RAM Plan - smartrail 4.0

Document Properties

Status: **awaiting Work Item approvals**

Version: **2**

Owner: Steiger Markus (I-SR40-PMO-EXT)

Contributors: Melchior Tom (I-SR40-PMO-EXT), Kuhn Markus (I-SR40-PMO-PLP), Steiger Markus (I-SR40-PMO-EXT), Doberanzke Georg (IT-SWE-CC1-JV2), Grabowski David (I-SR40-PMO-PLP)

Document history

Version (revision)	Changes	Document Owner	Approved	Signed
1 (344650)		Steiger Markus (I-SR40-PMO-EXT)	Steiger Markus (I-SR40-PMO-EXT)	
2 (346406)		Steiger Markus (I-SR40-PMO-EXT)		

Content

1 Einleitung

1.1 Ziele

SRP-20988 - Vorliegendes Dokument beinhaltet den RAM-Plan smartrail 4.0 (SR40) auf übergeordneter Ebene SR40. Das Dokument dient ebenfalls als Grundlage für den RAM-Plan der Entwicklungsgegenstände und stellt eine Richtlinie für die Projekte dar.

SRP-19457 - Der RAM-Plan bildet zusammen mit dem SR40 Safety Plan das RAMS-Programm. Im Programm SR40 werden die Themen RAM und S logisch und organisatorisch getrennt geführt.
Der RAM-Plan ist die Basis für das Management aller RAM-Aktivitäten über den gesamten Lebenszyklus. Dieser wird in Übereinstimmung mit der CENELEC-Norm SN EN 50126 erstellt und liefert einen Überblick über alle relevanten Aspekte des RAM-Managements.
Der RAM-Plan umfasst die Aufgaben und Massnahmen zur Erfüllung der RAM-Anforderungen auf Ebene SR40 bzw. zur Erfüllung der RAM-Anforderungen an die Entwicklungsgegenstände in den Projekten. Folgende Aufgaben sind relevant und werden im RAM-Plan aufgezeigt:

- Politik und Strategie, um die RAM-Anforderungen zu erreichen
- Lebenszyklus-/Projektphasen des Systems und Zuteilung der entsprechenden RAM-Aufgaben und -Massnahmen
- Rollen, Verantwortlichkeiten, Zuständigkeiten und die Beziehungen in der Organisation, die innerhalb des Lebenszyklus RAM-Aufgaben ausführen
- Verfahren und Methoden für die Umsetzung der einzelnen Aktivitäten / Aufgaben
- Vorgaben an die Dokumentation

SRP-23831 - Auf der Ebene SR40 erfolgt keine Entwicklung eines Gesamtsystems SR40. Dennoch wird im RAM-Management auf dieser Ebene ein Prozess in Anlehnung an den Lebenszyklus gemäss SN EN 50126 durchgeführt. Mit diesem Prozess sollen ein einheitliches, abgestimmtes RAM-Management in den Entwicklungsprojekten sowie die Definition und Überprüfung übergeordneter RAM-Ziele an die Entwicklungsgegenstände gewährleistet werden.

SRP-23830 - Auf Projektebene wird für die RAM-relevanten Entwicklungsgegenstände das Phasenmodell der Norm SN EN 50126 durchlaufen. Für jeden RAM-relevanten Entwicklungsgegenstand ist entsprechend ein RAM-Plan zu erstellen, wobei vorliegendes Dokument als Grundlage dient.

1.2 Geltungsbereich

SRP-20986 - Dieses Dokument gilt für die Systembeschreibung gemäss Kap. 3.1 (Ebene SR40 und RAM-relevante Entwicklungsgegenstände).
Der vorliegende RAM-Plan wird dem Projektstand entsprechend kontinuierlich in den Lebenszyklusphasen aktualisiert.

