel auf:

- *die Informationen, die im Infrastrukturregister enthalten sind, das in Übereinstimmung mit der Richtlinie (EU) 2016/797 (Artikel 49) eingerichtet wurde;*
- *den Inhalt der Schienennetz-Nutzungsbedingungen (insbesondere Abschnitt I), die in Übereinstimmung mit der Richtlinie 2012/34/EU erstellt wurden; und*
- *das Streckenbuch, das in Übereinstimmung mit der Verordnung (EU) 2019/773 (TSI OPE) erstellt wurde.*

Für die für die Beantragung einer Sicherheitsgenehmigung oder Sicherheitsbescheinigung bereitgestellten Informationen müssen ordnungsgemäße Quellenangaben und eine ausreichende Dokumentation vorgelegt werden, um die Einhaltung der entsprechenden EU-Gesetzgebung zu belegen.

Eine Angabe der aktuellen und vorgeschlagenen Personalausstattung innerhalb der Gültigkeitsdauer der einheitlichen Sicherheitsbescheinigung, sofern diese bekannt ist.

Ein Eisenbahnunternehmen sollte Informationen zu seinen Betriebsschnittstellen bereitstellen, einschließlich zu Infrastrukturbetreibern, anderen Eisenbahnunternehmen, Auftragnehmern und den Notfalldiensten. Zu diesen Informationen gehören auch besondere Vorgaben des Infrastrukturbetreibers, die sich auf das SMS des Eisenbahnunternehmens auswirken.

Für Eisenbahnunternehmen kann eine über die einzige Anlaufstelle eingereichte Abbildungstabelle als Teil der Antragsdatei für eine Sicherheitsbescheinigung verwendet werden, um die Konformität mit den Vorschriften und anderen relevanten Vorgaben zu erläutern.

Entsprechend sollte ein Infrastrukturbetreiber eine ähnliche Liste mit Parteien, mit denen er Betriebsschnittstellen hat, wie beispielsweise Eisenbahnunternehmen, die auf der kontrollierten Infrastruktur arbeiten, seine Auftragnehmer, benachbarte Infrastrukturbetreiber, Baustellen, örtliche Behörden (für Straßenschnittstellen) und die Notfalldienste, bereitstellen.

Informationen zu den gesetzlichen Bestimmungen (sowohl auf nationaler als auch europäischer Ebene), die er einhalten wird.

Eine Beschreibung (einschließlich eines Organigramms), die erläutert, wie das Sicherheitsmanagementsystem strukturiert ist und innerhalb der Organisation verwaltet wird, die ebenfalls Verknüpfungen zu den verschiedenen Abschnitten des Sicherheitsmanagementsystems enthält, in denen genauere Informationen wie Betriebsregeln zu finden sind.

Eine aktuelle Kopie des Jahresberichts, der die wichtigsten Risiken enthält, mit denen die Organisation konfrontiert ist, sowie die Ziele zu deren Kontrolle, und der die verwendete Methodik zu deren Bewertung und die Art und Weise ihrer Priorisierung beschreibt.

Eine Erklärung, ob eine zertifizierte für die Instandhaltung zuständige Stelle genutzt wird oder Fahrzeuge ausschließlich für den eigenen Betrieb instand gehalten werden.

Überblick über den Instandhaltungsprozess sowie Art und Umfang der durchgeführten Arbeiten.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Ein Risikoregister oder eine Übersicht, in der Risikoszenarien für die Betriebssicherheit dokumentiert werden, einschließlich der Berücksichtigung menschlicher und organisatorischer Faktoren:

- *Einzelpersonen (z. B. menschliches Versagen);*
- *Arbeitsplatz (z. B. physische Umgebung wie Lärm, Dunkelheit, Wetter); und*
- *Organisation (z. B. Arbeitsbelastung, Kompetenzmanagement, Aufgabengestaltung, Ressourcen, Schichten).*

Zur Festlegung der schwerwiegendsten Risiken werden Risikoszenarien bewertet, um eine Priorisierung der Risiken zu ermöglichen (dies ist im Risikobewertungsprozess zu finden, siehe 3.1.1). Das Risikoregister erfasst Risiken im Zusammenhang mit den Tätigkeiten der Organisation sowie Tätigkeiten, die von Auftragnehmern, Partnern oder Zulieferern unter ihrer Aufsicht ausgeführt werden. Für jedes schwerwiegende Risiko ist der Risikoverantwortliche im SMS klar definiert.

Das SMS enthält eine Beschreibung der Interessengruppen, die für das Sicherheitsmanagement relevant sind, und beschreibt, wie die Beziehungen zu diesen Interessengruppen geregelt werden. Es werden die Mittel genannt, mit denen die schwerwiegendsten Risiken den betroffenen Dritten mitgeteilt werden können, und es werden einige Beispiele genannt (z. B. Verträge, Sitzungsprotokolle).

1.6 Referenzen und Standards

- *TSI OPE-Beantragungsleitfaden*
- *Leitlinien für für die Instandhaltung zuständige Stellen*
- *UIC – IRS 40471-3 Prüfungen, die bei Sendungen gefährlicher Güter durchzuführen sind*

1.7 Aufsichtsaspekte

Prüfung der Genauigkeit der bereitgestellten Informationen anhand der bekannten Informationen über bestehende Betriebe im Fall eines Bescheinigungs-Verlängerungsantrags oder anhand anderer verfügbarer Informationen im Fall eines Neueintritts.

Prüfung, ob das beschriebene Sicherheitsmanagementsystem die entsprechenden Vorkehrungen umfasst, um die Sicherheit in der Praxis zu gewährleisten.

Prüfung, ob alle Schnittstellen, über welche die Organisation mit anderen Parteien verfügt, in den Vorkehrungen im SMS zur Kontrolle von Risiken berücksichtigt sind.

2 Führung

2.1 Führung und Verpflichtung

2.1.1 Regulatorische Anforderung

2.1.1. Die oberste Führungsebene muss Führung und Verpflichtung bei der Entwicklung, Umsetzung, Aufrechterhaltung und kontinuierlichen Verbesserung des Sicherheitsmanagementsystems demonstrieren, indem sie

(a) die umfassende Rechenschaftspflicht und Gesamtverantwortung für die Sicherheit übernimmt;

(b) durch ihre Handlungen und ihre Beziehungen zu den Mitarbeitern und Auftragnehmern sicherstellt, dass das Management auf allen Organisationsebenen der Sicherheit verpflichtet ist;

(c) sicherstellt, dass die Sicherheitsordnung und die Sicherheitsziele festgelegt und verstanden werden und mit der strategischen Ausrichtung der Organisation im Einklang stehen;

(d) sicherstellt, dass die Anforderungen des Sicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden;

(e) sicherstellt, dass die für das Sicherheitsmanagementsystem notwendigen Ressourcen zur Verfügung stehen;

(f) sicherstellt, dass die von der Organisation ausgehenden Sicherheitsrisiken durch das Sicherheitsmanagementsystem wirksam beherrscht werden;

(g) den Mitarbeitern Anreize bietet, die Einhaltung der Anforderungen des Sicherheitsmanagementsystems zu unterstützen;

(h) die kontinuierliche Verbesserung des Sicherheitsmanagementsystems fördert;

(i) gewährleistet, dass die Sicherheit bei der Erfassung und Beherrschung der Geschäftsrisiken der Organisation Berücksichtigung findet, und erläutert, wie Konflikte zwischen der Sicherheit und den anderen Geschäftszielen erkannt und gelöst werden;

(j) eine positive Sicherheitskultur fördert.

2.1.2 Zweck

Das Festlegen einer klaren und positiven Richtung für das Sicherheitsmanagement wird wichtige Auswirkungen darauf haben, wie Risiken gehandhabt werden. Die bewertende Behörde muss auf die Verpflichtung des Antragstellers vertrauen können, Ressourcen zuzuweisen, um der Organisation einen sicheren Betrieb zu ermöglichen und es ihr zu erlauben, die Risiken effektiv zu beherrschen. Außerdem vertraut sie darauf, dass die Führungsebene der Organisation des Antragstellers dafür sorgt, dass entsprechende Schritte unternommen werden. Die Verpflichtung des Managements zur Berücksichtigung menschlicher und organisatorischer Faktoren zeigt sich in Strategien und Zielen sowie Management- und Führungsverhaltensweisen. Darüber hinaus wird der von der Führungsebene verfolgte Ansatz in Bezug auf die menschlichen und organisatorischen Faktoren gewährleisten, dass die Entwicklung der Schulungen und Verfahren auf der Aufgabe basiert, die in ihrer natürlichen Umgebung auszuführen ist. Dies unterstützt die Optimierung der Risikokontrolle und der Leistungsfähigkeit, da eine genaue Beschreibung der Aufgabe („geleistete Arbeit“) zugrunde gelegt wird.

Die Sicherheitsordnung gibt die Wichtigkeit und Priorisierung der Sicherheit einschließlich der Einbindung menschlicher und organisatorischer Faktoren und die Förderung der Sicherheitskultur an.

Die Organisation fördert eine konstante und gemeinsame Wachsamkeit, mit der Bequemlichkeit („alles ist unter Kontrolle“) und übermäßiger Vereinfachung („die Einhaltung von Verfahren ist ausreichend, um Sicherheit zu gewährleisten“) entgegengewirkt und eine hinterfragende Einstellung entwickelt wird. Zudem sind sich alle Akteure in der Organisation bewusst, dass es stets eine Lücke zwischen geplanten Tätigkeiten und dem, was wirklich geschieht, geben kann, egal wie qualitativ hochwertig die Planung und Organisation sowie die technischen Sicherheitsbarrieren und Verfahren sind. Es werden alle möglichen Quellen verwendet, um jene Situationen, die nicht ausreichend antizipiert wurden, zu erkennen und gemeinsam zu analysieren.

Darüber hinaus entspricht die Kommunikation der Organisation in Bezug auf die Sicherheit der Realität der Managemententscheidungen.

Damit ein SMS effektiv arbeiten und sich in Zukunft verbessern kann, ist es wichtig, dass die Führungskräfte ihren Mitarbeitern und allen Beteiligten zeigen, dass sie eine positive Agenda vorgeben, in der die Sicherheit gelenkt werden kann. Es sind die Führungskräfte, die den größten Einfluss auf die Unternehmenskultur haben, und daher ist es entscheidend, dass sie die richtige Botschaft an diejenigen kommunizieren können, die unter ihnen arbeiten. Das Verhalten der Führungskräfte auf allen Ebenen der Organisation und die Wichtigkeit, die sie der Sicherheit bei ihren täglichen Entscheidungen beimessen, haben einen starken Einfluss auf das Verhalten anderer Akteure bei der Erfüllung ihrer Aufgaben. Manager sollten zudem die physischen und sozialen Arbeitsumgebungen schaffen, in denen die Arbeiten an vorderster Front sicher verrichtet werden.

2.1.3 Erläuterungen

„Oberste Führungsebene“ **(2.1.1)** bedeutet in diesem Kontext Personen, die als „leitende Köpfe“ der Organisation Entscheidungen treffen. Dies sind normalerweise der Geschäftsführer, Mitglieder der obersten Führungsebene, der Vorstandsvorsitzende und die Vorstandsmitglieder. Als Gruppe und als Einzelpersonen wird von der „obersten Führungsebene“ verlangt, durch das Sicherheitsmanagementsystem Führungsqualitäten und Engagement zu zeigen.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Sicherheitsrisiken muss genug Bedeutung beigemessen werden **(2.1.1 Buchstabe i)**, um andere Geschäftsrisiken auszugleichen, um eine Situation zu vermeiden, in der das Management die Geschäftsbedürfnisse auf eine Weise priorisiert, welche die Sicherheitsleistung schwächt. Die oberste Führungsebene muss sicherstellen, dass die Ziele so behandelt werden, dass die Sicherheitsleistung aufrechterhalten und die Risiken so weit wie möglich beherrscht werden. Zielkonflikte sollten nicht zu widersprüchlichen Aufgaben für den Einzelnen führen, die zu Sicherheitsproblemen führen könnten.

Ein Führungs- und Managementansatz in Bezug auf menschliche und organisatorische Faktoren bedeutet das Festlegen von Zielen, Erwartungen und Verantwortlichkeiten hinsichtlich der Sicherheitsverhaltensweisen auf allen Ebenen der Organisation, um eine zeitnahe Rückmeldung und Kommunikation zu gewährleisten.

2.1.4 Nachweise

- *Es gibt eine Sicherheitsordnung und Ziele sowie Nachweise dafür, dass diese für alle Mitarbeiter verfügbar sind und von ihnen verstanden werden. Es wird außerdem deutlich gemacht, wie diese mit anderen Geschäftsprozessen zusammenpassen und mit der kontinuierlichen Verbesserung zusammenhängen;* ***(2.1.1 Buchstaben a, b, g, e und h)***

- *In der Sicherheitsordnung wird betont, wie wichtig es ist, in allen sicherheitsrelevanten Prozessen einen Ansatz der menschlichen und organisatorischen Faktoren anzuwenden, um ein hohes Sicherheitsniveau in der Organisation zu erreichen. Die Organisation zeigt, wie die Bedürfnisse der menschlichen und organisatorischen Faktoren für den organisatorischen Prozess gelenkt werden;* ***(2.1.1 Buchstabe c)***
- *Die Beziehung zwischen dem Sicherheitsmanagementsystem und anderen Geschäftstätigkeiten ist eindeutig in einem Verfahren oder einem Organigramm dargelegt;* ***(2.1.1 Buchstabe i)***
- *In der Sicherheitsordnung oder anderen Prozessen sind Informationen verfügbar, die angeben, dass sich das Management verpflichtet hat, ausreichende Ressourcen bereitzustellen und aufrechtzuerhalten, damit das Sicherheitsmanagementsystem effektiv funktioniert und im Zeitverlauf verbessert wird;* ***(2.1.1 Buchstaben e und h)***
- *Es liegen Nachweise vor, die zeigen, dass die Führungsebene eine positive Sicherheitskultur fördert;* ***(2.1.1 Buchstaben j und h)***
- *Nachweise, die aufzeigen, wie gewährleistet wird, dass Mitarbeiter ihre Sicherheitsrollen und Verantwortlichkeiten verstehen und wie ihr Handeln sich auf die Fähigkeit der Organisation auswirkt, Risiken durch das Sicherheitsmanagementsystem zu kontrollieren;* ***(2.1.1 Buchstaben d, f und i)***
- *Im Rahmen der Sicherheitsordnung oder anderer Dokumente gibt es Hinweise darauf, dass die Organisation versucht, ihre Mitarbeiter über die wichtige Rolle zu informieren, die sie spielen, um sicherzustellen, dass das Sicherheitsmanagementsystem in der Praxis so funktioniert, dass eine sinnvolle Risikokontrolle gewährleistet ist;* ***(2.1.1 Buchstabe e)***
- *Es sind Prozesse eingerichtet, die festlegen, wie menschliche und organisatorische Faktoren innerhalb der Organisation angesprochen und kommuniziert werden sollen, die mit den Geschäftszielen und organisatorischen Prozessen der Organisation zusammenhängen, z. B. Projekte, Untersuchungen von Störungen und Unfällen, Risikoanalysen und andere sicherheitsrelevante Aktivitäten für das eigene Personal des Unternehmens, Auftragnehmer, Partner und Zulieferer;* ***(2.2.1 Buchstaben c, d und e)***
- *Es sind Nachweise dafür vorhanden, dass die Führungsebene Prozesse eingerichtet hat, die dafür sorgen, dass menschliche und organisatorische Faktoren im Zusammenhang mit dem Einsatz von Unterauftragnehmern des Unternehmens behandelt und kommuniziert werden.* ***(2.2.1 Buchstaben c bis e)***

2.1.5 Beispiele für Nachweise

Es wird eine vom Geschäftsführer unterzeichnete und datierte Sicherheitsordnung bereitgestellt, in der das Engagement des Managements für die Sicherheit und deren Verbesserung und die Einbeziehung des Personals in das Management von Sicherheitsrisiken klar festgelegt sind. Die Sicherheitsordnung gibt außerdem an, wie sie überprüft wird.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweise kommen in Betracht:

Ein klarer Satz an Sicherheitszielen für die Organisation, die spezifisch, messbar, ausführbar, realistisch und termingebunden (SMART) sind, und klare Methodik in einem Verfahren zum Festlegen dieser Ziele und zur Analyse des Erfolgs oder Misserfolgs beim Erreichen dieser Ziele. Das SMS enthält Nachweise dafür, dass das Management Ziele im Bereich der Betriebssicherheit verfolgt (neben Zielen im Bereich Sicherheit und Gesundheitsschutz am Arbeitsplatz).

Eine klare Aussage von der Führungsebene, wie die positive Sicherheitskultur der Organisation gefördert wird, und wie Mitarbeiter am Prozess beteiligt und einbezogen werden.

Ein Überblick über die Zusammenkünfte der obersten Führungsebene und deren Häufigkeit, bei denen die Sicherheit ein Standard-Berichtsthema ist.

Eine klare Aussage hinsichtlich des Engagements der Organisation, ausreichende Ressourcen bereitzustellen, um die effiziente Funktion des Sicherheitsmanagementsystems für die Kontrolle von Risiken zu ermöglichen.

Ein Organigramm führt eindeutig an, wie das Sicherheitsmanagementsystem funktioniert und wer für welche Aspekte verantwortlich ist.

Es wird bei der Konzipierung neuer Ausrüstungen, z. B. neuer Züge, ein Ansatz in Bezug auf die menschlichen und organisatorischen Faktoren verfolgt. Dies umfasst die Nutzung von Erfahrungen der aktuellen Benutzer beim Erstellen von Designanforderungen, bei der Analyse von Aufgaben zur Identifikation kognitiver und physiologischer Herausforderungen, bei der Reduzierung des Potenzials für fehlerhafte Leistung durch das Design, indem Leitlinien in Bezug auf menschliche Faktoren angewandt werden, wie beispielsweise verschiedene international anerkannte Normen, die Durchführung der Betriebsbelastungs- und Ermüdungsmanagementanalyse zur Gewährleistung, dass die Mitarbeiter die Aufgabenleistung erbringen können, sowie die Durchführung von Risikoanalysen zur Feststellung potenzieller Probleme und zur Ermittlung von Gegenmaßnahmen für diese. Umweltfaktoren, wie beispielsweise Schnee, Hitze, Regen usw. werden ebenso berücksichtigt wie sozioökonomische Faktoren, wie z. B. organisatorische Prioritäten, Auftragsvergabe und nationale Kultur.

Schulungen in Sicherheitsführung für Führungskräfte in sicherheitsrelevanten Positionen werden organisiert. Es liegen Nachweise für eine regelmäßige Schulung der Führungskräfte vor. Es gibt Nachweise dafür, dass die Managementschulung der Sicherheitsvision Rechnung trägt, wie sie in die Sicherheitsordnung integriert wurde und wie sie zu kommunizieren und anzuwenden ist.

Die Führungskräfte weisen durch Protokolle von Sicherheitstouren oder Begehungen vor Ort ihr Engagement für die Förderung einer positiven Sicherheitskultur sowie ihren Wunsch nach, durch gutes Beispiel voranzugehen.

2.1.6 Referenzen und Standards

- *Sicherheitskultur (ERA-Webpage)*

2.1.7 Aufsichtsaspekte

Das Ausmaß von Nichtübereinstimmungen zwischen Strategien und Verfahren, die als Teil des obigen Nachweises bereitgestellt werden, und der beobachteten Realität bei der Aufsicht sowie die Frage, in welchem Umfang die Organisation sich der Diskrepanz bewusst ist, sind wichtige Aspekte der Aufsicht.

Der Umfang der wahren Verpflichtung der Führungsebene gegenüber dem Sicherheitsmanagementsystem und der Förderung der Sicherheitskultur sowie die der Mitarbeiter gegenüber der Organisation sollten bei der Aufsicht anhand der Untersuchung der eigenen Mechanismen der Organisation zum Verständnis und zur Entwicklung dieser Kultur und des Sicherheitsmanagementsystems geprüft werden.

Prüfung, ob die Organisation nachweisen kann, dass ausreichende Ressourcen für die Entwicklung, Einführung, Aufrechterhaltung und kontinuierliche Verbesserung des Sicherheitsmanagementsystems bereitgestellt werden.

Prüfung anhand einer Befragung der obersten Führungsebene und anderer Mitarbeiter, wie sie ihre Verpflichtung zur Verbesserung der Sicherheit ausdrückt. Herausfinden, wie oft und auf welche Weise sie ihre Mitarbeiter bezüglich Sicherheitsproblemen und/oder zur Förderung der Sicherheitskultur (Workshops, Foren, spezielle Sicherheitstage usw.) kontaktiert.

Prüfung, ob von der obersten Führungsebene Mitteilungen in Bezug auf die Ziele erfolgen, die entweder darauf abzielen, alle Mitarbeiter zu einem Beitrag zu ihrer Erreichung zu ermutigen, oder darauf, allen für eine bessere Leistung zu danken.

2.2 Sicherheitsordnung

2.2.1 Regulatorische Anforderung

2.2.1. Die oberste Führungsebene erstellt ein Dokument mit einer Beschreibung der Sicherheitsordnung der Organisation, das

(a) der Art der Organisation und der Art und des Umfangs des Eisenbahnbetriebs angemessen ist;

(b) vom Geschäftsführer (oder einem bzw. mehreren Vertretern der obersten Führungsebene) genehmigt wird;

(c) aktiv umgesetzt und dem gesamten Personal mitgeteilt und zugänglich gemacht wird.

2.2.2. Die Sicherheitsordnung muss

(a) eine Verpflichtung zur Erfüllung aller rechtlichen und sonstigen Anforderungen in Bezug auf die Sicherheit umfassen;

(b) einen Rahmen vorgeben, um Sicherheitsziele festzulegen und die Sicherheitsleistung der Organisation anhand dieser Ziele zu bewerten;

(c) eine Verpflichtung zur Kontrolle von Sicherheitsrisiken enthalten, die sich entweder aus den eigenen Tätigkeiten ergeben oder von anderen verursacht werden;

(d) eine Verpflichtung zur kontinuierlichen Verbesserung des Sicherheitsmanagementsystems enthalten;

(e) im Einklang mit der Geschäftsstrategie und der Bewertung der Sicherheitsleistung der Organisation aufrechterhalten werden.

2.2.2 Zweck

Aus dem Dokument zur Sicherheitsordnung geht hervor, wie das Unternehmen seine Verantwortung im Sicherheitsbereich wahrnimmt, und es gibt Aufschluss über seine Führungstätigkeit und sein Engagement in Bezug auf ein ordnungsgemäßes Sicherheitsmanagement. Der Antragsteller sollte in der Lage sein, zu zeigen, dass er über eine Sicherheitsordnung verfügt, welche die obigen Anforderungen erfüllt und die grundlegende Struktur der Risikokontrolle zusammenfassend beschreibt.

2.2.3 Erläuterungen

Die Sicherheitsordnung ist ein Ausdruck der Philosophie der Führungsebene und demnach ist dieser Abschnitt eng mit Abschnitt 3.1 verbunden.

In Nummer 2.2.1 Buchstabe a des vorstehenden Rechtstextes wird in der englischen Fassung bei der Anforderung an Infrastrukturbetreiber „type“ durch „character“ ersetzt (diese Änderung betrifft nicht die deutsche Fassung, da darin beide Begriffe mit „Art“ übersetzt sind).

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

In der Sicherheitsordnung kommt die Sicherheitsvision zum Ausdruck: Wenngleich in der oben aufgeführten regulatorischen Anforderung menschliche und organisatorische Faktoren nicht explizit erwähnt werden, wird doch ein klarer Schwerpunkt auf Aspekte menschlicher Faktoren innerhalb der Organisation gelegt und die wichtige Rolle anerkannt, die der Mensch bei der Verwirklichung einer sicheren und effizienten Organisation

und der Erreichung von Geschäftszielen spielt. Die Rolle des Menschen wird bei jeder Überprüfung der operativen und wirtschaftlichen Entwicklung berücksichtigt.

2.2.4 Nachweise

- *Für ein Eisenbahnunternehmen: Eine schriftliche, vom Geschäftsführer unterzeichnete Sicherheitsordnung, welche die Art und den Umfang des Betriebs widerspiegelt, unterstützt die Konformität mit der Gesetzgebung und anderen Anforderungen, fördert eine kontinuierliche Verbesserung der Sicherheit und bietet einen Rahmen für die Festlegung von Sicherheitszielen;* ***(2.2.1 Buchstaben a und b), (2.2.2 Buchstaben a bis c)***
- *Für einen Infrastrukturbetreiber: Eine schriftliche, vom Geschäftsführer unterzeichnete Sicherheitsordnung, welche die Art und den Umfang des Eisenbahnbetriebs und der Infrastrukturentwicklung widerspiegelt, unterstützt die Konformität mit der Gesetzgebung und anderen Anforderungen, fördert eine kontinuierliche Verbesserung der Sicherheit und wird für die Festlegung von Sicherheitszielen verwendet;* ***(2.2.2 Buchstaben a bis c)***
- *Für beide: Informationen, die darauf hinweisen, dass die Sicherheitsordnung an alle Mitarbeiter kommuniziert wurde;* ***(2.2.1 Buchstabe c)***
- *Information, dass die Sicherheitsordnung so gepflegt wird, dass sie stets auf die Geschäftsstrategie und die Bewertung der Sicherheitsleistung der Organisation ausgerichtet ist;* ***(2.2.2 Buchstaben d und e)***
- *Nachweise, dass die Sicherheitsordnung das Ziel hat, die Sicherheitsleistung zu überwachen und nach der Überprüfung der Sicherheitsleistung der Organisation gemäß den festgelegten Zielen angepasst wird;* ***(2.2.2 Buchstaben b, d und e)***

2.2.5 Beispiele für Nachweise

Eine vom Geschäftsführer unterzeichnete und datierte Sicherheitsordnung, welche die Art und den Umfang des Betriebs präzise widerspiegelt. Das Dokument hat das erklärte Ziel einer kontinuierlichen Verbesserung des Sicherheitsmanagementsystems.

Die Sicherheitsordnung ist aktuell und verfügt über einen definierten Überprüfungszyklus, der an der Geschäftsstrategie ausgerichtet ist.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Die Sicherheitsordnung enthält Informationen oder Referenzen, die den Prozess für deren Überprüfung darlegen. Dadurch soll festgestellt werden, ob im Anschluss an eine Kontrolle der Sicherheitsleistung der Organisation anhand der festgelegten Ziele eine Änderung erforderlich ist.

Die Sicherheitsordnung und die zugehörigen Strategien werden als Schwerpunktthema für Führungskräfte verwendet, um zu erreichen, dass sie von allen Mitarbeitern einheitlich ausgelegt werden.

Die Mitarbeiter beteiligen sich aktiv an der Überprüfung und Überarbeitung der Sicherheitsordnung sowie an deren Umsetzung.

Die Sicherheitsordnung nimmt Bezug auf einen Prozess/eine Methodik für die risikobasierte Bewertung vorgeschlagener Entscheidungen (im Einklang mit der Sicherheitsvision). Bei diesem Prozess wird erläutert, wie die Sicherheit als vorrangiges Ziel berücksichtigt wird.

Gemäß der Sicherheitsordnung oder anderen Bestimmungen des SMS hat jeder Mitarbeiter seine Tätigkeit zu unterbrechen, wenn die Arbeitsbedingungen nicht mehr sicher sind.

Eine Basisbewertung der Organisation im Hinblick auf die Sicherheitskultur wurde durchgeführt. Schwachstellen wurden von der Organisation ermittelt, den Mitarbeitern mitgeteilt, und in der Sicherheitsordnung werden Verbesserungsmaßnahmen genannt.

Es ist ein Prozess für die Kommunikation der Sicherheitsordnung über das Intranet der Organisation und für deren Aushang an strategischen/operativen Orten eingerichtet.

Das Unternehmen ist nach außen orientiert und sucht nach externen Lernmöglichkeiten für die Entwicklung seiner Effizienz und Wirksamkeit, wobei die menschlichen Faktoren mit berücksichtigt werden.

2.2.6 Aufsichtsaspekte

Bei der Aufsicht wird es wichtig sein, zu prüfen, wie gut die Sicherheitsordnung gegenüber allen Mitarbeitern kommuniziert und von diesen verstanden wurde und welche Rolle sie in der Praxis bei der Festlegung des Sicherheitsrahmens spielt, in dem die Organisation arbeitet. Eine wichtige Frage ist, ob das Dokument dabei hilft, die Agenda festzulegen, oder ob es einfach nur existiert, weil dies gesetzlich vorgeschrieben ist.

Prüfung, dass Änderungen der Sicherheitsleistung der Organisation eine Überprüfung der Sicherheitsordnung ausgelöst haben.

Prüfung, dass die Sicherheitsordnung der Realität der Organisation entspricht.

2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse

2.3.1 Regulatorische Anforderung

2.3.1.	Die Zuständigkeiten, Rechenschaftspflichten und Befugnisse von Mitarbeitern mit Aufgaben, die die Sicherheit betreffen (einschließlich leitender und anderer Mitarbeiter mit sicherheitsrelevanten Aufgaben), sind auf allen Organisationsebenen festzulegen, zu dokumentieren, zuzuweisen und mitzuteilen.
2.3.2.	Die Organisation muss sicherstellen, dass Mitarbeiter mit nachgeordneten Zuständigkeiten für sicherheitsrelevante Aufgaben über die Befugnisse, Befähigung und notwendigen Ressourcen verfügen, um ihre Aufgaben unbeeinträchtigt durch die Tätigkeiten anderer Funktionsbereiche erfüllen zu können.
2.3.3.	Die Übertragung von Zuständigkeiten für sicherheitsrelevante Aufgaben muss dokumentiert und den betreffenden Mitarbeitern mitgeteilt und von ihnen akzeptiert und verstanden werden.
2.3.4.	Die Organisation muss beschreiben, wie die unter 2.3.1 genannten Aufgaben den einzelnen Funktionsbereichen innerhalb und gegebenenfalls außerhalb der Organisation (siehe 5.3 Auftragnehmer, Partner und Zulieferer) zugewiesen werden.

2.3.2 Zweck

Ziel dieser Anforderung ist es, dass der Antragsteller ein klares Bild über die Struktur der Organisation und die Verteilung und Aufrechterhaltung der Rollen und Verantwortlichkeiten im Laufe der Zeit von denjenigen, die an vorderster Front tätig sind, bis hin zur obersten Führungsebene vermittelt. Dies ist ausschlaggebend für das Verständnis, wie gut das Sicherheitsmanagementsystem einer Organisation Risiken kontrolliert. Der Antragsteller sollte aufzeigen, wie er kompetenten Mitarbeitern Tätigkeiten zuweist, wie er sicherstellt, dass diese Mitarbeiter ein klares Verständnis ihrer Rollen und Verantwortlichkeiten haben und wie die Mitarbeiter für ihre Leistung zur Rechenschaft gezogen werden.

2.3.3 Erläuterungen

Eventuell besteht eine Diskrepanz beim Verständnis zwischen den Sicherheitsmanagementbestimmungen auf betrieblicher Ebene und den Managementprozessen, anhand derer das Sicherheitsmanagementsystem funktionieren soll (z. B. Risikobewertung, Überwachung). Die Ermittlung von relevanten Rollen im Sicherheitsmanagementsystem **(2.3.1)** beschränkt sich nicht auf diejenigen, die rechenschaftspflichtig oder verantwortlich für das Management der Sicherheitsprozesse sind, wie beispielsweise den Sicherheitsmanager oder das Sicherheitsteam, sondern erstreckt sich auf sämtliche Funktionen, die an sicherheitsrelevanten Aufgaben beteiligt sind, wie beispielsweise Betriebsmitarbeiter; dies ist unabhängig davon, ob eine leitende oder nichtleitende Position in der Organisation eingenommen wird (d. h. hochrangige Führungskräfte, Vorgesetzte, andere Mitarbeiter/Angestellte/Arbeiter).

„Delegierung“ **(2.3.3)** bedeutet die Weitergabe von Verantwortlichkeiten von einer höheren an eine niedrigere Autoritätsposition, gewöhnlich mit dem Ziel, die Reaktion der Organisation auf auftretende Sachverhalte zu beschleunigen. Die Sicherheitsverantwortlichkeit kann im Rahmen der definierten Arbeitsverantwortlichkeiten delegiert, d. h. nach unten weitergegeben, werden, wenn eine solche Delegierung dokumentiert wird. Die Rechenschaftspflicht für die Sicherheit kann nicht delegiert werden, sie obliegt weiterhin rechtlich der oberen Führungsebene. Sie definiert die Verpflichtung einer Person, die zur Rechenschaft gezogen wird, wenn etwas nicht erledigt wird, nicht funktioniert oder sein Ziel nicht erreicht, die zufriedenstellende Erfüllung seiner/ihrer Sicherheitsverantwortlichkeiten nachzuweisen.

Die Zuweisung von Aufgaben **(2.3.4)** kann durch die Bereitstellung eines geeigneten Organisationsdiagramms oder Organigramms aufgezeigt werden.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Innerhalb der Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse **(2.3.1)** ist auch der Austausch von sicherheitsrelevanten Informationen abzudecken, beispielsweise wer für die Ausstellung der aktuellsten Änderungsmitteilungen für die Triebfahrzeugführer zuständig ist **(siehe ferner 4.4.1 und 4.4.2)**.

Das Sicherheitsmanagementsystem sollte mit den Anforderungen an die CSM-Bewertung **(1.1 Buchstabe d)** konform sein, und die oberste Führungsebene ist dafür verantwortlich zu gewährleisten, dass ihr Sicherheitsmanagementsystem mit diesen übereinstimmt. Die oberste Führungsebene kann einige ihrer Zuständigkeiten an relevante Mitarbeiter delegieren. Die Leistungsberichterstattung wird in Übereinstimmung mit den Anforderungen an die Managementbewertung **(6.3)** durchgeführt, wobei relevante Mitarbeiter dafür verantwortlich sind, der obersten Führungsebene hinsichtlich der Leistung des Sicherheitsmanagementsystems Bericht zu erstatten.

„Sicherheitsrelevante Aufgaben“ **(2.3.1)** sind nicht auf Aufgaben beschränkt, die direkt die Sicherheit verwalten (d. h. sicherheitsrelevante Aufgaben, die von Mitarbeitern durchgeführt werden, wenn diese die Bewegung eines Zuges steuern oder beeinflussen, was die Gesundheit und Sicherheit von Personen beeinträchtigen könnte, wie in den TSI OPE angegeben). Sie umfassen außerdem auch nicht betriebliche Aufgaben, welche sich auf die Sicherheit auswirken und mit der Risikobewertung verbunden sind (z. B. Betriebsplanung, Dienstplanung, Zuweisung von Fahrzeugen). Bei Prüfung neuer oder geänderter Aufgaben und Zuständigkeiten werden menschliche Einflüsse in Bezug auf die Änderung sowie die Art und Weise analysiert, in der die Pflichten derzeit im Unternehmen wahrgenommen werden.

Zuständigkeiten und Aufgaben werden auf der Grundlage bestimmter Kriterien und nach Ermittlung der erforderlichen Kompetenzen und Kenntnisse delegiert und zugewiesen. Da diese Kriterien bei der Zuweisung sicherheitsrelevanter Aufgaben angewendet werden, verfügen die Mitarbeiter, die diese Aufgaben ausführen, über die dafür erforderlichen Kompetenzen, Befugnisse und Ressourcen und sind sich der mit ihren Aufgaben verbundenen Risiken bewusst.

Die Kommunikation und Übernahme von Aufgaben **(2.3.3)**, einschließlich sicherheitsrelevanter Aufgaben, ist Teil des normalen Geschäftsprozesses dafür, wie Mitarbeitern Funktionen zugewiesen werden. Dies sollte im Rahmen eines Audits überprüft werden können. Die Zuweisung von Zuständigkeiten folgt einem systematischen Verfahren.

Das Management sollte über eine ausreichende Kenntnis und ein Verständnis der Probleme hinsichtlich menschlicher und organisatorischer Faktoren verfügen, um sicherzustellen, dass im Bedarfsfall Experten hinzugezogen werden. Die Aufgaben, Zuständigkeiten und Rechenschaftspflichten von Experten für menschliche und organisatorische Faktoren sollten gemäß den durchzuführenden Aufgaben definiert werden. **(2.3.3)**.

Es sollte ein Prozess eingerichtet sein, der sicherstellt, dass Personen Beinaheunfälle, Störungen und Unfälle ohne Angst vor Auswirkungen melden können. Die Politik unterstützt die Rechte und Zuständigkeiten von Personen, Sicherheitsbedenken zu äußern, und toleriert keine Belästigung, Einschüchterung, Vergeltung oder Diskriminierung für solche Handlungen. Der Schlüssel zum Erfolg einer gerechten Kultur ist Vertrauen und Offenheit in der Organisation. Diese(s) wird mit der Zeit aufgebaut und hängt von der Bereitschaft des Managements ab, umfassende Analysen nach Störungen und Unfällen durchzuführen sowie zuzuhören und zu lernen, bevor es reagiert. Die Kohärenz beim Umgang mit Sicherheitsbedenken ist wichtig für den Aufbau einer gerechten Kultur.

2.3.4 Nachweise

- *Ein Organigramm und relevante Erläuterungstexte, welche die Struktur der Organisation, entsprechende Sicherheitsverantwortlichkeiten und die Art, wie das Sicherheitsmanagementsystem aufgestellt und in den Kontext der Organisation eingebunden ist, erläutern;* ***(2.3.1), (2.3.4)***
- *Eine Liste weiterer Informationen, in der die Sicherheitsverantwortlichkeiten innerhalb der Struktur der Organisation aufgeführt sind;* ***(2.3.1), (2.3.3)***
- *Nachweise, dass ein Kompetenzmanagementsystem vorhanden ist und für alle Mitarbeiter gepflegt wird, das die Angemessenheit der Aufgaben mit zugewiesenen Verantwortlichkeiten, Kompetenzen und Ressourcen bewertet;* ***(2.3.2)***
- *Nachweise vom Kompetenzmanagementsystem oder anderen Verfahren im Bereich der Personalverwaltung wie Leistungsmanagement, dass die Organisation sicherstellt, dass Aufgaben und Zuständigkeiten Mitarbeitern kommuniziert und von diesen angenommen und eindeutig verstanden werden, und dass die Mitarbeiter für ihre Ausübung zur Rechenschaft gezogen werden;* ***(2.3.3)***
- *Eine Beschreibung der Verantwortlichkeiten für den Betrieb und die Instandhaltung, einschließlich einer Definition der Anforderungen, die Mitarbeiter bzw. Auftragnehmer gegebenenfalls erfüllen sollten;* ***(2.3.4)***
- *Die Strategie für menschliche und organisatorische Faktoren sollte Anforderungen dafür aufzeigen, wann und wie Fachwissen zu menschlichen und organisatorischen Faktoren herangezogen wird und was deren Aufgaben und Zuständigkeiten sind.* ***(2.3.1), (siehe ferner 4.6)***

2.3.5 Beispiele für Nachweise

Ein Organigramm, das durch zusätzlichen Text unterstützt wird und es dem Sachverständigen erlaubt, zu sehen, wie das Sicherheitsmanagementsystem strukturiert ist und wie die verschiedenen Teile miteinander in Verbindung stehen.

Verweis auf das Kompetenzmanagementsystem (CMS) mit Informationen über dessen Struktur sowie Links zu den detaillierten Angaben, einschließlich Beschreibungen der Personalverwaltungsprozesse, die es unterstützen, wie z. B. das Leistungsmanagement.

Ein Rückmeldeprozess wird bereitgestellt, um sicherzustellen, dass Informationen, die innerhalb der Organisation nach unten weitergegeben werden, klar verstanden werden.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Die Organisationsstruktur sieht eine eindeutige Zuweisung der Zuständigkeiten innerhalb der Organisation vor.

Die allgemeinen Strategien und Verfahren für die Aufgaben und Zuständigkeiten sind in der gesamten Organisation einheitlich.

Der Prozess, der abdeckt, wie Sicherheitsverantwortlichkeiten zugewiesen werden und wo Delegierungsbefugnisse erlaubt sind, mit Beispielen, die zeigen, wie der Prozess funktioniert hat, mit einer klaren Verknüpfung zu den Vereinbarungen über die Risikobewertung.

Beispiele für Aufgabenbeschreibungen von sicherheitsrelevanten Aufgaben, einschließlich derjenigen, die nicht direkt am Betrieb beteiligt sind und die die Durchführung des Betriebs indirekt beeinflussen (d. h. Zuweisung von Aufgaben, Betriebsplanung und Bereitstellung von betrieblichen Informationen für die Mitarbeiter, Aufsichtsmaßnahmen) sind verfügbar und werden bei Bedarf überprüft (z. B. bei Änderungen des Fahrplans).

Das SMS enthält Nachweise dafür, dass die Zuständigkeiten und Risiken im Zusammenhang mit den Aufgaben im Kompetenzmanagementsystem und in Schulungsprogrammen erfasst sind. Es liegen Nachweise vor (z. B. hat die Person, an die die Zuständigkeit delegiert wurde, dies schriftlich bestätigt), dass die Zuständigkeiten förmlich akzeptiert wurden.

Verfahren zur Erarbeitung, welche Kompetenzen und Ressourcen erforderlich sind, um die Sicherheitsaufgaben und -verantwortlichkeiten für alle Ebenen der Hierarchie zu unterstützen.

Die Strategie für menschliche und organisatorische Faktoren zeigt, wie diese in Prozessen und Projekten integriert sind. Das Fachwissen und die Tätigkeiten in Bezug auf menschliche und organisatorische Faktoren sind für den Umfang des Prozesses oder Projekts angemessen. Die Aufgaben und Zuständigkeiten, die Rechenschaftspflichten sowie die Phasen, in denen der Einsatz von Experten für menschliche Faktoren erforderlich ist, sind im Prozess- oder Projektplan definiert.

2.3.6 Referenzen und Standards

- *Rechenschaftspflichten und Verantwortlichkeiten hinsichtlich der Sicherheit (SKYbrary)*

2.3.7 Aufsichtsaspekte

Bei der Aufsicht ist das Ausmaß hier die zentrale Frage. Die Frage, die beantwortet werden muss, lautet: „Inwiefern spiegeln die bereitgestellten Informationen die Realität der Situation in der Praxis wider?“

Eine Untersuchung der Funktionsfähigkeit des Kompetenzmanagementsystems wird der Weg zur Beantwortung der meisten Fragen in diesem Abschnitt sein.

2.4 Konsultation der Mitarbeiter und anderer Beteiligter

2.4.1 Regulatorische Anforderung

2.4.1. Die Mitarbeiter, ihre Repräsentanten und – soweit angemessen und relevant – externe Beteiligte sind bei der Entwicklung, Aufrechterhaltung und Verbesserung der in ihre Zuständigkeit fallenden Teile des Sicherheitsmanagementsystems zu konsultieren, auch in Bezug auf die Sicherheitsaspekte von Betriebsverfahren.

2.4.2. Die Organisation muss die Konsultation der Mitarbeiter erleichtern, indem sie die Methoden und Mittel für die Einbeziehung des Personals bereitstellt, die Stellungnahmen des Personals festhält und Rückmeldungen zu den Stellungnahmen des Personals gibt.

2.4.2 Zweck

Der Antragsteller sollte Nachweise dafür bereitstellen, dass er seine eigenen Mitarbeiter (oder ihre Vertreter) sowie externe Interessengruppen aktiv an der Verwendung und Entwicklung des Sicherheitsmanagementsystems zur langfristigen Kontrolle der Risiken teilhaben lässt. Dies wird ebenfalls der bewertenden Behörde ebenfalls zeigen, wie die Sicherheitskultur innerhalb der Organisation aussieht und wie aktiv sie relevante Dritte am Management der Sicherheit in Bereichen beteiligt, in denen das Risiko geteilt ist.

Die Organisation bestätigt, dass keine einzelne Person über sämtliche Informationen verfügt, die benötigt werden, um die Sicherheit auf nachhaltige Art zu verwalten. Prozessexperten, Sicherheitsexperten, unterstützende Stellen, Mitarbeiter an vorderster Front, Führungs- und Aufsichtspersonen, Gewerkschaften und externe Auftragnehmer verfügen und nutzen allesamt Wissen und Informationen, die ausschlaggebend für die Sicherheit sind. Ihnen muss die Möglichkeit gegeben werden, sich zu treffen und ihre Ansichten zu diskutieren und auszudrücken, um das bestmögliche Verständnis der Realität am Arbeitsplatz zu erlangen. Besondere Beachtung muss den organisatorischen Schnittstellen zwischen Dienstleistungen, Abteilungen und Organisationen geschenkt werden. Der Austausch von Ideen und Informationen bei der Analyse und Behandlung von Risiken, Unfällen und Störungen sollte gefördert werden.

Die Beteiligung an der Meldung von sicherheitskritischen Informationen und die Teilnahme an der Analyse gefährlicher Situationen und Störungen werden durch ein Klima des Vertrauens unterstützt. Darüber hinaus werden frühe Angaben der Betriebsmitarbeiter bei der Durchführung der Risikobewertung, der Gestaltung oder Umgestaltung technischer Anlagen und beim Ausarbeiten neuer Verfahren aktiv eingeholt.

2.4.3 Erläuterungen

Externe Parteien **(2.4.1)** sind Organisationen, die eine Schnittstelle mit dem Antragsteller haben, wie zum Beispiel Auftragnehmer, Partner, Zulieferer, zuständige staatliche Stellen, örtliche Behörden oder die Notfalldienste.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Diese externen Gruppen **(2.4.1)** können bei für das Managementsystem relevanten Angelegenheiten hinzugezogen werden. Auftragnehmer können beispielsweise für sicherheitsrelevante Aufgaben wie die Vorbereitung der Züge oder die Instandhaltung der Infrastruktur verantwortlich sein. Wenn das Verfahren zur Vorbereitung der Züge oder zur Instandhaltung der Infrastruktur hinsichtlich Risiken bewertet wird, empfiehlt es sich, diese Auftragnehmer am Prozess zu beteiligen.

Das Fachwissen der Endnutzer ist wichtig, um ein gutes Verständnis der Arbeitsbedingungen sowie der Verfahren, Prozesse, Werkzeuge und Dokumentation zu gewährleisten, die mit ihrem Zweck in Einklang stehen. Die Konsultation der Mitarbeiter an vorderster Front von der Risikobewertung bis zur Auswahl und Erprobung von Dokumentation oder Ausrüstung wird dazu beitragen, eine nachhaltige und sichere Leistung (mit besserer Einhaltung durch das Personal) zu entwickeln.

Die Entwicklung einer positiven Sicherheitskultur wird durch eine gute Qualität und eine zeitnahe Mitteilung der relevanten Informationen an Personen, die diese benötigen, gefördert.

2.4.4 Nachweise

- *Der Antragsteller sollte Einzelheiten zum Prozess zur Konsultation von Mitarbeitern (oder ihren Vertretern) und relevanten Interessengruppen bereitstellen, einschließlich darüber, wie diese Konsultationen in Änderungen des Sicherheitsmanagementsystems oder spezifischer Betriebsverfahren umgesetzt werden;* ***(2.4.1), (2.4.2)***
- *Der Antragsteller sollte Informationen über das vorhandene System zur Rückmeldung der Ergebnisse der Konsultation an Mitarbeiter bereitstellen.* ***(2.4.2)***

2.4.5 Beispiele für Nachweise

Der Prozess oder das Verfahren zum Konsultieren von Mitarbeitern (und ggf. ihrer Vertreter) und Interessengruppen bei der Entwicklung des Sicherheitsmanagementsystems.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Beispiele für Protokolle von Konsultationssitzungen mit Mitarbeitern (und/oder ihren Vertretern) mit Aufzeichnungen der Ergebnisse.

Beispiele, wie Meinungen und Vorschläge von Mitarbeitern während des Änderungsmanagements (d. h. zu einem entworfenen/geänderten/neuen Betriebsverfahren) gesammelt werden und wie damit umgegangen wird.

Es wird ein Dokument/Verfahren bereitgestellt, das aufzeigt, wie die Betriebsmitarbeiter, die mit einem neuen oder entwickelten technischen System umgehen werden, in einem frühen Stadium (Planung und Entwicklung) der Arbeit beteiligt werden, um Angaben, die beispielsweise die Mensch-Maschine-Schnittstelle betreffen, zu sammeln.

Verfahren, die angeben, wie menschliche und organisatorische Faktoren in der Organisation in Verbindung mit den Geschäftszielen und den Prozessen der Organisation gehandhabt und ihre Ergebnisse kommuniziert werden sollen, z. B. Projekte, Untersuchungen von Störungen und Unfällen, Risikoanalysen und andere sicherheitsrelevante Aktivitäten für das eigene Personal, Auftragnehmer, Partner und Zulieferer.

Die Organisation sollte die Sicherheitserwartungen und erforderliche Verhaltensweisen klar definieren. Organisatorische Prioritäten werden abgestimmt, um in Konflikt stehende Ziele zu vermeiden. Es wird ein Prozess beschrieben zur Planung, Risikobewertung und Steuerung von Tätigkeiten, um sicherzustellen, dass die Sicherheit nicht durch andere geschäftliche Interessen beeinträchtigt wird, z. B. durch konservative Entscheidungsfindung. Sicherheitsziele stehen in Verbindung mit der Sicherheitskultur. Das Management übernimmt eine aktive Rolle bei der Planung und Einführung von erforderlichen Änderungen der Sicherheitskultur.

2.4.6 Aufsichtsaspekte

Die Konsultation und Beteiligung von relevanten Mitarbeitern ist sowohl intern als auch extern ein wichtiger Teil der Gewährleistung, dass Personen mit einschlägiger Erfahrung in der Lage sind, einen positiven Einfluss auf das Sicherheitsmanagementsystem der Organisation zu haben.

Die Aufsicht in diesem Bereich sollte auf die Aufzeichnungen abzielen, wie Mitarbeiter und externe Gruppen konsultiert werden und wie ihre Kommentare einfließen, sowie Aufzeichnungen der Änderungen am Sicherheitsmanagementsystem, die in diesem Bereich ihren Ursprung fanden, abdecken.

Besonderes Augenmerk sollte darauf gelegt werden, wie Rückmeldungen gegeben und daraus Erkenntnisse gewonnen werden.

3 Planung

3.1 Maßnahmen zur Beherrschung von Risiken

3.1.1 Regulatorische Anforderung

3.1.1. Risikobewertung

3.1.1.1. Die Organisation muss

(a) alle betrieblichen (einschließlich der menschlichen Leistungsfähigkeit), organisatorischen und technischen Risiken, die für die Art, den Umfang und Bereich von der Organisation durchgeführten Tätigkeiten relevant sind, erfassen und analysieren. Zu diesen Risiken zählen auch solche, die sich aus menschlichen und organisatorischen Faktoren wie Arbeitsbelastung, Arbeitsplatzgestaltung, Ermüdung oder der Eignung von Verfahren sowie aus den Tätigkeiten anderer Beteiligter ergeben (siehe 1. Kontext der Organisation);

(b) die unter Buchstabe a genannten Risiken mittels geeigneter Risikobewertungsmethoden evaluieren;

(c) Sicherheitsmaßnahmen entwickeln und in Kraft setzen sowie die damit verbundenen Zuständigkeiten angeben (siehe 2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse);

(d) ein System zur Überwachung der Wirksamkeit der Sicherheitsmaßnahmen entwickeln (siehe 6.1 Überwachung);

(e) die Notwendigkeit anerkennen, in Bezug auf gemeinsame Risiken und die Einführung geeigneter Sicherheitsmaßnahmen bedarfsweise mit anderen Beteiligten (u. a. Eisenbahnunternehmen, Infrastrukturbetreiber, Hersteller, Instandhaltungsbetriebe, für die Instandhaltung zuständige Stellen, Schienenfahrzeughalter, Dienstleister und Beschaffungsstellen) zusammenzuarbeiten;

(f) die Mitarbeiter und externe Beteiligte über Risiken informieren (siehe 4.4 Information und Kommunikation).

3.1.1.2 Bei der Risikobewertung muss die Organisation der Anforderung Rechnung tragen, eine sichere Arbeitsumgebung im Einklang mit den geltenden Rechtsvorschriften, insbesondere der Richtlinie 89/391/EWG, festzulegen, bereitzustellen und zu erhalten.

3.1.2. Planung von Änderungen

3.1.2.1. Bevor eine Organisation Änderungen vornimmt (siehe 5.4 Änderungsmanagement), muss sie im Einklang mit dem in der Durchführungsverordnung (EU) Nr. 402/2013 beschriebenen Risikomanagementprozess potenzielle Sicherheitsrisiken sowie geeignete Sicherheitsmaßnahmen ermitteln (siehe 3.1.1 Risikobewertung); dabei sind auch die sich aus dem Änderungsprozess selbst ergebenden Sicherheitsrisiken zu berücksichtigen.

3.1.2 Zweck

Diese Anforderung ist eines der zentralen Elemente des Sicherheitsmanagementsystems und zielt darauf ab, dass der Antragsteller aufzeigt, wie sein System die Risiken, mit denen er konfrontiert ist, identifiziert und

kontrolliert. Sie erfordert außerdem vom Antragsteller, zu zeigen, wie er die Ergebnisse der Risikobewertung in der Praxis anwendet, um die Risikokontrolle zu verbessern, und wie er dies im Laufe der Zeit überprüft. Es darf nicht vergessen werden, dass diese Anforderung sich nicht direkt mit dem Management der Risiken durch Änderungen (dies ist eine andere Anforderung) beschäftigt, sondern damit in Verbindung steht. Es sollte außerdem angemerkt werden, dass es eine spezifische Anforderung gibt, um mittels Risikobewertung Problemen in Bezug auf das menschliche Leistungsvermögen Rechnung zu tragen, wie beispielsweise die Arbeitsplatzgestaltung und das Risikomanagement bei Ermüdung.

Wie diese Informationen organisiert und als Teil des Sicherheitsmanagementsystems kommuniziert werden, muss der Antragsteller im Antrag beschreiben, und der Inhalt sollte die von der Organisation angetroffenen Risiken unter Berücksichtigung der Art, des Umfangs und des Bereichs des Betriebs (siehe den Kontext der Organisation) widerspiegeln. Es ist angemessen, sowohl den Risiken, für die der Antragsteller verantwortlich ist, als auch den Risiken, die sich aus Tätigkeiten Dritter ergeben, Rechnung zu tragen.

Ein allgemeines Verständnis in der gesamten Organisation, wie den Hauptrisiken vorgebeugt werden kann, wird als Priorität für ein gutes Sicherheitsmanagement angesehen. Die geringe Häufigkeit des Auftretens eines Szenarios sollte nicht dazu führen, dass es ignoriert wird. Um sicherzustellen, dass ein für die Risikobewertung ausgewähltes Szenario im Vergleich zum echten Betrieb realistisch ist, sollten Sicherheitsmanagementexperten und Betreiber an vorderster Front des Geschäfts darüber hinaus zur Sicherheitsanalyse und zur Risikobewertung beitragen. Die Ergebnisse dieser Bewertungen werden in einem zugänglichen und verständlichen Format an alle Akteure übermittelt, die zur Sicherheit beitragen. Das Management fördert Gespräche in Bezug auf die wichtigsten zu beherrschenden Risiken, um ein gemeinsames Verständnis und Bewusstsein zu gewährleisten. Zudem wird das Vorhandensein schwerwiegender Risiken im gesamten Lebenszyklus des Systems hervorgehoben.

3.1.3 Erläuterungen

Für die Zwecke der Bewertung eines Antrags sollte der Antragsteller zeigen, wie er die Richtlinie 89/391/EWG des Rates und damit verbundene Vorschriften einhält. Die Bewertung wird sich auf die Demonstration des Beherrschung dieser Probleme und nicht die Probleme selbst konzentrieren. Mit Problemen wie dem Ermüdungs- oder Stressmanagement sowie dem Testen der physischen und psychischen Eignung kann als rechtliches Problem im Rahmen der Gesundheit und Sicherheit am Arbeitsplatz umgegangen werden. Sie verfügen jedoch über eine Schnittstelle mit dem Kompetenzmanagementsystem (z. B. für Schulungen nach langer Abwesenheit) und der Arbeitszuweisung (Mitarbeitern sollten nur dann bestimmte Arbeiten zugewiesen werden, wenn sichergestellt wurde, dass sie sich dafür eignen), wie in den TSI OPE angegeben.

In Nummer 3.1.1.1 Buchstabe a des vorstehenden Rechtstextes wird in der englischen Fassung für die Zwecke der Bewertung bei der Anforderung an Infrastrukturbetreiber „type“ durch „character“ ersetzt (diese Änderung betrifft nicht die deutsche Fassung, da darin beide Begriffe mit „Art“ übersetzt sind).

„Tätigkeiten“ **(3.1.1.1 Buchstabe a)** sind hier sowohl die Aktionen, die Beteiligte (Auftragnehmer, Zulieferer und andere) im Namen von oder in Verbindung mit einem Antragsteller ausführen, als auch die Sachanlagen, die zur Unterstützung dieser Aktionen verwendet werden. Der Schlüsselpunkt liegt darin, dass der Antragsteller nachweisen muss, dass er über einen belastbaren Prozess für die Risikobewertung verfügt und dass allen relevanten Risiken Rechnung getragen wird. Einige Risiken (z. B. hydrogeologische Risiken, Risiken an Bahnübergängen, auf Züge geworfene Steine, unbefugte Personen) müssen ebenfalls von der Organisation berücksichtigt werden, wenn dies angemessen und zumutbar ist. Diese Probleme beziehen sich jedoch auf die Betriebsrisiken (da diese allesamt den Zugbetrieb betreffen) und eventuell nicht nur auf das menschliche Leistungsvermögen.

„Andere Beteiligte“ bezeichnet Organisationen und Personen. Diese Gruppen gehören unter Umständen nicht zum Eisenbahnnetz **(1.1 Buchstabe c)**.

Eine Änderung kann sicherheitsrelevant sein oder nicht **(3.1.2.1)**. Die Auswirkung von sicherheitsrelevanten Änderungen sollte bewertet und es sollten angemessene Sicherheitsmaßnahmen identifiziert werden, um die entsprechenden Risiken auf ein annehmbares Niveau zu reduzieren. Die Einführung eines Änderungsmanagementprozesses kann ebenso zu Sicherheitsrisiken führen, und zwar insbesondere dann, wenn entschieden wird, die Einführung einer Änderung zu verzögern, wenn es notwendig ist, die Entstehung eines weiteren Sicherheitsrisikos vollständig oder teilweise zu vermeiden. Das Risikomanagement **(3.1.1.1)** ist jedoch nicht allein auf das Änderungsmanagement beschränkt. Allgemein sollte die Organisation sicherstellen, dass die Sicherheitsrisiken in Bezug auf ihren Betrieb adäquat gehandhabt werden. Die Notwendigkeit der Identifizierung, Verwaltung und Kontrolle dieser Sicherheitsrisiken geht deshalb als Teil des Sicherheitsmanagementsystems des Antragstellers über das Änderungsmanagement und die Anwendung von CSM für die Evaluierung und Bewertung von Risiken hinaus.

Die CSM für die Evaluierung und Bewertung von Risiken gelten für alle technischen, betrieblichen und organisatorischen Änderungen (bei Letzteren für diejenigen, die sich auf den Betrieb oder die Wartung auswirken). Für jede sicherheitsrelevante Änderung muss der Antragsteller zuerst entscheiden, ob die Änderung signifikant ist (oder nicht). Wenn sie als signifikant angesehen wird, muss er nachweisen, dass die Risiken in Verbindung mit der Änderung unter Verwendung der in den CSM beschriebenen Grundsätze annehmbar sind und dass die Anforderungen, die sich aus diesem Nachweis ergeben, im geänderten System effektiv umgesetzt wurden. Die durchgeführte Risikobewertung wird dann durch eine unabhängige Bewertungs- oder eine anerkannte Stelle bewertet, die einen Bericht über die Annehmbarkeit (oder mangelnde Annehmbarkeit) der Analyse verfassen wird. Nationale Sicherheitsbehörden berücksichtigen solche Berichte bei ihren Aufsichtstätigkeiten, können die Ergebnisse des Berichts aber nur dann in Frage stellen, wenn sie Grund zu der Annahme haben, dass der Bewertungsprozess der Risikobewertung nicht korrekt befolgt wurde. Wenn die Änderung sicherheitsrelevant, aber nicht signifikant ist, muss der Antragsteller seine Entscheidung dokumentieren und muss trotzdem noch eine Risikobewertung der Änderung unter dem Risikomanagementprozess des Sicherheitsmanagementsystems durchführen. In diesem Fall unterliegt es der Verantwortung des Antragstellers, die angemessenen Risikobewertungsmethoden auszuwählen, um zu begründen, dass die Risikokontrollmaßnahmen, die er einführt, angemessen sind, um die zugehörigen Risiken auf ein annehmbares Niveau zu senken. Zwar ist die Auslösung der Anwendung der CSM für die Evaluierung und Bewertung von Risiken davon abhängig, ob eine Änderung signifikant ist oder nicht, jedoch kann die Organisation in jedem Fall die CSM für die Evaluierung und Bewertung von Risiken anwenden, zum Beispiel wenn sie der Ansicht ist, dass bei der Änderung aus geschäftlichen oder gesellschaftlichen Gründen eine unabhängige Bewertung der von der Organisation durchgeführten Arbeit angebracht ist. Weitere Informationen über den Handhabung signifikanter Änderungen sind dem ERA-Leitfaden zur gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken zu entnehmen.

Die CSM für die Evaluierung und Bewertung von Risiken enthält sechs Kriterien, die untersucht werden sollten, um die „Signifikanz“ zu bestimmen. Diese sind:

- ***Folgen von Ausfällen**: glaubhaftes schlimmstes anzunehmendes Szenario bei einem Ausfall des bewerteten Systems, unter Berücksichtigung des Vorhandenseins von Sicherheitsbarrieren außerhalb des Systems;*
- ***innovative Elemente in der Implementierung der Änderung**: Dies betrifft sowohl Innovativen im Eisenbahnbereich als auch Neues für die Organisation, welche die Änderung einführt;*
- ***Komplexität der Änderung**;*
- ***Überwachung**: die Unfähigkeit, die eingeführte Änderung im gesamten Lebenszyklus des Systems zu überwachen und entsprechende Maßnahmen zu ergreifen;*
- ***Umkehrbarkeit**: die Unfähigkeit, den Zustand, der vor der Änderung geherrscht hat, wiederherzustellen; und*

- ***Zusätzlichkeit**: Bewertung der Signifikanz der Änderung unter Berücksichtigung sämtlicher kürzlicher sicherheitsrelevanter Änderungen am bewerteten System und Festlegung, welche nicht als signifikant eingestuft werden.*

Diese Elemente sollten verwendet werden, um zu bewerten, wie von Organisationen gemäß der CSM für die Evaluierung und Bewertung von Risiken getroffene Entscheidungen über die „Signifikanz“ zustande gekommen sind.

Obwohl der in der CSM für die Evaluierung und Bewertung von Risiken angegebene Risikomanagementprozess im Falle von sicherheitsrelevanten und signifikanten Änderungen gilt, zählen die Grundsätze des Risikomanagementprozesses, die in dieser Vorschrift erlassen wurden, als bewährtes Verfahren für das Risikomanagement und können demnach in allen anderen Situationen angewandt werden, in denen eine Risikobewertung erforderlich ist.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Menschliche und organisatorische Faktoren kommen bei der Konzeption von (neuen) Systemen von Anfang an einheitlich zur Anwendung. Alle Ebenen der Organisation, einschließlich der Akteure an vorderster Front, werden proaktiv in die Risikobewertung einbezogen, wobei das Auftreten von Fehlern durch einen benutzerorientierten Ansatz frühzeitig erkannt wird, bei dem die Organisationsstruktur des Unternehmens, die Verfügbarkeit/Nutzung von Ausrüstung, die Gestaltung von Sicherheitsaufgaben, das Kompetenzmanagementsystem und die entsprechenden Verfahren bei der Bewertung von Sicherheitsrisiken und der Ermittlung von Sicherheitsmaßnahmen berücksichtigt werden.

Das Risikobewertungsverfahren umfasst Ansätze oder Methoden zur systematischen Berücksichtigung menschlicher und organisatorischer Faktoren und zielt darauf ab, bei allen SMS-Prozessen und -Verfahren nach Möglichkeit Risiken an der Quelle zu beseitigen. Wenn dies nicht möglich ist, sollte mit der Strategie für menschliche und organisatorische Faktoren angestrebt werden, die Folgen der Risiken so gering wie möglich zu halten.

Es gibt einen systematischen Ansatz für die Ermittlung der sicherheitsbezogenen Aufgaben und -prozesse und es werden Methoden aus dem Bereich der menschlichen und organisatorischen Faktoren für die Analyse der sicherheitskritischen Aufgaben verwendet, z. B. Aufgabenanalyse, hierarchische Aufgabenanalyse, tabellarische Aufgabenanalyse. Professionelles Fachwissen zu menschlichen und organisatorischen Faktoren sollte eingesetzt werden, um angemessene Methoden auszuwählen und anzuwenden.

Der Risikobewertungsprozess sollte die Beteiligung von Experten für menschliche und organisatorische Faktoren und die relevanten Kompetenzen für Benutzer und andere Interessengruppen beschreiben. Dies könnte beispielsweise eine Beschreibung umfassen, in welchem Ausmaß Experten für menschliche und organisatorische Faktoren an der Risikoanalyse beteiligt sein sollten und welcher Kompetenzgrad hinsichtlich menschlicher und organisatorischer Faktoren notwendig ist.

Es werden angemessene Methoden für die Integration von menschlichen und organisatorischen Faktoren in die Risikobewertung beschrieben, z. B. Aufgabenanalyse, Verwendbarkeitsanalyse, Simulation, menschliche HAZOP, Bow-Tie-Analyse.

3.1.4 Nachweise

- *Der Antragsteller sollte Nachweise dafür erbringen, dass er über einen Risikobewertungsprozess verfügt (einschließlich einer Beschreibung der verwendeten Methodologien, der beteiligten Mitarbeiter und einer etwaigen durchgeführten Validierung oder Verifizierung), der sowohl die im Rahmen der CSM für die Evaluierung und Bewertung von Risiken (Durchführungsverordnung (EU) Nr. 402/2013 der Kommission) als wichtige Änderungen identifizierten Risiken als auch die als nicht*

wichtig angesehenen Risiken, die dennoch kontrolliert werden sollten, erfasst. Der Prozess deckt sämtliche betrieblichen, organisatorischen und technischen Risiken ab; ***(3.1.1.1 Buchstaben a und b)***

- *Nachweis, dass Risiken im Zusammenhang mit Problemen der menschlichen und organisatorischen Faktoren in den Bewertungen berücksichtigt werden. Die Strategie für menschliche und organisatorische Faktoren muss aufzeigen, wann und wie menschliche und organisatorische Faktoren ein integraler Bestandteil des Risikobewertungsprozesses sind und die Anwendung von geeigneten Methoden und von Fachwissen demonstrieren;* ***(3.1.1.1 Buchstabe a)***
- *Nachweis für Mittel zum Hinzuziehen von Dritten zum Risikobewertungsprozess, wo dies angemessen ist, einschließlich einer Beschreibung, wie Risiken Dritter, welche den Betrieb des Eisenbahnunternehmens oder des Infrastrukturbetreibers beeinträchtigen, beherrscht werden;* ***(3.1.1.1 Buchstabe a), (3.1.1.1 Buchstabe e), (3.1.1.1 Buchstabe f)***
- *Nachweis, dass der Antragsteller über einen Prozess zur Entwicklung und Einführung von Risikokontrollmaßnahmen verfügt, einschließlich einer Definition der Person, die für die Gewährleistung von deren Durchführung verantwortlich ist;* ***(3.1.1.1 Buchstabe c)***
- *Der Antragsteller sollte angeben, wie er die Ergebnisse der Risikobewertung und die zugehörigen Kontrollmaßnahmen den relevanten Mitarbeitern mitteilt und diese daran beteiligt;* ***(3.1.1.1 Buchstabe f)***
- *Der Antragsteller sollte aufzeigen, wie er die Effektivität seiner Risikokontrollmaßnahmen überwacht, einschließlich der Art, wie Prozesse oder Verfahren nach Bedarf aktualisiert werden;* ***(3.1.1.1 Buchstabe d)***
- *Innerhalb der bereitgestellten Nachweise sollte der Antragsteller angeben, wie er die Notwendigkeit der Konformität mit anderen geltenden Rechtsvorschriften berücksichtigt, wie beispielsweise die unter der Richtlinie 89/391/EWG des Rates;* ***(3.1.1.2)***
- *Der Antragsteller bietet Nachweise, um als Teil seines Änderungsmanagementprozesses aufzuzeigen, dass der Einfluss von Änderungen systematisch beurteilt wird. Dies wird die Anwendung der Risikobewertung umfassen, einschließlich der Verwendung der CSM für die Evaluierung und Bewertung von Risiken zur Ermittlung der Risiken und der nötigen Kontrollmaßnahmen. Der Antragsteller stellt ebenfalls Nachweise dafür zur Verfügung, dass die während des Änderungsmanagementprozesses ermittelten Kontrollmaßnahmen eingeführt wurden.* ***(3.1.2.1)***

3.1.5 Beispiele für Nachweise

Ein Risikobewertungsprozess oder -verfahren, ggf. einschließlich einer Beschreibung, wie und wann die Ausfalleffektanalyse, die HAZOP-Studie oder andere Techniken verwendet werden, um die Einführung von Kontrollmaßnahmen zur Beherrschung von Risiken zu unterstützen.

Nachweise wie ein Gefahrenregister, das zeigt, dass die Organisation über einen Prozess zur systematischen Bewertung von Gefahren als ersten Schritt des Risikomanagements verfügt, und das mit den Ergebnissen der Überwachung gespeist wird, das immer dann aktualisiert wird, wenn neue Risiken erkannt werden, und mit geeigneten Informationen zu Sicherheitsmaßnahmen ergänzt wird, die eingeführt wurden, um das Risiko zu beherrschen (z. B. technische Ausrüstung, Liste sicherheitskritischer Komponenten, Betriebsverfahren, Mitarbeiterschulung).

Das Verfahren zur Einhaltung anderer relevanter EU-Rechtsvorschriften wie der Richtlinie 89/391/EWG des Rates, sofern Risiken in Bezug auf die Mitarbeiter (Tod, vorübergehende oder permanente Gesundheitsschädigungen, Beinaheunfälle) vom Rechtsrahmen für Sicherheit und Gesundheitsschutz am Arbeitsplatz abgedeckt werden können. Die Kontrollmaßnahmen sollten aber in die Betriebsregeln aufgenommen werden oder diese ergänzen.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Eine Übersicht über die Prozesselemente, anhand derer menschliche und organisatorische Faktoren bei der Risikobewertung berücksichtigt und Dritte soweit erforderlich einbezogen werden. Aus Sitzungsprotokollen geht hervor, dass die Endnutzer sowie die Experten für menschliche und organisatorische Faktoren teilgenommen haben und dass ihre Meinungen berücksichtigt wurden.

Beispiele für durchgeführte Analysen, bei denen Anzahl und Art der auszuführenden Aufgaben, ihre Komplexität, ihre Wiederholung, die Übertragung von Aufgaben, die Arbeitsbelastung (einschließlich Dienstplan, Schichten, Einsatz von Maschinen und einschlägigen Anweisungen usw.), die Klarheit und Vollständigkeit der Vorschriften und Arbeitsanweisungen, Rückmeldungen der Mitarbeiter und die Art und Weise, wie Abhilfemaßnahmen ergriffen werden, berücksichtigt werden.

Das Verfahren zur Mitteilung der Ergebnisse der Risikobewertungen an Mitarbeiter, gegebenenfalls mit veranschaulichenden Beispielen.

Eine Angabe des Prozesses, um sicherzustellen, dass die an jede Mitarbeiterkategorie delegierten sicherheitsrelevanten Aufgaben wie folgt gestaltet werden:

- *Das Volumen der auszuführenden Aufgaben ist zu Zeiten, in denen eine sicherheitsrelevante Aufgabe durchgeführt wird, nicht überhöht.*
- *Wo sicherheitsrelevante Aufgaben kombiniert werden, kann die Organisation aufzeigen, dass das Sicherheitsniveau beibehalten wird.*
- *Es gibt keine Widersprüche zwischen der Ausführung von sicherheitsrelevanten Aufgaben und anderen den Mitarbeitern zugewiesenen Zielen (in Übereinstimmung mit 2.1.1 Buchstabe j).*

Eine Strategie für menschliche und organisatorische Faktoren, die mit den Risikobewertungsprozessen verbunden ist. Dies zeigt auf, dass die Ergebnisse der Risikoanalysen verwendet und dass die Sicherheit verbessernde Maßnahmen eingeführt und beurteilt werden.

Einige menschliche und organisatorische Faktoren, die im Rechtsrahmen für Sicherheit und Gesundheitsschutz am Arbeitsplatz behandelt werden, sowie wichtige Themen wie Ermüdung, arbeitsbedingter Stress und physische Arbeitsumgebung (z. B. Sauberkeit, Temperatur, Licht); in diesem Fall sollte die Dokumentation zu Sicherheit und Gesundheitsschutz am Arbeitsplatz über das SMS verwaltet werden.

3.1.6 Referenzen und Standards

- *Leitfaden der Agentur zur Anwendung der CSM für die Risikobewertung*
- *Risikoakzeptanzkriterien für technische Systeme und in verschiedenen Industrien angewandte Betriebsverfahren*
- *Leitlinie zur Unterstützung der Umsetzung der Verordnung (EU) 2015/1136 im Hinblick auf harmonisierte Entwurfsziele (CSM DT) im Rahmen der CSM für die Risikobewertung*
- *ISO 31000:2018 Risikomanagement*
- *ISO 31010:2019 Risikomanagement – Verfahren zur Risikobeurteilung*
- *ISO 45001:2018 Managementsysteme für Sicherheit und Gesundheit bei der Arbeit – Praktischer Leitfaden für kleine Organisationen*
- *CENELEC – EN 50126 Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Grundlegende Anforderungen und genereller Prozess*
- *Office of the National Rail Safety Regulator - Asset management guideline (2019)*

3.1.7 Aufsichtsaspekte

Der Prozess der Risikobewertung sollte bei der Durchführung der Aufsicht im Mittelpunkt des Sicherheitsmanagementsystems stehen. Daher sollte es möglich sein, anhand von Interviews und Prüfungen der Dokumentation und der Prozesse festzustellen, ob dies tatsächlich der Fall ist. Ergebnisse aus der Aufsicht, die für die zukünftige Verlängerung einer einheitlichen Sicherheitsbescheinigung oder Sicherheitsgenehmigung relevant sein werden, sind dabei von zentraler Bedeutung. Zusätzlich sollten Ergebnisse aus der Aufsicht der Risikobewertungsprozesse nach Bedarf einen Beitrag zur Aufsichtsstrategie der nationalen Sicherheitsbehörde bilden.

Die folgenden Informationen können als Beiträge für spätere Aufsichtstätigkeiten dienen:

- *Gefahrenliste;*
- *Ergebnisse der Risikoanalyse, einschließlich, wo angemessen, Berichte der Risikobewertungsstelle bzw. -stellen;*
- *Begründung der Verwendung von Risikobewertungsmethoden (z. B. die Ausfalleffekt- und Ausfallkritizitätsanalyse, die Schnellmaßnahme, ETA und HAZOP), einschließlich der Art, wie Risikobewertungskriterien festgelegt werden und wie der Schweregrad und die Wahrscheinlichkeit des Auftretens der Gefahr bestimmt werden;*
- *Gegebenenfalls eine Einstufung der gefährlichen Ereignisse nach Gegenstand, Auswirkungen oder Ursachen (z. B. vorläufige Gefahrenliste).*

Mitarbeiter mit Verantwortlichkeiten in Verbindung mit der Risikobewertung sollten sich ihrer Rolle und der Wichtigkeit des Prozesses bewusst sowie kompetent sein, um sie effektiv auszuführen.

Es ist besonders wichtig, dass eine Reihe von Beispielen für Risikobewertungen untersucht wird, da diese zeigen werden, ob Risiken ordnungsgemäß anhand einer angemessenen Methodologie berücksichtigt wurden. Die Beobachtung in der Praxis sollte dann aufzeigen, dass die identifizierten Kontrollmaßnahmen vorhanden sind.

3.2 Sicherheitsziele und Planung

3.2.1 Regulatorische Anforderung

3.2.1. Die Organisation muss Sicherheitsziele für relevante Funktionen auf relevanten Ebenen festlegen, um ihre Sicherheitsleistung zu erhalten und, soweit nach vernünftigem Ermessen möglich, zu verbessern.

3.2.2. Die Sicherheitsziele müssen

(a) mit der Sicherheitsordnung und den strategischen Zielen der Organisation (soweit vorhanden) im Einklang stehen;

(b) mit den Hauptrisiken, die die Sicherheitsleistung der Organisation beeinflussen, verknüpft sein;

(c) messbar sein;

(d) den einschlägigen rechtlichen und sonstigen Anforderungen Rechnung tragen;

(e) im Hinblick auf die erzielten Erfolge überprüft und gegebenenfalls überarbeitet werden;

(f) kommuniziert werden.

3.2.3. Die Organisation muss über einen Plan bzw. Pläne verfügen, in denen beschrieben wird, wie die Sicherheitsziele erreicht werden sollen.

3.2.4. Die Organisation muss die Strategie und den Plan/die Pläne zur Überwachung der Erreichung der Sicherheitsziele beschreiben (siehe 6.1 Überwachung).

3.2.2 Zweck

Um sicherzustellen, dass die Organisation gesetzliche Anforderungen erfüllt und gewährleistet, dass das Konzept der kontinuierlichen Verbesserung der Sicherheit den Mitarbeitern kommuniziert und vom Management angenommen wird.

Der Antragsteller muss nachweisen, dass er über bedeutsame Ziele und einen Prozess zur Umsetzung und Überwachung dieser Ziele während ihrer Lebensdauer verfügt.

3.2.3 Erläuterungen

Sicherheitsleistung bedeutet hier die Leistung der Organisation im Vergleich zu ihren Sicherheitszielen und die Leistung des Sicherheitsmanagementsystems und aller Prozesse und Verfahren, die dies unterstützen.

Der Begriff „Sicherheitsziele“ ist mit dem Begriff „Sicherheitsvorgaben“ austauschbar, obwohl Letzterer eher eine numerische Bedeutung hat. Sicherheitsziele oder Sicherheitsvorgaben unterscheiden sich von gemeinsamen Sicherheitszielen (CST), die auf Ebene der Mitgliedstaaten festgelegt werden. Manche Unternehmen nutzen eventuell Letztere als die zu erreichenden Ziele, um ihre Sicherheitsleistung beizubehalten oder zu verbessern.

Die Ziele sollten regelmäßig mithilfe eines Planen-Umsetzen-Überprüfen-Handeln-Ansatzes überprüft werden, und beim Festlegen von Prioritäten sollten die Ergebnisse der Risikobewertung und vorheriger Überwachungen sowie Unfall- und Störungsuntersuchungen berücksichtigt werden, um die Sicherheitsleistung beizubehalten und, wo praktisch durchführbar, zu verbessern.

Die Festlegung und Überwachung von Sicherheitsleistungsindikatoren, welche die Entscheidungsfindung der Organisation hinsichtlich der Risikokontrolle unterstützen, und ob dies effektive Beiträge zur Bestimmung und Überprüfung von Sicherheitszielen sind.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Sicherheitsziele sind mit Risiken verbunden, da Letztere die Sicherheitsleistung der Organisation beeinflussen werden (d. h. die angestrebten Ergebnisse des Sicherheitsmanagementsystems und daher den Erfolg beim Erreichen der Ziele). Sicherheitsziele können quantitativ sein und werden durch eine Reduzierung der Anzahl an Ereignissen als Absolutwert oder als Prozentsatz dargestellt. Sicherheitsziele können auch qualitativ sein und werden dann als allgemeiner Wert ausgedrückt, wie „Sicherheit an Bahnübergängen wird verbessert“ oder „das aktuelle Sicherheitsniveau wird beibehalten“. In diesem Fall muss jedoch das Maß der Verbesserung oder das Niveau, auf dem die Sicherheit aufrechterhalten wird, anhand bestimmter Kriterien festgelegt und überwacht werden, um festzustellen, ob die Sicherheitsziele erreicht werden.

Die Organisation legt SMART-Ziele fest und teilt sie den Mitarbeitern mit, damit sie sich der Relevanz und Bedeutung ihrer Tätigkeiten bewusst werden und erkennen, wie sie zur Erreichung der Sicherheitsziele und zur Planung des Sicherheitsrisikomanagements beitragen. Die Mitarbeiter sind sich zudem bewusst, dass die Erreichung der Ziele überwacht und erforderlichenfalls überprüft wird.

Die Ziele werden gemäß der Risikobewertung und im Einklang mit der Sicherheitsordnung priorisiert.

3.2.4 Nachweise

- *Es gibt einen Satz von SMART-Sicherheitszielen, die in die weiter gefassten Geschäftsanforderungen der Organisationen passen;* ***(3.2.1), (3.2.2 Buchstaben a, b und c)***
- *Eine Aussage zu den gesetzlichen Anforderungen und wie diese eingehalten werden;* ***(3.2.2 Buchstabe d)***
- *Beschreibung, wie diese Ziele erreicht werden können und wie sie gegenüber den relevanten Mitarbeitern kommuniziert werden;* ***(3.2.2 Buchstabe f), (3.2.3)***
- *Es ist ein Überwachungsprozess eingerichtet, der mit den Anforderungen in den CSM für die Kontrolle (Verordnung (EU) Nr. 1078/2012) für die Ziele vereinbar ist, um sicherzustellen, dass die Ziele stets zweckmäßig sind und dass die Organisation ihre Ziele erreicht.* ***(3.2.2 Buchstabe e), (3.2.4)***

3.2.5 Beispiele für Nachweise

Der Prozess, anhand dessen Sicherheitsziele festgelegt, priorisiert und überwacht werden und die Art, wie Konflikte mit anderen Zielen vermieden und andernfalls behoben werden. Dies sollte die Ebene umfassen, auf der die Ziele festgelegt werden, die Art, wie diese gegebenenfalls zu anderen Zielen auf anderen Ebenen beitragen. Zudem sollten die Schnittstellen, die zeitliche Austaktung und alle notwendigen unterstützenden qualitativen oder quantitativen Daten erfasst sein.

Die Sicherheitsziele und der Plan für ihre Umsetzung sowie der Prozess, der zu befolgen ist, wenn sich herausstellt, dass die Sicherheitsziele verfehlt werden.

Die Sicherheitsziele stimmen mit der in der Sicherheitsordnung erklärten Mission und Vision überein und daher kann angenommen werden, dass sie von den Mitarbeitern geschätzt werden und ihr Engagement, diese zu erreichen, gestärkt wird.

Der Prozess oder das Verfahren, die Ergebnisse von Überwachungstätigkeiten in Sicherheitsziele umzuwandeln, die Planung der Tätigkeiten, um diese zu erreichen und zugehörige Erfolgsindikatoren.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Durch den strategischen Plan der Organisation, in dem die Sicherheit vorrangiges Ziel ist.

Bestimmungen im Rahmen des SMS (Risikomanagementprozess), in denen erläutert wird, wie Konflikte zwischen den Zielen zu bewältigen sind.

Ein Verfahren zur Konsultation der Mitarbeiter zu Sicherheitszielen und das Verfahren zur Festlegung und Mitteilung individueller Sicherheitsziele sowie zur Ermittlung ihrer formalen Akzeptanz durch die Mitarbeiter. Im Rahmen dieses Verfahrens wird erläutert, wo die Mitarbeiter die Ziele finden können, wie sie erfahren, welcher Beitrag von ihnen zur Erreichung dieser Ziele erwartet wird, und wie diese im Hinblick auf den Erfolg überprüft/gemessen werden, wie sie gestaltet und wie sie erreicht werden sollen.

Ein Verfahren für die Mitteilung von Zielen an die Mitarbeiter, das zeigt, wie die Sensibilisierung gestärkt und das Verständnis überprüft wird.

Ein Berichtsverfahren, bei dem die Mitarbeiter die Erreichung der Sicherheitsziele angeben.

3.2.6 Aufsichtsaspekte

Eine zentrale Frage für die Aufsicht wird sein, wie erreichbar die festgelegten Ziele in der Praxis sind und was tatsächlich passiert, wenn klar wird, dass sie wahrscheinlich nicht erzielt werden.

Wie die Sicherheitsziele festgelegt und überprüft werden – dass die Ziele sich auf empfindliche oder kritische Tätigkeiten/Kontrollen konzentrieren und Ergebnis- und Tätigkeitsindikatoren nutzen.

Wie die Organisation durch ihre Sicherheitsziele eine kontinuierliche Verbesserung der Risikokontrolle nachweist.

Wie die Organisation ihre Sicherheitsleistung effektiv überwachen und demnach die CSM für die Kontrolle nutzen kann, um die Leistung im Vergleich zu den Sicherheitszielen und den zugehörigen Sicherheitsleistungsindikatoren zu bewerten.

Wie Ziele (z. B. vor einigen Jahren definiertes Ziel) sich von ihrer Festlegung bis zur endgültigen Verwirklichung (oder Nichtverwirklichung) entwickeln.

4 Unterstützung

4.1 Ressourcen

4.1.1 Regulatorische Anforderung

4.1.1.	Die Organisation muss die für die Einführung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung des Sicherheitsmanagementsystems notwendigen Ressourcen bereitstellen, wozu auch qualifiziertes Personal sowie effiziente und benutzbare Betriebsmittel gehören.

4.1.2 Zweck

Der Zweck dieser Anforderung ist es, sicherzustellen, dass die Organisation über Prozesse verfügt, um ausreichende Ressourcen zur Verfügung zu stellen, wie beispielsweise technische Ausrüstungen, Systeme oder kompetente Mitarbeiter, um es ihrem Sicherheitsmanagementsystem zu ermöglichen, Risiken in Übereinstimmung mit ihren Zielen zu kontrollieren.

4.1.3 Erläuterungen

Die Zuweisung ausreichender Ressourcen ist eine Voraussetzung dafür, ein ausreichendes Maß an Sicherheit zu erreichen.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Das Unternehmen stellt sicher, dass den Mitarbeitern die notwendigen Ressourcen zur Verfügung gestellt werden, damit sie ihre Aufgaben sicher wahrnehmen können. Dazu gehören Personalausstattung, Ausrüstung und Dokumentation. Diese Anforderung steht zudem im Zusammenhang mit der Risikobewertung und den ermittelten Sicherheitsmaßnahmen.

4.1.4 Nachweise

- *Informationen hinsichtlich des Kompetenzmanagementsystems (CMS) oder, falls kein Kompetenzmanagementsystem vorhanden ist, ein Nachweis, wie die Organisation sicherstellt, dass sie über ausreichend kompetente Mitarbeiter verfügt;* ***(4.1.1)***
- *Informationen darüber, wie die Organisation sicherstellt, dass sie über ausreichend effektive und verwendbare Ausrüstung verfügt, um es ihr zu ermöglichen, ihre Dienstleistungsverpflichtungen zu erfüllen und ein effektives Sicherheitsmanagementsystem zu pflegen, das Risiken beherrscht;* ***(4.1.1)***
- *Informationen hinsichtlich der Organisation von Instandhaltungsfunktionen (siehe ferner Anhang II der Verordnung (EU) 2019/779 über die für die Instandhaltung zuständigen Stellen) und die Art, wie dies mit der Bereitstellung ausreichender Ressourcen in Verbindung steht, um es der Organisation zu ermöglichen, ihre Dienstleistungsverpflichtungen zu erfüllen;* ***(4.1.1)***

4.1.5 Beispiele für Nachweise

Das Kompetenzmanagementverfahren oder Angaben zum Prozess, mit dem sichergestellt werden soll, dass die Organisation über kompetente Mitarbeiter in relevanten Rollen verfügt, ggf. auch mit detaillierten Bewertungs- und Schulungsprogrammen. **(siehe ferner 4.2)**

Eine Erklärung, in der der Prozess der Ressourcenzuweisung beschrieben wird, um den betrieblichen Erfordernissen gerecht zu werden, sowie einschlägige Verweise auf Belege.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Eine Erklärung zu den Verfahren für die Entscheidung über den Personalbedarf, damit das SMS effizient funktioniert, zusammen mit Angaben zu relevanten Referenzverfahren oder Prozessen, in denen weitere Informationen zu finden sind.

Ein Prozess, in dem erläutert wird, wie die Ressourcen aufgrund der Risikobewertung und der zur Durchführung einer Aufgabe beschlossenen Sicherheitsmaßnahmen zugewiesen werden, darunter zeitliche und personelle Ressourcen sowie Kompetenzen (einschließlich überfachlicher Fähigkeiten), Verfahren, Werkzeuge und Ausrüstung.

Die Ergebnisse von Aufgabenanalysen, aus denen hervorgeht, dass unter Berücksichtigung der Arbeitsbelastung angemessene zeitliche und personelle Ressourcen festgelegt werden. Der Prozess wird in ähnlicher Weise für alle Sicherheitsaufgaben in allen Geschäftsbereichen durchgeführt (Fernverkehr/Kurzstreckenverkehr, Triebfahrzeugführer, Rangierdienste, Instandhaltung usw.).

Ein Dokument, in dem die zugewiesenen Ressourcen für geplante Änderungen in der Organisation dargelegt werden (einschließlich Personalausstattung und Bereitstellung nötiger Ausrüstung).

4.1.6 Aufsichtsaspekte

Prüfung, ob der Kompetenzrahmen und die Ausrüstungsanforderungen eindeutig mit den Ergebnissen der Risikobewertung verknüpft sind.

Durch die Prüfung der CMS sollte die nationale Sicherheitsbehörde prüfen, ob die Organisation über Mittel zur Identifizierung und Beibehaltung von Mitarbeitern mit den richtigen Fähigkeiten verfügt, um es ihnen zu ermöglichen, ihre Aufgaben sicher auszuführen. Von zentraler Bedeutung ist dabei, wie das CMS auf dem neuesten Stand gehalten wird.

Bei der Betrachtung der Instandhaltungstätigkeiten, die sich auf diese Vorgabe beziehen, sollten diejenigen, die eine Aufsicht durchführen, versuchen sicherzustellen, dass dort, wo diese Tätigkeiten an Unterauftragnehmer vergeben werden, das Eisenbahnunternehmen oder der Infrastrukturbetreiber seine Aufsichtsfunktion ausübt, um sicherzustellen, dass Auftragnehmer das richtige und verwendungssichere Produkt liefern.

Die Prüfung der Vakanz-Überbrückungen in bestimmten Bereichen des Sicherheitsmanagementsystems kann als Indikator für die Eignung oder Nicht-Eignung des Personals verwendet werden.

Die Art, wie Ausrüstung verwendet wird, z. B. wie viele Ersatzteile mit an die Arbeitsstelle gebracht werden, kann ebenso ein Hinweis auf die Qualität der bereitgestellten Ausrüstung und somit der Eignung der Ressourcen sein.

4.2 Kompetenz

4.2.1 Regulatorische Anforderung

4.2.1. Das Kompetenzmanagementsystem der Organisation muss sicherstellen, dass die Mitarbeiter mit Aufgaben, die die Sicherheit betreffen, zur Erfüllung der in ihre Zuständigkeit fallenden sicherheitsrelevanten Aufgaben befähigt sind (siehe 2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse). Es umfasst mindestens

(a) die Ermittlung der für die sicherheitsrelevanten Aufgaben notwendigen Kompetenzen (Kenntnisse, Fertigkeiten, nicht fachbezogene Verhaltensweisen und innere Einstellungen u. a.);

(b) Auswahlkriterien (Mindestausbildungsniveau, erforderliche psychische und physische Eignung);

(c) Erstausbildung, Erfahrung und Qualifikation;

(d) fortlaufende Schulungen und regelmäßige Aktualisierung vorhandener Kompetenzen;

(e) die regelmäßige Bewertung der Befähigung und Überprüfung der psychischen und physischen Eignung, um sicherzustellen, dass Qualifikationen und Fähigkeiten auf Dauer erhalten bleiben;

(f) spezifische Schulungen zu den relevanten Teilen des Sicherheitsmanagementsystems, damit die sicherheitsrelevanten Aufgaben erfüllt werden können.

4.2.2. Die Organisation muss für Mitarbeiter, die sicherheitsrelevante Aufgaben wahrnehmen, ein Programm für Schulungen nach Nummer 4.2.1 Buchstaben c, d und f bereitstellen, das Folgendes gewährleistet:

(a) das Schulungsprogramm wird entsprechend den ermittelten Kompetenzanforderungen und individuellen Bedürfnissen des Personals durchgeführt;

(b) soweit relevant wird durch die Schulung sichergestellt, dass das Personal unter allen Betriebsbedingungen (Regelbetrieb, gestörter Betrieb und Notfälle) eingesetzt werden kann;

(c) die Dauer der Schulung und die Häufigkeit der Auffrischungsschulung sind den Ausbildungszielen angemessen;

(d) für alle Mitarbeiter werden Aufzeichnungen geführt (siehe 4.5.3 Kontrolle dokumentierter Informationen);

(e) das Schulungsprogramm wird regelmäßig überprüft und Audits unterzogen (siehe 6.2 Interne Auditierung) sowie nach Bedarf geändert (siehe 5.4 Änderungsmanagement).

4.2.3. Für Mitarbeiter, die nach einem Unfall/Ereignis oder nach längerer Abwesenheit wieder an den Arbeitsplatz zurückkehren, müssen Regelungen für die Wiedereingliederung bestehen, wozu auch zusätzliche Schulungen gehören, wenn dies für notwendig erachtet wird.

4.2.2 Zweck

Zweck dieser Anforderung ist es, sicherzustellen, dass die Organisation über geeignete Strukturen und Ressourcen verfügt, um die Risiken, denen sie ausgesetzt ist, zu kontrollieren, und es ihr zu ermöglichen, Personal einzusetzen, das befähigt ist, die Sicherheitsaufgaben zu erfüllen, insbesondere die sicherheitskritischen Aufgaben, die es wahrnimmt. Das Kompetenzmanagementsystem wird es der Organisation zudem ermöglichen, die Fähigkeiten, das Wissen und die Erfahrung ihrer Mitarbeiter im Laufe der Zeit aufrechtzuerhalten.

Kompetenz spielt eine zentrale Rolle bei der Sicherstellung einer zufriedenstellenden Ausübung von Tätigkeiten. Der Bedarf an kompetentem Personal erstreckt sich sowohl auf den Front-Support (einschließlich Auftragnehmer, Berater und Anbieter von sicherheitsrelevanten Dienstleistungen) als auch auf das Führungspersonal. Die Anforderungen an die Managementkompetenz werden häufig übersehen, aber die Führungskräfte treffen wichtige Entscheidungen, die grundlegende und weitreichende Auswirkungen auf Gesundheit und Sicherheit haben können. Diese sollten Bestimmungen für die Schulung des gesamten Personals in Bezug auf die erforderlichen Sicherheitsstandards, für die Aufrechterhaltung der Kompetenz, unabhängig von den Umständen, einschließlich Fragen wie der Verfügbarkeit des Personals, und für die Überwachung der Kompetenzniveaus in Bezug auf die geforderten Standards enthalten.

In diesem Zusammenhang wird Sicherheit als integraler Bestandteil von professionellem Verhalten und Professionalität gesehen – und nicht als „zusätzliche Schicht“, die den beruflichen Fähigkeiten hinzugefügt werden soll. Auch die Fähigkeit einer Organisation, sich in Echtzeit mit unerwarteten Ereignissen zu befassen, hängt in hohem Maße von der Kompetenz der Mitarbeiter an vorderster Front und ihrer Vorgesetzten ab. Diese Kompetenzen können beispielsweise entwickelte Simulationen und regelmäßige Übungen komplexer Szenarien sein.

4.2.3 Erläuterungen

Ein Schulungsprogramm **(4.2.2)** kann über ein Schulungszentrum Dritter bereitgestellt werden. In diesem Fall sollte die Organisation sicherstellen, dass das Schulungszentrum befähigt ist, die entsprechenden Dienstleistungen zu erbringen, sei es, weil es im Rahmen eines nationalen oder europäischen Systems zertifiziert oder anerkannt wurde, oder durch direkte Überwachung der Schulungsaktivitäten und der daraus resultierenden Ergebnisse. Schulungszentren können sämtliche Schulungsbedürfnisse einer Organisation oder, basierend auf ihren Kompetenzen in den verschiedenen Bereichen, nur einige wenige davon abdecken. Wenn ein externes Schulungszentrum Schulungen für eine Organisation durchführt, dann muss diese Organisation prüfen, ob die Schulung die nötigen Elemente abdeckt, und falls nicht, muss die externe Schulung bei Bedarf durch interne Schulungen ergänzt werden.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Kompetenzen sind integraler Bestandteil des Kompetenzmanagementsystems, einschließlich überfachlicher Fähigkeiten, Haltungen und Verhaltensweisen. Die für die Ausführung einer Aufgabe erforderlichen Kompetenzniveaus werden mit Bezug zur Risikobewertung und zu den Aufgabenanalysen festgelegt.

„Haltung“ **(4.2.1 Buchstabe a)** wird verwendet, um zu beschreiben, wie Personen auf bestimmte Situationen reagieren und wie sie sich allgemein verhalten (z. B. ob sie proaktiv sind, mit anderen Personen auskommen können). Dies ist bei der Herstellung von Verbindungen innerhalb der Sicherheitsmanagementsystemarbeit sehr wichtig.

Es gibt einen systematischen Ansatz, der sicherstellt, dass die Kompetenz hinsichtlich menschlicher und organisatorischer Faktoren in relevanten Rollen basierend auf Risikobewertungen und Aufgabenanalysen zugänglich ist.

Die Kompetenz hinsichtlich menschlicher und organisatorischer Faktoren kann beispielsweise in Projekten in Verbindung mit neuen oder geänderten Designs, in der Bewertung und Verbesserung der Leistung zur Bereitstellung einer überfachlichen Perspektive oder in Bezug auf Fragen hinsichtlich des menschlichen Leistungsvermögens angewandt werden. Um Führungskräfte und Mitarbeiter, die Sicherheitsaufgaben wahrnehmen, zu sensibilisieren, erhalten sie spezielle Schulungen zu menschlichen und organisatorischen Faktoren.

4.2.4 Nachweise

- *Der Antragsteller sollte Informationen über sein Kompetenzmanagementsystem und dessen Funktionsweise bereitstellen, um den in den Anforderungen festgelegten Belangen gerecht zu werden;* ***(4.2.1), (4.2.2 Buchstaben a bis f)***
- *Die Nachweise müssen Einzelheiten über die für das Personal bestehenden Schulungsprogramme (einschließlich bei Bedarf Informationen zu den Anforderungen der Organisation an die Kompetenz der Ausbilder) enthalten sowie darüber, wie diese auf dem neuesten Stand gehalten und überprüft werden (einschließlich bei Bedarf an die Rolle des Sicherheitsberaters im Rahmen der RID) oder soweit anwendbar an die Kompetenz des Instandhaltungspersonals gemäß den Anforderungen der Anhänge I und II der Verordnung (EU) 2019/779 über für die Instandhaltung zuständigen Stellen;* ***(4.2.2 Buchstaben a bis e)***
- *Nachzuweisen ist auch, dass das Personal nach Unfällen und Störungen oder bei längerer Abwesenheit von der Arbeit wieder in den Arbeitsalltag zurückkehren kann, einschließlich der Art und Weise, wie etwaiger zusätzlicher Schulungsbedarf ermittelt wird;* ***(4.2.3)***
- *Wenn der Antragsteller ein anerkanntes Ausbildungszentrum nutzt, das nach den EU-Vorschriften zertifiziert wurde, wird durch eine Kopie des entsprechenden Zertifikats die Vermutung der Konformität mit den oben genannten Elementen begründet, sofern sie von diesem Zertifizierungsverfahren erfasst werden;* ***(4.2.1 Buchstabe a, Buchstaben c bis f, 4.2.2)***
- *Der Antragsteller sollte angeben, wie er sicherstellt, dass es bei gleichartigen Aufgaben keinen Unterschied zwischen der Kompetenz seines eigenen Personals und der Kompetenz von Auftragnehmern, Lieferanten und Beratern, die er beschäftigt, gibt;* ***(4.2.1 Buchstaben a bis f)***
- *Führungskräfte und Mitarbeiter, die Sicherheitsaufgaben wahrnehmen, erhalten angemessene Schulungen zu menschlichen und organisatorischen Faktoren und Sensibilisierung;* ***(4.2.1), (4.2.2)***
- *Der Antragsteller sollte angeben, wie der Bedarf an Kompetenzen hinsichtlich menschlicher und organisatorischer Faktoren bewertet wird. Dies umfasst die Definition, in welchen Rollen und Prozessen die Kompetenz hinsichtlich menschlicher und organisatorischer Faktoren benötigt wird und welcher Kompetenzgrad erforderlich ist. Das verfügbare Potential menschlicher Faktoren (z. B. förmliche Qualifikationen hinsichtlich menschlicher Faktoren, d. h. akademische Abschlüsse, intern/extern anerkannte Kompetenzen und Erfahrung) ist maßgeschneidert und proportional zur Reife und Komplexität des Unternehmens;* ***(4.2.1 Buchstaben a bis f)***
- *Der Antragsteller sollte Informationen über den Prozess vorlegen, mit dem Mitarbeiter die Wahrnehmung wichtiger Aufgaben gestattet wird, einschließlich der laufenden Verwaltung der Mitarbeiterkompetenzen.* ***(4.2.1 Buchstaben a bis f, 4.2.2 Buchstabe d)***

4.2.5 Beispiele für Nachweise

Das Kompetenzmanagementsystem mit einer Erläuterung seiner Funktionsweise im Zeitablauf, gegebenenfalls auch für nicht an vorderster Front tätige Mitarbeiter, sowie Links zu der stützenden Dokumentation, einschließlich der verschiedenen Schulungsprogramme und der Art und Weise, wie die von Unterauftragnehmern betriebenen Schulungszentren verwaltet werden.

Die vertraglichen Vereinbarungen (einschließlich der Leistungsbeschreibung) mit allen zertifizierten Schulungszentren sowie der Nachweis ihrer Zertifizierung.

Beispiele für Schulungsprogramme für Mitarbeitergruppen.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Der Prozess, der zeigt, wie die Anforderungen und Qualifikationen, einschließlich der psychischen oder physischen Eignung, die für bestimmte sicherheitsbezogene Aufgaben als notwendig erachtet werden, verwaltet und eingehalten werden, einschließlich einer Verknüpfung zur Risikobewertung und zu den Aufgabenanalysen.

Ein Prozess, der zeigt, wie die Anforderungen an die Mitarbeiter und ihre Qualifikationen verwaltet werden, und zwar sowohl in Bezug auf:

- *Einhaltung der geltenden Anforderungen an die physische und psychische Eignung;*
- *Festlegung der für die einzelnen sicherheitsbezogenen Aufgaben als notwendig erachteten beruflichen Kompetenzen.*

Die Prozesse zur regelmäßigen Überprüfung der Anforderungen und Schulungsprogramme zeigen eine aktuelle Situation und werden kontinuierlich an technische, betriebliche und organisatorische Veränderungen angepasst.