1.3 Abkürzungen

SRP-20987 -

Abkürzung	Erläuterung
APS	Advanced Protection System, vormals ES
ATO	Automatic Train Operation
COAT	CCS Onboard Application Platform For Trackside Related Functions
DMDC	Diagnose, Monitoring & Device Configuration
ES	ETCS Stellwerk
ETCS	European Train Control System
FAT	Factory Acceptance Test
FMECA	Failure Modes, Effects and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRMCS	Future Railway Mobile Communication System
FQT	Fachliche Querschnittsthemen
FTA	Fault Tree Analysis
GLAT	Genaue lokalisierbare allgemeinverwendbare Endgerätetechnik
GSM-R	Global System for Mobile Communication - Rail(way)
ILTIS	Integrales Leit- und Informationssystem
LCC	Life Cycle Costing
LCS	Lokalisierung, Connectivity, Security
LRU	Line Replaceable Unit
MTC	Manoeuver Train Control

OC	Object Controller
OCT	Operation Center Technik
PAS	Produktions-Automatisierungssystem
PL	Projektleiter
QM	Qualitätsmanagement
RAC	Risikoakzeptanzkriterien
RAM(S)	Reliability, Availability, Maintainability (Safety) - Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit (Sicherheit)
RAP	Risikoakzeptanzprinzipien
RBD	Reliability Block Diagram
RCM	Reliability Centered Maintenance
SAT	Site Acceptance Test
SLA	Service-Level-Agreement
SPM	Smartrail Prozess Modell
SW	Software
TMS	Traffic Management System
ZVmin	Zugverspätungsminuten

1.4 Begriffe

SRP-21021 -

Begriff	Definition
Ausfall	Verlust der Fähigkeit, wie gefordert zu funktionieren
Ausfallrate	Grenzwert des Quotienten der bedingten Wahrscheinlichkeit, dass der Zeitpunkt T des Ausfalls in ein gegebenes Zeitintervall (t, t+Δt) fällt, und der Länge dieses Intervalls Δt, wenn Δt gegen 0 geht, vorausgesetzt, das Produkt ist zu Beginn des Zeitintervalls in betriebsfähigem Zustand Kenngrösse λ
Common Cause Failure	Ausfälle aufgrund gemeinsamer Ursache: Ausfälle

(CCF)	mehrerer Einheiten, die ansonsten als voneinander unabhängig gesehen würden, aufgrund einer einzigen Ursache
Fehler, Fehlfunktion	Abweichung vom spezifizierten Verhalten einer Einheit
Fehlzustand	Störung
Instandhaltbarkeit	Fähigkeit, unter gegebenen Anwendungs- und Instandhaltungsbedingungen in einem wie geforderten Zustand erhalten bzw. in ihn zurückversetzt werden zu können
Instandhaltung	Kombination aller technischen und unternehmerischen Massnahmen, mit denen eine Einheit in einem Zustand erhalten oder in ihn zurückversetzt werden soll, in dem sie wie gefordert funktionieren kann
Instandhaltungsvermögen	Fähigkeit einer Instandhaltungsorganisation die richtige Instandhaltungsunterstützung am Ort an dem sie gebraucht wird, um die erforderliche Instandhaltungstätigkeit zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls auszuführen, zur Verfügung zu stellen
Instandsetzung, korrektive Instandhaltung	Instandhaltung, ausgeführt nach einer Fehlzustandserkennung, mit der Absicht der Wiederherstellung
Lebenszyklus	Abfolge identifizierbarer Stufen, die eine Einheit durchläuft von ihrer Konzeption bis zur Entsorgung
Risiko	Die Norm SN EN 50126 definiert das Risiko als Kombination aus erwarteter Häufigkeit eines Schadens und erwartetem Schweregrad dieses Schadens. Vorliegend wird für die Bewertung von RAM-Äquivalenten der Risikobegriff erweitert als Kombination aus erwarteter Häufigkeit einer Störung (Störungen pro Jahr) und erwartetem Schweregrad dieser Störung (Störungsdauer in Minuten x Zugverspätungsminuten pro Minute Störungsdauer).
Sicherheit	Freiheit von inakzeptablem Risiko
Störung	Fehlzustand, der zu einem Fehler oder Ausfall in einem

	System führen kann
Störungsrate	Kehrwert der mittleren Zeit zwischen Ausfällen (MTBF) Parameter ω = 1/MTBF
Subsystem	Teil eines Systems, das für sich selbst ein System ist
System	Menge an miteinander in Beziehung stehender Elemente bzw. Subsysteme
systematischer Ausfall	Ausfall, der regelmässig unter bestimmten Handhabungs-, Lagerungs-oder Einsatzbedingungen eintritt
Validierung	Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für eine spezifische beabsichtigte Anwendung erfüllt worden sind
Verfügbarkeit	Fähigkeit eines Betriebsmittels, zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die erforderlichen äusseren Hilfsmittel zur Verfügung stehen Kenngrösse A
Verifizierung, Verifikation	Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind
Wartung, vorbeugende / präventive Instandhaltung	Instandhaltung mit der Absicht, eine etwaige Funktionsminderung zu vermeiden und die Ausfallwahrscheinlichkeit zu vermindern
zufälliger Fehler	nicht vorhersagbarer Fehler, der sich aus einem oder mehreren der möglichen Degradationsmechanismen ergibt
Zuverlässigkeit	Fähigkeit, unter gegebenen Bedingungen und für ein gegebenes Zeitintervall wie gefordert ohne Ausfall zu funktionieren

1.5 Kenngrössen

SRP-20992 -

Abkürzung	Bezeichnung	Definition
A	Availability	Verfügbarkeit = MTTF / (MTTF + MTTR)
DC	Duty Cycle	Quotient aus Betriebszeit und Kalenderzeit = Betriebszeit / Kalenderzeit
F(t)	Failure Probability	Ausfallwahrscheinlichkeit
MFDT	Mean Failure Detection Time	Mittlere Ausfalloffenbarungszeit: mittlere Zeitspanne, die zu dem Zeitpunkt beginnt, an dem ein Ausfall auftritt, und die endet, wenn das Vorhandensein dieses Ausfalls erkannt wird
MLD	Mean Logistik Delay	Mittlere logistische Verzugsdauer, welche die beiden Anteile "mittlere administrative Verzugsdauer (für Instandsetzung)" und "mittlere technische Verzugsdauer" enthält
MTBF	Mean Time Between Failures	Mittlere (Betriebs-)Dauer zwischen Ausfällen (für instandsetzbare Elemente) = MTTF + MTTR = MTTF + MDT
MTBM	Mean Time Between Maintenance	Mittlere (Betriebs-)Dauer zwischen Instandhaltungen (präventiv, Wartungsintervall)
MTTF	Mean Time To Failure	Mittlere (Betriebs-)Dauer bis zum Ausfall (für nicht instandsetzbare bzw. irreparable Elemente)
MTTM	Mean Time To Maintain	Mittlere Instandhaltungszeit (präventiv)
MTTR	Mean Time To Restoration	Mittlere Dauer bis zur Wiederherstellung = MFDT + MLD + MRT
MRT	Mean Repair Time	Mittlere Reparaturdauer (vor Ort): Summe aus Fehlzustandslokalisierungszeit,

		Fehlzustandsbehebungszeit und Funktionsprüfungszeit (vom Beginn der Vor-Ort-Diagnose bis zum Abschluss der Wiederinbetriebnahme)
R(t)	Reliability	Zuverlässigkeit, Überlebenswahrscheinlichkeit = 1 - F(t)
U	Unavailability	Nichtverfügbarkeit (Unverfügbarkeit) = 1 - A
λ	Failure Rate	Ausfallrate
ω	Fault Rate	Störungsrate