Ein Verfahren oder Prozess zur Gewährleistung, dass Mitarbeiter für die folgenden Bereiche spezifische und Auffrischungsschulungen erhalten:

- *Geplante Änderungen, die interne Vorschriften, die Infrastruktur, die Organisationsstruktur, usw. betreffen;*
- *Aktualisierungen der zugewiesenen Aufgaben (z. B. für Triebfahrzeugführer, neue Strecken, neue Lokomotiventypen, neue Dienstleistungsarten).*

Beschreibung im SMS, wie der Schulungsbedarf für Sicherheitsaufgaben entsprechend den spezifischen Funktionen ermittelt und umgesetzt wurde. Die prozessbezogenen Informationen werden genutzt, um Schulungsmaterial zu erstellen, und die Bestimmungen gewährleisten, dass die beteiligten Mitarbeiter sich mit den von ihren Tätigkeiten ausgehenden Risiken vertraut machen.

Ein Unfall- und Störungsuntersuchungsverfahren, soweit es Maßnahmen zur Änderung der Schulungsprogramme im Hinblick auf Unfälle und Störungen, frühere Aufsicht usw. betrifft.

Ein Prozess, der es dem Personal ermöglicht, Verfahren und Entscheidungen zu hinterfragen und routinemäßige und ungewöhnliche Abweichungen zu melden.

Eine Beschreibung im SMS, welche Mechanismen für den Austausch von Wissen in der Organisation vorhanden sind.

Der Prozess zur Gewährleistung, dass:

- *die Kompetenz durch ausreichende Übung in der Praxis (z. B. für Triebfahrzeugführer Kenntnis der Betriebsbedingungen, Zugkategorien, Triebfahrzeuge, Gleise und Stationen) und/oder durch die Planung spezifischer Schulungen, insbesondere im Falle einer langen Abwesenheit vom Arbeitsplatz (z. B. Krankheit) oder von Unfällen/Störungen, aufrechterhalten wird;*
- *die Kompetenz regelmäßig bewertet wird, um sicherzustellen, dass die erworbene Kompetenz erhalten bleibt;*
- *notwendige Maßnahmen ergriffen werden, wenn festgestellte Abweichungen oder ungeeignete Verhaltensweisen vorliegen, wie z. B. Abzug einer Person oder Außerbetriebnahme eines Ausrüstungsgegenstands für einen bestimmten Zeitraum, Einschränkungen hinsichtlich anerkannter Fähigkeiten, bei denen eine Nichtübereinstimmung festgestellt wurde, spezifische Schulungen usw.;*
- *geeignete Maßnahmen für das Personal nach Unfällen und Störungen getroffen werden (z. B. für Triebfahrzeugführer, die ein Signal überfahren, Unfall mit einer Person usw. Die Organisation stellt beispielsweise sicher, dass der Triebfahrzeugführer wieder einsatzfähig ist oder durch einen anderen, der für die zu erbringende Leistung geeignet ist, ersetzt wird);*

- *nach schweren Unfällen oder anderen signifikanten Ereignissen die gewonnenen Erkenntnisse weitergegeben werden, insbesondere dann, wenn neue Risiken erkannt wurden und auf Betriebsebene beherrscht werden müssen;*
- *ein Überwachungsprozess für das Kompetenzmanagementsystem eingerichtet ist und dessen Wirksamkeit gemessen wird.*

Erläuterung im SMS, wie die Führungskräfte geschult werden, um Risikobewertungen im Vorfeld von Entscheidungen durchführen zu können, und Einbeziehung menschlicher und organisatorischer Faktoren in deren tägliche Tätigkeiten (Risikobewertung, Leistungsbewertung, Verbesserung usw.).

Ein Prozess zur Gewährleistung der Aufrechterhaltung des Betriebs und der Prozess für die Rückkehr in den Arbeitsalltag mit einer Verbindung zum Kompetenzmanagementsystem.

Das Schulungsprogramm, aus dem hervorgeht, dass die spezifischen Schulungsmethoden anhand der Schulungsziele und -kriterien festgelegt werden:

- *Mentoring;*
- *Ausbildung am Arbeitsplatz;*
- *Simulatoren;*
- *Schulung für Notfälle;*
- *Schulung zu Team Resource Management.*

Der Prozess, mit dem sichergestellt werden soll, dass die Mitarbeiter über angemessene Kompetenzen verfügen, einschließlich der Ermittlung der notwendigen Kompetenzen, ist mit der Risikobewertung verbunden. Dieser etablierte Prozess zeigt, dass ein systematischer Ansatz verfolgt wird, um für das mit der Durchführung der Risikobewertung und der Festlegung der sich daraus ergebenden Sicherheitsrollen und -kompetenzen betraute Personal Kompetenzen im Bereich menschlicher und organisatorischer Faktoren zu nutzen, um sicherzustellen, dass die erforderlichen Ressourcen und Kompetenzen zugewiesen werden.

Die Sicherheitskulturkompetenz basiert auf einer Bedürfnisanalyse. Die Bedürfnisse der Sicherheitskulturkompetenz werden bewertet und Strategien zur Gewährleistung der richtigen Fähigkeiten und Ressourcen aufgezeigt. Das Grundwissen zur Sicherheitskultur und seine Wichtigkeit werden sichtlich vom Management gefördert.

Ein Prozess, mit dem sichergestellt wird, dass Auftragnehmer, Partner und Zulieferer dieselben Kompetenzanforderungen erfüllen. Die vertraglichen Regelungen (oder Partnerschaftsvereinbarungen), die diesen Anforderungen Rechnung tragen, und die Überwachung der Erfüllung des Vertrags (oder der Partnerschaft).

4.2.6 Referenzen und Standards

- *ISO 10015:1999 „Qualitätsmanagement – Leitfaden für das Kompetenzmanagement und die Entwicklung von Personen“*
- *ISO 10018:2020 „Qualitätsmanagement – Leitfaden zum Engagement von Personen“*

4.2.7 Aufsichtsaspekte

Die Art, wie die Ergebnisse der Risikobewertung mit einer Überprüfung des Kompetenzmanagementsystems verknüpft werden.

Bei der Betrachtung des Kompetenzmanagementsystems ist zu bedenken, dass es Kompetenzanforderungen geben wird, die über das Personal der Organisation hinausgehen, aber auch Auswirkungen auf Auftragnehmer und andere haben werden.

Das CMS sollte daraufhin überprüft werden, ob es auf dem neuesten Stand ist und ob die darin durchgeführten Schulungsmaßnahmen den aktuellen Bedürfnissen der Organisationen entsprechen.

Die Organisation sollte über Mittel verfügen, mit denen sichergestellt werden kann, dass Vertragsbedienstete, die Tätigkeiten ausüben, entsprechende Kompetenz hierfür besitzen. Dies ist insbesondere dann ein Problem, wenn es sich um Lohnunternehmer handelt, bei denen die Kontrolle der Kompetenzen möglicherweise nicht so gründlich ist.

Der erforderliche Kompetenzgrad für ähnliche Tätigkeiten sollte für direkt eingestellte Mitarbeiter und Auftragnehmer identisch sein.

Es ist ein System vorhanden, das sicherstellt, dass Aufgaben und Stellen mit einem Sicherheitselement, einschließlich sicherheitskritischer Aufgaben, identifiziert werden.

Es gibt ein robustes und wirksames Kompetenzmanagementsystem, das Folgendes umfasst: Ermittlung der erforderlichen Kenntnisse und Fähigkeiten, Schulung, Instandhaltung und Ressourcen für Kompetenz; die Prozesse für die Einstellung, Ausbildung, Bewertung, Kompetenzüberwachung und die Führung von Aufzeichnungen, wobei angegeben wird, wie all dies zur Erlangung und Aufrechterhaltung der vorhandenen Kompetenz beiträgt.

Schwerpunkt auf menschliche Faktoren – wie führt die Organisation die Bewertung der physischen und psychischen Eignung durch (z B. für Triebfahrzeugführer und für andere Mitarbeiter, die sicherheitskritische Aufgaben ausführen).

4.3 Bewusstsein

4.3.1 Regulatorische Anforderung

4.3.1. Die oberste Führungsebene stellt sicher, dass sie und die mit sicherheitsrelevanten Aufgaben betrauten Mitarbeiter sich der Relevanz, Bedeutung und Folgen ihrer Tätigkeiten bewusst sind und dass ihnen klar ist, wie sie zur ordnungsgemäßen Anwendung und Wirksamkeit des Sicherheitsmanagementsystems sowie zur Erreichung der Sicherheitsziele beitragen (siehe 3.2 Sicherheitsziele und Planung).

4.3.2 Zweck

Bewusstsein bedeutet, dass sich die Mitarbeiter über die Sicherheitsordnung des Unternehmens, ihren Beitrag zur Sicherheit im Unternehmen, die Gefahren und Risiken sowie die Ergebnisse der Untersuchungen von Unfällen und Störungen im Klaren sind. Dazu gehört auch, dass den Mitarbeitern vermittelt wird, welche Auswirkungen es für sie selbst und die Organisation hat, wenn sie nicht zur Umsetzung des Sicherheitsmanagementsystems beitragen. Zweck dieser Anforderung ist es, Fragen der Sicherheitskultur innerhalb der Organisation anzusprechen. Sie richtet sich an die oberste Führungsebene, um die Agenda und die Richtung der Organisation festzulegen und zu erläutern, wie Geschäfte abgewickelt werden. Mitarbeiter, die innerhalb der Organisation am Betrieb mitwirken, richten sich nach dem Management. Der Antragsteller muss aufzeigen, wie er diesen Fragen im Rahmen seiner Prozesse und Verfahren Rechnung trägt.

4.3.3 Erläuterungen

Diese Anforderung steht im Zusammenhang mit menschlichen und organisatorischen Faktoren. Weitere Informationen zu menschlichen und organisatorischen Faktoren sind Anhang 5 zu entnehmen.

4.3.4 Nachweise

- Der Antragsteller sollte angeben, wo in seinen Personalmanagement- oder anderen Prozessen die Schlüsselrolle, die das Personal bei der Verwirklichung der Ziele der Organisation spielt, zum Ausdruck kommt, wie er dies zu messen versucht und welche Schritte er unternimmt, um dies aufrechtzuerhalten und zu verbessern; **(4.3.1) (siehe ferner 2.3)**
- Informationen über die Funktionsweise des Kompetenzmanagementsystems. **(4.3.1)**

4.3.5 Beispiele für Nachweise

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Eine Erklärung in der Sicherheitsordnung oder an anderer Stelle über die Verpflichtung der „leitenden Köpfe“ der Organisation zur Förderung der Sicherheitskultur der Organisation, um die Kontrolle der Risiken durch einen Managementsystemansatz zu gewährleisten. In dem Dokument wird auch die Aufgabe aller Mitarbeiter bei der Förderung der Sicherheitsordnung durch ihre Aktionen und durch das Erreichen der gesetzten Sicherheitsziele angegeben. Es werden Links zu den spezifischen Verfahren zur Verfügung gestellt, die darauf abzielen, diese Ideen in der gesamten Organisation zu verbreiten.

Der Überwachungsprozess umfasst einen Punkt, der sich mit dem Verständnis des Sicherheitsmanagementsystems in der Organisation sowie der Bedeutung jeder einzelnen Aufgabe und des diesbezüglichen Risikobewusstseins befasst.

Regelmäßige Erhebungen über das Engagement der Mitarbeiter mit Schwerpunkt auf der Sicherheit, aus denen hervorgeht, dass die Mitarbeiter verstehen, wie sich ihre Aufgabe in die allgemeinen Sicherheitsziele der Organisation einfügt.

Die Schulungsprogramme, einschließlich Erläuterungen zu Risiken, Sicherheitsmaßnahmen und Sicherheitszielen für die Wahrnehmung der Aufgaben und Teilaufgaben.

Ein Verfahren, nach dem Mitarbeiter, Auftragnehmer oder andere Interessengruppen die Risiken melden können, denen sie ausgesetzt sind.

Eine Erklärung, in der dargelegt wird, wie die Organisation ihren Ansatz für Sicherheitsbewusstsein, menschliche und organisatorische Faktoren sowie Sicherheitskultur bei ihren Auftragnehmern, Partnern und Zulieferern fördert.

Die Mitteilungen der obersten Führungsebene über die Ziele, entweder im Sinne der Ermutigung aller Mitarbeiter, zu ihrer Erreichung beizutragen, oder beispielsweise in Form von Glückwünschen für eine bessere Leistung.

Informationen, aus denen hervorgeht, dass die mittlere Führungsebene und die Betriebsmitarbeiter an Sicherheitsinitiativen an vorderster Front beteiligt sind (Workshops, Foren, spezielle Sicherheitstage, Schulungsprogramme, die darauf ausgerichtet sind, das Bewusstsein für ihre Aufgabe innerhalb des Sicherheitsmanagementsystems zu schärfen, usw.).

Eine Beschreibung der verwendeten Kommunikations- und sonstigen Kanäle, und wie menschliche und organisatorische Faktoren darin integriert werden.

Ein Prozess zur Entwicklung von Verfahren, in dem erläutert wird, wie die betroffenen Mitarbeiter eingebunden sind und wie Risiken und Sicherheitsmaßnahmen berücksichtigt werden und wie sich die Nichteinhaltung der Vorschriften möglicherweise auf die operativen Tätigkeiten auswirken könnte.

4.3.6 Aufsichtsaspekte

Bei der Befragung von Mitarbeitern zu diesem Thema ist es wichtig, die Art des Verständnisses zu ermitteln, das die Menschen von den Rollen und Verantwortlichkeiten haben, die für sie gelten. Dies zeigt an, ob die Organisation in der Lage ist, die Bedeutung einer effektiven Organisationskultur oder eines effektiven Bewusstseins für die Sicherheit durch das Sicherheitsmanagementsystem zu verstehen.

Die Frage, wie die Organisation ihre gegenwärtige Kultur als Grundlage festgelegt hat und welche Schritte zu ihrer Verbesserung und Weiterentwicklung unternommen werden, ist eine Schlüsselfrage für die Aufsicht.

Prüfung der Überwachung der Erfüllung von Gesundheits- und Sicherheitsaufgaben/-zielen, des Risikobewusstseins, der Berichtskultur – Suche nach Versäumnissen, Fehlern, Verstößen und anderen Inkongruenzen.

4.4 Information und Kommunikation

4.4.1 Regulatorische Anforderung

4.4.1. Die Organisation legt angemessene Kommunikationskanäle fest, um sicherzustellen, dass sicherheitsrelevante Informationen zwischen den verschiedenen Ebenen der Organisation sowie mit externen Beteiligten, einschließlich Auftragnehmern, Partnern und Zulieferern, ausgetauscht werden.

4.4.2. Um sicherzustellen, dass sicherheitsrelevante Informationen die Personen erreichen, die Beurteilungen vornehmen und Entscheidungen treffen, steuert die Organisation die Ermittlung, den Eingang, die Verarbeitung sowie die Erzeugung und Verbreitung sicherheitsrelevanter Informationen.

4.4.3. Die Organisation sorgt dafür, dass sicherheitsrelevante Informationen

(a) relevant, vollständig und für die vorgesehenen Nutzer verständlich sind;

(b) gültig sind;

(c) korrekt sind;

(d) konsistent sind;

(e) kontrolliert werden (siehe 4.5.3 Kontrolle dokumentierter Informationen);

(f) vor ihrem Wirksamwerden mitgeteilt werden;

(g) empfangen und verstanden werden.

4.4.2 Zweck

Die Einhaltung dieser Anforderungen soll zeigen, dass der Antragsteller in seinem Antrag nachgewiesen hat, dass er über die geeigneten Mittel verfügt, um sicherheitsrelevante Informationen auf verschiedenen Ebenen zu identifizieren und sie zur richtigen Zeit und an die richtigen Personen weiterzugeben. Eine Bestandsaufnahme zur Sicherstellung, dass die aktuellen Risikokontrollen relevant und aktuell bleiben und neue Bedrohungen und Gelegenheiten von externen Einflüssen (politisch, sozial, umwelttechnisch, ökonomisch und rechtlich) identifizieren können. Die Fähigkeit, gewährleisten zu können, dass der Antragsteller die geeigneten Mitarbeiter (insbesondere sicherheitskritische Mitarbeiter) in seiner Organisation erreicht, die darauf reagieren müssen. Dies umfasst, wie anderen Interessengruppen, mit denen eine Schnittstelle besteht, entsprechende sicherheitsrelevante Informationen bereitgestellt werden.

4.4.3 Erläuterungen

Die Organisation legt fest, welche Art von sicherheitsrelevanten Informationen zu übermitteln sind, wie sie kommuniziert werden**(siehe ferner 4.5)** und an wen und unter welchen Bedingungen dies veranlasst und verarbeitet werden soll. **(4.4.1)**. Sicherheitsrelevante Informationen werden zwischen Personal, das innerhalb der Organisation sicherheitsrelevante Aufgaben wahrnimmt, mit Unterauftragnehmern, Partnern oder Zulieferern, zwischen Eisenbahnunternehmen und Infrastrukturbetreibern und gegebenenfalls zwischen Infrastrukturbetreibern ausgetauscht.

Die verschiedenen Informationsarten können wie folgt unterschieden werden:

- *Die Dokumentation des Sicherheitsmanagementsystems **(siehe ferner 4.5)**;*

- *Statische Informationen, die vom Infrastrukturbetreiber für die Gestaltung des Eisenbahnbetriebs benötigt werden, wie Betriebsvorschriften und Merkmale der Schieneninfrastruktur (z. B. Spurweite, Zuglänge, Steigungen und Achslast);*
- *Informationen, die für die Planung des Eisenbahnbetriebs erforderlich sind, wie z. B. Netzfahrpläne, Streckenlisten, temporäre Geschwindigkeitsbeschränkungen, Änderungen der Schieneninfrastruktur, laufende Gleisarbeiten, Einschränkungen der Spurweite, von der geplanten Strecke abzuleitende Züge, als eingleisige Streckenabschnitte zu betreibende Streckenabschnitte, Zugverkehrsprognosen (einschließlich Änderungen der Zugstrecken und/oder Pendlerdienste);*
- *Informationen hinsichtlich des Zugverkehrsmanagements (zwischen Eisenbahnunternehmen und Infrastrukturbetreibern und, wo relevant, zwischen Infrastrukturbetreibern), einschließlich der Identifikation von kompetenten Mitarbeitern innerhalb jeder Organisation, die im Falle eines gestörten Betriebs oder bei Notfällen **(siehe ferner 5.5)** während oder außerhalb der Kernarbeitszeiten kontaktiert werden können.*

Grundanforderungen zum Zweck des Informationsaustauschs **(4.4.2)** werden in den TSI OPE zwischen dem Eisenbahnunternehmen und dem Infrastrukturbetreiber, in der Verordnung über die für Instandhaltung zuständigen Stellen (ECM) zwischen dem Eisenbahnunternehmen und der ECM und in den CSM zu Anforderungen an das Sicherheitsmanagementsystem zwischen dem Eisenbahnunternehmen/Infrastrukturbetreiber und den Behörden (der Agentur, der nationalen Sicherheitsbehörde) identifiziert.

Es gibt Regelungen für den Informationsaustausch mit den entsprechenden Parteien in Bezug auf Sicherheitsrisiken im Zusammenhang mit Fehlern und Baumängeln oder Störungen technischer Systeme, einschließlich struktureller Teilsysteme, darunter auch Informationen über ergriffene Korrekturmaßnahmen, zum Beispiel durch das SAIT (Safety Alert Tool)-System, das die Agentur mit dem Eisenbahnsektor gefördert hat. Durch Verwendung des SAIT wird die Verpflichtung erfüllt, die in der Richtlinie über die Eisenbahnsicherheit (Artikel 4 Absatz 5) sowie die Vorgabe im CSM für die Kontrolle (Artikel 4) und die Verordnung über die für die Instandhaltung zuständigen Stellen (Artikel 5 Absatz 5) über den Austausch dieser Informationen festgelegt wurde.

„Gültig“ im obigen Kontext **(4.4.3 Buchstabe b)** bedeutet aktuell.

„Konsistent“ im obigen Kontext **(4.4.3 Buchstabe d)** bedeutet, bei einem Ursprung aus verschiedenen Quellen nicht in Konflikt stehend.

„Verstanden“ im obigen Kontext **(4.4.3 Buchstabe g)** bedeutet, dass der Antragsteller aufzeigt, dass er Schritte unternommen hat, um sicherzustellen, dass sicherheitskritische Informationen von denjenigen aufgenommen wurden, an die sie gerichtet waren. Dies kann durch Ad-hoc-Schulungen, durch Fragen zur Überprüfung des korrekten Verständnisses bei Besprechungen oder bei sicherheitskritischer Kommunikation durch die Einführung von Protokollen geschehen, die die Wiederholung wichtiger Nachrichten erfordern, z. B. zwischen Weichensteller und Triebfahrzeugführer, um zu bestätigen, dass die Nachrichten korrekt empfangen wurden, oder durch andere Mittel, die die Anforderung erfüllen.

Diese Anforderung steht im Zusammenhang mit menschlichen und organisatorischen Faktoren. Weitere Informationen zu menschlichen und organisatorischen Faktoren sind Anhang 5 zu entnehmen.

4.4.4 Nachweise

- *Der Antragsteller identifiziert die verschiedenen Kommunikationskanäle, die in der Organisation vorhanden sind, sowie ihren Zweck; **(4.4.1)***
- *Der Antragsteller muss Nachweise erbringen, z. B. über ein internes Sicherheitswarnsystem, ein System zur Bereitstellung relevanter, aber routinemäßiger Informationen für das Personal und ein System zur Bereitstellung relevanter, aber Ad-hoc-Informationen für das Personal; **(4.4.2)***

- *Der Antragsteller gibt an, wie er sich vergewissert, dass die verbreiteten Informationen diejenigen erreicht haben, die damit erreicht werden sollen (insbesondere diejenigen in sicherheitskritischen Funktionen), und von ihnen verstanden wurden.* ***(4.4.3)***

4.4.5 Beispiele für Nachweise

Der Prozess/das Verfahren, mit dem sichergestellt wird, dass externen Gruppen, wie z. B. Infrastrukturbetreibern, (anderen) Eisenbahnunternehmen, Behörden usw. ein Kontakt zur Verfügung gestellt wird, der mit ihnen kommunizieren kann (z. B. Sprachfähigkeiten) und auf die richtige Informationsebene zugreifen kann.

Prozesse oder Verfahren zur Bestätigung der Bereitstellung sicherheitsrelevanter Dokumente.

Für Rollen, denen die Verwaltung von Schnittstellen anvertraut wurde: Nachweise, an wen die Sicherheitswarnung gesendet wurde, je nach geografischem Tätigkeitsgebiet (z. B. die Sicherheitswarnungen erscheinen im Streckenbuch oder in den Informationen zu „Late Notices“).

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Eine klare Aussage darüber, wie die Kommunikation sowohl nach oben als auch nach unten für verschiedene Arten und Ebenen von Informationen funktioniert, einschließlich Links zu den spezifischen Verfahren für Sicherheitswarnungen und Routinekommunikation.

Ein Prozess oder ein Verfahren, der bzw. das angibt, welche Schritte für verschiedene Kommunikationsarten unternommen werden, um sicherzustellen, dass sie das Personal erreichen, für das sie bestimmt sind, und dass dieses Personal versteht, was ihm mitgeteilt wird, z. B. sicherheitskritische Informationen.

Der Prozess bzw. das Verfahren, das sicherstellt, dass jeder Mitarbeiter, der an einer sicherheitsrelevanten Aufgabe beteiligt ist, zum richtigen Zeitpunkt mit der richtigen Version der Dokumente versorgt wird, um die Einbindung und die Fähigkeit zu gewährleisten, im Regelbetrieb, in gestörtem Betrieb und in Notfällen rasch zu handeln oder zu reagieren.

Die TSI OPE enthalten Anforderungen an verschiedene Dokumente, darunter einige, die sich auf die Kommunikation zwischen dem Personal der Eisenbahnunternehmen und der Infrastrukturbetreiber beziehen. All diese Dokumente (Regelwerk, Streckenbuch, Fahrpläne, Formularsammlungen usw.) sind bekannt und enthalten einen Satz Kommunikationsprotokolle oder Medien zum eindeutigen und schnellen Austausch formalisierter Informationen, die für den Betrieb, insbesondere für Zugbewegungen im gestörten Betrieb, relevant sind.

Die Sicherheitswarnungen müssen innerhalb der Organisation oder mit anderen Interessengruppen ausgetauscht werden. Typische Beispiele umfassen:

- *Die Eisenbahnunternehmen informieren die Infrastrukturbetreiber über etwaige Störungen, die sich auf die Zugbewegungen auswirken können (Störungen der Schienenfahrzeuge, z. B. heiße Achslager, damit der Infrastrukturbetreiber Maßnahmen zur Risikokontrolle ergreifen kann, wie z. B. die Sperrung des Verkehrs auf dem angrenzenden Gleis).*
- *Der Infrastrukturbetreiber stellt für alle Eisenbahnunternehmen, die im relevanten Bereich arbeiten, Informationen zu Infrastrukturstörungen und eventuellen temporären Sicherheitsmaßnahmen wie Geschwindigkeitsreduzierung bereit.*

Prozesse oder Verfahren zur Verbreitung von Informationen über Änderungen der Organisationsstruktur auf Mikro- und Makroebene.

Die Kopien der Anweisungen für Mitarbeiter, die sicherheitsrelevante Aufgaben durchführen und sich mit den für die Netze relevanten Betriebsregeln befassen, die folgende Eigenschaften aufweisen:

- *Vollständig: Alle Regeln und Anforderungen in Bezug auf Sicherheitsaufgaben, die für den Betrieb des Eisenbahnunternehmens relevant sind, werden in den relevanten Dokumenten identifiziert und transkribiert.*
- *Genau: Jede der Regeln und Anforderungen wird korrekt und fehlerfrei transkribiert (z. B. Verhalten vor einem Signal, sicherheitsrelevante Mitteilungen).*
- *Konsistent: Die Anforderungen, die für eine einzige Person oder ein einziges Team aus verschiedenen Quellen gelten, sind kompatibel und konsistent und stehen nicht miteinander in Konflikt.*

Der Prozess für die Aufzeichnung von Informationen ist in den einschlägigen internen Vorschriften unter Verwendung des geeigneten Kommunikationskanals festgelegt.

In den Schulungsprogrammen wird ermittelt, wie die Kommunikation gesteuert wird und wie Kommunikationsfähigkeiten in das Kompetenzmanagementsystem integriert werden.

In dem Meldeprozess, das es dem Personal ermöglicht, Sicherheitsprobleme im Rahmen der Just Culture Policy zu melden, wird erläutert, wie diese Rückmeldungen analysiert und bewertet werden, damit drohende Systemausfälle im Risikomanagementprozess erkannt und berücksichtigt werden können. Der Prozess umfasst auch die Art und Weise, wie die Mitarbeiter Rückmeldung zu den von ihnen gemeldeten Problemen erhalten.

Das Verfahren, in dem die verschiedenen Arten von Sitzungen und relevante Ergebnisse (z. B. Sitzungsprotokolle, Vermerke usw.) erläutert werden, zeigt, wie die Sicherheitskommunikation im gesamten Unternehmen sowohl nach oben als auch nach unten gesteuert wird.

4.4.6 Aufsichtsaspekte

Prüfung, ob Techniken und Prozesse verwendet werden, um bei der Risikokontrolle aktuell zu bleiben, Bestandsaufnahme von Chancen oder Bedrohungen.

Prüfung, ob es einen Prozess zur Überwachung der Verwendung formalisierter Informationen gibt.

Zentrale Themen der Aufsicht sind unter anderem, wie aktuell die Informationen sind und ob sie rechtzeitig **alle** relevanten Mitarbeiter erreichen, z. B. während der Nachtschicht oder wenn diese nicht in den Hauptniederlassungen der Organisation arbeiten.

4.5 Dokumentierte Informationen

4.5.1 Regulatorische Anforderung

4.5.1. Dokumentation des Sicherheitsmanagementsystems

4.5.1.1. Es muss eine Beschreibung des Sicherheitsmanagementsystems vorhanden sein mit folgendem Inhalt:

(a) Ermittlung und Beschreibung der Prozesse und Handlungen im Zusammenhang mit der Sicherheit des Eisenbahnbetriebs, einschließlich sicherheitsrelevanter Aufgaben und der damit verbundenen Zuständigkeiten (siehe 2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse);

(b) Wechselwirkung dieser Prozesse;

(c) Verfahren oder sonstige Dokumente, die beschreiben, wie die Umsetzung dieser Prozesse erfolgt ist;

(d) Ermittlung von Auftragnehmern, Partnern und Zulieferern mit einer Beschreibung der Art und des Umfangs der erbrachten Dienstleistungen;

(e) Ermittlung der vertraglichen Vereinbarungen und anderen geschäftlichen Abmachungen zwischen der Organisation und anderen unter Buchstabe d genannten Beteiligten, die für die Beherrschung der durch die Organisation und den Einsatz von Auftragnehmern entstehenden Sicherheitsrisiken erforderlich sind;

(f) Verweise auf die gemäß dieser Verordnung vorgeschriebenen dokumentierten Informationen.

4.5.1.2. Die Organisation stellt sicher, dass der/den zuständigen nationalen Sicherheitsbehörde(n) gemäß Artikel 9 Absatz 6 der Richtlinie (EU) 2016/798 ein jährlicher Sicherheitsbericht vorgelegt wird, der Folgendes enthält:

(a) eine zusammenfassende Darstellung der Entscheidungen über die Signifikanz der sicherheitsrelevanten Änderungen, einschließlich eines Überblicks über wesentliche Änderungen, im Einklang mit Artikel 18 Absatz 1 der Durchführungsverordnung (EU) Nr. 402/2013;

(b) die Sicherheitsziele der Organisation für das/die folgende(n) Jahr(e) sowie Angaben darüber, welchen Einfluss ernste Sicherheitsrisiken auf die Festlegung dieser Sicherheitsziele haben;

(c) die Ergebnisse interner Untersuchungen von Unfällen/Störungen (siehe 7.1 Lehren aus Unfällen und Störungen) und anderer Überwachungstätigkeiten (siehe 6.1 Überwachung, 6.2 Interne Auditierung und 6.3 Managementbewertung) im Einklang mit Artikel 5 Absatz 1 der Verordnung (EU) Nr. 1078/2012;

(d) Einzelheiten zu den erzielten Fortschritten bei noch offenen Empfehlungen der nationalen Untersuchungsstellen (siehe 7.1 Lehren aus Unfällen und Störungen);

(e) die Sicherheitsindikatoren der Organisation für die Bewertung ihrer Sicherheitsleistung (siehe 6.1 Überwachung);

(f) gegebenenfalls die Schlussfolgerungen des Jahresberichts des Sicherheitsberaters (Gefahrgutbeauftragten) im Sinne der RID über die Tätigkeiten der Organisation auf dem Gebiet des Transports gefährlicher Güter.

4.5.2. Erstellung und Aktualisierung

4.5.2.1. Die Organisation muss sicherstellen, dass bei der Erstellung und Aktualisierung von dokumentierten Informationen über das Sicherheitsmanagementsystem geeignete Formate und Medien verwendet werden.

4.5.3. Lenkung dokumentierter Informationen

4.5.3.1. Die Organisation muss dokumentierte Informationen im Zusammenhang mit dem Sicherheitsmanagementsystem lenken, insbesondere was ihre Aufbewahrung und Verteilung sowie die Kontrolle der Änderungen anbelangt, um die Verfügbarkeit, die Eignung und gegebenenfalls den Schutz dieser Informationen zu gewährleisten.

4.5.2 Zweck

Der Antragsteller muss aufzeigen, dass das gesamte Sicherheitsmanagementsystem für die Art und den Umfang der ausgeführten Dienstleistungen angemessen und in der Lage ist, die entstehenden Risiken zu verwalten. Dies erfordert:

- eine Erläuterung der Sicherheitsordnung des Antragstellers, der Organisation und der hochrangigen Vorkehrungen des Sicherheitsmanagementsystems; und
- die detaillierteren Regelungen, wie sie in den Anforderungen der vorstehenden Nummer 4.5.1.1 Buchstaben a bis f und Nummer 4.5.1.2 Buchstaben a bis f festgelegt sind.

Der Antragsteller muss ebenfalls zeigen, wie die Dokumentation seines Sicherheitsmanagementsystems verwaltet wird, d. h. die Identifikation, Erstellung, Pflege, Verwaltung, Speicherung und Aufbewahrung dokumentierter Informationen (d. h. Dokumente und Aufzeichnungen/Daten), um sicherzustellen, dass sie aktuell ist und die korrekten Versionen bei Bedarf für die entsprechenden Mitarbeiter zur Verfügung stehen.

4.5.3 Erläuterungen

Dokumente, in denen der Antragsteller die Konformität seines Sicherheitsmanagementsystems mit den geltenden Anforderungen zeigt **(4.5.1.1 Buchstabe f)**, sind Teil der dokumentierten Informationen des Sicherheitsmanagementsystems.

Die folgende Abbildung 3 zeigt eine typische Dokumentationsstruktur:

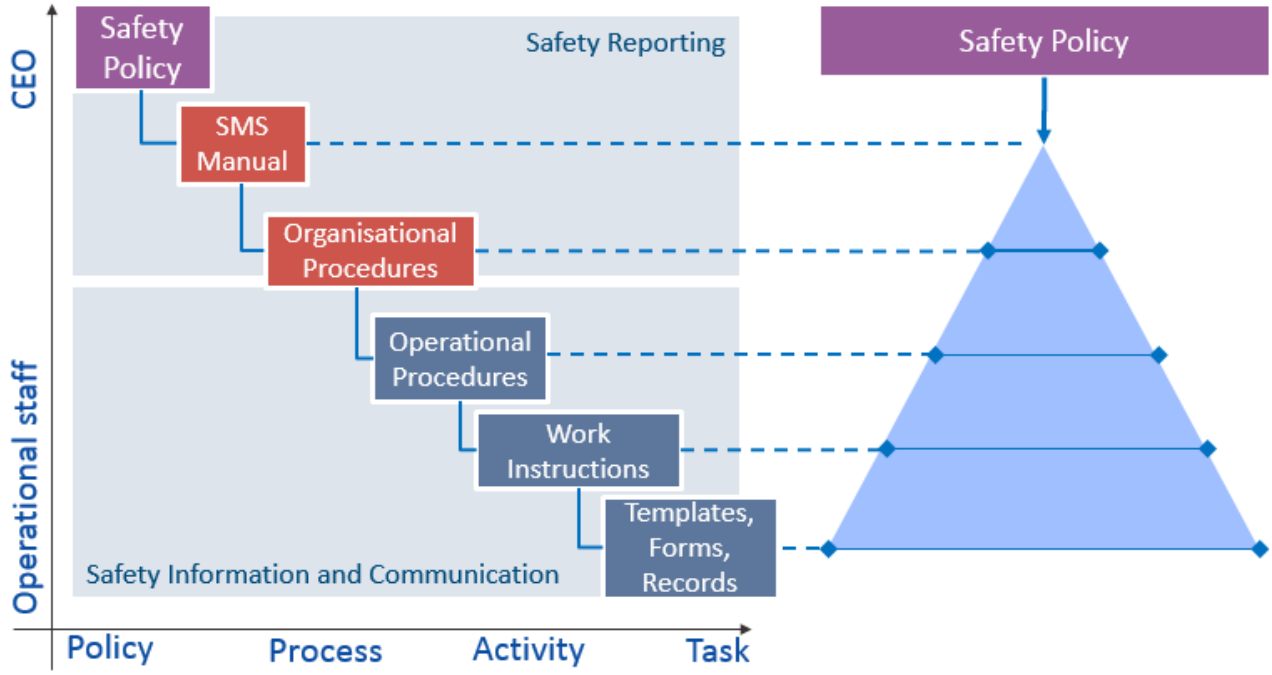

Abbildung 3: Typische Dokumentationsstruktur

Je nach geografischem Tätigkeitsgebiet können Eisenbahnunternehmen verschiedene Berichte **(4.5.1.2)** an die nationalen Sicherheitsbehörden der Mitgliedstaaten, in denen ihr Betrieb stattfindet, übermitteln. Der Anwendungsbereich des Berichts bezieht sich im Allgemeinen nur auf den Teil des Betriebs im jeweiligen Mitgliedstaat. Die Agentur empfiehlt allerdings, dass derselbe Bericht das gesamte geografische Tätigkeitsgebiet abdeckt. Dies sollte die Weitergabe von Informationen zwischen den nationalen Sicherheitsbehörden, die dasselbe Eisenbahnunternehmen überwachen, erleichtern.

Jahresbericht des Sicherheitsbeauftragten **(4.5.1.2 Buchstabe f)**: Im Falle der Beförderung gefährlicher Güter, wie von Richtlinie 2008/68/EG in der jeweils gültigen Fassung und der RID gefordert, ist der Jahresbericht des Sicherheitsbeauftragten für gefährliche Güter ebenfalls Dateneingabe für den jährlichen Sicherheitsbericht. Der Sicherheitsbeauftragte hat bestimmte Aufgaben zu erfüllen, einschließlich der Beratung des Unternehmens, das ihn bestellt hat, in Gesundheits-, Sicherheits- und Umweltfragen im Zusammenhang mit der Beförderung gefährlicher Güter und der Erstellung der erforderlichen Berichte.

Die Identifikation, das Format (z. B. Sprache, Softwareversion und Grafiken) und das Medium (z. B. Papier, elektronisch) für die dokumentierten Informationen **(4.5.2.1)** sind der Organisation überlassen. Es muss kein schriftliches Dokument in Papierform sein.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Die Dokumentkontrolle **(4.5.3.1)** bezeichnet den Prozess (oder das Verfahren), das die internen Kontrollen festlegt, insbesondere die Überprüfung und Genehmigung der Eignung vor der Ausstellung und Verwendung, die für Informationen, die dokumentiert werden müssen, zu berücksichtigen und umzusetzen sind. Sie zielt darauf ab, den aktuellen Überprüfungsstatus der Dokumente zu identifizieren, um die Verwendung ungültiger oder veralteter Dokumente auszuschließen. Insbesondere wird so gewährleistet, dass:

- *die entsprechenden Ausgaben der jeweiligen Dokumente an allen Orten verfügbar sind, an denen für das effektive Funktionieren des Sicherheitsmanagementsystems ausschlaggebende Tätigkeiten durchgeführt werden;*

- *ungültige oder veraltete Dokumente unverzüglich aus allen Ausgabe- oder Verwendungsstellen entfernt oder anderweitig gegen unbeabsichtigten Gebrauch gesichert werden;*
- *veraltete Dokumente, die zu rechtlichen Zwecken oder zur Wissenskonservierung behalten wurden, entsprechend identifiziert werden.*

4.5.4 Nachweise

- *Der Antragsteller muss gegebenenfalls eine Beschreibung des Sicherheitsmanagementsystems und seiner Funktionsweise mit angemessenen Hinweisen auf relevante Verfahren bereitstellen;* ***(4.5.1.1 Buchstaben a bis c)***
- *Der Antragsteller sollte darlegen, wer seine Auftragnehmer, Zulieferer und Partner sind und wie die Beziehungen kontrolliert und überwacht werden, um sicherzustellen, dass Sicherheitsrisiken sowohl des Antragstellers als auch derjenigen, mit denen er vertragliche Beziehungen unterhält, ordnungsgemäß gesteuert werden, um die Sicherheit zu gewährleisten;* ***(4.5.1.1 Buchstaben d bis e)***
- *Der Antragsteller sollte das (die) entsprechende(n) Verfahren vorlegen, mit dem bzw. denen nachgewiesen wird, dass er dokumentierte Informationen kontrollieren kann;* ***(4.5.1.1 Buchstabe f)***
- *Der Antragsteller sollte die Rollen und Verantwortlichkeiten im Zusammenhang mit sicherheitsrelevanten Aufgaben und die Art und Weise, wie die Risiken aus den Tätigkeiten des Antragstellers und anderer Personen gehandhabt werden, benennen;* ***(4.5.1.1 Buchstabe a)***
- *Der Antragsteller muss Nachweise erbringen, dass er über einen jährlichen Sicherheitsbericht verfügt (oder Vorkehrungen getroffen hat, damit dieser erstellt wird), der die Punkte in 4.5.1.2 oben abdeckt;* ***(4.5.1.2 Buchstaben a bis f)***
- *Der Antragsteller sollte angeben, wie das Dokumentenverwaltungssystem funktioniert, einschließlich der Art und Weise, wie Informationen zur Verfügung gestellt werden und wann und wo sie benötigt werden, wie sie kontrolliert innerhalb des Systems geändert werden und wie sie gespeichert und gepflegt werden, sodass sie leicht abrufbar sind. Das Dokumentenverwaltungssystem sollte es ermöglichen, Informationen in Einrichtungen aufzubewahren, die ein geeignetes Umfeld bieten, um Verschlechterungen oder Schäden zu minimieren und Verluste zu vermeiden.* ***(4.5.2.1), (4.5.3.1)***

4.5.5 Beispiele für Nachweise

Eine Beschreibung des Sicherheitsmanagementsystems und seiner Gesamtstruktur sowie Links zu den Dokumenten, welche die darin enthaltenen Prozesse unterstützen (z. B. manuelle, organisatorische und betriebliche Verfahren, Arbeitsanweisungen). Ungeachtet des neuen Konzepts der dokumentierten Informationen, die von ISO eingeführt wurden, kann die Organisation die traditionelle Architektur der Dokumentation bewahren, wenn sie zweckmäßig ist.

Ein Überblick darüber, wie die verschiedenen Dokumente strukturiert, veröffentlicht, verfügbar gemacht, abgelegt, gepflegt/überarbeitet und mit Bezug auf die verschiedenen Dokumentkontrollverfahren außer Kraft gesetzt werden.

Das Verfahren für die Erstellung des Jahresberichts des Antragstellers zusammen mit einer Kopie einer früheren Fassung, falls der Antragsteller neu ist. Das Verfahren gibt die vorgeschlagene Gestaltung des Berichts an.

Es werden Aufbewahrungszeiträume für Dokumente und Aufzeichnungen umgesetzt, dokumentiert und eingehalten.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Die Dokumentenverwaltungsprozesse oder -verfahren, die sich damit befassen, wie Dokumente nach regelmäßigen Überarbeitungen und nach Unfällen oder Störungen aktualisiert werden. Die Prozesse oder Verfahren behandeln den Eskalationsprozess in Fällen, in denen vereinbarte Aktualisierungen nicht innerhalb des erforderlichen Zeitrahmens stattgefunden haben oder in denen keine Vereinbarung zur Aktualisierung des Dokuments vorliegt.

Es wird eine kontrollierte Sprache (d. h. die Verwendung kurzer, klarer Sätze und die Vermeidung von Fachsprache) verwendet, um ein gemeinsames Verständnis und eine hohe Qualität der Daten zu fördern.

Soweit durchführbar, die Art der Änderungen im Dokument oder die entsprechenden Anlagen, um ihre Überprüfung und Genehmigung sowie ihr Verständnis durch das Personal zu erleichtern.

Im Prozess zur Entwicklung von Verfahren wird erläutert, wie menschliche und organisatorische Faktoren berücksichtigt werden, z. B.:

- *Inhalt und Relevanz: Relevanz für die von der/den Person(en) wahrgenommene Aufgabe, einschließlich der Art und Weise, wie die an vorderster Front tätigen Akteure aktiv an der Konzeption dieser Verfahren beteiligt sind.*
- *Ablauf: Wie ist die Beschreibung von Prozessen und relevanten Zuständigkeiten (wer tut was) definiert, durch Ablaufdiagramme veranschaulicht.*
- *Anwendungsbereich: Integration eines umfassenderen Betriebsszenarios, um das Verständnis der für die durchzuführende Aufgabe erforderlichen Mittel und des angestrebten Ergebnisses zu gewährleisten.*
- *Schnittstellen: Enthält eine umfassende Benennung und Beschreibung der Schnittstellen. Es ist klar, wann das Verfahren eingesetzt werden sollte und wann es aufgrund von Änderungen der Aufgabe oder der Arbeitssituation nicht mehr anwendbar ist. Klare Regeln für Zweck und Anwendungsbereich im Hinblick auf die Nutzung des Verfahrens.*
- *Gültigkeit: aktualisiert und rechtzeitig für die Durchsetzung bereitgestellt.*
- *Angemessenheit und Vollständigkeit: angemessen im Hinblick darauf, wie die Arbeiten durchgeführt werden sollten, und mit vollständigen Angaben zu allen erforderlichen Einzelheiten.*
- *Sensibilisierung: Die Mitarbeiter haben ein solides Verständnis der bestehenden Verfahren/Vorschriften/Anforderungen und sind mit den sicherheitsbezogenen Gründen für die Verfahren und die möglichen Auswirkungen der Nichteinhaltung auf die operativen Tätigkeiten vertraut.*
- *Befolgung/Reaktion: Aus den Verfahren geht eindeutig hervor, welche Maßnahmen nach jeder Mitteilung zu ergreifen sind, und die erwartete Reaktion*
- *Leistung in Stress-/Notfallsituationen: Die Verfahren sind in Stress- oder Notfallsituationen leicht durchzuführen.*
- *Flexibilität: Die Prozesse ermöglichen den Beschäftigten Flexibilität bei der Reaktion auf Notfälle, um die negativen Folgen so gering wie möglich zu halten.*
- *Konsultation der Mitarbeiter: Die Mitarbeiter werden während der Entwicklung der Verfahren konsultiert – sie wissen am besten, wie die Aufgabe zu erledigen ist – und können Kommentare abgeben oder alternative Lösungen anbieten.*
- *Probezeit: Das Verfahren wird während einer Probezeit getestet, wobei das Ergebnis vor dem Inkrafttreten überprüft wird.*
- *Überarbeitung: Die Wirksamkeit des Verfahrens wird regelmäßig überprüft, wobei die Ergebnisse der Überwachung, die Prüfungen und die aus früheren Ereignissen gewonnenen Erkenntnisse berücksichtigt werden. Die Überarbeitung erfolgt im Sinne des Konzepts der kontinuierlichen Verbesserung und des organisatorischen Lernens.*
- *Änderungsmanagement: Die Verfahren werden überprüft, wenn neue Ausrüstungen oder Prozesse eingeführt werden. Das Änderungsmanagement in Bezug auf Verfahren ist wichtig, da es ermöglicht,*

diese an die Ziele und Regelungen der Unternehmen anzupassen und sicherzustellen, dass die entsprechenden Risiken beherrscht werden.

Die Mitarbeiter, welche die zu veröffentlichenden Dokumenten genehmigen dürfen, stellen sicher, dass die Inhalte richtig sind und von allen Endbenutzern (oder Empfängern), für die sie gelten, verstanden werden können.

4.5.6 Referenzen und Standards

- *Leitlinien zu den Anforderungen für dokumentierte Informationen in ISO 9001:2015, ISO/TC 176/SC2/N1286*

4.5.7 Aufsichtsaspekte

Prüfung, ob die vertraglichen Vereinbarungen eine effektive Überwachung und Kontrolle von Risiken durch die Organisation bereitstellen (d. h. bei der vertraglichen Untervergabe von Dienstleistungen).

Von entscheidender Bedeutung bei der Durchführung der Aufsicht ist es, festzustellen, wie sich das Verhältnis zwischen denjenigen, die das Dokumentenverwaltungssystem kontrollieren, und denjenigen, die für die Aktualisierung der Informationen und die Kontaktaufnahme mit den ersteren verantwortlich sind, in der Praxis darstellt. Auf dieser Ebene kann es oft zu einem Ausfall bei der Kontrolle der Dokumentation kommen, da die zwei Teile des Prozesses wahrscheinlich in zwei verschiedenen Verwaltungsketten stattfinden. Dies könnte beispielsweise dazu führen, dass die Wichtigkeit der Arbeit zur Aktualisierung der Dokumentation anders wahrgenommen wird, was zu Verzögerungen bei der Entwicklung und Aktualisierung von Dokumentationen mit den entsprechenden Risiken führt.

Die Fähigkeit der Mitarbeiter, auf aktuelle Informationen/Dokumentationen zuzugreifen.

Die Struktur des Sicherheitsmanagementsystems und der Betriebsmodus sollten die Realität der Art und Weise widerspiegeln, wie die Arbeit durchgeführt wird, und Gewohnheit und Praxis nicht künstlich überlagern.

4.6 Integration menschlicher und organisatorischer Faktoren

4.6.1 Regulatorische Anforderung

4.6.1. Die Organisation muss nachweisen, dass sie innerhalb des Sicherheitsmanagementsystems einen systematischen Ansatz zur Integration menschlicher und organisatorischer Faktoren verfolgt. Dieser Ansatz muss

(a) die Entwicklung einer Strategie sowie die Nutzung von Fachwissen und anerkannten Methoden auf dem Gebiet menschlicher und organisatorischer Faktoren umfassen;

(b) sich mit Risiken beschäftigen, die mit der Konzeption und Nutzung von Ausrüstung, den Aufgaben sowie den Arbeitsbedingungen und organisatorischen Regelungen zusammenhängen, wobei den menschlichen Fähigkeiten und Grenzen und den Einflüssen auf die menschliche Leistungsfähigkeit Rechnung zu tragen ist.

4.6.2 Zweck

Der Antragsteller zeigt, dass die Verwendung eines Ansatzes hinsichtlich systematischer menschlicher und organisatorischer Faktoren bei der Risikobewältigung ein integraler Bestandteil des Sicherheitsmanagementsystems ist. Die Erfüllung dieser Kriterien ist wichtig, um nachzuweisen, dass der Antragsteller befähigt ist, einen Eisenbahnbetrieb zu führen, und dass die Risikokontrollsysteme in einem Sicherheitsmanagementsystem eingebettet sind, um die Risiken, denen er ausgesetzt ist, zu beherrschen.

4.6.3 Erläuterungen

Menschliche und organisatorische Faktoren umfassen eine systemische Perspektive, bei der die Interaktionen zwischen menschlichen, technologischen und organisatorischen Faktoren berücksichtigt werden. Die Organisation sollte menschliche und organisatorische Faktoren im Sinne eines Lebenszyklusansatzes berücksichtigen. Dies bedeutet, dass menschliche und organisatorische Faktoren in Sicherheitsmanagementaktivitäten im Zusammenhang mit Geschäftszielen, Management, Betrieb, menschlicher Leistungsfähigkeit sowie Aufgaben- und Arbeitsplatzgestaltung in allen Phasen des Systemlebenszyklus, z. B. von der Inbetriebnahme bis zur Außerbetriebnahme, identifiziert und berücksichtigt werden. Eine Strategie für menschliche und organisatorische Faktoren spezifiziert einen systematischen Ansatz zur Einbindung menschlicher und organisatorischer Faktoren in Aktivitäten des Sicherheitsmanagements.

Die Organisation sollte die Kompetenz in Bezug auf menschliche und organisatorische Faktoren entwickeln, die sie benötigt, um ihre Geschäftstätigkeit insbesondere in Bezug auf Sicherheitsaufgaben zu unterstützen. Dies gilt auch für Mitarbeiter, die für die Integration menschlicher und organisatorischer Faktoren in die Risikobewertung zuständig sind. Fachwissen zu menschlichen und organisatorischen Faktoren bedeutet, dass die betreffenden Mitarbeiter eine spezielle Schulung gemäß der Definition im Kompetenzmanagementsystem erhalten haben. Professionelles Fachwissen zu menschlichen und organisatorischen Faktoren bedeutet, dass entweder Mitarbeiter auf einem geeigneten Niveau geschult sein müssen, um die Anforderung zu erfüllen, oder Zugang zu einer Person vorhanden ist, die nach einem bestimmten nationalen und/oder internationalen Standard für das Thema qualifiziert ist. Große Organisationen können eine Abteilung für menschliche Faktoren mit professionellen Experten für menschliche Faktoren haben, welche die Organisation unterstützt. Eine kleine Organisation kann Führungskräften auf allen Ebenen Verantwortung übertragen, um den Bedarf an externen professionellen Experten für menschliche Faktoren nach Bedarf zu identifizieren.