2 Normative Grundlagen und Anforderungen

2.1 Normen

SRP-20995 -

[1]	SN EN 50126-1:2017	Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS Prozess - Software für Eisenbahnsteuerungs- und Überwachungssysteme
[2]	SN EN 50128:2011	Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme
[3]	SN EN 60812:2006	Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart und -auswirkungsanalyse (FMEA)
[4]	SN EN 61078:2016	Zuverlässigkeitsblockdiagramme
[5]	IEC 61025:2006	Fault Tree analysis (FTA)
[6]	SN EN 60300-3-11:2009	Zuverlässigkeitsmanagement - Teil 3-11: Anwendungsleitfaden - Auf die Funktionsfähigkeit bezogene Instandhaltung
[7]	SN EN	Funktionale Sicherheit sicherheitsbezogener

	61508-6:2010	elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3
[8]	SN 29500	Siemens Norm SN 29500 bestehend aus Teilen 1 bis 16

2.2 Grundlegendes RAMS-Verständnis gemäss SN EN 50126

SRP-19455 - Gemäss Norm SN EN 50126 ist der Begriff RAMS eine Charakteristik für das Langzeitbetriebsverhalten eines Systems und wird durch das Anwenden anerkannter technischer Konzepte, Verfahren, Werkzeugen und Techniken während des gesamten Lebenszykluses des Systems erreicht. RAMS für ein System lässt sich als qualitative und quantitative Angabe des Grades beschreiben, bis zu welchem man sich darauf verlassen kann, dass das System oder die Subsysteme und Komponenten, aus denen das System besteht, über einen bestimmten Zeitraum wie festgelegt funktioniert (funktionieren) und ebenso verfügbar und sicher ist (sind). Unter RAMS für ein System wird im Kontext der SN EN 50126 eine Kombination aus Zuverlässigkeit (Reliabilty R), Verfügbarkeit (Availability A), Instandhaltbarkeit (Maintainability M) und Sicherheit (Safety S) verstanden (Begriffsdefinition siehe Kap. 1.4). RAMS hat auch massgebliche Auswirkung auf die Gesamt-Lebenszykluskosten, diese stellen jedoch nicht das direkte primäre Ziel dar.

2.2.1 RAMS-relevante Einflüsse und Auswirkungen

SRP-20277 - Ausfälle in einem System, das innerhalb der Anwendung und innerhalb der Umgebung geltenden Grenzen arbeitet, wirken sich auf die Zuverlässigkeit, Verfügbarkeit und Sicherheit des Systems aus, wobei das Ausmass durch die Funktionalität und den Entwurf des Systems bestimmt wird. Auch die Umgebung und die Betriebsregeln können Einfluss auf diese Auswirkungen haben. Diese Verknüpfungen sind in nachfolgender Abbildung dargestellt.