Diese Anforderung steht im Zusammenhang mit menschlichen und organisatorischen Faktoren. Weitere Informationen zu einer Strategie für menschliche und organisatorische Faktoren sind Anhang 5 zu entnehmen.

4.6.4 Nachweise

- *Der Antragsteller beschreibt in einer Strategie, wie menschliche und organisatorische Faktoren systematisch integriert werden, sodass die Risiken, die mit der Interaktion zwischen menschlichem Verhalten, organisatorischen Bedingungen und Technologie verbunden sind, in den Prozessen des Sicherheitsmanagementsystems angemessen berücksichtigt werden. Dabei sollte der Antragsteller deutlich machen, wo weitere Angaben zu den jeweiligen Verfahren oder zu Aktionsplänen für die schrittweise Integration/Entwicklung zu finden sind, denen die Tätigkeiten, wer mit ihrer Wahrnehmung betraut ist und der Zeitplan zu entnehmen sind;* ***(4.6.1)***
- *Es werden verfügbare Designstandards und vorbildliche Verfahren für menschliche und organisatorische Faktoren verwendet. Die entsprechenden Normen sind zum Beispiel die ISO-Reihe 11064 Ergonomische Gestaltung von Leitzentralen und die ISO-Reihe 9241 Ergonomie der Mensch-System-Interaktion;*
- *Beispielsweise kommt in Bezug auf neues oder geändertes Design, Verfahren, Schulungen, Arbeitsbelastung und Arbeitsumgebung ein benutzerzentrierter Designprozess auf Grundlage menschlicher und organisatorischer Grundsätze und Methoden sowie eine Einbeziehung der Nutzer zur Anwendung, um die lebenslange Sicherheit und Wirksamkeit eines Systems zu gewährleisten. Endnutzer werden in den Designprozess einbezogen, zum Beispiel in die Festlegung von Anforderungen, die nachfolgende Entwicklung und den Prüfprozess.*
- *Ein benutzerzentrierter Designprozess ist ein iterativer Prozess, der mehrere Phasen umfasst. Es werden Analysen durchgeführt, um den Kontext der Nutzung zu verstehen und genauer festzulegen (zum Beispiel Personalausstattung und Kompetenzanalyse, Aufgabenanalyse und Risikoanalyse). Auf Grundlage dieser Analysen werden die Anforderungen der Nutzer festgelegt. Designlösungen einschließlich der Gestaltung von Schnittstellen, Arbeitsplätzen, Schulungen, Verfahren und Organisation werden entwickelt, um die Anforderungen der Nutzer zu erfüllen. Die Designlösungen werden unter Verwendung formaler Methoden wie zum Beispiel Aufgabenanalyse, Simulation, Risikobewertung, Gutachten, Nutzerbewertungen, Verifizierung und Validierung bewertet. Dies umfasst insbesondere die Integration menschlicher und organisatorischer Faktoren in Risikobewertung, Information und Kommunikation sowie dokumentierte Informationen;* ***(3.1, 4.4 und 4.5)***
- *Hersteller und Zulieferer sind an der Entwicklung von Fahrzeugen, Ausrüstungen (Mensch-Maschine-Schnittstelle) und IT-Systemen beteiligt und wissen um die Bedeutung menschlicher Faktoren, und die notwendigen Anforderungen, die sich aus dem im vorstehenden Aufzählungspunkt beschriebenen Prozess ergeben, fließen in die Spezifikationen und in Verträge ein;* ***(5.2)***
- *Partner, Zulieferer und Auftragnehmer sind an der Förderung und Integration menschlicher und organisatorischer Faktoren beteiligt;* ***(5.3)***
- *Die Leistungsbewertungsprozesse umfassen Grundsätze und Methoden im Bereich menschlicher und organisatorischer Faktoren, die sich aus der Risikobewertung ergeben;* ***(6)***
- *Die Verbesserungsprozesse, einschließlich Unfalluntersuchung, umfassen die Analyse menschlicher und organisatorischer Faktoren.* ***(7)***

4.6.5 Beispiele für Nachweise

Eine Kopie der Strategie für menschliche und organisatorische Faktoren, in der detailliert dargelegt wird, wie der Einsatz von Fachwissen und Techniken im Bereich der menschlichen und organisatorischen Faktoren

berücksichtigt wird. In der Sicherheitsordnung wird auf die Strategie für menschliche und organisatorische Faktoren Bezug genommen.

Die Organisation führt anhand evidenzbasierter Methoden in Bezug auf betriebliche und unterstützende Prozesse in allen Phasen des Lebenszyklus, vom Design bis hin zur Entsorgung, eine Risikoanalyse durch. Bei der Analyse sollten alle menschlichen und organisatorischen Faktoren sowie die leistungsbeeinflussenden Faktoren, die sich auf die Eisenbahnsicherheit auswirken werden, und die Maßnahmen des Sicherheitsmanagements, die zur Beherrschung der festgestellten Risiken erforderlich sind, ermittelt werden.

Die Strategie für menschliche und organisatorische Faktoren zeigt die bestehenden Aktivitäten des Sicherheitsmanagements sowie einen Ansatz zur Überwachung und Verbesserung der Wirksamkeit der Strategie auf. Die Strategie beruht auf einem proaktiven Ansatz, umfasst bei Bedarf aber auch reaktive Maßnahmen.

Methoden im Bereich der menschlichen Faktoren, z. B. Aufgabenanalysen und Verwendbarkeitsanalysen, werden als Input für die Gestaltung, den Aufbau und den Inhalt der Verfahren verwendet, und bei Vollsimulationen werden aktuelle Mitarbeiter aus dem operativen Bereich einbezogen, um die Verfahren zu optimieren. Aktivitäten des Sicherheitsmanagements sollten in Bezug auf Unterstützungsfunktionen, Aufgabengestaltung, Personalbesetzung, Schulung, Gestaltung und Verwendung von Ausrüstung, Verfahren und Kommunikationsprotokollen ermittelt und mit den Ergebnissen der Risikobewertung verknüpft werden.

Die Strategie beinhaltet, wie menschliche und organisatorische Faktoren in den Änderungsmanagementprozess aufgenommen werden. „Integration menschlicher Faktoren“ ist der Prozess zur Integration von menschlichen Faktoren und Ergonomie in den systemtechnischen Prozess. Der Plan zur Integration menschlicher Faktoren bietet einen systematischen Ansatz zur Definition der Beziehung zwischen allen Projekttätigkeiten und dem Bereich der menschlichen Faktoren. Human Factors Engineering bedeutet die Integration menschlicher Eigenschaften in die Definition, Gestaltung, Entwicklung und Beurteilung eines Systems, um die Mensch-Maschine-Leistung unter betrieblichen Bedingungen zu optimieren.

Da die Betriebsprozesse unregelmäßige Arbeitszeiten umfassen, sollte die Strategie für menschliche und organisatorische Faktoren ein Programm zum Management von Ermüdungsrisiken vorsehen.

Es besteht ein klarer Zusammenhang zwischen den Ergebnissen der Risikobewertung, der Strategie für menschliche und organisatorische Faktoren und den Sicherheitszielen. Letztere umfassen die schrittweise Integration menschlicher und organisatorischer Faktoren, z. B.: Bestandsaufnahme der tatsächlichen Situation des Unternehmens, Ermittlung von Lücken, Entwicklung von Plänen für die Integration menschlicher und organisatorischer Faktoren in das SMS und für deren Verbesserung, sodass der Prozess und die einschlägige Dokumentation im Laufe der Zeit kontrolliert werden.

Es wird erläutert, wie die Strategie den Mitarbeitern ganz oder teilweise im Wege verschiedener Prozesse wie Bekanntgabe der Sicherheitsordnung, Sensibilisierung oder Sicherheitsziele vermittelt wird.

4.6.6 Referenzen und Standards

- *Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004). An Introduction to Human Factors Engineering. New Jersey: Pearson Education. ISBN-13: 978-0131837362*
- *ISO-Normenreihen, z. B.*
- *ISO-Reihe 6385:2004 Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen*
- *ISO-Reihe 11064 Ergonomische Gestaltung von Leitzentralen*
- *ISO-Reihe 9241 Ergonomie der Mensch-System-Interaktion*
- *ISO-Reihe 10075 Ergonomische Grundlagen bezüglich psychischer Arbeitsbelastung*

- *CENELEC - EN 50126-1 Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS-Prozess, Kapitel 5.6 (insbesondere § 5.6.4)*
- *EEMUA 191. Alarm systems, a guide to design, management and procurement [Alarmsysteme, ein Leitfaden zu Gestaltung, Management und Beschaffung]*
- *UIC 651 Gestaltung der Führerräume von Lokomotiven, Triebwagen, Triebwagenzügen und Steuerwagen*
- *Rail Safety & Standards Board (2008). Understanding Human Factors, a guide for the railway industry [Verständnis der menschlichen Faktoren, ein Leitfaden für die Eisenbahnindustrie]*

4.6.7 Aufsichtsaspekte

Prüfung, um sicherzustellen, dass die Belange der menschlichen Faktoren bei der Entscheidungsfindung für das Management von Risiken durch die Risikobewertung, das Änderungsmanagement und die Verwaltung von Sachanlagen berücksichtigt werden.

Prüfung, ob die betrieblichen Dokumente die Verpflichtung widerspiegeln, menschliche Faktoren durch ergonomisches Design zu managen (z. B.: benutzerfreundliches Design, einfache Sprache, Grafiken zur Unterstützung von Anweisungen, einfache Verwaltung von Updates), um das Risikomanagement zu unterstützen.

Prüfung, ob das Eisenbahnunternehmen/der Infrastrukturbetreiber bei der Überwachung der Leistung den Schwerpunkt seiner Analyse auf menschliche Faktoren als primäre oder zugrundeliegende Ursache von Unfällen, Störungen oder gefährlichen Situationen legt.

Prüfung, ob dokumentierte Beispiele für ergriffene Korrekturmaßnahmen vorliegen, die darauf abzielen, Faktoren zu beseitigen, die die menschliche Leistungsfähigkeit und die Sicherheit beeinträchtigen.

5 Betrieb

5.1 Betriebsplanung und -steuerung

5.1.1 Regulatorische Anforderung

5.1.1. Bei der Planung, Entwicklung, Anwendung und Überprüfung ihrer Betriebsverfahren stellt die Organisation sicher, dass während des Betriebs

(a) Kriterien für die Risikoakzeptanz und Sicherheitsmaßnahmen Anwendung finden (siehe 3.1.1 Risikobewertung);

(b) ein Plan bzw. Pläne zur Erreichung der Sicherheitsziele bereitgestellt werden (siehe 3.2 Sicherheitsziele und Planung);

(c) Informationen gesammelt werden, um die ordnungsgemäße Durchführung und Wirksamkeit der Betriebsabläufe zu messen (siehe 6.1 Überwachung).

5.1.2. Die Organisation stellt sicher, dass ihre Betriebsabläufe den Sicherheitsanforderungen der geltenden technischen Spezifikationen für die Interoperabilität sowie den jeweiligen nationalen Vorschriften und sonstigen einschlägigen Anforderungen entsprechen (siehe 1. Kontext der Organisation).

5.1.3. Zur Beherrschung der relevanten Risiken im Zusammenhang mit der Betriebssicherheit (siehe 3.1.1 Risikobewertung) ist mindestens Folgendes zu berücksichtigen:

(a) Planung bestehender oder neuer Zugverbindungen und neuer Eisenbahndienste; dies umfasst auch die Einführung neuer Fahrzeugtypen, die Notwendigkeit der Anmietung von Fahrzeugen und/oder der Einstellung von Personal von externen Beteiligten sowie den Austausch von Instandhaltungsinformationen für Betriebszwecke mit den für die Instandhaltung zuständigen Stellen;

(b) Erstellung und Durchführung von Zugfahrplänen;

(c) Vorbereitung von Zügen oder Fahrzeugen vor der Fahrt, einschließlich Kontrollen vor der Abfahrt und Zugbildung;

(d) Betrieb von Zügen/Fahrzeugen unter verschiedenen Betriebsbedingungen (Regelbetrieb, gestörter Betrieb und Notfälle);

(e) Anpassung des Betriebs bei Aufforderungen zur Außerbetriebnahme von Fahrzeugen und bei Meldungen ihrer Wiederinbetriebnahme durch die für die Instandhaltung zuständigen Stellen;

(f) Befugnisse zur Bewegung von Fahrzeugen;

(g) Nutzbarkeit der Schnittstellen im Führerstand und in den Zugleitstellen sowie mit den vom Instandhaltungspersonal verwendeten Ausrüstungen.

5.1.3 Zur Beherrschung der relevanten Risiken im Zusammenhang mit der Betriebssicherheit (siehe 3.1.1 Risikobewertung) ist mindestens Folgendes zu berücksichtigen:

(a) Bestimmung der Grenzen eines sicheren Verkehrs für die Verkehrsplanung und Verkehrssteuerung auf der Grundlage der Konstruktionsmerkmale der Infrastruktur;

(b) Verkehrsplanung, einschließlich Fahrplanerstellung und Zuweisung von Zugtrassen;

(c) Echtzeit-Verkehrsmanagement im Regelbetrieb und bei gestörtem Betrieb mit Anwendung von Verkehrsbeschränkungen und Störungsmanagement;

(d) Festlegung der Bedingungen für außergewöhnliche Frachten.

5.1.4. Zur Kontrolle der Zuweisung von betriebssicherheitsrelevanten Zuständigkeiten ermittelt die Organisation die Verantwortlichkeiten für die Koordinierung und Steuerung des sicheren Betriebs von Zügen und Fahrzeugen und legt fest, wie die einschlägigen, die sichere Erbringung aller Dienstleistungen betreffenden Aufgaben qualifizierten Mitarbeitern innerhalb der Organisation (siehe 2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse) und gegebenenfalls anderen qualifizierten externen Beteiligten (siehe 5.3 Auftragnehmer, Partner und Zulieferer) zugewiesen werden.

5.1.4 Zur Kontrolle der Zuweisung der betriebssicherheitsrelevanten Verantwortlichkeiten ermittelt die Organisation die Zuständigkeiten für die Planung und den Betrieb des Schienennetzes und legt fest, wie die einschlägigen, die sichere Erbringung aller Dienstleistungen betreffenden Aufgaben qualifizierten Mitarbeitern innerhalb der Organisation (siehe 2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse) und gegebenenfalls anderen qualifizierten externen Beteiligten (siehe 5.3 Auftragnehmer, Partner und Zulieferer) zugewiesen werden.

5.1.5. Zur Kontrolle der betriebssicherheitsrelevanten Information und Kommunikation (siehe 4.4 Information und Kommunikation) sind die betroffenen Mitarbeiter (z. B. das Zugpersonal) über alle besonderen Bedingungen der Fahrt genau zu unterrichten; dazu gehören auch Änderungen, die eine Gefahr verursachen können, vorübergehende oder dauerhafte Betriebseinschränkungen (z. B. aufgrund besonderer Fahrzeugtypen oder Strecken) und Bedingungen für außergewöhnliche Frachten, soweit zutreffend.

5.1.5 Zur Kontrolle der betriebssicherheitsrelevanten Information und Kommunikation (siehe 4.4 Information und Kommunikation) sind die betroffenen Mitarbeiter (z. B. Fahrdienstleiter) über besondere Anforderungen an die Streckenführung für Züge und Fahrzeuge zu unterrichten; dazu gehören auch Änderungen, die eine Gefahr verursachen können, vorübergehende oder dauerhafte Betriebseinschränkungen (z. B. aufgrund von Fahrweginstandhaltungen) und Bedingungen für außergewöhnliche Frachten, soweit zutreffend.

5.1.6. Zur Kontrolle der betriebssicherheitsrelevanten Kompetenzen (siehe 4.2 Kompetenz) stellt die Organisation nach den geltenden Rechtsvorschriften (siehe 1. Kontext der Organisation) in Bezug auf ihr Personal sicher, dass

(a) den Schulungs- und Arbeitsanweisungen Folge geleistet und falls erforderlich Korrekturmaßnahmen ergriffen werden;

(b) bei zu erwartenden Änderungen, die die Betriebsabläufe oder die Aufgabenstellungen betreffen, spezifische Schulungen stattfinden;

(c) nach Unfällen und Störungen geeignete Maßnahmen getroffen werden.

5.1.2 Zweck

Der Antragsteller sollte nachweisen, dass er über die entsprechenden Verfahren zur Beherrschung betrieblicher Risiken durch das Sicherheitsmanagementsystem verfügt, einschließlich der Sicherstellung, dass die Mitarbeiter ihre Rolle, die betrieblichen Risiken, denen sie ausgesetzt sind, und die Kontrollmaßnahmen verstehen, und dass sie über die entsprechende Kompetenz und Ausbildung verfügen, um diese Risiken gemäß der Dokumentation des Sicherheitsmanagementsystems zu beherrschen.

Der Antragsteller sollte sicherstellen, dass die Schienenfahrzeuge oder die Infrastruktur unter verschiedenen Betriebsbedingungen (d. h. Regelbetrieb, gestörter Betrieb und Notfälle), einschließlich der Verwendung von Sachanlagen zu Testzwecken (z. B. Prüfung des Fahrverhaltens von Schienenfahrzeugen vor Erteilung der Genehmigung) und unter außergewöhnlichen Umständen (z. B. außergewöhnliche Sendungen wie der Transport von großen unteilbaren Stücken, die nicht mit anderen Transportmitteln befördert werden können, wie Betonpfeiler/Träger für Brücken usw.), sicher gemäß den geltenden Anforderungen betrieben werden/wird.

5.1.3 Erläuterungen

In den Nummern 5.1.3, 5.1.4 und 5.1.5 des vorstehenden Rechtstextes werden bei der Anforderung an Infrastrukturbetreiber die Bestimmungen in Schwarz durch die Bestimmungen in Blau ersetzt.

Richtlinie (EU) 2016/798 fordert von den Eisenbahnunternehmen und Infrastrukturbetreibern, ein Sicherheitsmanagementsystem einzurichten, um die Sicherheitsrisiken ihres Eisenbahnbetriebs zu verwalten. Der allgemeine Konsens des Sicherheitsmanagements ist, dass die Sicherheit so weit wie möglich in normale Geschäftsprozesse integriert werden sollte. Der Grund dafür ist, dass der Geschäftsfokus dann genauso sehr auf Sicherheit liegt wie auf jedem anderen Geschäftsprozess, was die Konflikte zwischen den verschiedenen Prozessen reduziert.

Die ISO stellt in ihrem Leitfaden (N360), der Anhang SL unterstützt, fest, dass die Absicht von Klausel 8 (Betrieb) darin besteht, die Elemente zu spezifizieren, die innerhalb der Betriebsabläufe der Organisation umgesetzt werden müssen, um sicherzustellen, dass die Anforderungen an das Managementsystem erfüllt werden, sowie sicherzustellen, dass die vorrangigen Risiken und Chancen angegangen werden. Darüber hinaus wird angegeben, dass zusätzliche Anforderungen (disziplinspezifisch) in Bezug auf die Betriebsplanung und -kontrolle vorgeschrieben werden können. Insbesondere, dass sie nicht schädlich für das Geschäft des Unternehmens sind, sondern einen ausreichenden Rahmen bieten, um zu kontrollieren, wie wichtige Sicherheitsfragen innerhalb der Geschäftsprozesse des Unternehmens gehandhabt werden.

Es wurden explizite Verknüpfungen zwischen Betriebsanforderungen und Anforderungen an andere Managementsysteme hinzugefügt (ähnlich dem in Anhang III der Verordnung (EU) 2019/779 übernommenen Ansatz), um klarzustellen, dass spezifische Betriebsbedingungen hinsichtlich der relevanten Anforderungen an das Managementsystem berücksichtigt werden müssen (z. B. ist die Planung von Strecken für Eisenbahnunternehmen eine Tätigkeit, die der Risikobewertung unterliegen sollte). Dieser Ansatz ist nicht erschöpfend, sondern zielt darauf ab, bestimmte Fragen zu identifizieren, die die Behörden aufgrund ihrer Erfahrung für bedeutsam halten und die daher im Rahmen ihrer Bewertungs- oder Aufsichtstätigkeiten geprüft werden sollten. Eisenbahnunternehmen und Infrastrukturbetreiber sollten sich beim Entwickeln und Umsetzen ihrer Vorkehrungen des Sicherheitsmanagementsystems nicht nur auf diese spezifischen Anforderungen konzentrieren (beispielsweise durch Nichtbeachtung anderer Sicherheitsrisiken). Eisenbahnunternehmen und Infrastrukturbetreiber müssen auf jeden Fall die Anforderungen an das Sicherheitsmanagementsystem (z. B. Risikobewertung, Überwachung, Kompetenz, Information und Kommunikation) auf alle ihren relevanten Geschäftsprozesse anwenden, um aufzuzeigen, dass die Sicherheitsrisiken angemessen kontrolliert werden.

Die Integration des Sicherheitsmanagementsystems in die Geschäfts-/Betriebsprozesse ist von höchster Wichtigkeit und um dieses Ziel zu erreichen, muss die Organisation mit den geltenden TSI **(5.1.2)**, wie TSI OPE, und notifizierten nationalen Vorschriften konform sein, wenn die Schnittstellenanforderungen nicht vollständig in den TSI vorgeschrieben sind. Der Mitgliedstaat oder seine Behörde können auch annehmbare Nachweisverfahren veröffentlichen, um die Einhaltung der nationalen Vorschriften zu erleichtern. Es sollten, falls relevant, mindestens die folgenden Betriebsprozesse berücksichtigt werden:

- *Betrieb der Infrastruktur (Kontrolle von Infrastrukturstrecken und Ausrüstung, Genehmigung der Fahrzeugbewegungen unter allen Bedingungen und Sicherstellung der Infrastrukturwartung: Zugsteuerungs-/Zugsicherungs und Signalgebungssysteme);*
- *Betrieb von Zügen (Entwicklung von Strecken und entsprechenden Fahrplänen, Verwaltung der Zugvorbereitung, Gewährleistung der Zugfahrt, Begleitung, Prüfung, Instandhaltung und Reparatur von Schienenfahrzeugen);*
- *Rangieren (Bewegung von Schienenfahrzeugen zur Kopplung und Entkopplung von Zügen).*

Das TSI-OPE ist hier ausschlaggebend, da es die prinzipiellen Funktionsweisen (FOP) festlegt, die in den relevanten Teilen des Sicherheitsmanagementsystems widergespiegelt werden sollten, und deshalb kann die Konformität mit dem TSI-OPE verwendet werden, um die Konformität mit den obigen relevanten Anforderungen an das Sicherheitsmanagementsystem aufzuzeigen.

Der Infrastrukturbetreiber sollte die Bedingungen und Maßnahmen für die Nutzung eines Fahrzeugs für Tests auf dem Netz innerhalb des in Artikel 21 Absatz 3 und Artikel 21 Absatz 5 der Richtlinie (EU) 2016/797 festgelegten Zeitrahmens festlegen und bereitstellen **(5.1.2)**.

Protokolle über die Prüfung der Kompatibilität von Strecken enthalten auch die Eigenschaften des Fahrzeugs/Zugs unter Berücksichtigung der geplanten Betriebsstrecken, einschließlich möglicher Ausweichstrecke(n), die von den Infrastrukturbetreibern ermittelt wurden (siehe Abschnitt 4.2.2.5 der TSI OPE).

Die Eigenschaften der Betriebsstrecken basieren auf dem Infrastrukturregister (RINF) und/oder den Informationen, die vom Infrastrukturbetreiber vorgelegt wurden.

Wenn eine der Parteien Probleme erkennt, sollte eine gemeinsame Lösung zwischen dem Bahnunternehmen und dem Infrastrukturbetreiber angestrebt werden.

Neuer Zugverkehr **(5.1.3 Buchstabe a)** kann neue Arten von zu befördernden Gütern umfassen.

„Grenzen eines sicheren Verkehrs“ **(5.1.3 Buchstabe a)** bedeutet für Infrastrukturbetreiber sowohl sichere Grenzen der physischen Infrastruktur, wenn dies erforderlich ist, als auch Grenzen der Sicherheit für die Infrastruktur sowie für Steuerung und Sicherung, sofern diese aufgrund der Designgrenzen dieser Infrastruktur erforderlich sind.

Die Bewegung von Fahrzeugen **(5.1.3 Buchstabe d)** hat eine weitläufigere Bedeutung als nur die Bewegung von Zügen (d. h. geplante Bewegung von Fahrzeugen) und die Erteilung von Genehmigungen vor Abfahrt des Zuges. Sie kann auch eine Wiederinbetriebnahme eines ausgefallenen Zuges, die Bewegung von Schienenwartungsfahrzeugen oder den ungeplanten Austausch eines beschädigten Fahrzeugs in einem Zug vor der Abfahrt des Zuges umfassen.

In Übereinstimmung mit dem UIC-Merkblatt 502-1, Artikel 1.1 wird die folgende Definition des Begriffs „außergewöhnliche Sendungen“ **(5.1.5)** vorgeschlagen: *„Eine Sendung gilt als außergewöhnlich, wenn sie wegen ihren äußeren Abmessungen, ihres Gewichtes oder ihrer Beschaffenheit mit Rücksicht auf die Bahnanlagen oder Wagen einer der am Transport Beteiligten besondere Schwierigkeiten verursacht und deshalb nur unter besonderen technischen oder betrieblichen Bedingungen zugelassen werden kann.“* Im Sinne der TSI OPE bezeichnet Sondertransport *“[e]in Fahrzeug und/oder die beförderte Ladung, die aufgrund von Bauart/Auslegung, Abmessungen oder Gewicht nicht den Parametern der Strecke entspricht und eine Sondererlaubnis für die Fahrt erfordert und besondere Bedingungen für einen Teil oder die gesamte Fahrt erfordern kann”.*

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Der Austausch von Informationen für betriebliche Zwecke bei der Fahrzeugwartung **(5.1.3 Buchstabe a)** mit ECM und Haltern wird in Artikel 5 Absatz 3 der Verordnung (EU) 2019/779 festgelegt. Dies beinhaltet von der

ECM während der Instandhaltung ausgestellte Instandhaltungspläne und etwaige Einschränkungen (Kurzzeitplanung).

Wird auf die Entwicklung und Umsetzung von Zugfahrplänen verwiesen **(5.1.3 Buchstabe b)**, so bedeutet dies, dass der Antragsteller nachweisen sollte, wie er das Risiko, das von der Tätigkeit innerhalb seiner Organisation und an der Schnittstelle zu anderen Akteuren ausgeht, durch eine Risikobewertung bewältigt hat. Beispielsweise sollte er aufzeigen, dass er Folgendes berücksichtigt hat:

- *die zusätzliche Arbeitslast an signalgebende Mitarbeiter, wenn die Anzahl an Zügen zu bestimmten Zeiten erhöht wird;*
- *die angemessenen Betriebsvereinbarungen mit den relevanten Infrastrukturbetreibern für das Anhalten des Verkehrs, die Wiederinbetriebnahme, den Informationsaustausch und alle anderen Dienstleistungen, die als notwendig erachtet werden:*
- *Verwaltung der Risiken in Bezug auf die Streckenwartung, wenn Züge 24 Stunden am Tag betrieben werden.*

Die Organisation wendet einen proaktiven Risikobewertungsprozess an, der die Ermittlung von Risiken ihres Eisenbahnbetriebs ermöglicht, einschließlich der gemeinsamen Schnittstellenrisiken und der von menschlichen und organisatorischen Faktoren ausgehenden Risiken (siehe ferner 3.1). Außerdem verringert dieser Prozess das Risiko, sich allzu sehr auf übernommene Verfahren oder Vorschriften zu stützen.

Die Organisation wendet Kriterien für die Risikoakzeptanz an, um festzustellen, ob die bestehenden Maßnahmen ausreichen, um die Risiken auf ein annehmbares Maß zu begrenzen oder zu verringern, oder ob auf andere Weise neue Maßnahmen festzulegen sind. Die Organisation integriert sodann ihre betrieblichen Tätigkeiten und die Einhaltung der TSI, soweit diese den Betrieb betreffen, in ihren Überwachungsprozess (siehe Abschnitt ***6 Leistungsbewertung)***).

Menschliche und organisatorische Faktoren sollten bei der betrieblichen Planung mit Blick auf die kontinuierliche Verbesserung der Sicherheitskultur in Verbindung mit z. B. Arbeitsplänen, Ermüdungsmanagement, Stress, (physische und psychosoziale) Arbeitsumgebung, Arbeitsplätzen und Arbeitsprozessen usw. berücksichtigt werden. Dadurch soll sichergestellt werden, dass die Konsequenzen der Änderungen oder Vorkehrungen keinen negativen Einfluss auf das menschliche Leistungsvermögen oder die Organisationssicherheit haben.

5.1.4 Nachweise

- *Informationen, aus denen hervorgeht, dass der Antragsteller bei der Planung, Entwicklung, Umsetzung und Überprüfung seiner betrieblichen Prozesse die Erreichung von Sicherheitszielen plant, Maßnahmen zur Risikobewertung anwendet und die Ergebnisse überwacht, einschließlich der entsprechenden Hinweise, wo zusätzliche Informationen über Verfahren zu finden sind;* ***(5.1.1 Buchstaben a bis c)***
- *Nachweise, dass sich die Organisation sämtlicher Kategorien der obligatorischen Sicherheitsanforderungen, die für ihren Betrieb gelten, bewusst ist und diese tatsächlich umsetzt und festlegt, wie das Sicherheitsmanagementsystem die Konformität mit diesen gewährleistet;*
- *Information, dass der Antragsteller sicherstellt, dass seine betrieblichen Vorkehrungen mit den geltenden Anforderungen (Gesetzgebung, Normen usw.) konform sind;* ***(5.1.2)***
- *Im Rahmen der Fahrzeugtypzulassung und/oder Fahrzeugzulassung zum Inverkehrbringen kann der Infrastrukturbetreiber Folgendes identifizieren und bereitstellen* ***(5.1.2)****:*
    - *betriebliche Bedingungen, die auf die Verwendung von Fahrzeugen für Tests auf dem Netz angewandt werden, basierend auf den vom Antragsteller für die Zulassung bereitgestellten Informationen;*

- *notwendige, auf der Infrastrukturseite zu ergreifende Maßnahmen zur Gewährleistung eines sicheren und zuverlässigen Betriebs während der Tests auf dem Netz und/oder*
- *notwendige Maßnahmen in den Infrastrukturinstallationen, um die Tests auf dem Netz durchzuführen.*

- *Zur Prüfung vor Nutzung genehmigter Fahrzeuge (Artikel 23 Absatz 1 der Richtlinie (EU) 2016/797) und insbesondere zur Prüfung der Streckenkompatibilität (Artikel 23 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/797) kann das Bahnunternehmen im Rahmen seines SMS Nachweisverfahren und -unterlagen ermitteln und zur Verfügung stellen **(5.1.3 Buchstabe a)**, die zeigen, dass das Fahrzeug mit der Strecke kompatibel ist, auf der es eingesetzt werden soll, und dass es ordnungsgemäß in den Zug integriert ist (siehe ferner Abschnitt 4.2.2.5 der TSI OPE).*
- *Nachweis der Übereinstimmung der Betriebsdokumentation mit den Anforderungen für das Management des Betriebs (und der Instandhaltung) an organisatorischen und physischen Grenzen, z. B. organisatorische, technische und betriebliche Schnittstellen zu benachbarten Infrastrukturen, Grenzstationen, Interaktionen mit anderen Eisenbahnunternehmen oder Infrastrukturbetreibern usw.; **(5.1.2)***
- *Informationen darüber, wie die Risiken betrieblicher Tätigkeiten im Rahmen des Risikobewertungsprozesses beherrscht werden und die in den oben genannten Anforderungen dargelegten Elemente abdecken, einschließlich in Bezug auf menschliche und organisatorische Faktoren; **(5.1.3 Buchstabe a, Buchstaben c bis f)***
- *Nachweise, dass Artikel 14 Absatz 2 der Richtlinie (EU) 2016/798 von der für die Instandhaltung verantwortlichen Stelle eingehalten wird; **(5.1.3 Buchstabe f)***
- *Informationen darüber, wie die Verantwortlichkeiten, einschließlich der Verantwortlichkeit für das Management von Ermüdungsrisiken, für die Sicherheit der betrieblichen Tätigkeiten verwaltet werden; **(5.1.4)***
- *Informationen darüber, wie die Organisation Informationen und Kommunikationen für die Sicherheit der betrieblichen Tätigkeiten verwaltet; **(5.1.5)***
- *Informationen über das Kompetenzmanagementsystem und die damit verbundenen Verfahren und deren Verknüpfung mit spezifischen Arbeits- oder Aufgabenanweisungen zur Aufrechterhaltung der Sicherheit betrieblicher Tätigkeiten; **(5.1.6)***
- *Nachweis, dass die Betriebsdokumentation (Verfahren, Arbeitsanweisungen usw.) bei Bedarf aktualisiert wird. **(siehe ferner 4.5.3)***

5.1.5 Beispiele für Nachweise

Eine Liste der verpflichtenden Anforderungen (einschließlich TSI) und wie der Antragsteller diese erfüllt **(siehe ferner 2)**.

Erläuterung, wie betriebliche Risiken im Rahmen des Risikobewertungsprozesses beherrscht werden und wie sichergestellt wird, dass die Ziele der Betriebssicherheit erreicht werden. Es werden Links zu den relevanten Verfahren bereitgestellt.

Eine Erklärung darüber, wie das Kompetenzmanagementsystem zur Kontrolle betrieblicher Risiken beiträgt und wie der Informations- und Kommunikationsfluss gesteuert wird, um sicherzustellen, dass die Risiken angemessen kontrolliert werden.

Angaben zum Instandhaltungssystem für Schienenfahrzeuge.

Angaben zum Verfahren für die Prüfungen vor der Abfahrt (TSI OPE), die durchgeführt werden, um eine Konformitätsprüfung der folgenden Punkte zu gewährleisten:

- *Bremsleistung (Vorbereitung des Bremszettels),*
- *Zugzusammensetzung;*

- *Vordere und hintere Signale;*
- *Last und Zustand der gezogenen Wagen.*

Eine Kopie des Verfahrens zur Feststellung von Verstößen und Informationen darüber, wie sichergestellt wird, dass alle erforderlichen Maßnahmen ergriffen werden, wie z. B. die Maßnahmen, die zur Außerbetriebnahme des Fahrzeugs, zum Austausch ausgefallener/defekter Komponenten/Ausrüstung/Fahrzeuge oder zur Einführung von Betriebsbeschränkungen führen.

Ein Dokument, aus dem hervorgeht, welche Arten von Fahrzeugen auf den einzelnen Strecken eingesetzt werden sollen und welche Art von Vorgängen durchzuführen sind, insbesondere:

- *betriebliche Einschränkungen aufgrund spezifischer Fahrzeugtypen;*
- *Einschränkungen aufgrund des Betriebs spezifischer Fahrzeugtypen auf bestimmten Strecken;*
- *zusätzliche Instandhaltungsanforderungen für spezifische Strecken* ***(siehe ferner 5.2)****.*

In Bezug auf die Konformität mit den prinzipiellen Funktionsweisen der TSI OPE werden Nachweise geliefert, die zeigen, dass das Eisenbahnunternehmen Folgendes gewährleisten kann (nur zu Veranschaulichungszwecken):

- *Ein Zug kann über einem Teil der Linie betrieben werden, wenn die Zugzusammensetzung mit der Infrastruktur kompatibel ist (FOP 3).*

  Dies bezieht sich auf die Bestätigung der Kompatibilität des Zuges mit der Infrastruktur der Strecke, über die er fahren soll, bevor die Bewegung genehmigt wird. Die Kompatibilität zwischen einem Zug und der Infrastruktur wird in erster Linie durch die Abmessungen des Fahrzeugs und der auf ihm befindlichen Last, die Abstände zwischen dem Zug und der Infrastruktur bzw. den Zügen auf benachbarten Gleisen (Spurweite), die minimal erforderliche Bremsleistung des Zuges, das Gewicht und die Länge eines Zuges sowie die Kapazität und Leistungsfähigkeit der Infrastruktur beeinflusst.

  Es liegen Nachweise darüber vor, dass:

- *Prüfungen vor der Abfahrt stattfinden, um vor Beginn oder bei Fortsetzung der Fahrt zu gewährleisten, dass ein Zug seine Fahrgäste, Mitarbeiter und Fracht sicher befördert (FOP 4).*

  Dies betrifft den Zug und seine Bewegungsbereitschaft. Dazu gehören beispielsweise die Bremsleistung des Zuges, die Geschwindigkeit, mit der der Zug fahren darf, die Bildung und Kopplung des Zuges, die Identifizierung, Verladung und Sicherung der Fracht, die Bereitstellung angemessener Informationen für die Zugvorbereitung und das Betriebspersonal. Das Ziel besteht darin, Zusammenstöße und Entgleisungen aufgrund einer Reihe von Risiken zu vermeiden.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Ein Dokument, das zusätzliche Anforderungen zur Verwaltung von Störungssituationen (z. B. Störungen bei einem Fahrzeug) für die betroffenen Netze nach geografischem Tätigkeitsgebiet beschreibt.

Die Personen, die für die Planung und Durchführung der operativen Tätigkeiten zuständig sind, werden darin geschult, menschliche und organisatorische Faktoren zu berücksichtigen sowie den Fähigkeiten und Grenzen in Verbindung mit dem menschlichen Leistungsvermögen, einschließlich ermittelter Risiken und Sicherheitsmaßnahmen, Rechnung zu tragen.

Ermittlung von Sicherheitsinformationen und Einhaltung der Grundsätze menschlicher und organisatorischer Faktoren (siehe Abschnitt ***4.4 Information und Kommunikation***).

Ein Prozess für das Ermüdungsmanagement, der für Mitarbeiter mit unregelmäßigen Arbeitszeiten gilt. Der Prozess beruht auf evidenzbasierten Methoden und professionellem Fachwissen. Der Prozess berücksichtigt, dass eine Reihe von Faktoren in Betracht gezogen werden muss, wenn ein umfassender Ansatz für das

Management von Ermüdungsrisiken verfolgt wird. Das Ermüdungsmanagementprogramm umfasst Planung und Kontrolle der Arbeitsumgebung und -aufgaben, um so weit wie vernünftigerweise umsetzbar die Auswirkungen von Müdigkeit auf die Aufmerksamkeit und Leistung der Mitarbeiter auf eine Weise zu minimieren, die dem Niveau der Risikoexposition und der Betriebsart angemessen ist.

5.1.6 Referenzen und Standards

- *ISO N360 JTCG Konzeptdokument zur Unterstützung von Anhang SL*
- *UIC-Merkblatt 502-1*
- *Anhang II der Richtlinie 2008/68/EG (RID)*
- *Leitlinien zur TSI OPE*

5.1.7 Aufsichtsaspekte

Die Aufsicht der betrieblichen Tätigkeit sollte durch die Konzentration auf einzelne Bereiche und deren eingehende Prüfung erfolgen, um festzustellen, wie sie sich im Sicherheitsmanagementsystem der zu überwachenden Organisation widerspiegeln und ob die richtigen Mitarbeiter am richtigen Ort das Richtige tun. Auf diese Weise kann die nationale Sicherheitsbehörde sehen, ob die Aktivitäten im Rahmen des Sicherheitsmanagementsystems als kohärentes Ganzes erfasst werden oder ob sie getrennt verwaltet werden, mit schwachen Verbindungen zu den Sicherheitszielen und der Gesamtstrategie.

Bei der Aufsicht sollte insbesondere Folgendes geprüft werden:

- *Wie sich SMS-Unterlagen höherer Ebenen in einheitliche lokale Anweisungen umsetzen lassen, die zum Risikomanagement auf Betriebsebene verwendet werden;*
- *Das Management von Notfallsituationen oder nicht routinemäßigen Situationen;*
- *Die Art, wie Betriebsgrenzen/-einschränkungen verwaltet werden, einschließlich der Schnittstellenvereinbarungen mit anderen Parteien;*
- *Vorkehrungen zum Ermüdungsmanagement;*
- *Umgang mit gefährlichen Stoffen;*
- *Vorkehrungen für die Beförderung gefährlicher Güter, einschließlich der Schulung, Aufgaben und Zuständigkeiten für die Mitarbeiter der Organisation nach den Kapiteln 1.3, 1.4 und 1.8 der RID, bei Bedarf Kontaktaufnahme mit anderen für die Beförderung gefährlicher Güter zuständigen Behörden;*
- *Konformität mit den in den TSI OPE festgelegten prinzipiellen Funktionsweisen.*

5.2 Verwaltung von Sachanlagen

5.2.1 Regulatorische Anforderung

5.2.1. Die Organisation muss die mit den Sachanlagen verbundenen Sicherheitsrisiken während ihres gesamten Lebenszyklus (siehe 3.1.1 Risikobewertung) von der Konstruktion bis zur Entsorgung beherrschen und die durch menschliche Faktoren bedingten Anforderungen in allen Phasen des Lebenszyklus erfüllen.

5.2.2. Die Organisation muss

(a) die bestimmungsgemäße Verwendung der Sachanlagen gewährleisten und dabei deren sicheren Betriebszustand gemäß Artikel 14 Absatz 2 der Richtlinie (EU) 2016/798, soweit anwendbar, und erwartetes Leistungsniveau aufrechterhalten;

(b) die Sachanlagen im Regelbetrieb und bei gestörtem Betrieb verwalten;

(c) Fälle der Nichteinhaltung von Betriebsanforderungen vor oder während des Betriebs der Sachanlage so rasch wie nach vernünftigem Ermessen möglich erkennen und gegebenenfalls Nutzungsbeschränkungen anwenden, um den sicheren Betriebszustand der Sachanlage zu gewährleisten (siehe 6.1 Überwachung).

5.2.3. Die Organisation muss dafür sorgen, dass ihre Regelungen für die Verwaltung der Sachanlagen gegebenenfalls den grundlegenden Anforderungen der betreffenden technischen Spezifikationen für die Interoperabilität sowie allen sonstigen einschlägigen Anforderungen entsprechen (siehe 1. Kontext der Organisation).

5.2.4. Zur Beherrschung der relevanten Risiken im Zusammenhang mit der Instandhaltung (siehe 3.1.1 Risikobewertung) ist mindestens Folgendes zu berücksichtigen:

(a) Ermittlung des Instandhaltungsbedarfs auf der Grundlage der geplanten und tatsächlichen Nutzung sowie der Konstruktionsmerkmale der Sachanlagen, um sie in sicherem Betriebszustand zu halten;

(b) Management der Außerbetriebnahme der Sachanlage zu Instandhaltungszwecken, wenn Defekte festgestellt werden oder ihr Zustand sich soweit verschlechtert, dass der sichere Betriebszustand gemäß Buchstabe a nicht mehr gewährleistet ist;

(c) Management der Wiederinbetriebnahme der Sachanlage nach erfolgter Instandhaltung mit etwaigen Nutzungsbeschränkungen, um den sicheren Betriebszustand zu gewährleisten;

(d) Management von Überwachungs- und Messausrüstungen, damit die Anlage entsprechend ihrem Verwendungszweck eingesetzt werden kann.

5.2.5. Zur Lenkung der für die sichere Verwaltung von Sachanlagen relevanten Information und Kommunikation (siehe 4.4 Information und Kommunikation) muss die Organisation Folgendes berücksichtigen:

(a) den Austausch relevanter Informationen innerhalb der Organisation oder mit externen für die Instandhaltung zuständigen Stellen (siehe 5.3 Auftragnehmer, Partner und Zulieferer), insbesondere in Bezug auf sicherheitsrelevante Fehlfunktionen, Unfälle, Störungen und etwaige Nutzungseinschränkungen der Sachanlage;

(b) die Nachverfolgbarkeit aller notwendigen Informationen, einschließlich der Informationen betreffend Buchstabe a (siehe 4.4 Information und Kommunikation und 4.5.3 Kontrolle dokumentierter Informationen);

(c) die Erstellung und Führung von Aufzeichnungen, einschließlich des Managements von Änderungen, die sich auf die Sicherheit der Sachanlagen auswirken (siehe 5.4 Änderungsmanagement).

5.2.2 Zweck

Der Antragsteller sollte nachweisen, wie er den Lebenszyklus seiner Sachanlagen von der Konstruktion bis zur Entsorgung durch die im Sicherheitsmanagementsystem beschriebenen Verfahren und Vorkehrungen verwaltet. Der Antragsteller sollte aufzeigen, dass er in jeder Phase des Lebenszyklus einen menschenzentrierten Ansatz verfolgt hat. Er sollte detailliert angeben, wo die Verwaltung von Sachanlagen mit verschiedenen Elementen seines Sicherheitsmanagementsystems verbunden ist, wie beispielsweise dem Kompetenzmanagement, der Betriebsplanung und der Überwachung. Das Ziel des Antragstellers sollte darin liegen, aufzuzeigen, dass er über ein solides System für die Verwaltung von Sachanlagen verfügt, das die Risiken widerspiegelt, die durch die Art und den Umfang seines Betriebs entstehen.

5.2.3 Erläuterungen

„Sachanlage“ **(5.2)** bedeutet sämtliche Ausrüstungen (fest oder mobil), Struktur, Software oder anderen Komponenten, die mit der Zeit eine Instandhaltung erfordern und bereitgestellt werden, um einen Eisenbahnbetrieb zu führen. Die Sachanlagen werden aufgeteilt in die vom Eisenbahnunternehmen verwalteten (hauptsächlich Fahrzeuge, aber auch andere Ausrüstungen, z. B. Radsatzdrehmaschinen, Schutzausrüstung und Computerprogramme, die für die sichere Instandhaltung der Anlagen bereitgestellt werden) und die von einem Infrastrukturbetreiber verwalteten (alle Infrastrukturkomponenten wie Gleise, Ausrüstung für Zugsteuerung/Zugsicherung und Signalgebung, Stellwerke, Stromversorgung, Bahnübergänge, Hoch- und Tiefbauwerke wie Brücken, Viadukte, Tunnel, Bahnsteige, Aufzüge, Fahrtreppen usw.). Eine vollständige Liste ist Anhang I der Richtlinie (EU) 2012/34) zu entnehmen.

Der Lebenszyklus einer Sachanlage umfasst die folgenden Phasen:

a) Design;
b) Umsetzung (Konstruktion/Herstellung, Installation, Prüfung und Inbetriebnahme);
c) Betrieb und Instandhaltung;
d) Reparatur, Umbau und Nachrüstung, Hinzuziehen des Änderungsmanagements;
e) Verlängerung, Außerbetriebnahme und Entsorgung.

Für eine Organisation ist es wichtig aufzuzeigen, wie sie (System- und) Sicherheitsanforderungen für ihre Sachanlagen erfasst und pflegt und wie diese verifiziert, validiert und nachverfolgt werden.

Wenn ein Dritter mit der Instandhaltung beauftragt wird, unterliegt es der Verantwortung der Organisation, darzulegen und zu überwachen, dass die Leistung der Sachanlage den festgelegten Standards der Organisation entspricht.

Sobald Prozesse zur Steuerung des Risikos vorhanden sind, das mit sicherheitskritischen Sachanlagen einhergeht, sollte die Organisation die Leistung der Sachanlage anhand dieser Risiken und ihrer eigenen Erwartungen überwachen.

Wenn Sachanlagen voraussichtlich ersetzt, außer Betrieb genommen oder entsorgt werden, legt die Organisation Prozesse zur Steuerung der mit diesen Tätigkeiten verbundenen Risiken fest und dokumentiert diese.

Diese Prozesse sind nur für solche Organisationen relevant, die diese Tätigkeiten ausführen oder wahrscheinlich ausführen.

Beim Ersatz einer Sachanlage, die das Ende ihrer Nutzungsdauer bald erreicht hat, sorgt die Organisation dafür, dass die Ersatzsachanlage den festgelegten Sicherheitsleistungskriterien entspricht. Als Teil dieses Prozesses werden sämtliche Sicherheitsanalysen überprüft.

Anforderungen in Bezug auf die Instandhaltung **(5.2.4)** ergeben sich aus der Verordnung (EU) 2019/779, wobei die Schienenfahrzeuge eine Sachanlage sind, die ein Eisenbahnunternehmen und möglicherweise ein Infrastrukturbetreiber verwalten sollte. Diese Anforderungen in Anhang II der Verordnung (EU) 2019/779 sind spezifischer und verbindlich zu erfüllen, während die oben genannten Anforderungen hauptsächlich die Schnittstelle zwischen dem Sicherheitsmanagementsystem des Eisenbahnunternehmens oder Infrastrukturbetreibers und dem Instandhaltungssystem der ECM betreffen, um sicherzustellen, dass die Anlagen sicher zu betreiben und zu warten sind. Weitere Einzelheiten sind der ECM-Verordnung und dem zugehörigen Leitfaden zu entnehmen. Die Risikobewertung sollte sich auch mit den potenziellen Sicherheitsauswirkungen einer Ersetzung im Rahmen der Instandhaltung (die Teil des Lebenszyklus der Sachanlage ist) gemäß den Anforderungen der Richtlinie (EU) 2016/797 und der einschlägigen TSI befassen.

Es werden nicht alle Sachanlagen von TSI geregelt **(5.2.3)**, und auch wenn eine TSI gilt (z. B. TSI INF), wird nur das Nötigste für die Interoperabilität geregelt, was bedeutet, dass immer noch andere Sicherheitsanforderungen gebraucht werden können. Die Einhaltung der grundlegenden Anforderungen der einschlägigen TSI (nicht nur der grundlegenden Sicherheitsanforderungen) ist im Falle der Ersetzung, Verlängerung oder Umrüstung aufrechtzuerhalten.

Der Begriff „sicherer Betriebszustand“ **(5.2.4 Buchstabe a)** bedeutet, dass die Sachanlage innerhalb ihrer sicheren Einsatzgrenzen betrieben werden kann. Die sicheren Einsatzgrenzen können sich während der Lebensspanne des Systems weiterentwickeln, müssen aber unter Berücksichtigung der Interoperabilitätsparameter definiert werden. Defekte können identifiziert **(5.2.4 Buchstabe b)** und basierend auf einer Ursachenanalyse können die sicheren Einsatzgrenzen entsprechend übernommen werden. Für Fahrzeuge bedeutet „sicherer Betriebszustand“ einen sicheren Betriebszustand im Sinne von Artikel 14 Absatz 2 der Richtlinie (EU) 2016/798.

Die Konfiguration der Sachanlagen **(5.2.5 Buchstabe c)** umfasst die eindeutige Identifizierung der Sachanlagen, ihren Standort, durchgeführte Instandhaltung usw. (und nicht nur das Konfigurationsmanagement von Änderungen). Das Konfigurationsmanagement von (technischen) Änderungen gilt für die Ersetzung.

Es muss in Übereinstimmung mit Artikel 14 Absatz 1 der Richtlinie (EU) 2016/798 eine für die Instandhaltung zuständige Stelle (ECM) zugewiesen werden, um sicherzustellen, dass sich die Fahrzeuge für deren Instandhaltung sie verantwortlich ist, in einem sicheren Betriebszustand befinden. Es ist nicht erforderlich, die Tätigkeiten einer ECM, die nach der Verordnung (EU) 2019/779 zertifiziert ist, detailliert zu beschreiben. Andererseits ist anzugeben, welche Elemente und welche Aspekte durch das ECM-Zertifikat abgedeckt sind und wie die Schnittstelle zur ECM verwaltet wird, insbesondere welche Informationen zwischen dem Antragsteller und der ECM ausgetauscht werden und wie dies geschieht. Wenn die ECM nicht direkt vom Eisenbahnunternehmen beauftragt wird, sondern als Dritter an einem Vertrag zwischen einem Fahrzeugeigentümer (oder -halter) und dem Eisenbahnunternehmen beteiligt ist, kann der Informationsaustausch über eine zwischengeschaltete Stelle erfolgen, muss aber dennoch in beide Richtungen effizient und zeitnah ablaufen.

Im Falle einer Partnerschaft zwischen Eisenbahnunternehmen bleibt jedes Eisenbahnunternehmen voll verantwortlich für den sicheren Betrieb und damit für die Beherrschung der mit seiner Tätigkeit verbundenen Risiken. Die Verwendung der Sicherheitsbescheinigung des Partner-Eisenbahnunternehmens als Mittel zur Beherrschung der mit der Instandhaltung verbundenen Risiken durch ein Eisenbahnunternehmen ist nicht ausreichend, wenn sie nicht durch vertragliche Vereinbarungen zwischen den Partner-Eisenbahnunternehmen gestützt wird. Diese vertraglichen Vereinbarungen müssen von jedem Partner gemeinsam entwickelt und überwacht werden und sind auch Bestandteil jedes Sicherheitsmanagementsystems und unterliegen daher der Aufsicht der jeweiligen nationalen

Sicherheitsbehörde. Die jeweiligen nationalen Sicherheitsbehörden sollten sich koordinieren, um etwaige grenzüberschreitende Schnittstellenprobleme, die möglicherweise von den Auftraggebern geschaffen wurden, anzugehen.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Menschliche Faktoren werden über den Lebenszyklus aller Systeme und Teilsysteme auf der Grundlage der Ergebnisse der Risikobewertung, die bereits menschliche und organisatorische Faktoren und die festgelegten Sicherheitsmaßnahmen umfasst, integriert.

Dazu gehört ein benutzerzentrierter Ansatz in der Designphase des Systems, der aus Funktionszuweisung (Mensch/Maschine), Befragungen und Aufgabenanalysen (für jede Teilaufgabe) bestehen kann. Die Spezifikationen für die Sachanlagen basieren auf den Bedürfnissen der Nutzer, einschließlich der Leistungsfähigkeit und der Einschränkungen der Nutzer.

Sicherheitsmaßnahmen werden unter Berücksichtigung der Arbeitsumgebung, der Organisation und des Personalbestands, der Teams und der Kommunikation, der Gestaltung von Verfahren (einschließlich des Betriebs und der Instandhaltung der Sachanlage) und angemessener Ressourcen in Bezug auf die Sachanlage festgelegt, um sicherzustellen, dass menschliche und organisatorische Faktoren berücksichtigt werden und ihnen angemessen Rechnung getragen wird. Dies kann Spezifikationen z. B. in Bezug auf die Gestaltung des Arbeitsplatzes, die ergonomische Gestaltung der Ausrüstung (Werkzeuge, Maschinen, Materialien), die Nutzbarkeit der Ausrüstung, die erwarteten Rückmeldungen, die Qualität der Ausrüstung, den Inspektions-/Instandhaltungsplan und die Fehlertoleranz umfassen.

5.2.4 Nachweise

- *Informationen hinsichtlich des Sachanlagenmanagements innerhalb des Sicherheitsmanagementsystems der Organisation, einschließlich relevanter Verknüpfungen zu anderen Bereichen, wie der Risikobewertung, der Betriebsplanung, des Änderungsmanagements usw.* ***(5.2.1), (5.2.2), (5.2.5 Buchstaben a bis b)****:*

  Designphase

  - *Nachweis der Prozesse und Konsultation zur Bestimmung der Anforderungen an die Sachanlagen;*
  - *Nachweis von Risikomanagementstrategien in Bezug auf die Beschaffung und Inbetriebnahme von neuen oder modifizierten Sachanlagen;*
  - *Dokumentation aller relevanter Prozesse zur Gestaltung und Bereitstellung von Sachanlagen;*
  - *Prozesse zur Verwaltung von Risiken in der Designphase;*
  - *Nachweis der Werkzeuge zur Gewährleistung der Sicherheit;*
  - *Einzelheiten zu den Normen oder anderen Sicherheitsinformationen, auf die sich die Gestaltung und Instandhaltung der Sachanlagen stützt, sowie alle Tests, die zur Bestätigung der Konformität verwendet werden;*
  - *Das Vorhandensein eines Handbuchs oder eines ähnlichen Dokuments, das die Prozesse für den Betrieb und die Instandhaltung von Sachanlagen und für die Beherrschung von Risiken in der Betriebs- und Instandhaltungsphase umfasst.*

  Implementierungsphase

  - *Nachweis von Sicherheitsrisikomanagement sowie Test- und Validierungsprozessen, die die Konstruktion/Fertigung und Inbetriebnahme der Anlage und deren Betriebsbereitschaft umfassen.*

Betrieb- und Instandhaltungsphase

- *Nachweis der fortlaufenden Konformität mit den Normen und Prozessen sowie Management der ermittelten Risiken;*
- *Instandhaltungspläne und -verfahren für Sachanlagen;*
- *Nachweis der Tätigkeiten der Organisation in Verbindung mit der Ermittlung und Beseitigung von Risiken;*
- *Nachweis der Prozesse, die für die Berichterstattung und das Management von Sicherheitsleistungsproblemen und Korrekturmaßnahmen verwendet werden;*
- *Nachweis für den Einsatz der laufenden Leistung im Vergleich zur prognostizierten strategischen Lebensdauer einer Sachanlage zur Nachverfolgung der Leistung und Planung von Verlängerungen;*
- *Prozesse zur Erkennung von Fehlern und Störungen und zur Durchführung von Korrekturmaßnahmen;*
- *Management von Notfallsituationen oder nicht routinemäßigen Situationen, die die Sicherheit der Sachanlage beeinträchtigen können;*
- *Nachweis der Berücksichtigung der Sachanlagenverwaltung bei meldepflichtigen Ereignissen und Beherrschung gemeinsamer Risiken an den Schnittstellen* ***(siehe ferner 3.1)****.*

Verlängerung, Außerbetriebnahme und Entsorgung

- *Nachweis von Prozessen zur Beherrschung von Risiken im Zusammenhang mit der Verlängerung, Außerbetriebnahme oder Entsorgung von Sachanlagen, die je nach Umfang und Art der Organisation angemessen sind;*

- *Nachweis eines systematischen Ansatzes zum Umgang mit menschlichen und organisatorischen Faktoren in sämtlichen Lebenszyklusphasen der Sachanlagenverwaltung;* ***(5.2.1)***
- *Nachweis der Übereinstimmung der Betriebsdokumentation mit den Anforderungen an das Management (Betrieb) und die Instandhaltung an organisatorischen und physischen Grenzen, z. B. organisatorische, technische und betriebliche Schnittstellen zu benachbarten Infrastrukturen, Grenzbahnhöfen, Interaktionen mit anderen Eisenbahnunternehmen oder Infrastrukturbetreibern;* ***(5.2.3)***
- *Informationen, aus denen hervorgeht, dass der Antragsteller nachweist, dass seine Instandhaltungsvorkehrungen mit den einschlägigen Anforderungen (Rechtsvorschriften, Normen usw.) übereinstimmen;* ***(5.2.3)***
- *Bei Fahrzeugen eine Kopie des ECM-Zertifikats (das im Besitz des Eisenbahnunternehmens oder einer Stelle sein könnte, die im Auftrag des Eisenbahnunternehmens die Instandhaltung des Fahrzeugs durchführt, oder es könnte sogar in Bezug auf Instandhaltungsfunktionen eine Auslagerung vorliegen) oder (bis zum 16. Juni 2022) der Nachweis, dass Artikel 14 Absätze 2 und 3 und Anhang III der Richtlinie (EU) 2016/798 von der für die Instandhaltung verantwortlichen Stelle eingehalten wird;* ***(5.2.4 Buchstaben a bis d)***

  Im Falle von Partnerschaften zwischen Eisenbahnunternehmen, bei denen das Fahrzeug vom Partner gewartet wird:
  Nachweis, dass zwischen den Partnern vertragliche Vereinbarungen gelten, einschließlich:
  - *Informationsaustausch nach Artikel 5 der Verordnung (EU) 2019/779;*
  - *Ggf. technischer Support, insbesondere für CCS-Altsysteme;*
  - *Kontrolle der Fähigkeit unter Vertrag genommener Instandhaltungswerkstätten, Instandhaltungsarbeiten bereitzustellen;*
  - *Überwachung von Fahrzeugen und Austausch relevanter Informationen, der sich aus dieser Überwachung ergibt;* ***(siehe ferner 6.1)***
- *Im Fall von Sachanlagen, für die nach EU-Recht oder nationalen Vorschriften eine Konformitätsbescheinigung erforderlich ist, ist eine Kopie dieser Bescheinigung mit einer Erläuterung*

des Umfangs, in dem sie als Teil des Sicherheitsmanagementsystems verwendet wird, erforderlich; ***(5.2.4 Buchstaben a bis d)***

- *Informationen über die Funktionsweise des Dokumentverwaltungsteils des Sicherheitsmanagementsystems im Zusammenhang mit der Sachanlagenverwaltung, einschließlich des Nachweises, dass die Instandhaltungsdokumentation (Verfahren, Arbeitsanweisungen usw.) aktualisiert wird, wann und wo dies erforderlich ist;* ***(5.2.5 Buchstaben a bis c)***
- *Nachweis für das Konfigurationsmanagement der Sachanlagen in ihrem gesamten Lebenszyklus, einschließlich vorhandener Änderungsmanagementprozesse zum Umgang mit Basis-Neukonfigurationen.* ***(5.2.5 Buchstabe c)***

5.2.5 Beispiele für Nachweise

Designphase

Die Organisationsdokumente aller relevanten sicherheitstechnischen Prozesse und Informationen hinsichtlich der Gestaltung und Lieferung von Sachanlagen durch den Einsatz von Konfigurationsmanagementprozessen (oder eines Konfigurationsmanagementsystems). Diese legen die technischen und organisatorischen Tätigkeiten fest, welche die Kontrolle der Sachanlagen über ihren gesamten Lebenszyklus hinweg etablieren und aufrechterhalten.

Die Organisation etabliert und dokumentiert einen Prozess für die Beherrschung der Risiken in Verbindung mit der Gestaltung der Sachanlagenlösung durch:

- *die Bestimmung von Anforderungen für neue und/oder modifizierte Sachanlagen* ***(siehe ferner 1)*** *und die Besprechung dieser mit relevanten Interessengruppen* ***(siehe ferner 2.4)****;*
- *die Beherrschung der Risiken in Verbindung mit der Umsetzung solcher Änderungen* ***(siehe ferner 3.1);*** *und*
- *die Beherrschung der Risiken in Verbindung mit der Beschaffung von Sachanlagen und, wo relevant, dem Vertragsmanagement* ***(siehe ferner 3.1 und 5.3)****.*

Dazu gehören auch Gefahren-/Sicherheitsanalysen zur Identifizierung der am stärksten gefährdeten Bereiche, die anhand des Gefahrenprotokolls der Organisation überprüft werden. Dies kann durch die Identifizierung sicherheitskritischer Systeme und die Festlegung wichtiger Leistungsziele durch den Einsatz geeigneter Techniken zur Risikoidentifizierung erreicht werden, wie z. B.:

- *Analyse der Zuverlässigkeit, Verfügbarkeit, Wartbarkeit und Sicherheit (RAMS) der Gestaltung von Sachanlagen (bei der den Konstrukteuren die wichtigsten Leistungskriterien für die Sicherheit mitgeteilt werden, um sicherzustellen, dass die Sachanlage für einen bestimmten Zweck geeignet ist); und*
- *Ausfalleffekt- und Ausfallkritizitätsanalyse (FMECA-Analyse) und/oder zuverlässigkeitsorientierte Instandhaltung (RCM) zur Beherrschung von Risiken während der Designphase und zur Unterstützung der Festlegung eines Instandhaltungsplans.*

Diese Anforderungen werden im Vergleich zu den spezifischen Standards und Prozessen zur Gestaltung, Instandhaltung und zum Betrieb der Eisenbahninfrastruktur und der Schienenfahrzeuge wie durch die Organisation identifiziert verwaltet. Die Organisation weist nach, dass:

- *sicherheitskritische Systeme nach funktionalen Spezifikationen entworfen werden;*
- *es einen Validierungs- und Inbetriebnahmeprüfungsplan gibt, der bestätigt, dass die Sachanlage für einen bestimmten Zweck geeignet ist und sicher betrieben und gewartet werden kann; und*
- *die Betriebs- und Instandhaltungsdokumentation vorbereitet wurde, die Prozesse zur Aktualisierung, Überprüfung und Instandhaltung von Sachanlagen aufführt* ***(siehe ferner 4.5)****.*

Die Organisation demonstriert, dass sie in ihrem Entwurfs- und Beschaffungsansatz geeignete systemtechnische Prozesse und Sicherheitsverfahren (z. B. EN50126/8/9 für komplexe Systeme) einsetzt. Dies kann durch die Erstellung eines „Plans zur Verwaltung der Systemtechnik“ (SEMP, en: Systems Engineering Management Plan) erzielt werden, der das Verfahren zur Identifikation und Aufzeichnung von Interessengruppen, Systemanforderungen und Sicherheitsbedürfnissen spezifizieren würde.

Implementierungsphase

Um die erfolgreiche und sichere Implementierung der Sachanlage zu gewährleisten, legt die Organisation Prozesse fest, um die Risiken, die mit ihrer Konstruktion, Prüfung und Inbetriebnahme verbunden sind, in Übereinstimmung mit den Prozessen des Sicherheitsmanagementsystems zu beherrschen.

Sie implementiert außerdem einen Prozess zur Verwaltung folgender Punkte:

- *der Prüfung, Verifizierung und Validierung der System- und Sicherheitsanforderungen der Sachanlage, die mithilfe eines „Plans zur Verwaltung der Prüfung und Inbetriebnahme“ oder einem ähnlichen Dokument erzielt werden können; und*
- *der Betriebsbereitschaft der Sachanlage, die anhand einer Prüfliste für die Betriebsbereitschaft erzielt werden kann.*

Betrieb- und Instandhaltungsphase

Die Organisation hat eine Betriebs- und Instandhaltungsdokumentation für Sachanlagen entwickelt, welche die Sicherheitsmanagementprozesse zur Aktualisierung, Prüfung und Instandhaltung ihrer Sachanlagen festlegt. Sie beschreibt den Anwendungsbereich des Betriebs und ggf. die vorhandenen Risikomanagementstrategien zur Abdeckung sämtlicher relevanter Tätigkeiten.

Diese Dokumentation:

- *gewährleistet, dass die Sachanlage in Übereinstimmung mit dem Design der Sachanlage betrieben und gewartet wird;*
- *identifiziert und integriert sämtliche sicherheitsrelevanten Bedingungen, die festlegen, wie die Verwendung der Sachanlage eingeschränkt werden kann, sowie die vorhandenen Bedingungen für ihre Verwendung; und*
- *spezifiziert die durchzuführenden fortlaufenden Prüfungen.*

Der Prozess zur Konfiguration der Gestaltung und Lieferung vorgeschlagener Sachanlagen (in der Designphase beschrieben) wird erweitert, um ihren gesamten Lebenszyklus durch Folgendes abzudecken:

- *Festlegung und Pflege der Aufzeichnungen aller Sachanlagen durch die Erstellung eines Sachanlagenregisters. Dieses enthält Informationen wie die einzigartige Identifikation der Sachanlagen, ihren Standort, durchgeführte Instandhaltungen usw.;*
- *Verwaltung von Dokumenten und Informationen über die Sachanlagen in Übereinstimmung mit dem Sicherheitsmanagementsystem der Organisation **(siehe ferner 4.4 und 4.5)**; und*
- *Festlegung der Kritikalität der Sachanlagen, basierend auf den Ergebnissen der Sicherheitsrisikobewertung. Es werden sicherheitskritische Sachanlagen im Sachanlagenregister identifiziert.*

Die Organisation zeigt, wie Informationen über Sachanlagen entwickelt, gepflegt und in ihr Gefahrenprotokoll integriert werden.

Die Organisation überwacht die laufende Einhaltung der von ihr festgelegten Normen und Prozesse, um sicherzustellen, dass ihr Eisenbahnbetrieb auch weiterhin sicher und effizient funktioniert. Zu diesem Zweck legt die Organisation Prozesse fest, um zu gewährleisten, dass:

- *Sachanlagen in Übereinstimmung mit den relevanten Handbüchern betrieben und gewartet werden;*
- *der Zustand der Sachanlagen überwacht wird;*

- *die Ausrüstung zur Prüfung oder Untersuchung von Sachanlagen ordnungsgemäß kontrolliert, kalibriert und gewartet wird;*
- *Risiken in Verbindung mit dem Betrieb und der Instandhaltung der Sachanlagen in Übereinstimmung mit den Risikomanagementprozessen und allen Gesetzen zur Gesundheit und Sicherheit am Arbeitsplatz verwaltet werden; und*
- *besonders für sicherheitskritische Sachanlagen Ersatzteile für die Instandhaltung verfügbar sind. Dies könnte dadurch erreicht werden, dass der Ersatzteilbedarf für die Sachanlagen auf der Grundlage der Kritikalitätskriterien ermittelt wird, die durch den Einsatz der zuverlässigkeitsorientierten Instandhaltung identifiziert werden.*

Die Organisation weist die Planung der Instandhaltung der Sachanlagen nach, um:

- *den Anforderungen bezüglich Kompetenz, Kapazität und Ressourcen Rechnung zu tragen;*
- *die Informationsverwaltung und die Aufbewahrung von Aufzeichnungen sicherzustellen;*
- *detaillierte Pläne zu liefern, die im Rahmen eines risikobasierten Prozesses erstellt wurden und die die verschiedenen Instandhaltungsebenen definieren sowie etablierte Organisationsstrukturen, Verfahren und Verantwortlichkeiten für die Instandhaltung von Sachanlagen festlegen; und*
- *die Kalibrierung der Werkzeuge und Ausrüstungen, die bei der Instandhaltung verwendet werden, zu gewährleisten.*

Dies kann insbesondere Folgendes umfassen:

- *Einen „technischen Instandhaltungsplan“ (TMP, en: Technical Maintenance Plan); und*
- *Arbeitsanweisungen, die auf der Grundlage des technischen Instandhaltungsplans entwickelt und anhand diesem geprüft wurden.*

Die Planung wird durch die Verwendung eines Computerwartungsmanagementsystems dokumentiert und kontrolliert **(siehe ferner 4.5)**.

Die Organisation verfügt über Prozesse, die sicherstellen, dass:

- *wenn ein Fahrzeug oder eine Ausrüstung einer Aufgabe zugewiesen wird:*
  - *die Konformität mit der auszuführenden Aufgabe/Mission (z. B. technische Kompatibilität jedes Schienenfahrzeugtyps mit den Strecken) bei der Dienstplanung und vor der Abfahrt geprüft wird;*
  - *die Instandhaltung mindestens der sicherheitskritischen Komponenten gemäß dem Plan durchgeführt wird (vorbeugende Instandhaltung mit der Häufigkeit und Art der Eingriffe);*
  - *Instandhaltungseingriffe definiert werden, wenn Defekte festgestellt werden oder wenn sie ihre sicheren Einsatzgrenzen (korrektive Instandhaltung) überschreiten, außer es werden Betriebsbeschränkungen umgesetzt;*
  - *so bald wie möglich notwendige Maßnahmen im Anschluss an die Feststellung des Änderungsbedarfs ergriffen werden, wie beispielsweise Außerbetriebnahme oder die Festlegung von Betriebsbeschränkungen.*
- *Arbeitsanweisungen für alle sicherheitskritischen Tätigkeiten verfügbar sind;*
- *alle Aufgaben zu Konformitätszwecken abgezeichnet werden;*
- *die Dokumentation über die durchgeführte Instandhaltung kontrolliert wird **(siehe ferner 4.5)**; und*
- *kompetenzbasierte Schulungen zu allen sicherheitskritischen Systemen verfügbar sind **(siehe ferner 4.1)**.*

Es ist ein Prozess/Verfahren vorhanden, um sicherzustellen, dass vorübergehende oder dauerhafte Betriebsbeschränkungen (z. B. aufgrund eines bestimmten Fahrzeugtyps oder bestimmter Strecken)

- *berücksichtigt werden, wenn das Fahrzeug oder eine Ausrüstung einer Aufgabe/Mission zugewiesen wird;*
- *zeitnah an Mitarbeiter, die das Fahrzeug oder die Ausrüstung bedienen (z. B. Triebfahrzeugführer, Zugmanager), kommuniziert werden.*

Die Organisation weist nach, dass sie:

- *die Leistung ihrer sicherheitskritischen Sachanlagen versteht, indem sie identifiziert, was überwacht, gemessen und berichtet werden muss;*
- *die Methode und die Häufigkeit der Überwachung, Messung, Analyse und Beurteilung der Leistung sicherheitskritischer Sachanlagen festlegt und aufzeichnet;*
- *die laufende Leistung hinsichtlich der prognostizierten strategischen Lebensdauer einer Sachanlage überwacht **(siehe ferner 6.1)**;*
- *Leistungsprobleme basierend auf dem Sicherheitsrisikoniveau meldet und Sicherheitsleistungsprobleme eskaliert, sodass ihnen angemessen Rechnung getragen wird;*
- *die Ergebnisse der Überwachung nutzt, um den Instandhaltungsplan gegebenenfalls anzupassen;*
- *Kanäle zur Mitteilung sämtlicher Ergebnisse festlegt **(siehe ferner 4.4)**;*
- *die Konformität der sicherheitskritischen Sachanlagen mit Normen verbessert, indem sie:*
  - *Betriebs- und Instandhaltungskontrollen überprüft und die Risiken der Sachanlagen, die nicht den vorbestimmten Normen entsprechen, bewertet;*
  - *die Ursache(n) der Sicherheitsleistungsprobleme ermittelt; und*
  - *Maßnahmen, die zur Wiederherstellung des sicheren Betriebszustands einer Sachanlage benötigt werden könnten, identifiziert;*
- *das Sicherheitsmanagementsystem kontinuierlich verbessert, indem sie potenzielle Risiken identifiziert und Korrekturmaßnahmen ergreift **(siehe ferner 7.2)**; und*
- *dokumentiert, wo Gelegenheiten ergriffen wurden, um Risiken zu reduzieren oder zu beseitigen, und wie dies erreicht wurde.*

Die Organisation verfügt über Prozesse zur Identifizierung von Fehlern oder Ausfällen, die bei ihren Sachanlagen auftreten könnten, und zur Gewährleistung, dass die angemessenen Korrekturmaßnahmen ergriffen werden. Diese stimmen mit den Bestimmungen und Instandhaltungsprogrammen oder -plänen überein und:

- *gewährleisten die angemessene Aufzeichnung von Ausfällen und den sich daraus ergebenden Korrekturmaßnahmen;*
- *beschäftigen sich mit sicherheitskritischen Ausfällen;*
- *gewährleisten die angemessene Berichterstattung meldepflichtiger Ereignisse; und*
- *koordinieren nicht geplante Reparaturen für sicherheitsrelevante Sachanlagen.*

Die Organisation:

- *dokumentiert den Ausfallmanagementprozess;*
- *nutzt angemessene Analysetechniken für sicherheitskritische Funktionen, wie z. B. die „Ursachenanalyse“ (RCA, Englisch: Root Cause Analysis);*
- *implementiert eine Aufzeichnung von Ausfällen; dies kann Fehlercodes, Fehlermodi, Auswirkungen, Kritikalität und Korrekturmaßnahmen umfassen;*
- *entwickelt Verfahren zur Verwaltung allgemeiner Reparaturarbeiten; und*
- *führt einen Rückmeldeprozess für die Ingenieur- oder technischen Teams ein, um Systeme zu überprüfen und zu verbessern und das Risiko zukünftiger Ausfälle zu minimieren.*

Dies wird durch den Einsatz von Fehlermeldungen, Analysen und Korrekturmaßnahmen (FRACAS, Englisch: fault reporting, analysis, and corrective actions) erreicht, wodurch:

- *Störungen erfasst werden, die während der Prüfung und Inbetriebnahme erkannt und aufgezeichnet wurden, sowie Störungen, die während des Betriebs oder der Instandhaltung aufgetreten sind; und*
- *nachfolgende Korrekturmaßnahmen zu deren Behebung verwaltet werden.*

Die Organisation dokumentiert alle Störungen und Korrekturmaßnahmen und erfordert eine technisch kompetente Person zur Prüfung nicht geplanter Reparaturen.

Es gibt einen Prozess/ein Verfahren, der bzw. das Management von gestörtem Betrieb oder Notfallsituationen bei Sachanlagen regelt.

Die Organisation hat Prozesse zur Beherrschung von Schnittstellenrisiken festgelegt, die während des Betriebs oder der Instandhaltung ihrer Sachanlagen auftreten **(siehe ferner 3.1.1)**. Dies umfasst Schnittstellen zwischen Sachanlagen und zwischen den Akteuren, die diese verwenden.

Verlängerungs-, Außerbetriebnahme- und Entsorgungsphase

Die Organisation versteht den Zustand ihrer Sachanlagen und reagiert entsprechend, wenn diese verfallen, indem sie sie ersetzt oder wartet.

Die Organisation hat einen Validierungs- und Inbetriebnahmeprüfungsplan erstellt, um zu bestätigen, dass eine neue Sachanlage für ihren Zweck geeignet ist und sicher betrieben und gewartet werden kann. Wenn die Organisation die Lebensdauer einer vorhandenen Sachanlage verlängert, sucht sie nach entsprechenden Sicherheitsinformationen wie historischen Daten, um sicherzustellen, dass sie betriebssicher bleibt.

Es erfolgt eine Überwachung der Trends anhand der erwarteten Leistung (siehe Betriebs- und Instandhaltungsphase).

Wenn Eisenbahninfrastrukturen oder Schienenfahrzeuge entsorgt werden, beherrscht die Organisation die Risiken im Zusammenhang mit der Außerbetriebnahme der Sachanlage auf angemessene Weise.

Verwaltung der Änderungen an sicherheitskritischen Sachanlagen

In Situationen, in denen die Organisation versucht, die Konfigurationsbasislinie von sicherheitskritischen Sachanlagen zu ändern, implementiert sie einen Änderungsmanagementprozess, um eine effektive Beherrschung von Sicherheitsrisiken zu gewährleisten, indem sie Konfigurationsbasislinien für alle sicherheitskritischen Sachanlagen mit zugehöriger Software erstellt (unabhängig davon, ob diese in bestehende Systeme oder eigenständige Programme eingebettet ist). Wenn ein Betreiber die Konfigurationsbasislinie sicherheitskritischer Sachanlagen ändert, führt er, wo möglich, Folgendes durch:

- *Beherrschung der Risiken durch Änderungen an diesen Sachanlagen;*
- *Nachverfolgung der Serien- und Modellnummern;*
- *Validierung der Funktionsanforderungen im Vergleich zu Spezifikationen und Risikokontrollmaßnahmen;*
- *Kontrolle der Freigabe von Konfigurationsartikeln; und*
- *Gewährleistung, dass der Status von Sachanlagen unter dem Konfigurationsmanagement aktuell ist.*

Änderungen der Organisation an den festgelegten Basislinien, Betriebsbedingungen oder dem Instandhaltungsplan der sicherheitskritischen Sachanlagen beeinträchtigen in keiner Weise die Sicherheit des Eisenbahnbetriebs.

Anwendung gängiger Sicherheitsmethoden

Es existiert ein Prozess/ein Verfahren zur Überwachung, dass die für die Instandhaltung verantwortlichen Stellen (z. B. ECM) die Anwendung der CSM für die Evaluierung und Bewertung von Risiken und die CSM für die Kontrolle, soweit anwendbar (d. h. entweder gesetzlich und/oder vertraglich vorgeschrieben), zur Überwachung verwenden.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Das Risikoregister der Organisation, das Sicherheitsrisiken im Zusammenhang mit allen Phasen des Lebenszyklus der Verwaltung der Sachanlagen enthält und die den menschlichen und organisatorischen Faktoren zugrunde liegenden Ursachen für jedes Risikoszenario in Verbindung mit dem Lebenszyklusmanagement von Sachanlagen ermittelt.

Das Programm der Organisation gibt einen Rahmen vor, in dem festgelegt wird, wie identifizierte menschliche und organisatorische Risiken überprüft, abgestimmt und weiterentwickelt werden, um Lösungen während des gesamten Design- oder Änderungsmanagementprozesses zu erreichen. Das Programm spezifiziert die Beziehung mit anderen Parteien in Bezug auf die Design- oder Änderungstätigkeit.

Zum Beispiel:

- *Endnutzer sind Teil der Bedarfsanalyse; dies kann Aufgabenanalysen und Befragungen umfassen, wobei einige Vertreter der Mitarbeiter von der Design- bis zur Testphase beteiligt werden.*
- *Es gibt Verfahren und spezielle Mittel, um eine klare Kommunikation zwischen den Betriebs- und Instandhaltungsteams sowie mit der/den für die Instandhaltung zuständigen Stelle(n) zu gewährleisten.*
- *Endnutzer sind zudem an den Änderungsmanagementprozessen, einschließlich Automatisierung, beteiligt. Die Mitarbeiter können dem Projektteam Rückmeldungen geben. Diese Rückmeldungen werden analysiert und Verbesserungsmaßnahmen ergriffen. Aus den Sitzungsprotokollen und den Berichten über das Änderungsmanagement geht klar hervor, wie sich die Mitarbeiter engagieren und wie ihre Bedenken berücksichtigt werden.*
- *Alle betroffenen Nutzer werden im Rahmen der Risikobewertung identifiziert, und sie erhalten im Rahmen des Kompetenzmanagementsystems Schulungen, um die Qualifizierung der Mitarbeiter zu gewährleisten.*
- *Hersteller und Zulieferer sind in den Prozess des Design- und Änderungsmanagements eingebunden, um eine angemessene Berücksichtigung menschlicher Faktoren zu gewährleisten.*

Informationen über die Anwendung des Safety Alert Information Tool (SAIT) werden zur Verfügung gestellt **(siehe 5.4.3)**.

5.2.6 Referenzen und Standards

- *ECM-Leitlinien*
- *ERA Clarification note on safe integration (Erläuternder Vermerk der ERA zur sicheren Integration)*
- *CENELEC - EN 50126 Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Grundlegende Anforderungen und genereller Prozess*
- *Office of the National Rail Safety Regulator - Asset management guideline (2019)*
- *ISO 55000:2014 Asset Management – Übersicht, Leitlinien und Begriffe*
- *ISO 55001:2014 Asset Management – Managementsysteme – Anforderungen*

5.2.7 Aufsichtsaspekte

Im Hinblick auf die Aufsicht ist es wichtig, dass der Schwerpunkt auf der Verwaltung der Sachanlage über ihren Lebenszyklus hinweg, von der Gestaltung bis hin zur Entsorgung, liegt und nicht auf einzelnen Störungen bei der Verwaltung der Sachanlage, es sei denn, diese haben unmittelbare Auswirkungen auf die Sicherheit.

Bei der Aufsicht sollte berücksichtigt werden, wie bestehende Sachanlagen, die vor den aktuellen Normen vorhanden waren, verwaltet und gewartet werden.

Bei der Aufsicht sollte berücksichtigt werden, ob und wie die Organisation das SAIT verwendet.

5.3 Auftragnehmer, Partner und Zulieferer

5.3.1 Regulatorische Anforderung

5.3.1. Die Organisation muss die mit ausgelagerten Tätigkeiten verbundenen Sicherheitsrisiken ermitteln und beherrschen; dies schließt auch Tätigkeiten oder die Zusammenarbeit mit Auftragnehmern, Partnern und Lieferanten ein.

5.3.2. Zur Beherrschung der unter 5.3.1 genannten Sicherheitsrisiken muss die Organisation die Kriterien für die Auswahl der Auftragnehmer, Partner und Zulieferer sowie die von ihnen zu erfüllenden Vertragsbedingungen festlegen, darunter

(a) die rechtlichen und sonstigen Bedingungen in Bezug auf die Sicherheit (siehe 1. Kontext der Organisation);

(b) das für die vertraglichen Aufgaben erforderliche Kompetenzniveau (siehe 4.2 Kompetenz);

(c) die Zuständigkeit für die zu erbringenden Leistungen;

(d) die erwartete Sicherheitsleistung, die während der Vertragsdauer aufrechterhalten werden muss;

(e) die Verpflichtungen bezüglich des Austauschs sicherheitsrelevanter Informationen (siehe 4.4 Information und Kommunikation);

(f) die Rückverfolgbarkeit sicherheitsrelevanter Dokumente (siehe 4.5 Dokumentierte Informationen).

5.3.3. Entsprechend dem Prozess gemäß Artikel 3 der Verordnung (EU) Nr. 1078/2012 muss die Organisation Folgendes überwachen:

(a) die Sicherheitsleistung sämtlicher Tätigkeiten und Abläufe der Auftragnehmer, Partner und Zulieferer, um sicherzustellen, dass sie den Anforderungen des Vertrags entsprechen;

(b) das Bewusstsein der Auftragnehmer, Partner und Zulieferer für die von ihnen ausgehenden Sicherheitsrisiken für den Betrieb der Organisation.

5.3.2 Zweck

Der Antragsteller muss nachweisen, dass er in der Lage ist, Risiken zu identifizieren, zu bewerten und zu kontrollieren, die sich aus den Tätigkeiten von Auftragnehmern und anderen Lieferanten ergeben, mit denen er in einer Arbeitsbeziehung steht. Dies ist nicht nur eine Frage der Risikobewertung und erfordert auch keine Auflistung aller Risiken oder Kategorien relevanter Risiken, sondern verlangt vom Antragsteller, dass er darlegt, wie seine Systeme und Verfahren insgesamt konzipiert und organisiert sind, um die Identifizierung, Bewertung und Kontrolle dieser Risiken zu erleichtern. Dazu zählt auch die Notwendigkeit, im Vertrag festzulegen, wie sicherheitstechnische Informationen ausgetauscht werden. Der Einsatz von gut formulierten Verträgen ist eine allgemein akzeptierte Methode zur Risikobeherrschung. Die Hauptverantwortung für die Verwaltung der Auftragnehmer und die Kontrolle ihrer Lieferung anhand der festgelegten Spezifikationen liegt jedoch bei der Organisation. Der Einsatz von (Unter-)Auftragnehmern bedeutet nicht, dass das Eisenbahnunternehmen/der Infrastrukturbetreiber seine Verantwortlichkeiten delegiert, um sicherzustellen, dass die vertraglich vereinbarten Leistungen gemäß den vor dem Betrieb festgelegten Standards erbracht werden.

Der Antragsteller sollte nachweisen, dass er über Prozesse verfügt, um die Kompetenz von Auftragnehmern und anderen Lieferanten zu ermitteln und deren Sicherheitsleistung im Rahmen seines Beschaffungsprozesses zu bewerten.

Jede Organisation ist dafür verantwortlich, den in den CSM für die Kontrolle festgelegten Überwachungsprozess durchzuführen und durch vertragliche Vereinbarungen sicherzustellen, dass auch die von ihren Auftragnehmern durchgeführten Risikokontrollmaßnahmen in Übereinstimmung mit den CSM überwacht werden. Wenn Organisationen relevante Sicherheitsrisiken bezüglich Defekten oder Störungen der technischen Ausrüstung feststellen, sind sie gemäß den CSM für die Kontrolle dazu verpflichtet, diese Risiken den anderen beteiligten Parteien zu melden, damit diese erforderliche Korrekturmaßnahmen ergreifen können, um die Sicherheit des Systems zu gewährleisten.

5.3.3 Erläuterungen

Weitere Informationen zu vertraglichen Vereinbarungen und Partnerschaften sind Anhang 3 zu entnehmen.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Zu den vom Unternehmen festgelegten Verfahren zur Beherrschung seiner Risiken gehören die Tätigkeiten von Auftragnehmern, Partnern und Zulieferern. Die vom Unternehmen festgelegten Risiken und Sicherheitsmaßnahmen werden den Auftragnehmern, Zulieferern und Partnern mitgeteilt und in die Spezifikationen für jede ausgelagerte Tätigkeit aufgenommen. Dies kann auch die Überwachung der Durchführung der ausgelagerten Tätigkeit umfassen (siehe Abschnitt ***6.1 Überwachung***).

Die Strategie für menschliche und organisatorische Faktoren kann sich auf relevante Fragen erstrecken, die Auftragnehmer, Partner und Zulieferer betreffen.

Die Aufgaben, Zuständigkeiten und Kompetenzen, die für die Ausführung der ausgelagerten Tätigkeiten erforderlich sind, sind in den Verträgen klar festgelegt. Diese Kompetenzen entsprechen den Kompetenzen, die im Kompetenzmanagementsystem für interne Mitarbeiter beschrieben sind.

Die Verträge enthalten Bestimmungen darüber, wie Sicherheitsinformationen und Sicherheitskommunikation geregelt werden, um das gleiche Sicherheitsniveau wie für interne Informationen und Kommunikation zu gewährleisten. Dies schließt auch den Wissensaustausch ein.

5.3.4 Nachweise

- *Nachweis der Art, wie das Sicherheitsmanagementsystem der Organisation mit den Managementsystemen der Auftragnehmer und Zulieferer verbunden ist, um Risiken zu kontrollieren;* ***(5.3.1)***
- *Nachweis, dass vertragliche Vereinbarungen auf der Grundlage der Ergebnisse der Risikobewertung entwickelt werden;* ***(5.3.1) (siehe ferner 3.1)***
- *Es gibt Prozesse, die festlegen, wie menschliche und organisatorische Faktoren behandelt und an Unterauftragnehmer und deren Management und kommuniziert werden sollen;* ***(5.3.1)***
- *Nachweis der Art, wie die Organisation die Dokumentation für Auftragnehmer und Zulieferer verwaltet;* ***(5.3.2 Buchstaben a bis d)***
- *Nachweis der Art, wie die Organisation Auftragnehmer und Zulieferer auswählt, um sicherzustellen, dass diese kompetent sind und dass Sicherheitsrisiken korrekt gehandhabt werden;* ***(5.3.2 Buchstaben a bis e)***
- *Der vorhandene Prozess zur Gewährleistung, dass wichtige Sicherheitsinformationen an Auftragnehmer und Zulieferer weitergegeben oder von ihnen gemeldet werden;* ***(5.3.2 Buchstabe d)***
- *Nachweis, wie das Dokumentenkontrollverfahren das Management sicherheitsrelevanter Dokumente gewährleistet, die für Auftragnehmer und Zulieferer relevant sind;* ***(5.3.2 Buchstabe f)***

- *Der/das von der Organisation eingeführte Prozess bzw. Verfahren, mit dem sichergestellt werden soll, dass Vertragspartner und Zulieferer, mit denen die in Organisation einer Arbeitsbeziehung steht, in der Lage sind, die Risiken, denen sie ausgesetzt sind, zu beherrschen;* ***(5.3.3 Buchstaben a bis b)***
- *Nachweis, dass Auftragnehmer, Partner oder Zulieferer regelmäßig gemäß den CSM für die Kontrolle (Verordnung (EU) Nr. 1078/2012) überwacht werden, um sicherzustellen, dass das Produkt oder die Dienstleistung bestimmten Anforderungen und Sicherheitszielen entspricht.* ***(5.3.3 Buchstabe a) (siehe ferner 6.1)***

5.3.5 Beispiele für Nachweise

Nachweis der Sicherheitsziele (oder Vorgaben), deren Erfüllung von den Auftragnehmern, Partnern und Zulieferern erwartet wird, und der Indikatoren, die zu deren Messung verwendet werden.

Das Dokumentenverwaltungsverfahren, das sich mit den von Auftragnehmern, Partnern und Zulieferern anzuwendenden Standards der Organisation befasst (siehe ferner 4.5.1.1 Buchstabe e Dokumentenmanagement).

Eine Liste/Übersicht über ihre Auftragnehmer, Partner und Lieferanten zum internen oder externen Gebrauch, mit einer genauen Angabe der von ihnen bereitgestellten Produkte und/oder Dienstleistungen **(siehe ferner 4.5.1.1 Buchstaben d und e)** und eine Angabe, welche Auswirkungen auf die Sicherheit es gibt, zusammen mit den Maßnahmen zur Kontrolle der ermittelten Risiken (z. B. Informationsaustausch, Klärung von Zuständigkeiten, Schulung) **(siehe ferner 3.1.1.1 Buchstabe a)**.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Der entsprechende Audit-/Inspektionsplanungsprozess für Auftragnehmer, Partner und Zuliefere mit einigen Beispielaufzeichnungen dieser Tätigkeiten, wie z. B. Audit-/Inspektionsberichte oder -ergebnisse sowie die zugehörigen Aktionspläne.

In der Strategie für menschliche und organisatorische Faktoren wird dargelegt, wie diese Fragen mit Auftragnehmern, Partnern und Zulieferern behandelt werden.

Ein Verfahren, anhand dessen Auftragnehmer, Partner und Zulieferer ausgewählt und überwacht werden. Das Verfahren macht deutlich, dass die von den Auftragnehmern anzuwendenden Standards dieselben sind wie die Standards für direkt angestellte Mitarbeiter und welche Rollen und Verantwortlichkeiten sie haben. Das Verfahren dokumentiert den erforderlichen Informationsaustausch zwischen den Sicherheitsmanagementsystemen an den Antragsteller und die Auftragnehmer, Partner und Lieferanten.

Das Verfahren des Kompetenzmanagementsystems, das mit dem Verfahren der Auftragnehmer, Partner und Zulieferer verknüpft ist.

Der Prozess/das Verfahren zur Verwaltung von Auftragnehmern, Partnern und Zulieferern, darunter auch die Frage, wie Schnittstellenrisiken, die sich aus der Tätigkeit von Auftragnehmern, Partnern oder Zulieferern ergeben, gesteuert und diesen mitgeteilt werden, wie diese in die vertraglichen Vereinbarungen einbezogen werden und wie der Informationsaustausch innerhalb des SMS integriert wird.

Der Prozess oder das Verfahren, mit dem die für die Vertragspartner, Partner oder Lieferanten geltenden einschlägigen Anforderungen ermittelt und ihnen mitgeteilt werden, und gegebenenfalls die Art und Weise, wie sie in vertragliche Vereinbarungen einbezogen werden, die im Rahmen des Dokumentenverwaltungssystems ordnungsgemäß dokumentiert sind, um die Rückverfolgbarkeit der Informationen zu gewährleisten.

Das Verfahren des Dokumentationsmanagementsystems für die Verwaltung der Bescheinigungen, Genehmigungen, Anerkennungen oder andere Arten von Nachweisen der Konformität mit den Anforderungen für Auftragnehmer, Partner oder Lieferanten, welches die Gültigkeit ihrer Validierung im Laufe der Zeit kontrolliert (z. B. durch Überwachungstätigkeiten).

5.3.6 Aufsichtsaspekte

Wenn eine Organisation beaufsichtigt wird, kann es möglicherweise notwendig sein, Aufsichtstätigkeiten bei einem für diese Organisation tätigen Auftragnehmer oder Lieferanten durchzuführen, um ein vollständiges Bild über das Ausmaß der Kontrolle und Überwachung zu erhalten. Es kann auch notwendig sein, auf die Dokumentation zuzugreifen, nach welcher der Auftragnehmer oder Lieferant arbeitet, und zu prüfen, inwiefern dies mit den im Sicherheitsmanagementsystem der Organisation festgelegten Verfahren zusammenhängt.

Vorkehrungen, um sicherzustellen, dass die Sicherheitsleistung von Auftragnehmern und Lieferanten sowie die Kompetenz ein integraler Bestandteil des Beschaffungsprozesses ist.

5.4 Änderungsmanagement

5.4.1 Regulatorische Anforderung

5.4.1. Zur Aufrechterhaltung oder Verbesserung der Sicherheitsleistung muss die Organisation Änderungen des Sicherheitsmanagementsystems vornehmen und kontrollieren. Dazu gehören auch Entscheidungen in den verschiedenen Phasen des Änderungsmanagements und die anschließende Überprüfung der Sicherheitsrisiken (siehe 3.1.1. Risikobewertung).

5.4.2 Zweck

Es ist wichtig, dass der Antragsteller in der Lage ist, neue Risiken, die sich bei seinem Betrieb ergeben können, zu erkennen und darauf zu reagieren, indem er gegebenenfalls die CSM für Evaluierung und Bewertung von Risiken ((EU) 402/2013) anwendet. Das Sicherheitsmanagementsystem sollte nachweisen, dass es über Verfahren zur Beurteilung dieser Risiken und gegebenenfalls zur Einführung neuer Risikokontrollmaßnahmen verfügt. Dies sollte allen Arten und Ebenen von Veränderungen gerecht werden – signifikant und geringfügig, dauerhaft und vorübergehend, unmittelbar und langfristig. Es sollte für Änderungen technischer, betrieblicher oder organisatorischer Art gelten.

5.4.3 Erläuterungen

Nicht alle Änderungen unterliegen einer Risikobewertung **(5.4.1)**. Werden Änderungen aktiv durch andere Prozesse im Sicherheitsmanagementsystem, wie z. B. das Tagesgeschäft, verwaltet, sollten sie nicht als eine Änderung angesehen werden, die ein Management im Rahmen des formalen Änderungsprozesses erfordert.

Zu definierende Rollen, Verantwortlichkeiten, Rechenschaftspflichten und Behörden **(siehe ferner 2.3)** umfassen das Änderungsmanagement **(5.4.1)**, z. B. die Zuweisung von Rollen zu einem Änderungskontrollausschuss.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Der Änderungsmanagementprozess ermöglicht es, Risiken verhältnismäßig und robust zu bewerten, gegebenenfalls unter Einbeziehung menschlicher und organisatorischer Faktoren, und angemessene Kontrollmaßnahmen zu ergreifen.

Mitarbeiter werden während des Änderungsmanagementprozesses hinzugezogen **(siehe ferner 2.4)**.

Sicherheitsrisiken aufgrund von Stellenabbau oder infolge der Auslagerung von Tätigkeiten, einschließlich des Betriebs oder der Zusammenarbeit mit Auftragnehmern, Partnern und Zulieferern, werden wie interne Risiken gesteuert und priorisiert.

5.4.4 Nachweise

- *Eine Beschreibung des Änderungsmanagementprozesses;* ***(5.4.1)***
- *Eine Beschreibung der angewendeten Verfahren und Methoden, um neue oder veränderte Risiken zu beurteilen und neue umzusetzen;* ***(5.4.1)***
- *Kontrollmaßnahmen, einschließlich Hinweise darauf, wo detaillierte Prozesse gefunden werden können;* ***(5.4.1)***
- *Informationen darüber, wie die Organisation wesentliche Änderungen feststellt und Entscheidungen darüber trifft, wann die Prozesse in den CSM für die Evaluierung und Bewertung von Risiken*

anzuwenden sind oder wann eine Risikobewertung im Rahmen der Verfahren des Sicherheitsmanagementsystems durchzuführen ist; ***(5.4.1)***

- *Informationen über die Vorkehrungen im Änderungsmanagement, welche die Organisation für die Verwaltung von Fahrzeugzulassungen und Änderungen der einheitlichen Sicherheitsbescheinigung oder Sicherheitsgenehmigung trifft;* ***(5.4.1)***
- *Informationen über den Prozess zur Benachrichtigung der zuständigen nationalen Sicherheitsbehörde bei Änderungen vor dem Start eines neuen Schienentransportbetriebs.* ***(5.4.1)***

5.4.5 Beispiele für Nachweise

Eine Kopie des Änderungsmanagementverfahrens als Teil des Antrags. Dieses Dokument deckt den Bedarf für die Risikobewertung aller Änderungen nach den unterschiedlichen gesetzlichen Bestimmungen ab. Ein Beispiel für ein Fehler- und Annahmenprotokoll, das regelmäßig überprüft wird, wenn die Änderung fortschreitet, wird bereitgestellt. Schließlich deckt das Verfahren auch den Prozess ab, mit dem relevante nationale Sicherheitsbehörden über Änderungen informiert werden.

Der Änderungsmanagementprozess bezieht sich auf die Anwendung des Risikobewertungsprozesses, und die Ergebnisse werden bei der Entwicklung, Umsetzung und Überprüfung der betrieblichen Prozesse berücksichtigt.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Änderungen von Aufgaben, Zuständigkeiten, Werkzeugen und Ausrüstung, Arbeitsumgebungen, Prozessen und Verfahren werden durch eine Analyse menschlicher und organisatorischer Faktoren untermauert, bei der mögliche Sicherheitsrisiken im Zusammenhang mit dem Wandel ermittelt werden. Zu den verwendeten Methoden gehören z. B. Aufgabenanalyse, Verwendbarkeitsanalyse, Simulation, Risikobewertung, HAZOP und Erhebung über die Sicherheit. Es gibt Beispiele für Änderungen, denen eine Risikobewertung unter Anwendung eines Ansatzes für menschliche und organisatorische Faktoren vorausgeht. Dies gilt insbesondere für Änderungen der Arbeitsverfahren aufgrund geänderter Ausrüstung, Änderungen der Arbeitspläne oder Neuzuweisung von Zuständigkeiten.

Bei Beispielen von Projekten, die zeigen, wie menschliche und organisatorische Faktoren bei der Bewältigung des Wandels von Beginn an durch die Analyse der Bedürfnisse des Unternehmens berücksichtigt wurden: technische Änderungen wie neue Ausrüstung(en) oder Modernisierungen, organisatorische oder betriebliche Änderungen mit erwarteten Auswirkungen auf die bestehende Situation usw., wodurch eine mangelhafte Gestaltung vermieden wird, die die Leistungsfähigkeit des Unternehmens beeinträchtigt hätte. Es liegen Sitzungsprotokolle vor, in denen die Auswirkungen der Änderung auf die Kultur der Organisation und die Art und Weise, wie dies dem Management mitgeteilt wurde, analysiert werden.

Die Aufgaben und Zuständigkeiten für die Bewältigung von Veränderungen und der damit verbundenen Sicherheitsrisiken sind ausreichend definiert, und das Kompetenzmanagementsystem zeigt, dass die Verantwortlichen geschult wurden, um menschliche und organisatorische Faktoren zu integrieren.

Das bei jedem Projekt erstellte Gefahrenprotokoll, in dem die den menschlichen und organisatorischen Faktoren zugrunde liegenden Ursachen für jedes sicherheitsrelevante Risikoszenario ermittelt werden. Das Gefahrenprotokoll erfasst auch die möglichen Auswirkungen auf Auftragnehmer, Partner und Zulieferer, die erforderlichenfalls beteiligt sind.

Projektrisikobewertungen, die in der Anfangsphase des Projekts durchgeführt werden und an denen die Endnutzer beteiligt sind. Die Risikobewertung wird als ein kontinuierlicher Prozess betrachtet, der laufende

Probleme während des Änderungsprozesses in Angriff nimmt (z. B. sich weiterentwickelnde Annahmen und Aktualisierung neuer ermittelter Risiken).

In Verwaltungsverfahren/-vereinbarungen zwischen verschiedenen Organisationen, Bereitstellung von Plänen und Projektdetails usw. für verschiedene Parteien. Gewerkschaften und andere Interessengruppen werden frühzeitig in den Prozess einbezogen, wenn es um wichtige Entscheidungen oder Änderungen geht.

Es werden dieselben Instrumente verwendet wie im Kapitel Risikobewertung, d. h. Aufgabenanalyse, Verwendbarkeitsanalyse, Simulation, Risikobewertung, HAZOP, Erhebung über die Sicherheit.

5.4.6 Aufsichtsaspekte

Um festzustellen, ob die Vorkehrungen des Änderungsmanagements im Sicherheitsmanagementsystem beständig genug sind, ist es notwendig, eine Reihe verschiedenartiger Änderungen über den definierten Prozess hinweg vorzunehmen, um zu prüfen, ob sie (a) angemessen verwaltet wurden und die sich aus Änderungen ergebenden Risiken richtig berücksichtigt wurden, und (b) ob gewonnene Erkenntnisse in die Überarbeitungen der Verfahren des Sicherheitsmanagementsystems aufgenommen wurden.

Die Bewertung der Konformität der Vorkehrungen des Änderungsmanagements mit den CSM für die Evaluierung und Bewertung von Risiken.

Die Organisation verfügt über Verfahren zur Umsetzung und fortlaufenden Überwachung der einschlägigen TSI, der nationalen Vorschriften und anderer Normen, gegebenenfalls unter Angabe der Art und Weise, wie diese während des gesamten Lebenszyklus einer Anlage oder eines Betriebs angewandt werden.

5.5 Notfallmanagement

5.5.1 Regulatorische Anforderung

5.5.1. Die Organisation muss die Notfälle und die damit verbundenen zeitgerechten Maßnahmen erfassen, die zu ihrer Beherrschung (siehe 3.1.1 Risikobewertung) und zur Wiederherstellung des Regelbetriebs gemäß der Verordnung (EU) 2015/995 ergriffen werden müssen.

5.5.2. Die Organisation muss für jede erfasste Art von Notfall sicherstellen, dass

(a) die Notfalldienste unverzüglich benachrichtigt werden können;

(b) den Notfalldiensten alle relevanten Informationen sowohl im Voraus, um Notfallmaßnahmen vorbereiten zu können, als auch zum Zeitpunkt des Notfalls zur Verfügung stehen;

(c) intern Erste Hilfe geleistet wird.

5.5.3. Die Organisation muss die Aufgaben und Zuständigkeiten aller Beteiligten im Einklang mit der Verordnung (EU) 2015/995 ermitteln und dokumentieren.

5.5.4. Die Organisation muss über Einsatz-, Alarm und Informationspläne für Notfälle mit Vorkehrungen verfügen, um

(a) das gesamte für das Notfallmanagement zuständige Personal zu alarmieren;

(b) allen Beteiligten (z. B. Infrastrukturbetreibern, Eisenbahnunternehmen, Auftragnehmern, Behörden, Notfalldiensten) Informationen zu übermitteln, einschließlich Notfallanweisungen für die Fahrgäste;

(c) je nach Art des Notfalls die notwendigen Entscheidungen zu treffen.

5.5.5. Die Organisation muss beschreiben, wie die Ressourcen und Mittel für das Notfallmanagement zugewiesen (siehe 4.1 Ressourcen) und der Schulungsbedarf ermittelt wurde (siehe 4.2 Kompetenz).

5.5.6. Die Notfallvorkehrungen werden regelmäßig in Zusammenarbeit mit anderen interessierten Parteien getestet und gegebenenfalls aktualisiert.

5.5.7. Die Organisation muss sicherstellen, dass das zuständige Personal, das über ausreichende Sprachkenntnisse verfügt, vom Infrastrukturbetreiber problemlos und unverzüglich kontaktiert werden kann und diesen mit angemessenen Informationen versorgt.

5.5.7. Die Organisation muss mit allen Eisenbahnunternehmen, die ihre Infrastruktur nutzen, mit den Notfalldiensten zur Erleichterung ihres schnellen Eingreifens sowie mit allen sonstigen Akteuren, die an einer Notsituation beteiligt sein könnten, Notfallpläne koordinieren.

5.5.8. Die Organisation muss über ein Verfahren verfügen, um in Notfällen die für die Instandhaltung zuständige Stelle oder den Schienenfahrzeughalter zu benachrichtigen.

5.5.8. Die Organisation muss über Vorkehrungen verfügen, um bei Bedarf den Betrieb und den Eisenbahnverkehr unverzüglich zu stoppen und alle Beteiligten über diese Maßnahme zu informieren.

5.5.9. Bei grenzüberschreitender Infrastruktur wird die erforderliche Koordinierung und Vorbereitung der zuständigen Notfalldienste beiderseits der Grenze durch die Zusammenarbeit zwischen den betroffenen Infrastrukturbetreibern erleichtert.

5.5.2 Zweck

Robuste Systeme für die Notfallplanung sind für jeden Diensthabenden unerlässlich und sollten die Informationen abdecken, die den Notfalldiensten zur Verfügung gestellt werden müssen, damit sie ihre Pläne für die Reaktion auf größere Störungen erstellen können. Wichtig sind auch die Aspekte des Sicherheitsmanagementsystems, die für die Notfallmaßnahmen unmittelbar relevant sind, wie z. B. die Schulung für Notfälle und die Erprobung von Notfallplänen.

5.5.3 Erläuterungen

Notfallsituationen **(5.5.1)** sind mit Ergebnissen der Risikobewertung der Organisation verbunden, obwohl TSI OPE (siehe Abschnitt 4.2.3.7) eine nicht erschöpfende Liste von Notfallsituationen bereitstellt.

Interne Leistung Erster Hilfe **(5.5.4 Buchstabe c)** bedeutet, dass das Unternehmen in der Lage ist, die Bereitstellung Erster Hilfe in den in Nummer 5.5.1 genannten Notfällen zu regeln.

In **Nummern 5.5.7 und 5.5.8** des vorstehenden Rechtstextes werden bei der Anforderung an Infrastrukturbetreiber die Bestimmungen in Schwarz durch die Bestimmungen in Blau ersetzt. Die vorstehende **Nummer 5.5.9** in Blau bezieht sich nur auf den Infrastrukturbetreiber.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Das Notfallmanagement ist mit Ressourcenmanagement, Aufgaben und Zuständigkeiten sowie mit dem Kompetenzmanagementsystem verknüpft, um die Sensibilisierung und Schulung der Mitarbeiter (einschließlich der Aufrechterhaltung der Kompetenz) sicherzustellen. Dazu gehört auch die Entwicklung von Kompetenzen (einschließlich überfachlicher Fähigkeiten wie Stressresistenz, Widerstandsfähigkeit usw.) für die mit den Notfallplänen und -verfahren befassten Akteure.

5.5.4 Nachweise

Vom Antragsteller wird erwartet, eine Übersicht über Folgendes bereitzustellen:

- *Die Arten der abgedeckten Notfälle, einschließlich gestörten Betriebs und der Verfahren zu ihrer Bewältigung;* ***(5.5.1)***
- *Die vom Antragsteller übermittelten Informationen, die es den Rettungsdiensten ermöglichen, ihre Reaktion auf einen schweren Eisenbahnunfall zu planen, gegebenenfalls unter Bezugnahme auf Pflichten nach geltendem EU-Recht und einschlägige grenzüberschreitende Vereinbarungen;* ***(5.5.2 Buchstaben a und b)***
- *Es wird erwartet, dass die Unternehmen im Rahmen ihrer Risikobewertung ermitteln, welche Erste Hilfe sie selbst erbringen können und welche von den Notfalldiensten zu erbringen wäre;* ***(5.5.2 Buchstabe c).***
- *Pläne, Aufgaben und Zuständigkeiten (einschließlich derjenigen, die über bestimmte Fähigkeiten zur Unterstützung des Infrastrukturbetreibers verfügen oder umgekehrt), Schulungen und Vorkehrungen zur Aufrechterhaltung der Kompetenz sowie Vorkehrungen für eine wirksame Kommunikation mit den Notfalldiensten, zuständiges Personal sowie Kommunikation mit den von Störungen betroffenen Personen wie Passagieren oder betroffenen Dritten (dies sollte ein Dokument umfassen, in dem die Rollen und Zuständigkeiten aller Beteiligten, die Zuweisung von Ressourcen und Mitteln und die Ermittlung des Schulungsbedarfs festgelegt sind); die Verfahren zur Wiederaufnahme des normalen Betriebs nach einem Notfall;* ***(5.5.1), (5.5.3), (5.5.4 Buchstaben a bis c), (5.5.5), (5.5.7) (5.5.8 und 5.5.9 nur aus den regulatorischen Anforderungen des Infrastrukturbetreibers)***

- *Diese spezifischen Aspekte des Sicherheitsmanagementsystems, die direkt für die Notfallvereinbarungen relevant sind, z. B. Schulung für Notfälle und Erprobung von Notfallplänen, um Schwächen zu identifizieren;* ***(5.5.6)***
- *Das Verfahren, relevante für die Instandhaltung verantwortliche Stellen oder den Halter im Falle eines Notfalls, der eines seiner Fahrzeuge betrifft, zu kontaktieren.* ***(5.5.8 nur aus den regulatorischen Anforderungen des Eisenbahnunternehmens)***

5.5.5 Beispiele für Nachweise

Eine Kopie der Notfallmanagementverfahren und der zugehörigen Pläne (z. B. Wiederbelebungsmaßnahmen). Das Verfahren umfasst das gesamte betriebene Netz mit spezifischen Vorkehrungen, die für Tunnel und andere Orte mit hohem Risiko sowie für die grenzüberschreitende Zusammenarbeit, Personalausstattung, Rollen und Zuständigkeiten erforderlich sind, und schließt Verknüpfungen zu den Notfallregelungen des Infrastrukturbetreibers und gegebenenfalls zur Kontaktaufnahme mit anderen relevanten Parteien, wie z. B. der ECM, ein. Wenn in einem geografischen Tätigkeitsgebiet eines Eisenbahnunternehmens mehrere Infrastrukturbetreiber tätig sind, sollte das Eisenbahnunternehmen die Unterschiede zwischen den Notfallregelungen (und den Nutzervereinbarungen) bei diesen Infrastrukturbetreibern berücksichtigen.

Das Notfallverfahren umfasst den Prozess, bei dem die Opfer von Störungen und ihre Familienangehörigen in Bezug auf Beschwerdeverfahren beraten werden.

Das Verfahren (sofern relevant) enthält Informationen darüber, was in einer Notsituation passiert, in der gefährliche Güter beteiligt sind. Die Organisation (Eisenbahnunternehmen) verfügt über einen Prozess, der gewährleistet, dass:

- *der Belader, der Eigentümer des Tankwagens (falls sich dieser in Privatbesitz befindet), der Eigentümer oder der Halter und der Betreiber im Falle eines Tankcontainers, der Empfänger, usw. umgehend kontaktiert werden können;*
- *dem Infrastrukturbetreiber so schnell wie möglich relevante Informationen zur Verfügung gestellt werden (z. B. Zulassungsnummer der Wagen, Position der Wagen im Zug, UN-Nummer, RID-Klassifizierungscode und Gefahrenidentifikationsnummer der gefährlichen Güter in Übereinstimmung mit den RID-Bestimmungen);*
- *die Organisation (Infrastrukturbetreiber) über einen Prozess verfügt, um sicherzustellen, dass die Behörden (z. B. Rettungsdienste, Polizei, andere Notfalldienste und Behörden) mit relevanten Informationen über gefährliche Güter (siehe Beispiele oben) versorgt werden.*

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Das Verfahren, mit dem die Szenarien ermittelter potenzieller Notfallsituationen festgelegt werden, um die mit den verschiedenen Situationen (mit den ermittelten Schnittstellen) verbundenen Risiken, einschließlich der Risiken, die sich aus menschlichen und organisatorischen Faktoren ergeben, zu bewerten. Die zur Minderung dieser Risiken festgelegten Sicherheitsmaßnahmen sind in die betreffenden Pläne, Prozesse und Verfahren (einschließlich Betriebsverfahren) integriert.

Die Verfahren zur Beschreibung des Zusammenhangs zwischen Notfallplanung und Risikomanagement.

Verweise im Verfahren auf die Anforderungen an das Kompetenzmanagementsystem für Mitarbeiter, die auf Notfälle reagieren müssen, und Gewährleistung, dass Vertragspersonal in der Lage ist, dieselben Standards zu erfüllen.

Es gibt ein Verfahren, in dem die regelmäßige Durchführung von (theoretischen und praktischen) Notfallübungen mit allen (sowohl internen als auch externen) Beteiligten beschrieben wird, wie Rückmeldungen aus Notfallübungen im Rahmen von Überwachungstätigkeiten (siehe Abschnitt ***6.1 Überwachung***) gesammelt werden, um Aktionen/Maßnahmen zur Verbesserung der Notfallpläne und -verfahren sowie der Kompetenz aller betroffenen Akteure in die Wege zu leiten (siehe ***7.2. Kontinuierliche Verbesserung***).

Es gibt ein Verfahren, das Informationen darüber enthält, wie Notfallübungen für das Kompetenzmanagement und die Prozessverbesserung eingesetzt werden.

Es gibt ein Verfahren zur Beschreibung des Betriebskontinuitätsmanagements, das eingerichtet werden muss, um Abweichungen von Standards/Verfahren zu vermeiden, wenn die Organisation unerwarteten Auswirkungen auf den Betrieb ausgesetzt ist.

Es gibt ein Verfahren, in dem beschrieben wird, wie die Notfallpläne umgesetzt werden, um ein effizientes und rasches Eingreifen zu gewährleisten, um nach einem Unfall Leben zu retten.

Die Bestimmungen, die gewährleisten, dass die Mitarbeiter und die Notfalldienste der Organisation einfachen Zugang zu Unterlagen im Zusammenhang mit Notfall- und Betriebskontinuitätsplänen haben, um eine weitere Verschlechterung der Lage zu vermeiden.

Es gibt ein Verfahren, in dem beschrieben wird, wie Empfehlungen anderer Parteien (Behörden, Notfalldienste) und bewährte Verfahren bei der Überprüfung der Notfallpläne und -verfahren berücksichtigt werden.

5.5.6 Aufsichtsaspekte

Um die Verfahren im Sicherheitsmanagementsystem für das Notfallmanagement richtig bewerten zu können, kann es notwendig sein, die Verfahren des Sicherheitsmanagementsystems mit denen der relevanten Schnittstellenakteure (insbesondere die Beziehung zwischen den Hauptakteuren wie Eisenbahnunternehmen, Infrastrukturbetreiber und Notdienst) zu vergleichen, um sicherzustellen, dass die für die Bewältigung solcher Störungen bestehenden Prozesse ein kohärentes Ganzes darstellen.

Prüfung, ob für alle vorhersehbaren Notfälle Pläne bestehen.

Vorkehrungen für die Erprobung von Notfallplänen und koordinierte Vorkehrungen mit Notfalldiensten, die nicht auf Planübungen beschränkt sind.

Schnittstellenvereinbarungen mit anderen Interessengruppen liegen vor und umfassen Prüfung, Kontrolle, Kommunikation, Koordination und Kompetenz.

6 Leistungsbewertung

6.1 Überwachung

6.1.1 Regulatorische Anforderung

6.1.1. Die Organisation führt Überwachungen im Einklang mit der Verordnung (EU) Nr. 1078/2012 durch, um

(a) die ordnungsgemäße Anwendung und Wirksamkeit aller Prozesse und Verfahren im Sicherheitsmanagementsystem, einschließlich der betrieblichen, organisatorischen und technischen Sicherheitsmaßnahmen, zu überprüfen;

(b) die ordnungsgemäße Anwendung des Sicherheitsmanagementsystems insgesamt zu überprüfen und festzustellen, ob die erwarteten Ergebnisse erzielt wurden;

(c) zu untersuchen, ob das Sicherheitsmanagementsystem den Anforderungen dieser Verordnung entspricht;

(d) im Fall von Nichteinhaltungen bezüglich der Buchstaben a, b und c geeignete Korrekturmaßnahmen zu ermitteln, einzuführen und auf ihre Wirksamkeit hin zu bewerten (siehe 7.2 Kontinuierliche Verbesserung).

6.1.2. Die Organisation muss regelmäßig auf allen Organisationsebenen die Erfüllung sicherheitsrelevanter Aufgaben überwachen und eingreifen, wenn diese Aufgaben nicht ordnungsgemäß erfüllt werden.

6.1.2 Zweck

Die Organisation sollte den Nachweis erbringen, dass sie über einen Prozess zur Überwachung der Anwendung und Wirksamkeit des Sicherheitsmanagementsystems verfügt und dass dieses Verfahren für die Größe, den Umfang und die Art des Betriebs angemessen ist. Die Organisation sollte aufzeigen, dass der Prozess sämtliche Defekte in der Funktionsweise des Sicherheitsmanagementsystems identifizieren, beurteilen und korrigieren kann.

6.1.3 Erläuterungen

Wirksamkeit der Kontrollmaßnahmen bedeutet, dass die Organisation über einen Prozess verfügt, mit dem überprüft werden kann, ob nach Durchführung einer Risikobewertung und Anwendung geeigneter Kontrollmaßnahmen diese nach einer gewissen Zeit überprüft werden, um sicherzustellen, dass die erwartete Verringerung des Sicherheitsrisikos durch ihre Anwendung erreicht wurde (6.1.1. Buchstabe d).

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Selbstkritische und objektive Bewertungen der Sicherheitskulturprogramme, Praktiken und Leistungen der Organisation werden routinemäßig durchgeführt. Sicherheitsinformationen, wie z. B. aus dem Korrekturprogramm, der menschlichen Leistungsfähigkeit, der Störungs- und Unfallanalyse, Umfragen und relevanten internen und externen Betriebserfahrungen, werden systematisch gesammelt und ausgewertet,

um Trends zu erkennen und organisatorische und individuelle Abweichungen oder Bequemlichkeit zu vermeiden.

Eine erfolgreiche Bewertung ist in der Lage, sich an der Verbesserung der Sicherheit durch die Bereitstellung eines klaren Bildes davon, wie die Sicherheitskultur der Organisation die Sicherheit beeinflusst, zu beteiligen. Die Bewertung zielt darauf ab, Stärken und Schwächen der Sicherheitskultur zu identifizieren, indem man vergleicht, was die Kultur ist und was sie sein sollte. Dies ermöglicht die Priorisierung von Bereichen für Verbesserungen und die Umsetzung von Änderungen, z. B. an Prozessen, Schulungen und Verhaltensweisen. Die Sicherheitskulturbewertung ist ein Mittel, um proaktiv an der Verbesserung der Sicherheitsleistung und der Erhöhung der Sicherheitsmargen zu arbeiten. Die Anwendung unabhängiger Bewertungen der Sicherheitskultur wird alle drei bis fünf Jahre empfohlen, organisatorische Selbsteinschätzungen jedes Jahr oder alle zwei Jahre.

6.1.4 Nachweise

- *Informationen darüber, wie der Antragsteller die CSM für die Kontrolle umgesetzt hat Verordnung (EU) Nr. 1078/2012); **(6.1.1 Buchstabe a)***
- *Informationen darüber, wie der Überwachungsprozess den Erfolg oder Misserfolg der Erfüllung der erwarteten Sicherheitsergebnisse ermittelt; **(6.1.1 Buchstabe b)***
- *Nachweis, dass das Sicherheitsmanagementsystem als Folge der Korrektur von bei der Überwachung identifizierten Fehlern in den Prozessen des Sicherheitsmanagementsystems verändert wurde; **(6.1.1 Buchstabe c)***
- *Nachweis, dass die Wirksamkeit der ergriffenen Korrekturmaßnahmen überprüft wird, nachdem nachgewiesen wurde, dass die SMS-Prozesse nicht eingehalten wurden; **(6.1.1 Buchstabe d)***
- *Die Organisation sollte über einen Prozess zur Festlegung von Leistungsstandards und Indikatoren für die Überwachung im Zusammenhang mit betrieblichen Prozessen sowie für implementierte Änderungen verfügen. Es sollte ein Programm für die kontinuierlich Bewertung der Leistung der Prozesse im Zusammenhang mit menschlichen und organisatorischen Faktoren sowie dem Ergebnis dieser Prozesse geben, z. B. Einhaltung der Verfahren durch die Mitarbeiter sowie der Einsatz neuer Ausrüstung; **(6.1.2)***
- *Die Sicherheitsleistung wird systematisch im Hinblick auf die Strategie zur Verbesserung der Sicherheitskultur bewertet. Dies bedeutet, dass die Organisation prüfen sollte, wie Verbesserungen der Sicherheitskultur zur Sicherheitsverbesserung passen und Teil dieses Ziels sind. **(6.1.2)***

6.1.5 Beispiele für Nachweise

Eine Erklärung, dass die CSM für die Kontrolle Verordnung (EU) Nr. 1078/2012) angewendet wird und dass es ein Verfahren gibt, das diese Tätigkeit abdeckt. Das Verfahren beschreibt, wie die Leistung im Vergleich mit den Sicherheitszielen durch das Änderungsmanagement und den Risikobewertungsprozess gemessen und korrigiert werden und wie Fehler im Sicherheitsmanagementsystem behoben werden.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Die Organisation verfügt über Prozesse und Verfahren zur systematischen Beurteilung, ob die Vorkehrungen zur Aufnahme der menschlichen und organisatorischen Faktoren angemessen sind und ob die erzielten Ergebnisse den Leistungsstandards entsprechen.

Die Organisation verfügt über Prozesse und Verfahren zur systematischen Beurteilung der Mitarbeiterleistung bei sicherheitskritischen Arbeitsaufgaben. Diese Prozesse basieren auf einem proaktiven

Ansatz, der Standards für Leistung und systematische Bewertung setzt. Es werden evidenzbasierte Methoden verwendet, z. B. das effektive Arbeiten als Besatzung.

Der Überwachungsprozess, einschließlich der Bestimmungen über die zugewiesenen Ressourcen sowie der Personalausstattung und der Kompetenzen der mit Überwachungstätigkeiten betrauten Mitarbeiter.

Die durchgeführte Überwachung, welche die Kontrolle der Umsetzung und der Wirksamkeit von Prozessen und Verfahren umfasst, welche die sich aus dem Risikobewertungsprozess ergebenden menschlichen und organisatorischen Faktoren integrieren. Bei der Überwachung werden daher spezifische Elemente menschlicher und organisatorischer Faktoren auch in operative Tätigkeiten integriert. Dies umfasst auch die Bewertung und Aufrechterhaltung der Kompetenzen (technische und überfachliche Fähigkeiten, Einstellungen, Verhaltensweisen usw.) der (internen oder externen) Mitarbeiter, die Sicherheitsaufgaben wahrnehmen (siehe Abschnitt ***4.2 Kompetenz***).

Die durchgeführte Überwachung einschließlich der Analyse des Erfolgs der Strategie für menschliche und organisatorische Faktoren.

Das Überwachungsverfahren einschließlich der Analyse der Berichterstattung durch die Mitarbeiter. Das SMS sieht einen Prozess der gerechten Kultur vor, bei dem grobe Fahrlässigkeit, vorsätzliche Verstöße und zerstörerische Handlungen geahndet werden. Ziel ist es, eine Berichterstattungskultur zu entwickeln, in der die Mitarbeiter keine Vorbehalte haben, Meldung zu machen, weil sie nicht für fahrlässige Fehler oder Unterlassungen verantwortlich gemacht werden. Erklärt wird darin auch, wie sicherheitsbezogene Probleme/Störungen von Mitarbeitern, Auftragnehmern oder anderen relevanten Interessengruppen gemeldet werden können.

Der Überwachungsprozess ist ein Element zur Verbesserung des organisatorischen Lernens. Die Analyse der Berichterstattung durch die Mitarbeiter wird im Rahmen des Überwachungsprozesses analysiert, um die Sicherheitsmaßnahmen und die SMS-Prozesse und -Verfahren zu verbessern.

Die Überwachungsergebnisse werden aus Sicht der Sicherheitskultur analysiert und in den Prozess der Bewertung der Sicherheitskultur einbezogen.

6.1.6 Referenzen und Standards

- *CSM on Monitoring application guide (Leitfaden für die Anwendung der CSM für die Kontrolle)*

6.1.7 Aufsichtsaspekte

Die Untersuchung des Überwachungsprozesses und der sich daraus ergebenden Erkenntnisse und Maßnahmen ist entscheidend für die Feststellung, ob das Sicherheitsmanagementsystem ein „lebendiges“ und sich entwickelndes Dokument ist, da die Erfahrung Verbesserungen hervorruft, oder ob es sich um ein festes Dokument handelt, das sich im Laufe der Zeit nicht ändert.

Die Prüfung einer Reihe wichtiger Risikobereiche und -kontrollen sowie die Überprüfung ihrer korrekten Anwendung und Wirksamkeit durch das Sicherheitsmanagementsystem ist von entscheidender Bedeutung, damit die nationale Sicherheitsbehörde die Einhaltung der CSM für die Kontrolle sicherstellen kann.

6.2 Interne Auditierung

6.2.1 Regulatorische Anforderung

6.2.1. Die Organisation führt interne Audits auf unabhängige, unparteiliche und transparente Weise durch, um für die Zwecke ihrer Überwachungstätigkeiten Informationen zu sammeln und auszuwerten (siehe 6.1 Überwachung). Dies umfasst Folgendes:

(a) einen Zeitplan für geplante interne Audits, der abhängig von den Ergebnissen vorheriger Audits und der Leistungsüberwachung überarbeitet werden kann;

(b) Ermittlung und Auswahl qualifizierter Prüfer (siehe 4.2 Kompetenz);

(c) Analyse und Bewertung der Auditergebnisse;

(d) Ermittlung des Bedarfs an Korrektur- oder Verbesserungsmaßnahmen;

(e) Verifizierung der Durchführung und Wirksamkeit dieser Maßnahmen;

(f) die sich auf die Durchführung der Audits und ihre Ergebnisse beziehenden Unterlagen;

(g) Mitteilung der Auditergebnisse an die oberste Führungsebene.

6.2.2 Zweck

Der Antragsteller sollte nachweisen, dass er über ein internes Auditsystem verfügt, das kompetentes Personal einbezieht und aussagekräftige Ergebnisse liefert, die vom Management berücksichtigt werden und sicherstellt, dass das Sicherheitsmanagementsystem den gesetzlichen Bestimmungen entspricht.

6.2.3 Erläuterungen

Interne Audits **(6.2.1)** sind Überwachungswerkzeuge im Sinne der CSM für die Kontrolle (Verordnung (EU) Nr. 1078/2012). Obwohl dies eine separate Anforderung ist, soll sie zur Erreichung der Ziele der Überwachung in Übereinstimmung mit den CSM für die Kontrolle beitragen.

Interne Audits **(6.2.1)** zielen darauf ab, Informationen darüber, ob das Sicherheitsmanagementsystem den geltenden Anforderungen **(6.1.1 Buchstabe c)** entspricht oder nicht, und ob es effektiv umgesetzt und gepflegt wird, bereitzustellen **(6.1.1 Buchstaben a, b und d)**. Die geltenden Anforderungen beziehen sich auf die Anforderungen in Anhang I und Anhang II der Verordnung (EU) 2018/762 und damit auf alle anderen geltenden Anforderungen, denen sich die Organisation verpflichtet **(siehe ferner 1.1)**.

Die Prüfer sind dafür verantwortlich, den Abschluss und die Wirksamkeit der Korrektur- oder Verbesserungsmaßnahmen zu überprüfen **(6.2.1 Buchstabe c)**, die zur Behandlung der Feststellungen des Audits zu ergreifen sind.

6.2.4 Nachweise

- *Nachweis, dass es ein internen Auditprozess oder -rahmen gibt, der geplante Audits und zusätzliche gezielte Audits als Reaktion auf die Sicherheitsleistungsdaten vorsieht;* ***(6.2.1 Buchstabe a)***
- *Nachweis eines Kompetenzmanagementsystems, das Elemente enthält, welche die Kompetenz der internen Prüfer ansprechen;* ***(6.2.1 Buchstabe b)***
- *Nachweis der Ergebnisse von internen und externen Audits, nach denen gehandelt wurde;* ***(6.2.1 Buchstaben c bis f)***
- *Nachweis dafür, dass die Ergebnisse der Audits auf der obersten Führungsebene besprochen und folglich entsprechende Maßnahmen ergriffen wurden.* ***(6.2.1 Buchstabe g)***

6.2.5 Beispiele für Nachweise

Es gibt ein internes Auditverfahren für geplante und zusätzliche Audits, einschließlich Besprechung der Ergebnisse auf der oberen Führungsebene.

Beispiele für Auditberichte und ein Protokoll über die Ergebnisse der internen Audits, die angeben, welche Maßnahmen ergriffen wurden, um ihnen Rechnung zu tragen.

Ergebnisse der Auditaktivitäten, die in der gesamtem Organisation durchgeführt wurden, werden gesammelt, analysiert und als Empfehlungen für die regelmäßige Managementbewertung verwendet.

Das Verfahren bezieht sich auf das Kompetenzmanagementsystem. Das Kompetenzmanagementsystem zeigt, dass die Prüfer entsprechende Prüferschulungen befolgt haben (z. B. ISO).

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Der interne Auditprozess, einschließlich der Bestimmungen über die zugewiesenen Ressourcen sowie der Personalausstattung und der Kompetenzen der beteiligten Mitarbeiter. Kompetenzanforderungen an die Mitarbeiter, die interne Audits durchführen, sind in das Kompetenzmanagementsystem integriert, auch in Bezug auf die spezifischen Kompetenzen im Bereich menschlicher und organisatorischer Faktoren. Schulungsbeispiele zeigen, dass menschliche und organisatorische Faktoren einbezogen wurden.

Das interne Audit, das die Kontrolle der Umsetzung und der Wirksamkeit von Prozessen und Verfahren umfasst, welche die sich aus dem Risikobewertungsprozess ergebenden menschlichen und organisatorischen Faktoren integrieren (siehe ***6.1 Überwachung***).

Die Organisation verfügt über Prozesse und Verfahren zur systematischen Integration menschlicher und organisatorischer Faktoren in ihre internen Audits. Ziel ist es, die Wirksamkeit der Sicherheitsmaßnahmen in Bezug auf menschliche und organisatorische Faktoren zu überprüfen und die Verwirklichung der Sicherheitsziele, einschließlich menschlicher und organisatorischer Faktoren, zu bewerten.

Beispiele für interne Audits, aus denen hervorgeht, dass menschliche und organisatorische Faktoren bei der Analyse der Ergebnisse der Audits, der Ermittlung der Notwendigkeit von Korrektur- oder Verbesserungsmaßnahmen und deren Mitteilung an die oberste Führungsebene berücksichtigt werden.

Die Organisation verfügt über Prozesse und Verfahren zur systematischen Integration der Evaluierung der Leistung der Mitarbeiter, die sicherheitskritische Aufgaben und operative Tätigkeiten wahrnehmen.

Ein Prozess zur Beschreibung des Kommunikationsmanagements in Bezug auf die Ergebnisse, Empfehlungen/Maßnahmen, der einen gemeinsamen und transparenten Ansatz erkennen lässt.

6.2.6 Referenzen und Standards

- *ISO 19011:2018 – Leitfaden zur Auditierung von Managementsystemen*
- *CSM on Monitoring application guide (Leitfaden für die Anwendung der CSM für die Kontrolle)*

6.2.7 Aufsichtsaspekte

Bei der Durchführung der Aufsicht ist es ausschlaggebend, dass die Planung und die Ergebnisse der Audits geprüft werden. Dadurch wird gezeigt, ob die Audits auf die richtigen Bereiche abzielen, ob die Ergebnisse angemessen sind und ob die Mitarbeiter, welche die Audits durchführen, kompetent und unabhängig sind.

Prüfung, ob die ausgewählten Bereiche für das Audit am Risikoprofil der Organisation ausgerichtet wurden.

Es gibt einen Mechanismus, um ungeplante Audits auszulösen, und dieser Mechanismus wird durch die Überprüfung einer Reihe von Beispielen genutzt.

6.3 Managementbewertung

6.3.1 Regulatorische Anforderung

6.3.1. Die oberste Führungsebene muss die fortlaufende Eignung und Wirksamkeit des Sicherheitsmanagementsystems regelmäßig überprüfen und dabei mindestens Folgendes berücksichtigen:

(a) Einzelheiten zu den erzielten Fortschritten bei noch offenen Maßnahmen aus früheren Managementbewertungen;

(b) Veränderungen interner und äußerer Umstände (siehe 1. Kontext der Organisation);

(c) die Sicherheitsleistung der Organisation in Bezug auf:

(i.) die Erreichung ihrer Sicherheitsziele;

(ii.) die Ergebnisse ihrer Überwachungstätigkeiten, einschließlich der Ergebnisse interner Audits, und internen Untersuchungen von Unfällen/Störungen sowie den Status der jeweils ergriffenen Maßnahmen;

(iii.) relevante Ergebnisse von Aufsichtstätigkeiten der nationalen Sicherheitsbehörde;

(d) Empfehlungen für Verbesserungen.

6.3.2. Auf der Grundlage der Ergebnisse ihrer Managementbewertung übernimmt die oberste Führungsebene die Gesamtverantwortung für die Planung und Umsetzung der notwendigen Änderungen des Sicherheitsmanagementsystems.

6.3.2 Zweck

Eine starke Sicherheitsführung des Managements ist entscheidend für die effiziente und effektive Funktionsweise des Sicherheitsmanagementsystems einer Organisationen sowie seiner weiteren Entwicklung im Laufe der Zeit. Die Organisation sollte nachweisen, dass das Management aktiv an der Überprüfung der Leistung des Sicherheitsmanagementsystems und seiner Entwicklung für die Zukunft beteiligt ist.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Die Managementbewertung ist mit allen Prozessen und Verfahren des Sicherheitsmanagementsystems verknüpft und kann darüber hinaus menschliche und organisatorische Faktoren einbeziehen, um sie zu verbessern.

6.3.3 Nachweise

- *Prozesse für die Managementsitzungen, bei denen die Überprüfung des Sicherheitsmanagementsystems und die Fortschritte in Bezug auf interne Empfehlungen durch Audits und Überprüfungen behandelt werden;* ***(6.3.1 Buchstaben a bis d)***
- *Aufzeichnungen darüber, wie die Organisation im Vergleich zu ihren Sicherheitszielen abgeschnitten hat;* ***(6.3.1 Buchstabe c, Buchstabe i)***
- *Nachweis, dass die Empfehlungen der relevanten nationalen Sicherheitsbehörden im Sicherheitsmanagementsystem berücksichtigt wurden;* ***(6.3.1 Buchstabe c Ziffer iii)***

- *Die Organisation kann nachweisen, dass sie über Prozesse zur Ermittlung und Festlegung von Zielen verfügt, die mit der Art, dem Umfang und relevanten Risiken übereinstimmen, sie regelmäßig die Leistung im Hinblick auf die Ziele bewertet, sie Verfahren einhält und Sicherheitsdaten nutzt, um Änderungen betrieblicher Vorkehrungen zu überwachen, zu überprüfen und umzusetzen;* ***(6.3.1)***
- *Nachweis, dass das Management eine aktive Rolle bei der Planung und Umsetzung der notwendigen Änderungen am Sicherheitsmanagementsystem übernimmt;* ***(6.3.2)***
    - *Es existieren Prozesse und Tools zur systematischen Meldung aller Arten von identifizierter Risiken, Fehlern, Beinaheunfällen, Mängeln und Vorkommnissen sowie zur Kategorisierung und Analyse der Meldungen aus Sicht menschlicher und organisatorischer Faktoren, damit die zugrunde liegenden Ursachen und wirksame Maßnahmen ermittelt werden können.*
    - *Im Unfalluntersuchungsprozess werden Fachkenntnisse über menschliche und organisatorische Faktoren herangezogen.*
    - *Es gibt systematische Prozesse zur Einbindung gewonnener Erfahrungen zu Themen im Zusammenhang mit menschlichen und organisatorischen Faktoren in Schulung und Design.*
    - *Die gewonnenen Erfahrungen im Zusammenhang mit Unfall- und Störungsuntersuchungen werden den Mitarbeitern in der Organisation kommuniziert und fließen in Schulung, Design und andere Bereiche ein, um die Wahrscheinlichkeit eines erneuten Auftretens zu verringern.*
    - *Über die Ergebnisse der Unfalluntersuchungen wird bei Managementsitzungen Bericht erstattet, und sie werden als wichtiges Werkzeug zum Lernen und für Verbesserungen angesehen.*
- *Es ist ein Gewährleistungsprozess für Unfalluntersuchungen vorhanden.*

6.3.4 Beispiele für Nachweise

Das Verfahren, das die Überprüfung und den Fortschritt in Bezug auf interne Empfehlungen durch von der oberen Führungsebene durchgeführte Audits und Überprüfungen abdeckt, zusammen mit Protokollen ausgewählter Sitzungen.

Das Problemprotokoll zeigt Empfehlungen, die ausgesprochen wurden, und Fortschritte bei der Behebung von Fehlern, die vom Management nachverfolgt werden.

Das Verfahren für die Überprüfung der Ergebnisse von internen Unfalluntersuchungen durch das Management und die entsprechenden Beiträge der Aufsicht durch die nationale Sicherheitsbehörde.

Es werden Informationen darüber vorgelegt, welche Indikatoren die oberste Führungsebene mit welcher Häufigkeit nachverfolgt.

Die oben genannten Beispiele für Nachweise sollten zeigen, wie menschliche und organisatorische Faktoren in die Managementbewertung integriert werden.

6.3.5 Aufsichtsaspekte

Bei der Aufsicht ist es wichtig zu beachten, dass der Prozess, der gewährleistet, dass das Management die Wirksamkeit des Sicherheitsmanagementsystems überprüft, zu echten Veränderungen auf Betriebsebene führt.

Kenntnis des Managements der Veränderungen interner und äußerer Umstände. Führt das Management zum Beispiel Bestandsaufnahmen oder andere Techniken wie zum Beispiel PEST-LE (politische, wirtschaftliche, soziale und technologische, rechtliche und ökologische)-Analysen durch, um die Entwicklung seines Sicherheitsmanagementsystems durch Informationen zu unterstützen?

Die Verbindung/Verknüpfung zwischen den Ergebnissen der Managementbewertung und wie diese in den jährlichen Sicherheitsbericht einfließen.

7 Verbesserung

7.1 Lehren aus Unfällen und Störungen

7.1.1 Regulatorische Anforderung

7.1.	Lehren aus Unfällen und Störungen
7.1.1.	Unfälle und Störungen, die den Eisenbahnbetrieb der Organisation betreffen, müssen
	(a) zur Ermittlung ihrer Ursachen gemeldet, protokolliert, untersucht und analysiert werden;
	(b) gegebenenfalls den nationalen Stellen gemeldet werden.
7.1.2.	Die Organisation muss sicherstellen, dass
	(a) Empfehlungen der nationalen Sicherheitsbehörde, der nationalen Untersuchungsstelle, der Branche bzw. Empfehlungen aus internen Untersuchungen evaluiert und gegebenenfalls umgesetzt oder in Auftrag gegeben werden;
	(b) einschlägige Berichte bzw. Informationen anderer Beteiligter wie Eisenbahnunternehmen, Infrastrukturbetreiber, für die Instandhaltung zuständige Stellen und Schienenfahrzeughalter zur Kenntnis genommen und berücksichtigt werden.
7.1.3.	Die Organisation muss die aus den Untersuchungen gewonnenen Informationen dazu verwenden, die Risikobewertung zu überprüfen (siehe 3.1.1. Risikobewertung), Lehren im Hinblick auf die Verbesserung der Sicherheit zu ziehen und gegebenenfalls Korrektur- und/oder Verbesserungsmaßnahmen zu beschließen (siehe 5.4). Änderungsmanagement).

7.1.2 Zweck

Die Organisation sollte nachweisen, dass sie Unfälle und Störungen untersucht, um die Risikokontrolle zu erlernen und zu verbessern, dass das Personal, das mit entsprechenden Aufgaben betraut ist, befähigt ist, Untersuchungen durchzuführen, auch in Bezug auf menschliche und organisatorische Faktoren, dass Unfälle an die zuständigen Behörden gemeldet werden und dass Empfehlungen und Berichte ausgesprochen bzw. erstellt und vom Management befolgt werden.

Darüber hinaus wendet die Organisation „Double-Loop-Learning“ an: Nicht nur die Realität der Ereignisse steht im Mittelpunkt des Lernens, sondern auch die Fähigkeit der Organisation, sich zu verbessern, indem sie sich auf jene Elemente konzentriert, die den Wissens- und Informationstransfer innerhalb der Organisation entweder fördern oder behindern.

7.1.3 Erläuterungen

Die Begriffe „Beinaheunfälle“ und „sonstige Gefährdungen“ sind in der Definition der „Störung“ im Sinne der Richtlinie (EU) 2016/798 enthalten. Es ist ebenso wichtig, Beinaheunfälle und sonstige Gefährdungen zu untersuchen, um die Sicherheit proaktiv zu steuern.

Lehren aus Unfällen und Störungen sollte den Austausch von Informationen mit anderen Interessengruppen (Infrastrukturbetreiber, andere Eisenbahnunternehmen, ECM, um die Zusammenarbeit zu entwickeln und die allgemeine Verbesserung der Leistung des Sicherheitsmanagementsystems zu fördern) unterstützen.

Für Überprüfungen, die eine Perspektive der menschlichen und organisatorischen Faktoren benötigen, sollten Prüfer entweder geschult sein oder auf geeignetes Fachwissen Zugriff haben, um die betreffenden Probleme zu untersuchen.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Bei der Analyse von Unfällen/Störungen sollte nicht Einzelnen die Schuld zugewiesen oder einer Abteilung bescheinigt werden, dass sie „mehr als andere verantwortlich ist", sondern eher Verständnis und die Verbesserung der organisatorischen Schwächen, die diese möglich gemacht haben, angestrebt werden. Die wichtigste Herausforderung bei der Analyse von Ereignissen ist die Vermeidung von „Nachbarereignissen". Wenn die Analyse bei der Identifizierung der unmittelbaren Ursachen aufhört, kann nur das nächste ähnliche Ereignis verhindert werden. Wenn die Analyse hingegen die Identifizierung von technischen und organisatorischen „Grundursachen" ermöglicht, können mit den Verbesserungsmaßnahmen andere Unfallarten, die dieselben Mechanismen haben, verhindert werden. Wenn zum Beispiel die Analyse deutlich macht, dass ein Verfahren nicht aktualisiert wurde und dass die Korrekturmaßnahme nur auf die Korrektur dieses Verfahrens abzielt, stellt sich nur ein begrenzter Effekt ein. Wenn durch eine ausführlichere Analyse Schwachstellen im Prozess der Aktualisierung von Verfahren aufgezeigt werden, kann der positive Effekt einer Verbesserungsmaßnahme viel größer sein.

Das Unternehmen kann die Berichterstattungsstruktur gemäß Artikel 4 der Verordnung (EU) 2020/572 „*über die zu befolgende Berichterstattungsstruktur für Berichte über die Untersuchung von Eisenbahnunfällen und -störungen*" verwenden, um die zu untersuchenden Elemente menschlicher und organisatorischer Faktoren zu ermitteln und sie in seine Berichte aufzunehmen. Hinweis: Dies ist jedoch nur eines der vorhandenen Referenzmodelle, das verwendet werden kann.

Die Meldung von gefährlichen Situationen und Störungen mit „großem Potenzial" wird gefördert und erleichtert. Bei Bedarf existieren Mechanismen, die eine anonyme Meldung ermöglichen. Wenn die Meldung namentlich erfolgt, helfen die Mitarbeiter und Teams, durch die die Meldungen erfolgen, bei der Analyse und der Suche kurzfristiger Reaktionen. Teambesprechungen werden organisiert, und die getroffenen Maßnahmen werden den betroffenen Mitarbeitern und ggf. innerhalb der gesamten Organisation kommuniziert.

7.1.4 Nachweise

- *Informationen über den Prozess der Berichterstattung über Unfälle/Störungen, einschließlich der Art und Weise, wie die Grundursachen ermittelt und analysiert werden, inklusive der Berichterstattung innerhalb der Organisation und an andere zuständige Behörden und andere Beteiligte;* ***(7.1.1)***
- *Informationen über die Methode, welche die Organisation in Bezug auf die Untersuchung nutzt, einschließlich des Elements der menschlichen und organisatorischen Faktoren, um die Risikoanalyse und den Beurteilungsprozess im Anschluss an ein Ereignis zu überprüfen;* ***(7.1.3)***
- *Nachweis, dass Empfehlungen von den zuständigen Behörden aus Unfall- und Störungsberichten sowie notwendige identifizierte Änderungen umgesetzt wurden;* ***(7.1.2 Buchstabe a, Buchstabe b)***
- *Überprüfung vergangener Störungen, um relevante Faktoren im Zusammenhang mit einer aktuellen Störung zu identifizieren. Es gibt Belege dafür, dass die Organisation aus Störungen und Erfahrungen auf nationaler und internationaler Ebene umfassender lernen kann;* ***(7.1.3)***
- *Es gibt eine Methodik zur Durchführung von Untersuchungen auf Grundlage der Kenntnisse über menschliche und organisatorische Faktoren und modernster Methoden.*
- *Es gibt ein Schulungsprogramm für Unfall- und Störungsprüfer, das eine Perspektive zu menschlichen und organisatorischen Faktoren anwendet.*

- *Es wird eine „gerechte Kultur" gefördert, die positive Sicherheitsinitiativen anerkennt und stärkt (Meldung von Störungen, die Einbeziehung der Mitarbeiter bei der Analyse und kontinuierlichen Verbesserung, Unterstützung für Kollegen usw.). Diese „gerechte Kultur" soll die Angst vor Schuldzuweisung nehmen, indem sie eine weitgehend akzeptierte Grenze zwischen dem, was akzeptiert wird und was nicht, definiert. Das Recht, einen Fehler zu machen, wird akzeptiert.*

7.1.5 Beispiele für Nachweise

Das Verfahren zur Unfalluntersuchung, das die Untersuchungsmethoden beschreibt und einen Verweis auf die Anforderungen des Kompetenzmanagements für Unfall- und Störungsermittler enthält.

Eine Probe von Unfall- und Störungsberichten verschiedener Arten, die darauf hindeuten, dass die Untersuchungen von einer kompetenten Person durchgeführt wurden, die Ergebnisse auf den Nachweisen basieren und die Empfehlungen umgesetzt wurden.

Eine Kopie der Verfahren/Prozesse mit Nachverfolgung der nach einem Unfall/einer Störung identifizierten Korrektur-/Abhilfemaßnahmen.

Es werden Informationen über die Nutzung des Safety Alert Information Tool (SAIT) zur Verfügung gestellt, um den Überblick über Angelegenheiten zu behalten, die sich auf bestimmte Sachanlagen auswirken, und um andere Organisationen diesbezüglich zu beraten.

Es stehen ausgebildete Prüfer zur Verfügung.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Kompetenzanforderungen an Untersuchungspersonal werden in das Kompetenzmanagementsystem des Unternehmens aufgenommen. Es gibt ein Schulungsprogramm für Unfall- und Störungsprüfer, in dem auch die Frage erörtert wird, wie menschliche und organisatorische Faktoren systematisch integriert werden können.

Die Berichte enthalten eine eingehende Analyse von Ereignissen, die zu kohärenten Aktionsplänen auf allen Ebenen des Sicherheitsmanagementsystems führen, wodurch die Bereitschaft gefördert wird, aus Störungen durch Verhaltensänderungen im gesamten Unternehmen zu lernen. Sitzungsprotokolle und der Austausch von Mitteilungen zeigen, dass es bei Störungen, die externe Parteien betreffen, Hinweise darauf gibt, dass die Ergebnisse von Analysen und Maßnahmen offen ausgetauscht werden.

Das Management erkennt an, dass Störungen und Unfälle durch mehrere Faktoren verursacht sind, die zum Teil auf Managemententscheidungen zurückzuführen sind, und aus Protokollen der Sitzungen des Leitungsorgans geht hervor, dass die Ergebnisse der Untersuchung von Unfällen und Störungen und die damit verbundenen Empfehlungen (d. h. Korrektur- und/oder Verbesserungsmaßnahmen) an das Management zurückgemeldet werden und die Überprüfung des Sicherheitsmanagementsystems unterstützen **(siehe ferner 6.3)**.

Bei der Untersuchung von Störungen und Unfällen wird ein Ansatz für menschliche und organisatorische Faktoren verfolgt und in den Strategien für menschliche und organisatorische Faktoren sowie für die Sicherheitskultur und in allen damit zusammenhängenden Prozessen (Risikobewertung, Leistungsbewertung, kontinuierliche Verbesserung usw.) genannt.

Die Erstausbildungs- und Weiterbildungsprogramme für die Mitarbeiter, aus denen hervorgeht, dass Maßnahmen auf der Grundlage der gewonnenen Erkenntnisse integriert sind, wobei ein besonderer Schwerpunkt auf den mit menschlichen und organisatorischen Faktoren verbundenen Risiken und deren Minderung liegt.

Die Untersuchungen nehmen eine systematische Perspektive ein, das heißt, nicht nur die menschlichen, technologischen und organisatorischen Faktoren als solche zu betrachten, sondern auch die Wechselwirkungen zwischen den Faktoren hervorzuheben. Wenn ein Triebfahrzeugführer zum Beispiel an einer SPAD-Störung (Signal Passed at Danger – überfahrenes Haltesignal) beteiligt war, werden als zu untersuchende Faktoren die relevanten Probleme vorgeschlagen, z. B. Ermüdung, kognitive Überlastung, Kompetenz, usw. (menschlich), der Einfluss der Technologie auf die Leistung, wie z. B. Mensch-System-Schnittstellen, Anordnung, Signalplatzierung (Technologie), der Einfluss der Organisation auf die Leistung, wie z. B. Schulung, Sicherheitsmanagementsystem, organisatorische Prioritäten (Organisation) sowie die Interaktion zwischen den drei Bereichen, wie z. B. der Einfluss der Vergabe in Bezug auf das Design oder das Änderungsmanagement bei der Einführung eines neuen Designs.

Die Analyse gefährlicher Ereignisse erfolgt bereichsübergreifend unter Nutzung unterschiedlicher Fähigkeiten und unter Berücksichtigung der Standpunkte aller Beteiligten (ggf. auch externer Parteien).

Eine Just Culture Policy und bestehende Berichterstattungsinstrumente, die eine Berichterstattungskultur und eine kritische Einstellung der Mitarbeiter fördern. Alle von Mitarbeitern gemeldeten routinemäßigen und ungewöhnlichen Abweichungen werden analysiert und führen erforderlichenfalls zur Umsetzung von Verbesserungsmaßnahmen. Die betroffenen Mitarbeiter werden systematisch darüber informiert, welche Maßnahmen ergriffen wurden.

7.1.6 Referenzen und Standards

- *Website der ERA zur Sicherheitskultur*
- *Website der ERA zu menschlichen und organisatorischen Faktoren*
- *Durchführungsverordnung (EU) 2020/572 der Kommission vom 24. April 2020 über die zu befolgende Berichterstattungsstruktur für Berichte über die Untersuchung von Eisenbahnunfällen und -störungen*
- *IAEA (2002) - Safety culture in nuclear installations: Guidance for use in the enhancement of safety culture. IAEA TECDOC-1529. Internationale Atomenergie-Organisation, Wien (2002).*
- *Mathis, T.L. & Galloway, S.M. (2013) - Steps to safety culture excellence.*
- *Kecklund, L., Lavin, M. & Lindvall, J. (2016) - Safety culture: A requirement for new business models. Lessons learned from other High-Risk Industries. In proceeding presented of The International Conference on Human and Organisational Aspects of Assuring Nuclear Safety – Exploring 30 Years of Safety Culture, Wien, 22. bis 26. Februar 2016*
- *RSSB (2015) - Safety Culture and behavioural development: Common factors for creating a culture of continuous development (www.sparkrail.org)*

7.1.7 Aufsichtsaspekte

Die Kompetenz der Unfall-/Störungsermittler ist entscheidend für die Ausarbeitung sinnvoller Empfehlungen und die Sicherung angemessener vorbeugender Maßnahmen. Die mit der Aufsicht beauftragten Personen sollten auf eine etwaige Beeinflussung der Ergebnisse der Unfall- und Störungsberichte durch das Management achten, die die Qualität des Berichts und daraus abgeleiteter Ergebnisse beeinträchtigen könnte.

Die Ergebnisse einer internen Untersuchung führten zum Lernen der Organisation, das in Dokumenten, Berichten oder anderen Informationskanälen (d. h.: Intranet, internes Unternehmensmagazin usw.) nachverfolgt wird.

Die Organisationskultur in Verbindung mit der Berichterstattung über Störungen und Beinaheunfälle.

7.2 Kontinuierliche Verbesserung

7.2.1 Regulatorische Anforderung

7.2.1. Die Organisation muss die Eignung und Wirksamkeit ihres Sicherheitsmanagementsystems kontinuierlich verbessern, wobei sie den in der Verordnung (EU) Nr. 1078/2012 vorgegebenen Rahmen und mindestens die Ergebnisse folgender Tätigkeiten berücksichtigt:

(a) Überwachung (siehe 6.1 Überwachung);

(b) interne Auditierung (siehe 6.2 Interne Auditierung);

(c) Managementbewertung (siehe 6.3 Managementbewertung);

(d) Lehren aus Unfällen und Störungen (siehe 7.1 Lehren aus Unfällen und Störungen).

7.2.2. Die Organisation muss im Rahmen des organisatorischen Lernens Mittel bereitstellen, um die Mitarbeiter und andere Beteiligte zu ermutigen, an der Verbesserung der Sicherheit aktiv mitzuwirken.

7.2.3. Die Organisation muss über eine Strategie zur ständigen Verbesserung ihrer Sicherheitskultur verfügen, die sich auf die Nutzung von Fachwissen und anerkannten Methoden stützt, um Fehlverhalten, das die verschiedenen Teile des Sicherheitsmanagementsystems beeinträchtigt, zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen.

7.2.2 Zweck

Die kontinuierliche Verbesserung ist ein wesentlicher Teil eines effektiven Sicherheitsmanagementsystems. Der Zweck dieser Anforderung ist es, den Antragsteller dazu zu bringen, zu zeigen, dass er sich für Verbesserungen einsetzt sein Sicherheitsmanagementsystem dies unterstützt.

Die oberste Führungsebene **reflektiert gemeinsam**, wie sich die Sicherheitskultur der Organisation stetig verbessern lässt.

Diese gemeinsame Reflexion wird durch eine Strategie verkörpert, die auf **kulturelle Merkmale** abzielt, die einen wesentlichen Einfluss auf die Sicherheitsleistung haben und die mehr Anerkennung verdienen oder zu ändern sind.

7.2.3 Erläuterungen

Der Schwerpunkt der kontinuierlichen Verbesserung **(7.2.1)** liegt auf den Elementen des Sicherheitsmanagementsystems, die zu Verbesserungsmaßnahmen führen und diese beurteilen, jedoch nicht auf Elementen, die bereits einer Verbesserung unterliegen, da sie bereits Teil des Umfangs der Überwachungstätigkeiten sind.

Wie werden menschliche und organisatorische Faktoren sowie die Sicherheitskultur integriert?

Organisatorisches Lernen **(7.2.2)** ist der Prozess der Verbesserungsmaßnahmen durch besseres Know-how und Verständnis.

Sicherheitskultur **(7.2.3)** hat hier die Definition gemäß 2.1.1 Buchstabe j. Eine positive Sicherheitskultur motiviert und ermöglicht es Organisationen und Einzelpersonen, die Verbesserung der Sicherheit und der Leistung anzustreben. Sie steigert die Arbeitszufriedenheit und Arbeitsplatzerhaltung und bietet Kostenvorteile. Sie kann auch dabei helfen, die regulatorischen Erwartungen zu erfüllen, da Sicherheitsbehörden und Regulierungsbehörden die Rolle, welche die Sicherheitskultur in einem effektiven

Sicherheitsmanagement spielt, zunehmend anerkennen. Genauer gesagt kann eine positive Sicherheitskultur zu Folgendem führen:

- *Verringerung der Betriebsrisiken durch eine umfassendere Risikobewertung und ein verbessertes Verständnis innerhalb der Belegschaft;*
- *Verringerung von Verletzungen von Arbeitnehmern durch Beseitigung der ermittelten Gefahrenquellen dank einer erhöhten Meldequote von Beinaheunfällen;*
- *Verringerung von sicherheitsgefährdenden Handlungen und Bedingungen durch bessere Einbeziehung der Arbeitnehmer und Führungskräfteentwicklung;*
- *Reduzierung der Kosten infolge von Verletzungen der Arbeitnehmer sowie sicherheitsgefährdenden Handlungen und Bedingungen;*
- *Leistungssteigerung durch Verbesserung der Ausbildung des Personals und des Engagements sowie durch Reduzierung von Verletzungen und unsicheren Handlungen und Zuständen;*
- *Verbessertes und effizienteres SMS, dessen Verfahren und Regeln besser zur Realität passen.*

Infolge der grundlegenden kulturellen Eigenschaften, die durch tägliche Wechselwirkungen entstehen und schwer zu ändern sind, gilt diese Strategie als langfristig und es wird davon ausgegangen, dass sie von der obersten Führungsebene verantwortet und gefördert wird.

Es gibt viele Arten zur Verbesserung der Sicherheitskultur:

- *Entwicklung eines Systems zum Austausch von Bedenken. Dies kann abhängig von der Reife der Organisation anonym, aber mit wachsendem Vertrauen offen und zugänglich für alle sein. Es ist wichtig, dass Rückmeldungen in das System integriert werden, um sicherzustellen, dass die Mitarbeiter ein Gefühl der Einbeziehung und Zugehörigkeit haben;*
- *Änderung der Beschaffung und Vertragsbedingungen, um eine gute Sicherheitskultur für Lieferanten zu fördern. Die Sicherheitskultur könnte ein Kriterium zur Auswahl von Lieferanten sein;*
- *Sichtbare Belohnung für sichere Verhaltensweisen. Die Belohnung kann viele Formen haben – von erhöhten jährlichen Zahlungen über Boni bis hin zu wöchentlichen Sicherheitsbelohnungen für hervorragende Leistungen;*
- *Erstellung von spezifischen Zielen für Führungskräfte in Bezug auf Führung im Bereich der Sicherheit, zum Beispiel Ermutigung des Managements, eine sichtbarere Rolle im Praxisbereich einzunehmen, um Standards durch eine Vorbildfunktion zu setzen;*
- *usw.*

Die Ergebnisse der Bewertungen sollten allen Ebenen der Organisation mitgeteilt werden. Sie sollten umgesetzt werden, um eine positive Sicherheitskultur zu fördern und aufrecht zu erhalten, um die Führungsqualitäten im Bereich Sicherheit zu verbessern und um eine Lernhaltung innerhalb der Organisation zu fördern.

Die Erkennung und Auswahl entsprechender kultureller Merkmale ist häufig eine komplexe Aufgabe[1], die sorgfältig ausgeführt werden sollte.

An dieser Aufgabe sollten Mitarbeiter aller Ebenen aus der gesamten Organisation und oft auch von außerhalb beteiligt werden (z. B. Auftragnehmer).

Auch wenn die Wahrnehmungen und Ansichten der Mitarbeiter mit Hilfe eines Fragebogens erfasst werden können, gilt diese Methode im Allgemeinen als unzureichend, um kulturelle Merkmale festzulegen, die sich auf die Sicherheit auswirken. Eventuell geleitet von den Umfrageergebnissen, sollten Fachleute Beobachtungen vornehmen, Einzelbefragungen durchführen und sich auf Fokusgruppen konzentrieren, um eine genauere Diagnose zu treffen.

[1] Diversität der Tätigkeiten und Größe der Organisation sind einfache Beispiele für Parameter, die mit der Komplexität dieser Aufgabe einhergehen.

Hinweis: Eine Fokusgruppe umfasst eine geringe Anzahl an Personen (normalerweise zwischen 4 und 15) mit einem Moderator und konzentriert sich auf ein bestimmtes Thema. Die hierzu eingegangenen Anmerkungen und die Tagesordnung für die zweite Sitzung sind unter „Arbeitsdokumente“ zu finden. Es folgt eine gesonderte E-Mail im Zusammenhang mit der Aktualisierung des Leitfadens zu den SMS-Anforderungen. Um Sie um Hilfe bei der Lösung einer offenen Frage zu bitten, werden in Kürze weitere Informationen folgen.

Auf Grundlage dieser Diagnose kann ein Maßnahmenplan festgelegt werden, der darauf abzielt, kulturelle Merkmale besser wertzuschätzen oder dazu beizutragen, diese zu ändern. Dieser Plan kann von der obersten Führungsebene gefördert werden. Die oberste Führungsebene überwacht die Umsetzung der ermittelten Maßnahmen und überprüft diese entsprechend.

Um die Nachhaltigkeit der Strategie zu gewährleisten, sollte die Diagnose alle 2-5 Jahre mit derselben Herangehensweise überprüft werden. Die Häufigkeit hängt von den Ergebnissen der ursprünglichen Übung ab.

In verschiedenen Branchen mit hohem Risiko wird diese Diagnose häufig innerhalb einer *Bewertung der Sicherheitskultur* durchgeführt. Eine Bewertung der Sicherheitskultur kann unabhängig von oder durch eine Selbstbewertung vorgenommen werden. Der Vorteil einer unabhängigen Bewertung besteht darin, dass die Organisation ein objektiveres Bild der Sicherheitskultur erhält, wobei jedoch das Risiko besteht, dass die Organisation missverstanden werden kann oder Schwierigkeiten haben kann, die Schlussfolgerungen zu akzeptieren. Vorteil einer Selbstbewertung ist, dass diese intern mit dem eigenen Personal der Organisation durchgeführt wird, die umfassende Kenntnisse über die Organisation verfügen. Der Nachteil dabei ist, dass Status und Hierarchien störend wirken können. Im Folgenden werden einige Merkmale einer Bewertung der Sicherheitskultur aufgeführt:

- *Umfasst einen 2/3-wöchigen Bewertungsprozess sowie eine Vorbereitungsphase.*
- *Bezieht ein interdisziplinäres Prüfungsteam ein.*
- *Die Datenerfassung stützt sich auf sozialwissenschaftliche Methoden (einschließlich Befragungen, Fokusgruppen, Beobachtungen).*
- *Die Bewertung erstreckt sich auf die gesamte Organisation und deren Schnittstellen.*
- *Basiert auf einem Sicherheitskulturmodell oder -rahmen.*
- *Die oberste Führungsebene engagiert sich und betrachtet die Bewertung als Chance, etwas zu lernen.*
- *Die Ergebnisse werden in der gesamten Organisation verbreitet.*
- *Auf die Ergebnisse wird reagiert, um eine Strategie zu entwerfen/überarbeiten, mit der die ausgewählten Merkmale der Sicherheitskultur ständig verbessert werden können.*

Die Verbesserung der Strategie und Prozesse zu menschlichen und organisatorischen Faktoren sind ein integraler Bestandteil der kontinuierlichen Verbesserung des Sicherheitsmanagementsystems.

Ein systematischer Ansatz wird als ein schrittweiser Prozess zum Umgang mit den Problemen im Zusammenhang mit der Sicherheitskultur definiert. Zum Beispiel das Verfügen über einen Prozess zur Risikobeobachtung, Störungs- und Unfallberichterstattung und die Art, wie die Informationen verwendet werden, sowie gewonnene Erkenntnisse für kontinuierliche Verbesserungen.

Weitere Informationen zur Sicherheitskultur und zu menschlichen und organisatorischen Faktoren sind Anhang 4 bzw. Anhang 5 zu entnehmen.

7.2.4 Nachweise

- *Informationen über den Prozess zum Zusammentragen von Nachweisen, um die kontinuierliche Verbesserung des Sicherheitsmanagementsystems zu demonstrieren;* ***(7.2.1)***

- *Verfahren, die angeben, wie die Organisation die Ergebnisse aus der Überwachung, internen Audits, der Managementbewertung und den Lehren aus Unfällen und Störungen berücksichtigt, um das Sicherheitsmanagementsystem zu verbessern;* ***(7.2.1)***
- *Informationen darüber, wie die Organisation versucht, Mitarbeiter und andere an der Verbesserung des Sicherheitsmanagementsystems zu beteiligen;* ***(7.2.2)***
- *Der Antragsteller sollte in einer Strategie ausführlich angeben, wie die Sicherheitskultur entwickelt wird, sodass die Risiken im Zusammenhang mit der Sicherheitskultur innerhalb der relevanten Prozesse des Sicherheitsmanagementsystems angemessen berücksichtigt werden. Dabei sollte der Antragsteller verdeutlichen, wo weitere Angaben zu den relevanten Verfahren zu finden sind;* ***(7.2.3)***
- *Die Sicherheitskultur wird kontinuierlich bewertet, um Verbesserungen zu ermitteln;* ***(7.2.3)***
- *Verbesserungen der Sicherheitskultur werden unter Verwendung des PDCA-Zyklus angewendet, um zu gewährleisten, dass die Maßnahmen Wirkung zeigen. Die gewonnenen Erfahrungen werden umgesetzt und systematisch auf ihre Wirkung überprüft.* ***(7.2.3)***

7.2.5 Beispiele für Nachweise

Das Verfahren, das die Überwachung, interne Audits, die Managementbewertung und Unfall- und Störungsuntersuchungen abdeckt, insbesondere die Abschnitte, die sich auf die gewonnen Erkenntnisse für das Sicherheitsmanagementsystem konzentrieren.

Die „Close-Call"-Initiative von Network Rail, bei der Mitarbeiter ermutigt werden, die Organisation aktiv auf Schwächen/Lücken oder Situationen, in denen ein Sicherheits- oder Gesundheitsrisiko besteht, aufmerksam zu machen.

Die Berücksichtigung menschlicher und organisatorischer Faktoren sowie die Verbesserung der Sicherheitskultur werden sich positiv auf die Einhaltung der einschlägigen SMS-Anforderungen auswirken. Als Nachweis kommen in Betracht:

Beispiele für die Protokolle der regelmäßigen Sitzungen der Gewerkschaften und des Managements im Bereich Gesundheit und Sicherheit am Arbeitsplatz, die zeigen, wo Situationen, die als unsicher eingestuft werden oder weiterer Überlegungen bedürfen, erörtert wurden.

Die Ergebnisse von Unfalluntersuchungen werden bei Managementsitzungen gemeldet und gelten als ein wichtiges Werkzeug für das Lernen und die Verbesserung, wobei menschliche und organisatorische Faktoren systemisch und systematisch Berücksichtigung finden.

Eine Kopie der Strategie zur Verbesserung der Sicherheitskultur und der Art, wie dies mit den verschiedenen Teilen des Sicherheitsmanagementsystems in Verbindung steht.

Die Strategie liefert hinreichende Nachweise dafür, dass es unter den Mitarbeitern, die für die Umsetzung und Entwicklung der Strategie eingesetzt werden, fachliche Kompetenz und gegebenenfalls Schulung und Erfahrung im Bereich der Sicherheitskultur gibt.

Die Art der erforderlichen Schulung und Kompetenz bezieht sich auf das Verständnis des Konzepts der Sicherheitskultur und der Mittel und Wege, um kontinuierliche Verbesserungen zu messen und zu erreichen. Entscheidend ist, dass es ein Verständnis von Sicherheitskultur als ganzheitliches Konzept gibt, das alle Teile des Sicherheitsmanagementsystems beeinflusst und dass Sicherheitskultur nicht als eigenständiges Element behandelt werden kann.

Es besteht ein Prozess zur kontinuierlichen Bewertung sicherheitsverbessernder Maßnahmen. Die Wirkungen der sicherheitsverbessernden Maßnahmen werden identifiziert und in die Praxis umgesetzt, sodass sie bewerten werden können.

Aus den Protokollen der Managementbewertung geht hervor, dass das Management anerkennt, dass Störungen, Unfälle und Abweichungen durch mehrere Faktoren verursacht sind, die zum Teil auf Verfahren und Managemententscheidungen zurückzuführen sind.

Aus den Protokollen der Managementbewertungssitzungen geht hervor, wie Korrekturmaßnahmen aus Überwachungstätigkeiten, internen Audits sowie der Untersuchung von Störungen und Unfällen menschliche und organisatorische Faktoren berücksichtigen und auf allen Ebenen des Sicherheitsmanagementsystems und der Organisation festgelegt werden. Sie zeigen zudem, wie die Ergebnisse zur Verbesserung der Risikobewertung genutzt werden **(siehe 3.1)**.

Die Verfahren für Überwachung, internes Audit, Managementbewertung und Untersuchung von Unfällen und Störungen, die mit dem Sensibilisierungsprozess **(siehe 4.3)** und dem Kompetenzmanagementsystem **(siehe 4.2)** verknüpft sind.

7.2.6 Aufsichtsaspekte

Bei der Aufsicht sollte die Verpflichtung des Managements zur kontinuierlichen Verbesserung des Sicherheitsmanagementsystems durch Interviews sowie durch eine Analyse der Dokumentation überprüft werden. Gibt es einen risikobasierten Ansatz zur gezielten Verbesserung, d. h. im Zusammenhang mit gefährdeten und kritischen Kontrollen?

Der Einsatz von Reifemodellen durch die Organisation zur Untersuchung der Leistung des Sicherheitsmanagementsystems sollte dort überprüft werden, wo diese vorhanden sind.

Anhang 1 – Entsprechungstabellen

Die folgenden Tabellen bieten einen direkten Vergleich zwischen den Anforderungen an die Bewertung gemäß Anhang II der vorherigen Verordnungen (EU) Nr. 1158/2010 und (EU) Nr. 1169/2010 und den Anforderungen gemäß Anhang I und Anhang II der Verordnung (EU) 2018/762. Sie zielt darauf ab, den Übergang von dem alten System der Sicherheitsbescheinigung gemäß der Richtlinie 2004/49/EG zu dem neuen System, das durch die Richtlinie (EU) 2016/798 eingeführt wurde, zu erleichtern.

Die Entsprechung mit der Verordnung (EU) 2018/762 liefert keinen Nachweis für die Fähigkeit von Eisenbahnunternehmen oder Infrastrukturbetreibern, die relevanten Anforderungen an das Sicherheitsmanagementsystem in Übereinstimmung mit Artikel 9 der Richtlinie (EU) 2016/798) zu erfüllen. Die Detailgenauigkeit zwischen den vorherigen und den neuen Bewertungsanforderungen kann immer noch variieren, obwohl sie in einem bestimmtem Maß gemeinsame Grundsätze teilen. Darüber hinaus verfügen nicht alle Bewertungsanforderungen in Anhang I und Anhang II der Verordnung (EU) 2018/762 über eine Entsprechung mit den vorherigen Verordnungen. Die Eisenbahnunternehmen und Infrastrukturbetreiber müssen dann weitere Nachweise erbringen, um die neuen Bewertungsanforderungen (oder Teile davon) zu erfüllen.

Die Anforderungen an das Sicherheitsmanagementsystem der Verordnung (EU) 2018/762, die über keine Entsprechung mit denen in Verordnung (EU) Nr. 1158/2010 und/oder in Verordnung (EU) Nr. 1169/2010 verfügen, müssen als neue Anforderungen angesehen werden. Dafür müssen zusätzliche Nachweise vom Antragsteller erbracht werden, um nachzuweisen, dass er diese erfüllt. In den meisten Fällen ist es nicht möglich, eine perfekte Übereinstimmung zwischen den Kriterien der alten und den Anforderungen der neuen CSM-Verordnung herzustellen. Deshalb basiert der Vergleich unter solchen Umständen auf der Absicht der Anforderungen. Es kann auch vorkommen, dass die Anforderungen in der Verordnung (EU) 2018/762 expliziter gemacht wurden, während dieselbe Absicht geteilt wurde. In einem solchen Fall sind die Anforderungen dieser Verordnung nicht als neu anzusehen, sondern können von den verschiedenen Parteien genutzt werden, um ihnen zu helfen, zu verstehen, welche Nachweise von dem Antragsteller erwartet werden können.

Eine Entsprechung mit der High Level Structure (HLS) der ISO[2] wird außerdem für Eisenbahnunternehmen und Infrastrukturbetreiber bereitgestellt, die die Entwicklung eines integrierten Managementsystems anstreben. Auch die Zertifizierung eines Managementsystems nach einem oder mehreren ISO-Managementsystemstandards (z. B. ISO 9001, ISO 14001 oder ISO 45001) ist kein Beweis dafür, dass Eisenbahnunternehmen oder Infrastrukturbetreiber in der Lage sind, die entsprechenden Anforderungen an das Sicherheitsmanagementsystem gemäß Artikel 9 der Richtlinie (EU) 2016/798 zu erfüllen.

Tabelle 1: Direkter Vergleich – Gemeinsame Bewertungskriterien/Anforderungen an Eisenbahnunternehmen und Infrastrukturbetreiber

Verordnung (EU) Nr. 1158/2010 & (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
A.1	3.1.1.1	6.1	
A.2	3.1.1.1	6.1	
A.3	6.1.1	9.1	

[2] ISO/IEC-Direktiven, Teil 1, konsolidierte Ergänzung 2016, Anhang SL Anlage 2.

Verordnung (EU) Nr. 1158/2010 & (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
A.4	3.1.1.1 Buchstabe e	k. A.	
A.5	4.4 4.5.1.1	7.4	
A.6	6.1.1 5.4.1	9.1 8.1	
B.1	5.2.4	k. A.	Die Instandhaltung ist eine Phase des Sachanlagen-Lebenszyklus.
B.2	5.2.4	k. A.	Die Instandhaltung ist eine Phase des Sachanlagen-Lebenszyklus.
B.3	2.3.1 4.2.1	5.3 7.2	Die Definition und Zuordnung der Verantwortlichkeiten für die Instandhaltung findet sich weitgehend in 2.3.1. Die Identifizierung der für die Instandhaltung erforderlichen Kompetenzen findet sich weitgehend in 4.2.1.
B.4	6.1.1 5.2.5	9.1 7.4	Die Datensammlung (Fehlfunktionen, Defekte) und -analyse ist Teil des Überwachungsprozesses. Der Datenaustausch zwischen den für den täglichen Betrieb und den für die Instandhaltung verantwortlichen Personen ist Teil des Informations- und Kommunikationsprozesses, der auf die Verwaltung von Sachanlagen angewandt wird.
B.5	6.1.1	k. A.	Behandelt in Artikel 4 Absatz 2 der CSM für die Kontrolle.
B.6	6.1.1	9.1	Die Bewertung der Leistung und der Ergebnisse der Instandhaltung ist Teil des Überwachungsprozesses, der auf die Instandhaltung angewandt wird.
C.1	5.3.2 Buchstabe a 5.3.3 Buchstabe a	8.1	
C.2	5.3.3 Buchstabe a	8.1	
C.3	5.3.2 Buchstabe b	k. A.	
C.4	5.2.5 Buchstabe b 5.3.2 Buchstabe c	k. A.	
C.5	5.3.2 Buchstabe c 5.3.3 Buchstabe a	k. A.	
D.1	3.1.1.1 Buchstabe a	k. A.	
D.2	3.1.1.1 Buchstabe c	k. A.	
D.3	6.1.1	k. A.	

Verordnung (EU) Nr. 1158/2010 & (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
E.1	1.1.1 Buchstabe a 1.1.1 Buchstabe b	4.1	
E.2	4.5.1.1 Buchstabe a	4.4	
E.3	4.5.1.1 Buchstabe c	7.5.1	
E.4	4.5.1.1 Buchstabe a 4.5.1.1 Buchstabe b	7.5.1	
F.1	4.5.1.1 Buchstabe a	4.4	
F.2	2,3 4.5.1.1 Buchstabe a	5.3 4.4	
F.3	2.3.1 2.3.4	k. A.	
F.4	4.5.1.1 Buchstabe a 4.2.1 2.3.1 2.3.2 2.3.3	4.4 5.3	Die Definition der sicherheitsrelevanten Aufgaben ist Teil der Beschreibung des Sicherheitsmanagementsystems, einschließlich der Zuweisung von Verantwortlichkeiten. Es werden die Verantwortlichkeiten für jede relevante Rolle im Sicherheitsmanagementsystem definiert.
G.1	4.5.1.1 Buchstabe a 2.3.1	4.4 5.3	Die Definition der sicherheitsrelevanten Aufgaben ist Teil der Beschreibung des Sicherheitsmanagementsystems, einschließlich der Zuweisung von Verantwortlichkeiten. Es werden die Verantwortlichkeiten für jede relevante Rolle im Sicherheitsmanagementsystem definiert.
G.2	6.1.1 6.2.1	9.1 9.2	Interne Audits zielen darauf ab, zu prüfen, dass die Organisation die geltenden Anforderungen erfüllt.
G.3	2.1.1 Buchstabe d Ziffer i 2.3.2	k. A.	
G.4	2.3.1	5.3	
G.5	4.1.1	7.1	Es ist zu beachten, dass hier ein Zusammenhang zum Kriterium in der Verordnung (EU) Nr. 1158/2010 N2(d) besteht.
H.1	2.4.1	k. A.	

Verordnung (EU) Nr. 1158/2010 & (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
H.2	(entfernt)	k. A.	Mitarbeiter, die sicherheitsrelevante Aufgaben durchführen, sollten an der Entwicklung, Pflege und Verbesserung des Sicherheitsmanagementsystems beteiligt werden. Es wird der Organisation überlassen, die Anforderung 2.4.1 so umzusetzen, dass die Konformität nachverfolgbar ist.
I	7.2.1	10.1 10.2	
J	2.2.1	5.2	
K.1	3.2.1 3.2.2 Buchstabe d	6.2	
K.2	3.2.2 Buchstabe a	6.2	Die Sicherheitsziele sollten mit der Sicherheitsordnung übereinstimmen, die für die Art und den Umfang des Eisenbahnbetriebs angemessen sein sollte.
K.3	3.2.4	6.2	Die Sicherheitsziele beschränken sich nicht auf die auf Mitgliedstaatenebene etablierten gemeinsamen Sicherheitsziele.
K.4	6.1.1 5.4	9.1 8.1	
K.5	3.2.4 (angepasst)	9.1	Vgl. die Überwachungsstrategie und Pläne in Übereinstimmung mit den CSM für die Kontrolle.
L.1	6.1.1 5.4	9.1 8.1	
L.2	4.2 4.4 4.5 5.2.2 Buchstabe a	k. A.	Der Einsatz von kompetenten Mitarbeitern, Verfahren, spezifischen Dokumenten und Schienenfahrzeugen wird im Kompetenz-, Informations- und Kommunikations- bzw. dokumentierten Informations- und Sachanlagenmanagement verwaltet.
L.3	1.1.1 Buchstabe e 6.1.1 6.1.2.	4.3 9.2	Die Einhaltung der geltenden Anforderungen ist insgesamt in 3.1.2.2 verankert (nicht instandhaltungsspezifisch). Die Überwachung stellt die korrekte Anwendung der Verfahren sicher. Die interne Auditierung gewährleistet die Konformität der Verfahren mit den geltenden Anforderungen.
M.1	3.1.2.1 5.4.1	6.1 8.1	In Übereinstimmung mit ISO gibt es zuerst eine Änderungsplanung, einschließlich der Risikoermittlung und -bewertung, und dann die Änderungsumsetzung.
M.2	3.1.2.1	k. A.	

Verordnung (EU) Nr. 1158/2010 & (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
M.3	5.4.1	8.1	
N.1	4.2.1 4.2.3	7.2	
N.2	4.5.1.1 Buchstabe a 2.3.1 2.3.2 2.3.4 6.1.1	k. A.	
O.1	4.4.1 4.4.2 4.4.3	7.4	
O.2	4.4.3	7.4	
O.3	4.4.1	k. A.	
P.1	4.4.3	k. A.	
P.2	4.5.2 4.5.3	7.5.2 7.5.3	
P.3	4.5.3	7.5.3	
Q.1	7.1.1	10,1	
Q.2	7.1.2	k. A.	
Q.3	7.1.3.	10.2	
R.1	5.5.1	k. A.	
R.2	5.5.2	k. A.	
R.3	5.5.3	k. A.	
R.4	5.5.4	k. A.	
R.5	5.5.5	k. A.	
R.6	5.5.1	k. A.	
R.7	5.5.6	k. A.	
S.1	6.2.1	9.2	
S.2	6.2.1 Buchstabe a	9.2	
S.3	6.2.1 Buchstabe b	9.2	

Verordnung (EU) Nr. 1158/2010 & (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
S.4	6.2.1 Buchstaben c bis f	9.2	
S.5	6.2.1 Buchstabe g 6.3.1	9.3	
S.6	6.2.1	9.2	

Die unten stehenden Tabelle bietet einen direkten Vergleich zwischen den vorherigen Bewertungskriterien und den neuen Anforderungen an das Sicherheitsmanagementsystem, die nur für Eisenbahnunternehmen gelten.

Tabelle 2: Direkter Vergleich – Für Eisenbahnunternehmen spezifische Bewertungskriterien/Anforderungen

Verordnung (EU) Nr. 1158/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anhang I Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
R.8	5.5.7	k. A.	
R.9	5.5.8	k. A.	

Die unten stehenden Tabelle bietet einen direkten Vergleich zwischen den vorherigen Bewertungskriterien und den neuen Anforderungen an das Sicherheitsmanagementsystem, die nur für Infrastrukturbetreiber gelten.

Tabelle 3: Direkter Vergleich – Für Infrastrukturbetreiber spezifische Bewertungskriterien/Anforderungen

Verordnung (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anhang II Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
R.8	5.5.7	k. A.	
R.9	5.5.8	k. A.	
T.1	5.2.1	k. A.	Die sichere Gestaltung und Installation der Infrastruktur ist Teil des Sachanlagen-Lebenszyklus.
T.2	3.1.2 5.4.1	k. A.	Die Identifizierung technischer Veränderungen der Infrastruktur findet sich weitgehend in 3.1.2. Das Management technischer Veränderungen der Infrastruktur findet sich weitgehend in 5.4.1.

Verordnung (EU) Nr. 1169/2010 Kriterien-ID	*Verordnung (EU) 2018/762 Anhang II Anforderungs-ID*	*ISO HLS Klausel Nr.*	*Kommentare*
T.3	3.1.2	k. A.	Die Einhaltung der geltenden Regeln für die Gestaltung der Infrastruktur findet sich weitgehend in 3.1.2.
U.1	5.1.1 5.1.3	k. A.	Das Management der Sicherheit der Infrastruktur findet sich weitgehend in 5.1.1.
U.2	5.1.1	k. A.	Das Management der Sicherheit an den physischen und/oder betrieblichen Grenzen der Infrastruktur findet sich weitgehend in 5.1.1.
U.3	5.1.3 Buchstabe c 5.5.7	k. A.	Die Verwaltung des normalen oder gestörten Betriebs findet sich weitgehend in 5.1.3 Buchstabe c.
U.4	5.1.2 5.2.3	k. A.	
V.1	5.2.4 6.1.1	k. A.	Die Instandhaltung der Infrastruktur findet sich weitgehend in 5.2.4. Die Audits und Inspektionen (wo relevant) sind Teil der Überwachungstätigkeiten.
V.2	5.2.4	k. A.	Die Instandhaltung der Infrastruktur findet sich weitgehend in 5.2.4.
V.3	5.2.3	k. A.	
W.1	5.1.3	k. A.	
W.2	5.1.1	k. A.	Das Management der Sicherheit an den physischen und/oder betrieblichen Grenzen des Verkehrssteuerungs- und Signalgebungssystems findet sich weitgehend in 5.1.1.
W.3	5.1.2 5.2.3	k. A.	

Die unten stehende Tabelle bietet einen direkten Vergleich zwischen der ISO HLS und den neuen Anforderungen an das Sicherheitsmanagementsystem.

Tabelle 4: Direkter Vergleich – High Level Structure der ISO

ISO HLS Klausel Nr.	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
4.1	1.1.1 Buchstabe a 1.1.1 Buchstabe b	
4.2	1.1.1 Buchstabe c 1.1.1 Buchstabe d	
4.3	1.1.1 Buchstabe e 1.1.1 Buchstabe f	

ISO HLS Klausel Nr.	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
4.4	4.5.1.1 Buchstabe a	
5.1	2.1	
5.2	2.2	
5.3	2.3	
6.1	3.1.1 3.1.2	Die CSM für die Evaluierung und Bewertung von Risiken wird angewandt, um zu bestimmen, ob eine Änderung sicherheitsrelevant ist (oder nicht) und anschließend, ob sie wichtig ist (oder nicht). Die von ISO vorgenommene „virtuelle“ Trennung zwischen der strategischen Ebene (ISO HLS Klausel 6) und der taktischen Ebene (ISO HLS Klausel 8) der Planung wird unter Berücksichtigung des EU-Rechtsrahmens und insbesondere der Anwendung der oben genannten CSM (unabhängig von der Art der Änderungen) neu bewertet.
6.2	3.2.1 3.2.2 Buchstabe a 3.2.2 Buchstabe d 3.2.4	
7.1	4.1	
7.2	4.2	
7.3	4.3	
7.4	4.4	
7.5.1	4.5.1	
7.5.2	4.5.2	
7.5.3	4.5.3	

ISO HLS Klausel Nr.	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
8.1	5.1 5.2 5.3 5.4 5.5	In Übereinstimmung mit dem ISO-Leitliniendokument (N360) ist die Absicht von Klausel 8 der ISO HLS, die Anforderungen zu spezifizieren, die innerhalb der Betriebsabläufe der Organisation umgesetzt werden müssen, um sicherzustellen, dass die Anforderungen an das Managementsystem erfüllt werden und die prioritären Risiken und Chancen angesprochen werden. Darüber hinaus wird angegeben, dass zusätzliche Anforderungen (disziplinspezifisch) in Bezug auf die Betriebsplanung und -kontrolle vorgeschrieben werden können. In diesem Sinne sind die Anforderungen unter 5.X mit dem ISO-Ansatz kohärent. Sie sind vor allem im Hinblick auf das Geschäft des Unternehmens nicht eingreifend, bieten aber einen ausreichenden Rahmen zur Kontrolle, wie die wichtigsten Sicherheitsfragen innerhalb der Geschäftsprozesse des Unternehmens gehandhabt werden.
9.1	6.1	Das Konzept der „Überwachung“ (bzw. gemäß der Terminologie der Verordnung (EU) Nr. 1078/2012 „Kontrolle“) bezieht sich auf den in den CSM für die Kontrolle definierten Überwachungsrahmen und hat daher eine breitere Bedeutung als das Konzept der Überwachung, Messung, Analyse und Bewertung, das in Abschnitt 9.1 der ISO HLS definiert wird.
9.2	6.2	Interne Audits sind Überwachungswerkzeuge im Sinne der CSM für die Kontrolle. Obwohl dies eine separate Anforderung ist, soll sie die Ziele der Überwachung in Übereinstimmung mit den CSM für die Kontrolle erreichen.
9.3	6.3	
10.1	7.1	
10.2	7.2	

Anhang 2 – Gegenseitige Anerkennung von Genehmigungen, Anerkennungen oder in Übereinstimmung mit dem Unionsrecht ausgestellten Bescheinigungen von Produkten oder Dienstleistungen

Die ausstellende Behörde für die einheitliche Sicherheitsbescheinigung oder Sicherheitsgenehmigung kann von anderen Stellen, wie z. B. ISO-Konformitätsbewertungsstellen, ausgestellte Bescheinigungen berücksichtigen, um doppelte Bewertungen und zusätzliche Kosten für den Antragsteller zu vermeiden. Die endgültige Entscheidung liegt stets bei der ausstellenden Behörde.

Gemäß Artikel 3 Absatz 12 der Verordnung (EU) 2018/763 erkennt die ausstellende Behörde jedoch für die Zwecke der Bewertung von Anträgen auf einheitliche Sicherheitsbescheinigungen die von Eisenbahnunternehmen oder deren Auftragnehmern, Partnern oder Lieferanten vorgelegten Bescheinigungen, Anerkennungen oder Genehmigungen für Produkte oder Dienstleistungen, die im Einklang mit den einschlägigen Rechtsvorschriften der Union ausgestellt wurden, als Nachweis dafür an, dass die Eisenbahnunternehmen in der Lage sind, die entsprechenden Anforderungen des Sicherheitsmanagementsystems an die jeweilige Art von Produkt oder Dienstleistung zu erfüllen. Obwohl es im EU-Recht keine gleichwertige Bestimmung für die Bewertung von Anträgen auf Sicherheitsgenehmigungen gibt, werden die nationalen Sicherheitsbehörden ebenfalls ermutigt, das gleiche Prinzip anzuwenden.

Die folgende Tabelle zeigt die verschiedenen Fälle, die bisher im EU-Rechtsrahmen bestehen, und zeigt veranschaulichende Beispiele für die Arten von Produkten oder Dienstleistungen, die von Fall zu Fall abgedeckt werden können.

Tabelle 5: Im Einklang mit den Rechtsvorschriften der Union ausgestellte Genehmigungen, Anerkennungen oder Bescheinigungen für Produkte oder Dienstleistungen

Fall	*Art von Produkten oder Dienstleistungen*	*Geltendes Unionsrecht*	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
ECM-Zertifikat	Instandhaltung von Fahrzeugen	Artikel 14 Absatz 4 der Richtlinie (EU) 2016/798 Veordnung (EU) 2019/779	5.2 5.3	In den in Artikel 14 Absatz 4 der Richtlinie (EU) 2016/798 vorgesehenen Fällen liefert die Zertifizierung von Stellen, die mit der Instandhaltung betraut sind, ausreichende Nachweise dafür, dass Eisenbahnunternehmen und Infrastrukturbetreiber durch ihr Sicherheitsmanagementsystem in der Lage sind, die mit der Instandhaltung von Fahrzeugen verbundenen Risiken, einschließlich des Einsatzes von Auftragnehmern, zu kontrollieren.

Fall	*Art von Produkten oder Dienstleistungen*	*Geltendes Unionsrecht*	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
Anerkennung	Schulung von Triebfahrzeugführern	Richtlinie 2007/59/EG Beschluss 2011/765/EU	4.2.2	Schulungszentren sollten von der zuständigen Aufsichtsbehörde für die Bereitstellung von Schulungskursen für Triebfahrzeugführer und die Ausbildung von sich bewerbenden Triebfahrzeugführern in Übereinstimmung mit Richtlinie 2007/59/EG anerkannt werden. Schulungszentren spielen eine wichtige Rolle bei der Gewährleistung, dass Triebfahrzeugführer für die ihnen übertragenen sicherheitsrelevanten Aufgaben kompetent sind. In dieser Hinsicht sollten Schulungszentren hinsichtlich der Schulungen, die sie durchführen, kompetent sein und ihre Anerkennung durch eine zuständige Aufsichtsbehörde sollte, wo relevant, von der Sicherheitsbescheinigungsstelle und der nationalen Sicherheitsbehörde berücksichtigt werden, wenn eine Bewertung des Kompetenzmanagementsystems durchgeführt wird.

Fall	*Art von Produkten oder Dienstleistungen*	*Geltendes Unionsrecht*	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
Lizenz und Bescheinigung des Triebfahrzeugführers	Kompetenz und Eignung von Triebfahrzeugführern	Richtlinie 2007/59/EG	4.2.1	Lizenzen und Bescheinigungen, die in Übereinstimmung mit Richtlinie 2007/59/EG ausgestellt werden, bieten ausreichend Nachweise für die Eignung und Kompetenz von Triebfahrzeugführern. Dies schließt nicht aus, dass die Organisation nachweist, dass ihre Vorkehrungen für Kompetenz und Eignung angemessen sind.

Fall	*Art von Produkten oder Dienstleistungen*	*Geltendes Unionsrecht*	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
Einheitliche Sicherheitsbescheinigung	Instandhaltung und Inspektion der Infrastruktur Rangieren Prüfung von Schienenfahrzeugen	Artikel 10 der Verordnung (EU) 2016/798	5.3	Infrastrukturbetreiber können die Instandhaltung oder Inspektion ihrer Infrastruktur an Unternehmen weiter vergeben, die Sonderfahrzeuge auf den Strecken betreiben. Von Rangier- oder Prüfbetreibern kann ebenfalls gefordert werden, dass sie über eine Sicherheitsbescheinigung verfügen. In den obigen Fällen liefert die einheitliche Sicherheitsbescheinigung einen ausreichenden Nachweis, dass Eisenbahnunternehmen und Infrastrukturbetreiber in der Lage sind, durch ihr Sicherheitsmanagementsystem die Risiken in Bezug auf den Einsatz von Auftragnehmern und Lieferanten zu kontrollieren.

Fall	*Art von Produkten oder Dienstleistungen*	*Geltendes Unionsrecht*	*Verordnung (EU) 2018/762 Anforderungs-ID*	*Kommentare*
Genehmigung für das Inverkehrbringen/Fahrzeugtypzulassung	Fahrzeug(typ)zulassung	Richtlinie (EU) 2016/797	5.2	Die Fahrzeug(typ)zulassung gewährleistet durch ihren Aufbau, ihre Gestaltung, sowie ihre Prüfung und Validierung die Übereinstimmung mit den grundlegenden Anforderungen aller geltenden Rechtsvorschriften (einschließlich der Sicherheit), sodass sie sicher auf den Schienennetzen, für die sie bestimmt ist, gemäß den in den technischen Unterlagen für das Fahrzeug/den Fahrzeugtyp festgelegten Einsatzgrenzen und -bedingungen verwendet werden kann.

In bestimmten Fällen reicht der Besitz einer gemäß dem Unionsrecht erteilten Bescheinigung (oder eines gleichwertigen Zertifikats) möglicherweise nicht aus, um alle Sicherheitsrisiken zu kontrollieren, die mit den an die Eisenbahnunternehmen und Infrastrukturbetreiber gelieferten Produkten oder den von ihnen in Anspruch genommenen Dienstleistungen verbunden sind.

Beispielsweise sind die Eisenbahnunternehmen in Partnerschaft weiterhin voll verantwortlich für den sicheren Betrieb und damit für die Beherrschung der mit ihren Tätigkeiten verbundenen Risiken, einschließlich der Versorgung der Fahrzeuge mit Wartungsarbeiten. Die Verwendung der einheitlichen Sicherheitsbescheinigung des Partners durch ein Eisenbahnunternehmen als Mittel zur Beherrschung der mit der Erbringung von Instandhaltungsleistungen verbundenen Risiken ist nicht ausreichend, wenn sie nicht durch wirksame und wirksame vertragliche Vereinbarungen zwischen den Partnern gestützt wird. Diese vertraglichen Vereinbarungen müssen bei der Anwendung der Verfahren des Sicherheitsmanagementsystems jedes Partners gemeinsam entwickelt und überwacht werden und sind auch Bestandteil jedes Sicherheitsmanagementsystems und unterliegen daher der Aufsicht der jeweiligen nationalen Sicherheitsbehörde.

Die einheitliche Sicherheitsbescheinigung kann demnach als Mittel zur Kontrolle der Risiken in Verbindung mit der Bereitstellung von Instandhaltungsarbeiten und als Konformitätsmittel zur Erfüllung der

Anforderungen hinsichtlich der Kontrolle von Risiken in Verbindung mit der Instandhaltung von Fahrzeugen verwendet werden, wenn die drei folgenden Bedingungen erfüllt sind:

1. *Es müssen vertragliche Vereinbarungen zwischen verpartnerten Eisenbahnunternehmen gelten, die Aspekte in Bezug auf die Instandhaltung von Fahrzeugen umfassen, wie beispielsweise:*

   a) *Informationsaustausch nach Artikel 5 der Verordnung (EU) 2019/779;*
   b) *Ggf. technischer Support, insbesondere für Zugsteuerungs-/Zugsicherungs-Altsysteme;*
   c) *Kontrolle der Fähigkeit unter Vertrag genommener Instandhaltungswerkstätten, Instandhaltungsarbeiten durchzuführen;*
   d) *effektive Überwachung von Fahrzeugen und Informationsaustausch, der sich aus dieser Überwachung ergibt.*

2. *Diese vertraglichen Vereinbarungen werden als Ergebnis der Risikobewertung entwickelt und müssen regelmäßig von jedem Eisenbahnunternehmen anhand der CSM für die Kontrolle (Verordnung (EU) Nr. 1078/2012) überwacht werden. Das Ergebnis dieser Überwachung wird dann zwischen beiden verpartnerten Eisenbahnunternehmen förmlich ausgetauscht.*
3. *Das Sicherheitsmanagementsystem beider Partner enthält angemessene Prozesse und Verfahren, um die vorstehend genannten Bedingungen 1 und 2 zu erreichen.*

In anderen Fällen kann das nationale Recht für eine bestimmte Art von Produkten oder Dienstleistungen verlangen, dass der Besitz einer nationalen Bescheinigung (oder eines gleichwertigen Zertifikats) von einer zuständigen Stelle (z. B. der nationalen Sicherheitsbehörde) ausgestellt wird, die auch als Nachweis dafür dienen könnte, dass die Eisenbahnunternehmen oder Infrastrukturbetreiber in der Lage sind, die einschlägigen Anforderungen der Verordnung (EU) 2018/762 zu erfüllen. Beispielsweise können nationale Bescheinigungen, die ECM und/oder Instandhaltungswerkstätten von anderen Fahrzeugen als Güterwagen erteilt werden, ähnlich wie das ECM-Zertifikat auch eine angemessene Gewähr dafür bieten, dass die Fahrzeuge, für die sie mit der Instandhaltung betraut sind, in einem sicheren Betriebszustand sind.

Anhang 3 – Betrieb auf Anschlussgleisen, vertragliche Vereinbarungen und Partnerschaften

Betrieb auf Anschlussgleisen

In diesem Dokument bedeutet „Anschlussgleise“ eine Eisenbahninfrastruktur, die an ein Eisenbahnnetz angeschlossen ist, das in die Zuständigkeit eines Infrastrukturbetreibers fällt (d. h. der Infrastrukturteil des Eisenbahnsystems fällt in den Anwendungsbereich der Richtlinie (EU) 2016/798). Anschlussgleise können Teil dieses Schienennetzes sein oder auch nicht, je nach Umsetzung der oben genannten Richtlinie in den einzelnen Mitgliedstaaten.

Tätigkeiten, die in Anschlussgleisen durchgeführt werden, wie z. B. das Beladen von Waggons, sind industrielle Tätigkeiten, die sich dann mit spezifischen Eisenbahntätigkeiten verbinden, wie z. B. die Zusammensetzung, Vorbereitung und Bewegung von Fahrzeuggruppen, die Züge sein können oder in Zügen eingesetzt werden sollen. Dies umfasst das Kuppeln verschiedener Fahrzeuge, um Fahrzeuggruppen oder Züge zu bilden, sowie deren Bewegung.

Diese Anschlussgleise können insbesondere Folgendes umfassen:

- *Infrastruktur zum Parken von Eisenbahnfahrzeugen zwischen Einsätzen.*
- *intermodale Terminals;*
- *Infrastruktur für Servicearbeiten an Fahrgastfahrzeugen wie Reinigung oder kleinere Instandhaltungsarbeiten;*
- *Infrastruktur, die zu einer Instandhaltungswerkstatt für Eisenbahnfahrzeuge gehört und von dieser verwaltet wird;*
- *Industriebereiche oder -anlagen, in denen die industriellen Tätigkeiten des Beladens/Entladens von Güterwagen durchgeführt werden.*

Diese in Anschlussgleisen durchgeführten Tätigkeiten werden von einem Anschlussgleisbetreiber vorgenommen. Ein Anschlussgleisbetreiber kann ein Eisenbahnunternehmen, ein Infrastrukturbetreiber, ein Dienstleister (z. B. Reinigung von Fahrgastfahrzeugen), eine industrielle Organisation (z. B. eine chemische Anlage, die Tankwagen belädt/entlädt) oder sogar ein Unterauftragnehmer dieser industriellen Organisation sein. Im ersteren Fall hat die Organisation die Geschäftsentscheidung getroffen, ein Eisenbahnunternehmen zu werden oder ist ein Eisenbahnunternehmen, das plant, Anschlussgleise zusätzlich zu seinen aktuellen Eisenbahntätigkeiten zu verwalten. Im letzteren Fall ist der Infrastrukturbetreiber der Infrastrukturbetreiber für die Anschlussgleise oder handelt unter seiner Sicherheitsgenehmigung als Eisenbahnunternehmen.

Der Anschlussgleisbetreiber kontrolliert die Risiken in Bezug auf die Gesundheit und Sicherheit am Arbeitsplatz durch sein Sicherheitsmanagementsystem für Gesundheit und Sicherheit gemäß der internationalen und nationalen Gesetzgebung. Wenn der Anschlussgleisbetreiber kein Eisenbahnunternehmen ist, berücksichtigt dieses Managementsystem die Verpflichtungen hinsichtlich der Gesundheit und Sicherheit in Bezug auf externe Arbeiter, insbesondere die von Eisenbahnunternehmen, zum Beispiel wenn Triebfahrzeugführer in die Anschlussgleise einfahren. Parallel dazu kontrolliert das Eisenbahnunternehmen die Risiken in Bezug auf die Gesundheit und Sicherheit am Arbeitsplatz durch sein Sicherheitsmanagementsystem für Gesundheit und Sicherheit gemäß der internationalen und nationalen Gesetzgebung.

Fall 1: Der Anschlussgleisbetreiber ist ein Eisenbahnunternehmen „Y“.

Dieses Eisenbahnunternehmen kontrolliert durch sein Sicherheitsmanagementsystem die Risiken in Bezug auf seinen Eisenbahnbetrieb in seiner Anschlussgleisinfrastruktur und im Eisenbahnnetz unter der Verantwortung eines Infrastrukturbetreibers. Diese Risikokontrolle umfasst Risiken, die mit Schäden an Fahrzeugen verbunden sind, die durch alle Tätigkeiten im Anschlussgleis verursacht werden, einschließlich der Zusammensetzung, Vorbereitung und des Betriebs von Zügen.

In der Praxis ist es manchmal schwierig, das verantwortliche Eisenbahnunternehmen zu bestimmen. Ein Zug eines Eisenbahnunternehmens „X“ kommt zum Beispiel in einem Anschlussgleis an (Triebfahrzeugführer und

Lokomotive wurden gemietet) und ein Eisenbahnunternehmen „Y“, das das Anschlussgleis betreibt, übernimmt ihn als neuen Zug (Triebfahrzeugführer und Lokomotive wurden gemietet), während gleichzeitig der Anschlussgleisbetrieb fortgeführt werden muss. In einem solchen Fall gilt das obige Sicherheitsprinzip. Es gibt gemeinsame Schnittstellenrisiken, die im Sicherheitsmanagementsystem des Eisenbahnunternehmens „Y“ berücksichtigt werden müssen (z. B. Schäden an Fahrzeugen durch Anschlussgleistätigkeiten wie Beladen). Darüber hinaus muss auch die Übermittlung von Informationen über die Fahrzeuge von Eisenbahnunternehmen „X“ an Eisenbahnunternehmen „Y“ in Betracht gezogen werden. Dazu gehört die Zusicherung, dass sich das Fahrzeug in einem sicheren Betriebszustand befindet, wenn das Eisenbahnunternehmen „X“ es an den Anschlussgleisbetreiber übergibt und ebenso, wenn es über das Eisenbahnunternehmen „Y“ weiterbefördert wird. Das für den Anschlussgleisbetrieb verantwortliche Eisenbahnunternehmen „Y“ bleibt für die Kontrolle der Risiken der anschließend durchgeführten Instandhaltungstätigkeiten vollumfänglich rechenschaftspflichtig.

Fall 2: Der Anschlussgleisbetreiber ist kein Eisenbahnunternehmen.

Es können vier Unterfälle in Betracht gezogen werden:

- ***Unterfall 2.1****, wenn der Anschlussgleisbetreiber der Infrastrukturbetreiber ist.*
- ***Unterfälle 2.2 und 2.3****, wenn der Anschlussgleisbetreiber, der kein Infrastrukturbetreiber ist, Tätigkeiten nur in seiner eigenen Infrastruktur durchführt, aber nicht im Eisenbahnnetz unter der Verantwortung des Infrastrukturbetreibers.*
- ***Unterfall 2.4*** *umfasst Eisenbahntätigkeiten, die von einem Anschlussgleisbetreiber, der kein Infrastrukturbetreiber ist, im Eisenbahnnetz unter der Verantwortung des Infrastrukturbetreibers durchgeführt werden.*

Unterfall 2.1: Werden die Tätigkeiten in den Anschlussgleisen zwischen Eisenbahnunternehmen und einem Infrastrukturbetreiber (oder einer in seinem Auftrag handelnden Organisation) aufgeteilt, so ist jedes Eisenbahnunternehmen über alle Sicherheitsereignisse zu unterrichten, die während der Tätigkeit des Infrastrukturbetreibers im Rahmen vertraglicher Vereinbarungen stattgefunden haben. Dies umfasst Schäden, Unfälle und Störungen in Verbindung mit Fahrzeugen.

Diese vertraglichen Vereinbarungen werden vom Sicherheitsmanagementsystem jedes Eisenbahnunternehmens bzw. dem Sicherheitsmanagementsystem des Infrastrukturbetreibers verwaltet.

Durch sein Sicherheitsmanagementsystem kontrolliert das Eisenbahnunternehmen die Risiken in Verbindung mit seinem eigenen Betrieb hinsichtlich der erhaltenen Informationen.

Unterfall 2.2: Die Zugzusammensetzung und -vorbereitung erfolgt durch das Eisenbahnunternehmen (Kopplung, Vorbereitung) auf der Anschlussgleisinfrastruktur. Das Eisenbahnunternehmen muss über alle (Sicherheits-)Ereignisse informiert werden, die während der Tätigkeiten des Anschlussgleisbetreibers (z. B. Beladen oder Reinigung) im Rahmen der vertraglichen Vereinbarungen aufgetreten sind. Dies umfasst Schäden, Unfälle und Störungen in Verbindung mit Fahrzeugen.

Diese vertraglichen Vereinbarungen werden durch das Sicherheitsmanagementsystem des Eisenbahnunternehmens verwaltet.

Durch sein Sicherheitsmanagementsystem kontrolliert das Eisenbahnunternehmen die Risiken, die mit seinen eigenen Folgeoperationen in Bezug auf die erhaltenen Informationen verbunden sind.

Unterfall 2.3: Die Zusammensetzung des Zuges wird vollständig/teilweise vom Anschlussgleisbetreiber oder einer Organisation im Namen des Anschlussgleisbetreibers vorgenommen.

Nachdem ein Zug zusammengesetzt wurde, wird er an ein Eisenbahnunternehmen übergeben.

Wie bei Unterfall 2.2 muss das Eisenbahnunternehmen über alle Ereignisse informiert werden, die während der Tätigkeiten des Anschlussgleisbetreibers (z. B. Beladen oder Reinigung) und während der

Zugzusammensetzung im Rahmen der vertraglichen Vereinbarungen aufgetreten sind. Ereignisse umfassen Schäden, Unfälle und Störungen in Verbindung mit Fahrzeugen.

Diese vertraglichen Vereinbarungen werden durch das Sicherheitsmanagementsystem des Eisenbahnunternehmens verwaltet.

Durch sein Sicherheitsmanagementsystem kontrolliert das Eisenbahnunternehmen die Risiken in Verbindung mit seinem eigenen Betrieb hinsichtlich der erhaltenen Informationen.

Unterfall 2.4: Dieser Unterfall ergänzt Unterfall 2.3. Deshalb werden im Folgenden nur die zusätzlichen Dienste des Eisenbahnunternehmens eingeführt.

Der Anschlussgleisbetreiber fährt Züge oder bewegt Wagengruppen unter der Verantwortung eines Infrastrukturbetreibers von seiner Eisenbahninfrastruktur auf das Eisenbahnnetz.

Zum Beispiel:

- *Bewegt den Zug oder die Wagengruppen von einem Betriebshof zu den Bahnsteigen Personenbahnhofs oder zu einem an einen Personenbahnhof angeschlossenen Parkplatz;*
- *Bewegt den Zug oder die Wagengruppen von einer Industrieanlage zu einem Übergangspunkt (Wechselanschlussgleis) an einem Güterbahnhof.*

Der Anschlussgleisbetreiber ist weder ein Eisenbahnunternehmen noch ein Infrastrukturbetreiber, aber die im Netz eines Infrastrukturbetreibers durchgeführten Tätigkeiten müssen durch eine einheitliche Sicherheitsbescheinigung oder eine Sicherheitsgenehmigung abgedeckt werden.

Der Eisenbahnbetrieb des Anschlussgleisbetreibers im Eisenbahnnetz unter der Verantwortung eines Infrastrukturbetreibers wird entweder durch eine einheitliche Sicherheitsbescheinigung eines Eisenbahnunternehmens oder die Sicherheitsgenehmigung eines Infrastrukturbetreibers abgedeckt. Dies bedeutet, dass das Eisenbahnunternehmen oder der Infrastrukturbetreiber die Risiken, die mit den vom Anschlussgleisbetreiber durchgeführten Tätigkeiten verbunden sind, durch die Regelungen für die Verwaltung von Unterauftragnehmern in seinem Sicherheitsmanagementsystem kontrollieren muss.

In jedem Fall müssen die Eisenbahnunternehmen und der Infrastrukturbetreiber den Umfang ihres gesamten Eisenbahnbetriebs und ihrer Tätigkeiten, die eine Schnittstelle mit anderen Eisenbahntätigkeiten haben, genau beschreiben, um die Aufsicht über das Sicherheitsmanagementsystem durch die nationalen Sicherheitsbehörden wirksam zu machen. Die Fähigkeit von Eisenbahnunternehmen und Infrastrukturbetreibern, ihren Betrieb sowie andere mit dem Eisenbahnbetrieb zusammenhängende Tätigkeiten klar und vollständig zu beschreiben, ist von wesentlicher Bedeutung, um die Wirksamkeit des Sicherheitsmanagementsystems und die Effektivität der Aufsicht durch die nationalen Sicherheitsbehörden zu gewährleisten.

Die vertraglichen Vereinbarungen in allen oben aufgeführten Unterfällen müssen unmissverständlich Folgendes umfassen (sind jedoch nicht darauf beschränkt):

- *was von jeder Vertragspartei getan werden muss;*
- *die erwartete Qualität der Ergebnisse/Dienstleistungen;*
- *Zuweisung der Rollen und Verantwortlichkeiten;*
- *was, wann und wie Informationen zwischen den Vertragsparteien ausgetauscht werden. Die Informationen umfassen die Berichterstattung über Ereignisse, wie sie in allen oben genannten Unterfällen beschrieben sind, und die besonderen Merkmale der Infrastruktur des Anschlussgleises wie Geschwindigkeitsbegrenzungen, Gewichtsbegrenzungen oder Steigungsbedingungen;*
- *kompetenzbezogene Anforderungen;*
- *Anforderungen an die Gesundheit und Sicherheit (abgeleitet aus der Risikobewertung, nationalen Anforderungen usw.).*

Vertragliche Vereinbarungen und Partnerschaften

Das Eisenbahnunternehmen ist für die Gewährleistung der sicheren Fahrt des Zuges durch die Koordination und Verwaltung des Zugbetriebs verantwortlich. Vertragliche Vereinbarungen (in der Regel bestehend aus Rahmenvereinbarungen, Sondervereinbarungen und Anhängen) bilden die Grundlage für eine wirksame Zusammenarbeit zwischen verschiedenen Eisenbahnunternehmen, seien es neue Marktteilnehmer oder etablierte Betreiber, und müssen den Bestimmungen des europäischen und nationalen Rechts sowie allen anderen anwendbaren Anforderungen entsprechen.

Deshalb muss das Eisenbahnunternehmen die Risiken seines Betriebs kontrollieren, einschließlich der Zusammenarbeit mit Partnern und des Einsatzes von (Unter-)Auftragnehmern. Die nationale Sicherheitsbehörde kontrolliert dann, dass das Eisenbahnunternehmen seine rechtlichen Verpflichtungen auf transparente und gewissenhafte Weise erfüllt.

Eisenbahnunternehmen können ihre Sicherheitsverantwortlichkeit für die Koordination und Verwaltung der sicheren Fahrt von Zügen nicht auslagern. Dies ist jedoch für das Bestehen von Kooperationsvereinbarungen zwischen Eisenbahnunternehmen nicht hinderlich. Die obigen Grundsätze gelten auch für die Zusammenarbeit zwischen Eisenbahnunternehmen. Das für die Gewährleistung der sicheren Fahrt der Züge verantwortliche Eisenbahnunternehmen muss in allen Vereinbarungen zwischen beteiligten Parteien klar benannt werden und über eine einheitliche Sicherheitsbescheinigung verfügen. Entweder verwaltet dieses Eisenbahnunternehmen die Ressourcen (Personal, Fahrzeuge) direkt über sein Sicherheitsmanagementsystem oder es kann beschließen, die Nutzung der Ressourcen (z .B. Leasing von Fahrzeugen, Vermietung von Triebfahrzeugführern) ganz oder teilweise an eine andere Partei weiterzuvergeben. Im letzteren Fall trägt das Eisenbahnunternehmen immer noch die Verantwortung für die Kontrolle der Risiken in Verbindung mit dem Einsatz von (Unter-)Auftragnehmern durch die Überwachung der Vertragserfüllung in Übereinstimmung mit Verordnung (EU) Nr. 1078/2012 über sein Sicherheitsmanagementsystem und muss demnach prüfen, ob diese Ressourcen den rechtlichen und anderen geltenden Sicherheitsanforderungen entsprechen (z. B. Fahrzeuge in einem sicheren Betriebszustand, Streckenkompatibilität, Mitarbeiterschulung, Triebfahrzeugführer mit einer gültigen Lizenz und Bescheinigung für eine bestimmte Strecke).

Eine einheitliche Sicherheitsbescheinigung, die von einer Sicherheitszertifizierungsstelle (und entsprechend von einer nationalen Sicherheitsbehörde beaufsichtigt) an den Vertragspartner (d. h. den Partner oder Unterauftragnehmer) ausgestellt wird, kann dem für den sicheren Betrieb verantwortlichen Eisenbahnunternehmen eine ausreichende Gewähr dafür bieten, dass die Vorkehrungen des Sicherheitsmanagementsystems den einschlägigen Anforderungen entsprechen. Die vertraglichen Vereinbarungen umfassen die Übermittlung von sicherheitsrelevanten Informationen (z. B. vorherige Ruhezeit der Triebfahrzeugführer) zwischen den Vertragsparteien.

Die Grundsätze für die Zusammenarbeit zwischen den Eisenbahnunternehmen bleiben unabhängig von den Kooperationsregelungen, d. h. Partnerschaft oder Untervergabe (ganz oder teilweise) von Eisenbahntätigkeiten im nationalen oder grenzüberschreitenden Verkehr, unverändert. Art und Umfang der von den Eisenbahnunternehmen durchzuführenden Maßnahmen sowie der Umfang, in dem die nationale Sicherheitsbehörde diese Kooperationsvereinbarungen zu überwachen hat, stehen jedoch in einem angemessenen Verhältnis zum Grad der Zusammenarbeit zwischen den Eisenbahnunternehmen.

Beispielsweise wird die grenzüberschreitende Zusammenarbeit zwischen Eisenbahnunternehmen (d. h. der Einsatz von externen Fahrzeugen und/oder Personal) wahrscheinlich mehr Kontrollen erfordern als andere Kooperationsregelungen, da der Betrieb an ein anderes Eisenbahnunternehmen mit unterschiedlichen Sprachen und Betriebsvorschriften für Schienenfahrzeuge übergeben wird, die sich von Mitgliedstaat zu Mitgliedstaat unterscheiden können. Im Gegensatz dazu würde das Einstellen von externen Triebfahrzeugführern oder das Mieten von entsprechenden Fahrzeugen natürlich weniger Überwachung und damit weniger Überwachungstätigkeiten durch die nationale Sicherheitsbehörde erfordern.

Anhang 4 – Sicherheitskultur

Einführung zu Sicherheitskultur und einer Strategie zur Verbesserung der Sicherheitskultur

Kultur entsteht aus den Interaktionen der Menschen im Alltag und hilft, die Verhaltenserwartungen und -normen der Gesellschaft zu definieren. Kultur ist ein komplexes Konzept mit zahlreichen Faktoren, das sich im Laufe der Zeit in Abhängigkeit von den Umständen, dem Umfeld und den Erfahrungen einer Nation, eines Staates, einer Gesellschaft und/oder einer Organisation entwickelt.

Sicherheitskultur bezieht sich auf die Elemente der Kultur, die sich speziell mit Sicherheit befassen. Während es möglich ist, einige der mitwirkenden Faktoren einer Sicherheitskultur zu beschreiben, ist es unmöglich, alle Informationen zu sammeln, die eine Sicherheitskultur verkörpern. Es gibt kein alleingültiges wissenschaftliches und objektives Maß für das Konzept der Sicherheitskultur. Denn die Faktoren, die dazu beitragen, variieren nicht nur zwischen den Organisationen, sondern auch innerhalb der Organisationen. Verschiedene Abteilungen haben verschiedene Sicherheitsanforderungen und -bedürfnisse, beispielsweise betrieblicher und finanzieller Art, und die aktuelle Sicherheitskultur entwickelt sich daraus. Externe Faktoren wie regulatorische Anforderungen, Bildungsniveaus, gesellschaftliche Strukturen sowie die nationale Kultur tragen ebenfalls zur Herausbildung der Sicherheitskultur einer Organisation bei.

Die Sicherheitskultur ist ein etabliertes Konzept. Es mangelt ihr jedoch an einer einheitlichen Definition. Vor diesem Hintergrund hat die Agentur zusammen mit Vertretern des Sektors folgendes Verständnis entwickelt, das von allen Eisenbahnorganisationen herangezogen werden kann: „*Der Begriff Sicherheitskultur bezieht sich auf die Wechselbeziehungen zwischen den Anforderungen des SMS (Sicherheitsmanagementsystems), darauf, wie Menschen aufgrund ihrer Einstellungen, Werte und Ansichten deren Sinn verstehen, und auf das, was sie dann tatsächlich tun, was sich dann in Entscheidungen und Verhaltensweisen niederschlägt*."

Eine einfache Art und Weise, Sicherheitskultur zu beschreiben, besteht darin, die Faktoren zu betrachten, die zum Verhalten beitragen. Das Sicherheitsmanagementsystem bietet durch die Definition und Vorgabe der erforderlichen Elemente anhand von Strategien und Verfahren die Grundlage dafür. In einer Utopie wäre das Sicherheitsmanagementsystem perfekt und alle Mitarbeiter würden sich daran halten. Leider ist eine Utopie eine Utopie und das Management und die Mitarbeiter versuchen, den Inhalt des Sicherheitsmanagementsystems basierend auf ihren Werten, Haltungen und Überzeugungen auf Grundlage persönlicher Erfahrungen in Kombination mit den Verhaltensnormen des Arbeitsplatzes und der Gesellschaft zu verstehen. Wenn das Sicherheitsmanagementsystem Sinn ergibt und eine Konformitätskultur vorhanden ist, dann werden die korrekten Verhaltensweisen folgen. Wenn nicht, wird individuell interpretiert und es werden alternative Lösungen angewandt. Diese werden auf einer individuellen Risikobewertung basieren, die Faktoren abwägt, welche sich auf die getroffenen Entscheidungen auswirken. Die Risikobewertung wird sich nicht nur auf das eigentliche Risiko konzentrieren, sondern auch Faktoren in Verbindung mit Bequemlichkeit, dem Risiko, erwischt zu werden, den Worten und Taten des Managements, usw. umfassen. Die gegenseitige Abhängigkeit zwischen dem Sicherheitsmanagementsystem, dem Verständnis und dem Verhalten definiert daher die Sicherheitskultur.

Will man „Sicherheitskultur" bewerten, so benötigt man einen Einblick in die drei Faktoren und ihre gegenseitige Abhängigkeit. Wie weiter oben angemerkt, gibt es kein alleingültiges wissenschaftliches und objektives Maß für das Konzept der Sicherheitskultur. Stattdessen können Eigenschaften, die einen Einfluss auf die Entwicklung der Sicherheitskultur haben, unter Berücksichtigung der drei Faktoren analysiert werden.

So kann z. B. nach einer Grundsatzerklärung wie „Safety first" untersucht werden, was sie für die Mitarbeiter bedeutet – glauben sie tatsächlich daran, lässt das Management Worten Taten folgen, wie werden Entscheidungen getroffen und aus welchen Gründen, wie reagiert die Organisation, wenn sie unter Druck steht usw. Ähnliche Untersuchungen können auch zu anderen Faktoren wie kontinuierlichem Lernen und einer hinterfragenden Haltung angestellt werden. Die Kombination der Analyseergebnisse ergibt ein Bild des gegenwärtigen Zustands der Kultur. Im Laufe der Zeit kann ein umfassenderes Bild erstellt werden, das stärkere Schlussfolgerungen zulässt.

Das Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr (siehe Abbildung 4) wurde als konzeptioneller und Evaluierungsrahmen entwickelt, der genutzt werden kann, um das Konzept der Sicherheitskultur besser zu verstehen und die Sicherheitskultur von Eisenbahnorganisationen zu bewerten und zu verbessern.

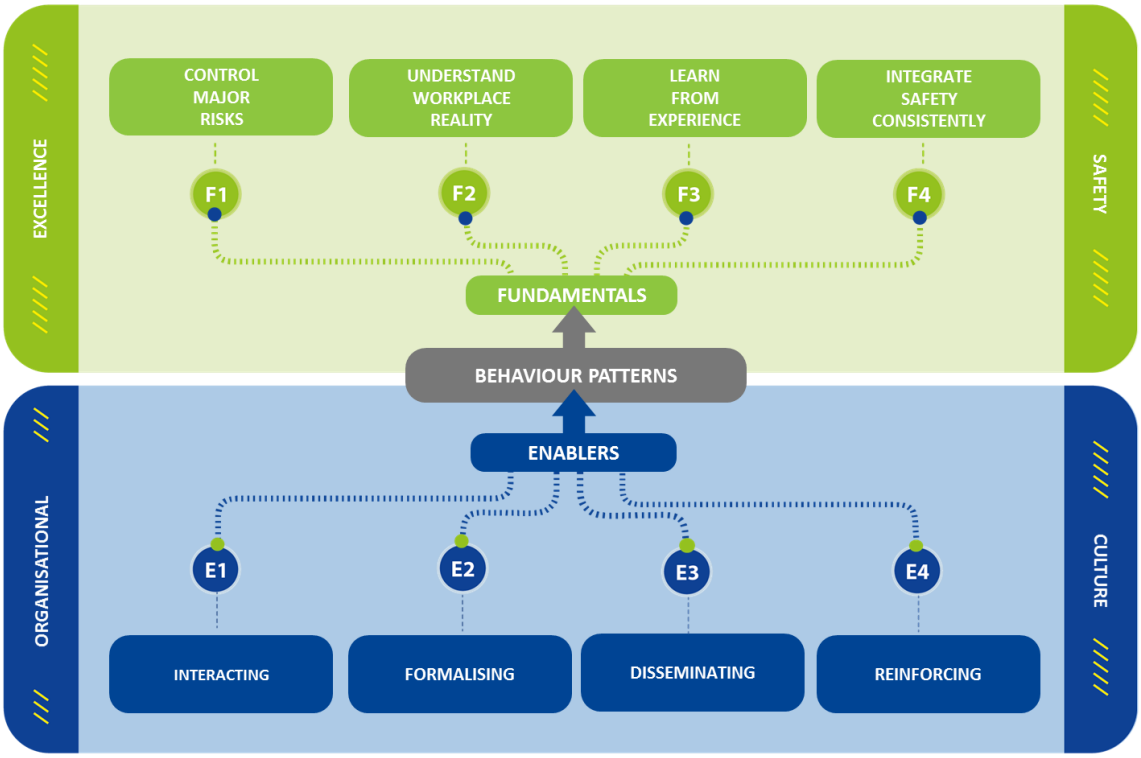

Abbildung 4: das Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr

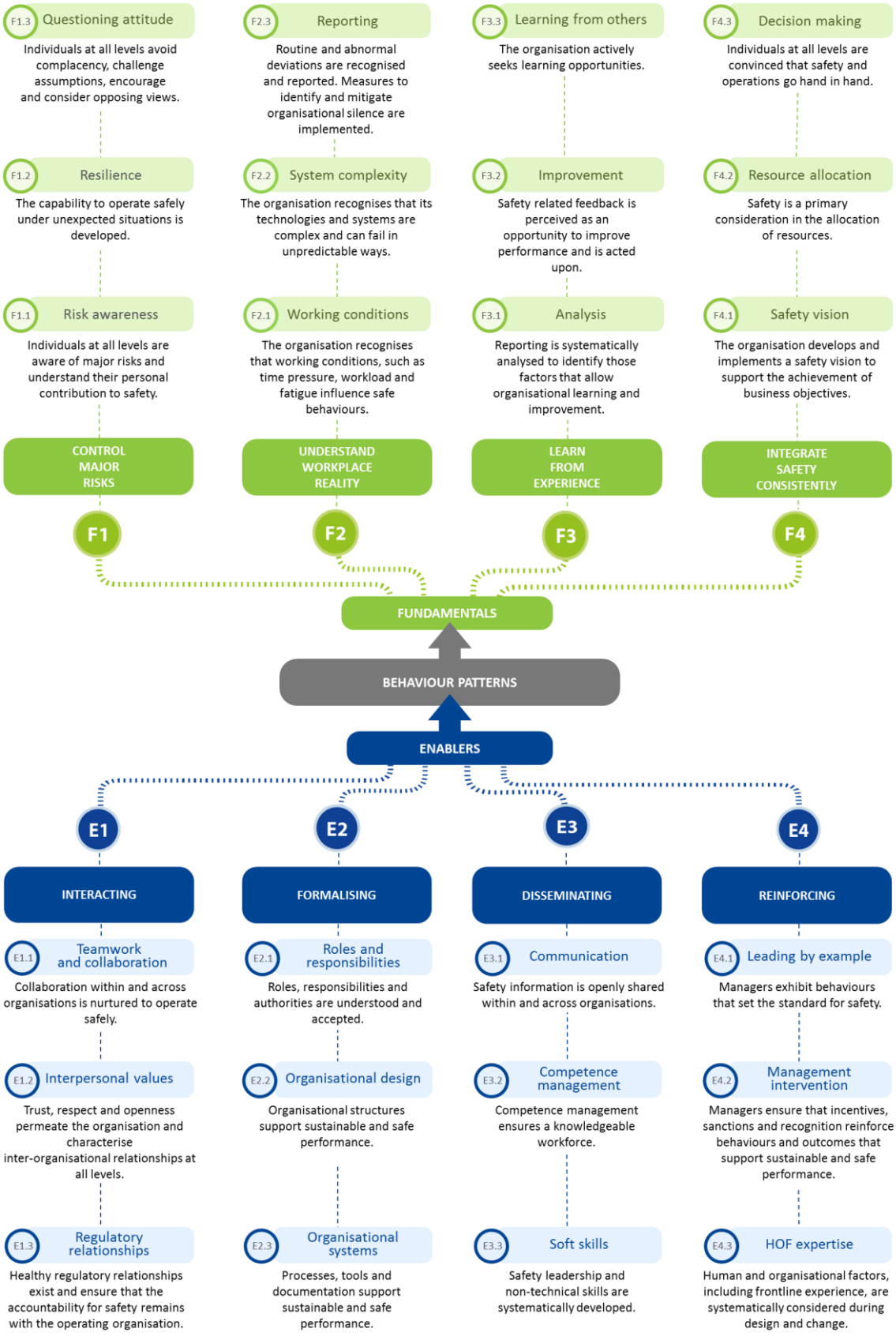

Abbildung 5: Eigenschaften des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr

Direkter Vergleich der SMS-Anforderungen mit dem Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr

Die nachstehenden Tabellen bieten einen direkten Vergleich zwischen den Grundvoraussetzungen und Wegbereitern des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr und den in der Verordnung (EU) 2018/762 festgelegten SMS-Anforderungen.

Die sorgfältige Verwendung der Tabellen sowie der Leitlinien zum Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr sollte es der Organisation ermöglichen zu erkennen, welche der SMS-Anforderungen in engem Zusammenhang mit den Eigenschaften des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr stehen, und es ihnen daher ermöglichen, Prozesse und Verfahren zu entwickeln, die den gewünschten organisatorischen Verhaltensweisen besser Rechnung tragen.

Tabelle 6: Direkter Vergleich – SMS-Anforderungen/Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr

Anforderung an das Sicherheitsmanagementsystem.	*Zusammenhang mit den Eigenschaften des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr*
1. Kontext der Organisation	F1.1, F2.2, F3.3 F4.1 E1.1, E2.1, E2.2, E3.1, E4.3
2.1 Führung und Verpflichtung	F1.1, F2.1, F2.2, F4.1 E1.1, E2.1, E3.1
2.2 Sicherheitsordnung	F1.1, F2.1, F2.2, F4.1 E1.1, E3.1
2.3 Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse	F1.1, F2.1, F2.2, F2.3, F3.1, F 3.2, F4.1, F4.2 E1.1, E2.1, E2.2, E3.1, E3.2, E4.3
2.4 Konsultation der Mitarbeiter und anderer Beteiligter	F1.1, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.2, E1.1, E2.2, E2.3, E3.1, E4.3
3.1 Maßnahmen zur Beherrschung von Risiken	F1.1, F2.1, F2.2, F2.3, F3.1, F3.2 F3.3, F4.1, F4.3 E1.1, E2.1, E2.2, E2.3, E3.1, E3.2, E4.3
3.2 Sicherheitsziele und Planung	F1.1, F2.1, F2.2, F2.3, F3.1, F 3.2, F4.1, F4.2 E1.1, E2.2, E2.3, E3.1, E4.3
4.1 Ressourcen	F1.1, F2.1, F2.2, F4.1, F4.2, E1.1, E1.2, E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.3
4.2 Kompetenz	F1.1,F1.2, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.2, F4.3 E1.1, E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
4.3 Bewusstsein	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E1.1, E1.2, E2.1, E3.1, E3.2, E3.3, E4.1, E4.2
4.4 Information und Kommunikation	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E3.1, E3.2, E3.3, E4.2
4.5 Dokumentierte Informationen	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.2
4.6 Integration menschlicher und organisatorischer Faktoren	F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.3
5.1 Betriebsplanung und -steuerung	F1.1, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2 E2.1, E2.3, E3.1, E3.2, E3.3, E4.3
5.2 Verwaltung von Sachanlagen	F2.1, F2.2, F4.1, F4.2, F4.3, E1.1, E2.3, E3.1, E3.2, E4.3

Anforderung an das Sicherheitsmanagementsystem.	*Zusammenhang mit den Eigenschaften des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr*
5.3 Auftragnehmer, Partner und Zulieferer	F1.1, F2.1, F2.2, F4.1, F4.2, F4.3 E1.1, E2.3, E3.1, E3.2, E4.3
5.4 Änderungsmanagement	F1.1, F2.1, F2.2, F4.1, F4.2, F4.3 E1.1, E2.3, E3.1, E3.2, E4.3
5.5 Notfallmanagement	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F3.3, F4.1, F4.2, F4.3 E1.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
6.1. Überwachung	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2 F4.3 E1.1, E1.2, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
6.2 Interne Auditierung	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3 E1.1, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
6.3. Managementbewertung	F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3 E1.1, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3
7.1. Lehren aus Unfällen und Störungen	F1.1, F1.3, F2.1, F2.2, F2.3, F3.1 , F3.2, F4.1, F4.3 E1.3, E2.1, E2.3, E3.1, E3.2, E3.3, E4.2, E4.3
7.2. Kontinuierliche Verbesserung	F1.1, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3 E2.1, E2.3, E3.1, E3.2, E3.3, E4.2, E4.3

Tabelle 7: Direkter Vergleich – Modell zur Sicherheitskultur im europäischen Eisenbahnverkehr/SMS-Anforderungen

Eigenschaften des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr	*Zusammenhang mit der SMS-Anforderung*
F 1.1 Risikobewusstsein	1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F1.2 Resilienz (Widerstandsfähigkeit)	4.1, 4.2, 4.3, 4.5, 4.6, 5.5, 6.1, 6.2, 6.3
F1.3 Hinterfragende Einstellung	5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F2.1 Arbeitsbedingungen	2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F2.2 Komplexität des Systems	1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F2.3 Berichterstattung	2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 7.1, 7.2
F3.1 Analyse	2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F3.2 Verbesserung	2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F3.3 Von anderen lernen	3.1, 5.5
F4.1 Sicherheitsvision	1, 2.1, 2.2,2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
F4.2 Ressourcenzuweisung	2.3, 2.4, 3.2, 4.1, 4.2, 5.1, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3
F4.3 Entscheidungsfindung	3.1, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2, 7.3
E1.1 Teamarbeit und Zusammenarbeit	1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E1.2 Interpersonelle Werte	4.1, 4.3, 6.1
E1.3 Regulatorische Beziehungen	7.1

Eigenschaften des Modells zur Sicherheitskultur im europäischen Eisenbahnverkehr	*Zusammenhang mit der SMS-Anforderung*
E2.1 Aufgaben und Verantwortlichkeiten	1, 2.1, 2.3, 3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.1, 6.2, 6.3, 7.1, 7.2
E2.2 Organisationsgestaltung	1, 2.1, 2.3, 2.4, 2.4, 3.1, 3.2, 4.1, 4.2, 4.4, 4.5
E2.3 Organisationssysteme	2.4, 3.1, 3.2, 4.1, 4.2, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.56.1, 6.2, 6.3, 7.1, 7.2
E3.1 Kommunikation	2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E3.2 Kompetenzmanagement	3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E3.3 Soft Skills/Nichttechnische Fähigkeiten	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.1, 6.2, 6.3, 7.1, 7.2
E4.1 Mit gutem Beispiel vorangehen	4.2, 4.3, 5.5, 6.1, 6.2, 6.3
E4.2 Intervention des Managements	4.2, 4.3, 4.4, 4.5, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2
E4.3 Expertise in Bezug auf menschliche und organisatorische Faktoren	1, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2

Weitere Informationen zur Sicherheitskultur sind der ERA-Website zu entnehmen.

Anhang 5 – Menschliche und organisatorische Faktoren

Einführung zu menschlichen und organisatorischen Faktoren

Menschliche und organisatorische Faktoren sind ein fachübergreifendes Feld, das sich darauf konzentriert, wie die Sicherheit verbessert, die Leistung gestärkt sowie die Benutzerzufriedenheit erhöht werden kann. Menschliche und organisatorische Faktoren ist ein benutzerzentrierter Ansatz, dessen Gestaltung auf einem expliziten Verständnis von Benutzern, Aufgaben und Umgebungen beruht. Ausgangspunkt sind immer die Fähigkeiten und Grenzen des Anwenders und die Art und Weise, wie diese beeinflusst werden und mit den Systemen interagieren, die bei der Ausführung der Aufgaben angetroffen werden. Das Ziel besteht darin, zu identifizieren, wie die Aufgabe am besten auf sichere und effiziente Weise erledigt wird. Der Schwerpunkt liegt dabei auf der Gebrauchstauglichkeit. Menschliche und organisatorische Faktoren werden sowohl als proaktives Mittel zur Sicherstellung guter Designprozesse als auch als reaktives Mittel zur Identifizierung von Schlüsselthemen eingesetzt, wenn etwas schief gelaufen ist.

Wenn beispielsweise neue Fahrzeuge entworfen werden, reicht es nicht aus, lediglich die Designstandards anzuwenden. Die Triebfahrzeugführer, Schaffner und Instandhaltungsmitarbeiter sollten einbezogen werden, um ihre Erfahrungen und ihr Verständnis der Art, wie die Aufgaben sicher und effizient durchgeführt werden können, einzubringen. Dies kann z. B. mit spezifischen Bahnhofs- oder Streckenproblemen, Zugänglichkeit und Zugang für Instandhaltungspersonal, Aufgabenprioritäten im Führerhaus, Kommunikationsanforderungen oder Fahrgastverhalten an Bahnhöfen zusammenhängen.

Die Einbeziehung des Wissens und der Erfahrung der verschiedenen Betreiber wird am besten durch einen iterativen Prozess erreicht, bei dem der Benutzer das Design und die Entwicklung des Zuges kontinuierlich bewertet, während Design und Entwicklung fortschreiten. Dies hilft, einen häufigen Fehler im Designprozess zu vermeiden, nämlich sich auf die Interaktion des Menschen mit einzelnen Systemen zu konzentrieren und nicht auf die Aufgabenerfüllung im Allgemeinen. Verschiedene Lieferanten haben beispielsweise unterschiedliche Vorstellungen davon, wie Alarme priorisiert werden sollten, und ohne eine ganzheitliche Perspektive wird der Anwender oft mit Informationen von eingeschränkter Relevanz für die Aufgabenerfüllung überladen. Nur weil das technische Design die Möglichkeit bietet, die Informationen anzuzeigen, heißt das nicht, dass der Benutzer diese benötigt. Die Analyse menschlicher und organisatorischer Faktoren hilft bei der Unterscheidung zwischen einer ausschlaggebenden und einer belanglosen Information.

Menschliche und organisatorische Faktoren bedeuten, eine systemische Perspektive einzunehmen, d. h. nicht nur die menschlichen, technologischen und organisatorischen Faktoren als solche zu betrachten, sondern auch die Wechselwirkungen zwischen den verschiedenen Faktoren hervorzuheben. Zum Beispiel, wenn ein Triebfahrzeugführer an einer Störung beteiligt war, wie z. B. ein bei Gefahr überfahrenes Signal, beziehen sich die zu untersuchenden Faktoren (keine umfassende Liste) auf Müdigkeit, kognitive Überlastung, Kompetenz, usw. (menschlich), den Einfluss der Technologie auf die Leistung, wie z. B. Mensch-System-Schnittstellen, Layout, Signalplatzierung (Technologie), den Einfluss der Organisation auf die Leistung, wie z. B. Schulung, Sicherheitsmanagementsystem organisatorische Prioritäten (Organisation) sowie die Interaktion zwischen den drei Bereichen, wie z. B. den Einfluss der Beschaffung auf die Gestaltung oder das Management von Veränderungen bei der Einführung eines neuen Designs.

Die Methoden stammen aus den verschiedensten Bereichen, wie z. B. experimentelle Psychologie, Wirtschaftsingenieurwesen, Organisationspsychologie, Soziologie, Betriebswirtschaft, Kognitionswissenschaften, Ergonomie, Informatik und Sicherheitstechnik.

Da der Schwerpunkt der menschlichen und organisatorischen Faktoren auf dem Anwender liegt, ist die Aufgabenanalyse eine häufig angewandte Methode. Eine Aufgabenanalyse liefert dem Konstrukteur ein Verständnis für die auszuführenden Aufgaben und deren Beziehung zu den Systemen, mit denen der Benutzer interagiert, sowie für die organisatorischen Bedingungen, die sich auf die Leistung auswirken. Basierend auf der Aufgabenanalyse kann eine weitere Analyse, wie Mensch-System-Interaktion,

Arbeitsbelastung, menschliche Zuverlässigkeit/Risiken, Anthropometrie und Biometrieanalysen, durchgeführt werden. Der Schlüssel liegt darin, sicherzustellen, dass der Benutzer die bestmögliche Arbeitssituation für eine sichere und effiziente Leistung hat.

Weitere Informationen zu menschlichen und organisatorischen Faktoren sind der ERA-Website zu entnehmen.

Strategie zur Unterstützung der Integration menschlicher und organisatorischer Faktoren in das Sicherheitsmanagementsystem

Die Organisation sollte eine Strategie entwickeln, die sicherstellt, dass Kenntnisse zu menschlichen Faktoren, Methoden und ein auf den Menschen ausgerichteter Ansatz systematisch und konsequent auf alle relevanten Prozesse innerhalb der Organisation angewendet werden. Ein solcher Ansatz bedeutet, zuerst die Bedürfnisse, Fähigkeiten und Verhaltensweisen der Menschen in Betracht zu ziehen und dann ein Design zu entwerfen, um diese Bedürfnisse, Fähigkeiten und Verhaltensweisen zu berücksichtigen.

Die Strategie für menschliche und organisatorische Faktoren kann Elemente enthalten mit Verbindung zu:

Führung

- *Führung und Verpflichtung*
  - *Die Verpflichtung des Managements gegenüber menschlichen und organisatorischen Faktoren wird in den Strategien und Zielen eindeutig angegeben.*
  - *Es gibt einen Prozess/Leitfaden, der aufzeigt, wie menschliche und organisatorische Faktoren in Projekten angewandt werden sollen.*
  - *Menschliche und organisatorische Faktoren sind ein integraler Bestandteil des Designprozesses und des Projektmanagements.*
- *Sicherheitsordnung*
  - *Die Sicherheitsordnung gibt eindeutig an, dass eine Perspektive in Bezug auf menschliche und organisatorische Faktoren in allen sicherheitsrelevanten Prozessen angewandt werden sollte.*
- *Organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse*
  - *Eindeutig definierte Aufgaben, Zuständigkeiten und Rechenschaftspflichten der Experten für menschliche und organisatorische Faktoren;*
  - *Es gibt einen Prozess dafür, wie Experten für menschliche und organisatorische Faktoren auf regelmäßiger Basis an Projekten und Prozessen teilnehmen.*

Planung

- *Maßnahmen zur Beherrschung von Risiken*
  - *Eine Beschreibung, wie die Perspektive in Bezug auf menschliche und organisatorische Faktoren in Risikoanalysen berücksichtigt wird;*
  - *das Hinzuziehen von Experten für menschliche und organisatorische Faktoren sowie Mitarbeitern an vorderster Front, einschließlich solcher mit Schnittstellen, bei Risikoanalysen.*

Unterstützung

- *Ressourcen und Befähigung*
  - *Systematischer Ansatz der Nutzung der Kompetenz im Bereich menschlicher und organisatorischer Faktoren, um sicherzustellen, dass für sicherheitsrelevante Aufgaben auf der Grundlage der Risikobewertung ausreichende Ressourcen vorgesehen werden.*
  - *Verknüpfung zwischen der Risikobewertung, den sicherheitsrelevanten Aufgaben und dem Kompetenzmanagementsystem, um sicherzustellen, dass das Personal die ermittelten Kompetenzen kontinuierlich nachweisen kann.*
  - *Es werden Zeit und Ressourcen zugewiesen, um sicherzustellen, dass die Anforderungen in Bezug auf menschliche und organisatorische Faktoren erfüllt werden.*
- *Sensibilisierung*
  - *Systematische Nutzung der Kompetenz im Bereich menschlicher und organisatorischer Faktoren innerhalb der Organisation, um sicherzustellen, dass sich die Mitarbeiter in relevanten Funktionen der Rolle bewusst sind, die sie für die Sicherheit spielen.*

Betrieb

- *Betriebsplanung und -steuerung*
  - *Menschliche und organisatorische Faktoren werden bei der betrieblichen Planung berücksichtigt.*
- *Verwaltung von Sachanlagen*
  - *Die Organisation hat Richtlinien für die Anwendung eines auf den Menschen ausgerichteten Ansatzes in jeder Phase des Lebenszyklus.*
- *Änderungsmanagement*
  - *Menschliche und organisatorische Faktoren müssen stets als Teil des Änderungsmanagementprozesses bewertet werden.*

Leistungsbewertung

- *Überwachung*
  - *Die Sicherheitsleistung wird systematisch im Rahmen der Strategie für menschliche und organisatorische Faktoren bewertet.*

Verbesserung

- *Lehren aus Unfällen und Störungen*
  - *Das Fachwissen und die Methoden zu menschlichen und organisatorischen Faktoren werden im Unfalluntersuchungsprozess verwendet.*
  - *Es gibt eine Methodik zur Durchführung von Untersuchungen basierend auf dem Fachwissen und den Methoden zu menschlichen und organisatorischen Faktoren.*
  - *Es gibt ein Schulungsprogramm für Unfall- und Störungsuntersuchungen, das eine Perspektive zu menschlichen und organisatorischen Faktoren anwendet.*
- *Kontinuierliche Verbesserung*
  - *Prozess zur ständigen Verbesserung der Prozesse der Organisation zur Verwaltung der menschlichen und organisatorischen Faktoren.*

Artikel 6 – Begriffsbestimmungen

Die Verwendung von Wörtern oder Begriffen wie „muss“ oder „sollte“ im gesamten Dokument zeigt an, dass eine gesetzliche Anforderung vorliegt, deren Einhaltung eine Notwendigkeit darstellt. Die Begriffsbestimmungen, die in den einschlägigen Rechtsvorschriften über die Eisenbahnsicherheit wie der Richtlinie (EU) 2016/798, der CSM für die Evaluierung und Bewertung von Risiken (Durchführungsverordnung (EU) Nr. 402/2013) und den einschlägigen technischen Spezifikationen für die Interoperabilität enthalten sind, finden auf dieses Dokument Anwendung, werden nachstehend jedoch nicht wiedergegeben.

Unfall	Ein unerwünschtes oder unbeabsichtigtes plötzliches Ereignis oder eine besondere Verkettung derartiger Ereignisse, die schädliche Folgen haben; Unfälle werden in folgende Kategorien eingeteilt: Kollisionen, Entgleisungen, Unfälle auf Bahnübergängen, Unfälle mit Personenschäden, unter Beteiligung von in Bewegung befindlichen Fahrzeugen, Brände und sonstige Unfälle (Richtlinie (EU) 2016/798).
Geografisches Tätigkeitsgebiet	Ein Netz oder mehrere Netze in einem oder mehreren Mitgliedstaaten, in denen ein Eisenbahnunternehmen seine Tätigkeit auszuüben beabsichtigt (Richtlinie (EU) 2016/798).
Verwaltung von Sachanlagen	Der von einer Organisation angewandte Ansatz, um sicherzustellen, dass physische Sachanlagen sicher, zweckmäßig und wirtschaftlich rentabel bleiben, von der Planung und Konstruktion über den gesamten Lebenszyklus bis hin zur Außerbetriebnahme.
Audit	Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und deren objektive Bewertung, um festzustellen, inwieweit die Auditkriterien erfüllt sind (ISO 9000).
Geschäftseinheit	Eine Geschäftseinheit bezeichnet eine Abteilung oder einen Funktionsbereich innerhalb einer Organisation. Sie kann unterschiedliche Aufgaben und Zwecke zum Gegenstand haben, z. B. Humanressourcen, Produktion, Fernverkehr, Logistik, Rangierbetrieb.
Art der Tätigkeit	Die Charakterisierung des Betriebs anhand seines Anwendungsbereichs, einschließlich Entwurf und Bau der Infrastruktur, Infrastrukturinstandhaltung, Verkehrsplanung, Verkehrsmanagement und Verkehrssteuerung, sowie anhand der Nutzung der Eisenbahninfrastruktur, einschließlich konventioneller und/oder Hochgeschwindigkeitsstrecken, Personen- und/oder Güterbeförderung.
Kompetenz	Fähigkeit, Wissen und Fertigkeiten anzuwenden, um die vorgesehenen Ergebnisse zu erzielen (ISO 9000).
Kontinuierliche Verbesserung	Wiederholende Tätigkeit zur Verbesserung der Leistung (d. h. messbares Ergebnis) (ISO 9000).
Dokumentenverwaltung	Der Prozess (oder das Verfahren) zur Identifizierung, Erstellung, Pflege, Verwaltung, Speicherung und Aufbewahrung von dokumentierten Informationen.

Betriebsumfang	In Bezug auf vom Eisenbahnunternehmen geführte Eisenbahnbetriebe der Umfang des Betriebs, gekennzeichnet durch die Beförderungsleistung im Personen-/Güterverkehr und/oder die überschlägige Größe eines Eisenbahnunternehmens hinsichtlich der Zahl der im Eisenbahnbereich tätigen Mitarbeiter (z. B. als ein Kleinstunternehmen, Kleinunternehmen, mittelgroßes Unternehmen oder Großunternehmen) (Richtlinie (EU) 2016/798). In Bezug auf den Eisenbahnbetrieb von Infrastrukturbetreibern der Umfang des Betriebs, der durch die Länge der Eisenbahnstrecken und die überschlägige Größe des Infrastrukturbetreibers hinsichtlich der Zahl der im Eisenbahnbereich tätigen Mitarbeiter gekennzeichnet ist (Verordnung (EU) 2018/762).
Gefährdung	Ein Umstand, der zu einem Unfall führen könnte (Verordnung (EU) 402/2013).
Menschliche und organisatorische Faktoren	Alle Eigenschaften des menschlichen Leistungsvermögens und organisatorischen Aspekte, die berücksichtigt werden müssen, um die lebenslange Sicherheit und Effektivität eines Systems oder einer Organisation zu gewährleisten.
Menschenzentrierter Ansatz	Ein Ansatz, der zuerst die Bedürfnisse, Fähigkeiten und Verhaltensweisen von Personen erfasst, um sodann konzeptionell diesen Bedürfnissen, Fähigkeiten und Verhaltensweisen gerecht zu werden.
Störung	Ein anderes Ereignis als ein Unfall oder schwerer Unfall, das den sicheren Eisenbahnbetrieb beeinträchtigt oder beeinträchtigen könnte (Richtlinie (EU) 2016/798). Dies umfasst Beinaheunfälle.
Infrastrukturbetreiber	Eine Stelle oder ein Unternehmen, die bzw. das insbesondere für die Einrichtung, Verwaltung und die Unterhaltung der Fahrwege der Eisenbahn, einschließlich Verkehrsmanagement, Zugsteuerung/Zugsicherung und Signalgebung, zuständig ist; mit den bei einem Netz oder Teilen eines Netzes wahrzunehmenden Funktionen des Infrastrukturbetreibers können verschiedene Stellen oder Unternehmen betraut werden (Richtlinie 2012/34/EU).
Interessengruppe	Person oder Organisation, die eine Entscheidung oder Tätigkeiten (ISO 9000) in Verbindung mit dem Sicherheitsmanagementsystem beeinflussen, davon beeinflusst werden, oder sich selbst als davon beeinflusst wahrnehmen kann.
Untersuchung	Ein Verfahren zum Zweck der Verhütung von Unfällen und Störungen, das die Sammlung und Auswertung von Informationen, die Erarbeitung von Schlussfolgerungen einschließlich der Feststellung der Ursachen und gegebenenfalls die Abgabe von Sicherheitsempfehlungen umfasst (Richtlinie (EU) 2016/798).
Managementsystem	Ein Satz an verbundenen oder interagierenden Elementen einer Organisation zur Etablierung von Strategien und Zielen sowie die Prozesse zum Erreichen dieser Ziele (ISO 9000).
Kontrolle	Die von den Eisenbahnunternehmen, Fahrwegbetreibern oder für die Instandhaltung zuständigen Stellen getroffenen Vorkehrungen für die Überprüfung der korrekten Anwendung und Effektivität ihres Managementsystems (Verordnung (EU) Nr. 1078/2012).

Nationale Vorschrift	Alle in einem Mitgliedstaat erlassenen verbindlichen Vorschriften – unabhängig davon, welche Stelle diese Vorschriften erlässt –, in denen die die Eisenbahnsicherheit betreffenden oder technischen Anforderungen – mit Ausnahme der durch Unionsvorschriften oder internationale Vorschriften festgelegten Anforderungen – enthalten sind und die in dem betreffenden Mitgliedstaat für Eisenbahnunternehmen, Infrastrukturbetreiber oder Dritte gelten (Richtlinie (EU) 2016/798).
Prozess	Satz an verbundenen oder interagierenden Aktivitäten, der Eingaben in Ergebnisse verwandelt (ISO 9000).
Eisenbahninfrastruktur	Die nötigen Einrichtungen zum Ermöglichen des Betriebs einer Eisenbahn, einschließlich: • Gleise und zugehörige Gleisstrukturen; • Bedienungswege, Signalgebungssysteme, Kommunikationssysteme, Schienenfahrzeuge; • Kontrollsysteme, Zugsteuerungssysteme und Datenmanagementsysteme; • Hinweise und Signale; • elektrische Energieversorgung und elektrische Zugförderungssysteme; • zugehörige Gebäude, Werkstätten, Lagerhallen und Zugdepots; und • technische Anlagen, Maschinen und Geräte.
Eisenbahnunternehmen	Ein Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU sowie jedes öffentliche oder private Unternehmen, dessen Tätigkeit im Erbringen von Eisenbahnverkehrsleistungen zur Beförderung von Gütern und/oder Personen besteht, wobei dieses Unternehmen die Traktion sicherstellen muss, einschließlich Unternehmen, die ausschließlich für die Traktion zuständig sind (Richtlinie (EU) 2016/798). Ein nach dieser Richtlinie zugelassenes öffentlich-rechtliches oder privates Unternehmen, dessen Haupttätigkeit im Erbringen von Eisenbahnverkehrsdiensten zur Beförderung von Gütern und/oder Personen besteht, wobei dieses Unternehmen die Traktion sicherstellen muss; dies schließt auch Unternehmen ein, die ausschließlich die Traktionsleistung erbringen (Richtlinie 2012/34/EU).
Risiko	Die Kombination der Häufigkeit des Eintretens von (durch Gefährdungen verursachten) Unfällen und Zwischenfällen, die zu einem Schaden führen, und des Ausmaßes dieses Schadens (Richtlinie (EU) 402/2013).
Risikoanalyse	Systematische Auswertung aller verfügbaren Informationen zur Ermittlung von Gefährdungen und Abschätzung von Risiken (Verordnung (EU) 402/2013).
Risikobewertung	Der aus Risikoanalyse und Risikoevaluierung bestehende Gesamtprozess (Verordnung (EU) 402/2013).
Risikoevaluierung	Ein auf der Risikoanalyse beruhendes Verfahren zur Feststellung, ob das Risiko auf ein vertretbares Niveau gesenkt wurde (Verordnung (EU) 402/2013).

Risikomanagement	Die systematische Anwendung von Managementstrategien, -verfahren und -praktiken bei der Analyse, Evaluierung und Beherrschung von Risiken (Verordnung (EU) 402/2013).
Sicherheitskultur	Die Wechselbeziehungen zwischen den Anforderungen des Sicherheitsmanagementsystems, der Frage, wie Menschen aufgrund ihrer Einstellungen, Werte und Ansichten deren Sinn verstehen, und dem, was sie dann tatsächlich tun, was sich dann in Entscheidungen und Verhaltensweisen niederschlägt. Eine positive Sicherheitskultur zeichnet sich durch ein gemeinschaftliches Bekenntnis von Führungspersönlichkeiten und Einzelpersonen zu einem stets sicheren Handeln aus, insbesondere dann, wenn sie mit widersprüchlichen Zielen konfrontiert sind (Verordnung (EU) 2018/762).
Ziel	Zu erreichendes Ergebnis. Ein Sicherheitsziel muss spezifisch, messbar, erreichbar, realistisch und zeitbasiert sein. Es muss außerdem in relevanten Funktionen und Ebenen innerhalb der Organisation gesetzt werden.
Partner	Eine kommerzielle Entität, mit der eine andere kommerzielle Entität eine Art Allianz gebildet hat. Diese Beziehung kann eine vertragliche, exklusive Bindung sein, in der beide Entitäten sich dazu verpflichten, keine Allianz mit Dritten einzugehen.
Partnerschaft	Eine Vereinbarung, bei der Parteien, die als Partner bekannt sind, einer Zusammenarbeit zustimmen, um ihre gemeinsamen Interessen zu fördern.
Sicherheitsmanagementsystem	Die von einem Infrastrukturbetreiber oder einem Eisenbahnunternehmen eingerichtete Organisation und die von ihm getroffenen Vorkehrungen und festgelegten Verfahren, die die sichere Steuerung seiner Betriebsabläufe gewährleisten (Richtlinie (EU) 2016/798).
Oberste Führungsebene	Person oder Gruppe von Personen, die eine Organisation auf der höchsten Ebene leitet und steuert (ISO 9000).
Betriebsart	Die Art des Betriebs, gekennzeichnet durch die Personenbeförderung unter Einschluss oder Ausschluss von Hochgeschwindigkeitsdiensten, die Güterbeförderung unter Einschluss oder Ausschluss der Beförderung gefährlicher Güter und den ausschließlichen Rangierbetrieb (Richtlinie (EU) 2016/798).