SRP-20994 -

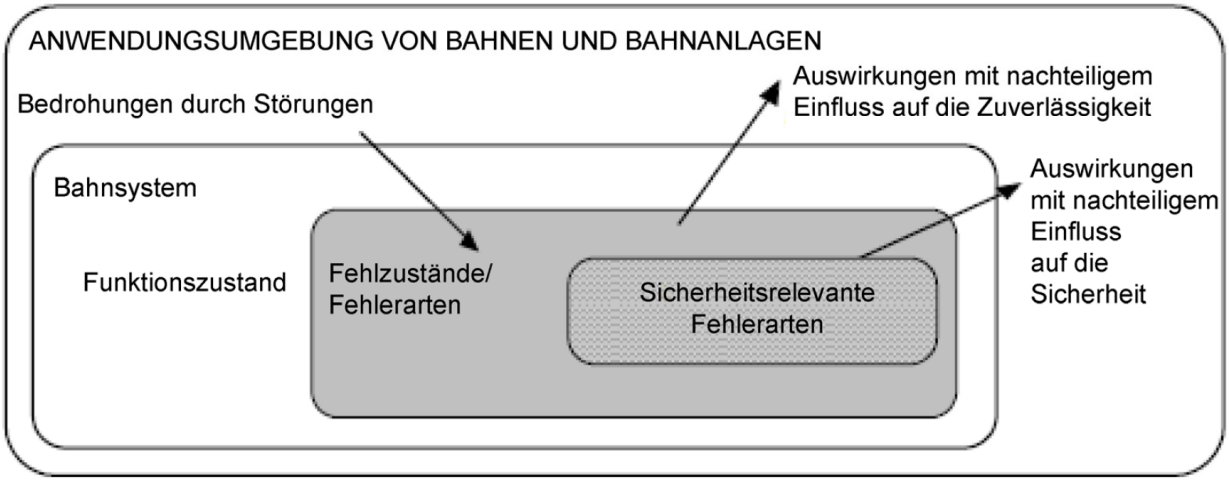


Figure 1: Auswirkungen von Ausfällen innerhalb eines Systems (SN EN 50126)

SRP-20990 - Die RAMS-Leistungsmerkmale eines Bahnsystems werden auf drei Weisen beeinflusst, die in Wechselwirkung miteinander stehen:

- durch Fehlerquellen, die innerhalb des Systems in beliebigen Phasen des System-Lebenszyklus auftreten;
- durch Fehlerquellen, denen das System während des Betriebs ausgesetzt ist; und
- durch Fehlerquellen, denen das System während der Instandhaltungsmassnahmen ausgesetzt ist.

SRP-20989 - Um betriebssichere Systeme zu erstellen, ist es notwendig, die Faktoren zu ermitteln, die die RAMS des Systems beeinflussen können, deren Auswirkungen zu beurteilen und die Ursachen dieser Auswirkungen über den gesamte Lebenszyklus des Systems durch Anwendung geeigneter Steuerungsmassnahmen zu lenken, um die Leistung des Systems zu optimieren.

SRP-20991 - Die Fehler in einem System, Produkt oder Prozess werden als zufällige oder systematische Fehler kategorisiert:

- Zufällige Fehler haben Ursachen, die durch statistische Verteilungen beschrieben werden können.
- Systematische Fehler sind Fehler, die in den Lebenszyklusaktivitäten des Systems verursacht werden, die zu einem deterministischen Ausfall des Produkts, Systems oder Prozesses unter bestimmten Kombinationen von Eingangsgrössen oder unter bestimmten Bedingungen führen (z.B. Kombination von Eingangsgrössen und/oder auslösenden Ereignissen wie der Nichteinhaltung von Umgebungs- und Anwendungsbedingungen). Systematische Fehler werden hauptsächlich durch menschliche Fehler in den verschiedenen Phasen des Systemlebenszyklus verursacht, z.B. Entwicklungsfehler (in der Spezifikation, bei der Software etc.). Deshalb werden systematische Fehler hauptsächlich durch Anwendung geeigneter Prozesse, Verfahren und Organisation behandelt. Systematische Fehler sind unter Voraussetzung gleicher Bedingungen reproduzierbar.

2.2.2 Systemlebenszyklus nach SN EN 50126

SRP-20999 - Der Systemlebenszyklus umfasst die Folge von Phasen und den jeweiligen Aktivitäten über die gesamte Lebensdauer eines Systems, vom Konzept bis zur Ausserbetriebnahme. Nachfolgende Abbildung zeigt den Lebenszyklus in der sogenannten «V»-Darstellung. Der abwärts gerichtete Ast (linke Seite) wird üblicherweise «Entwicklung» genannt und ist ein Verfeinerungsprozess, der mit dem Entwurf und der Implementierung endet. Der aufwärts gerichtete Ast (rechte Seite) bezieht sich auf die Herstellung bzw. Fertigung von Systemkomponenten, die Montage, die Installation, die Übergabe und anschliessend den Betrieb und die Instandhaltung sowie die Ausserbetriebnahme des gesamten Systems.

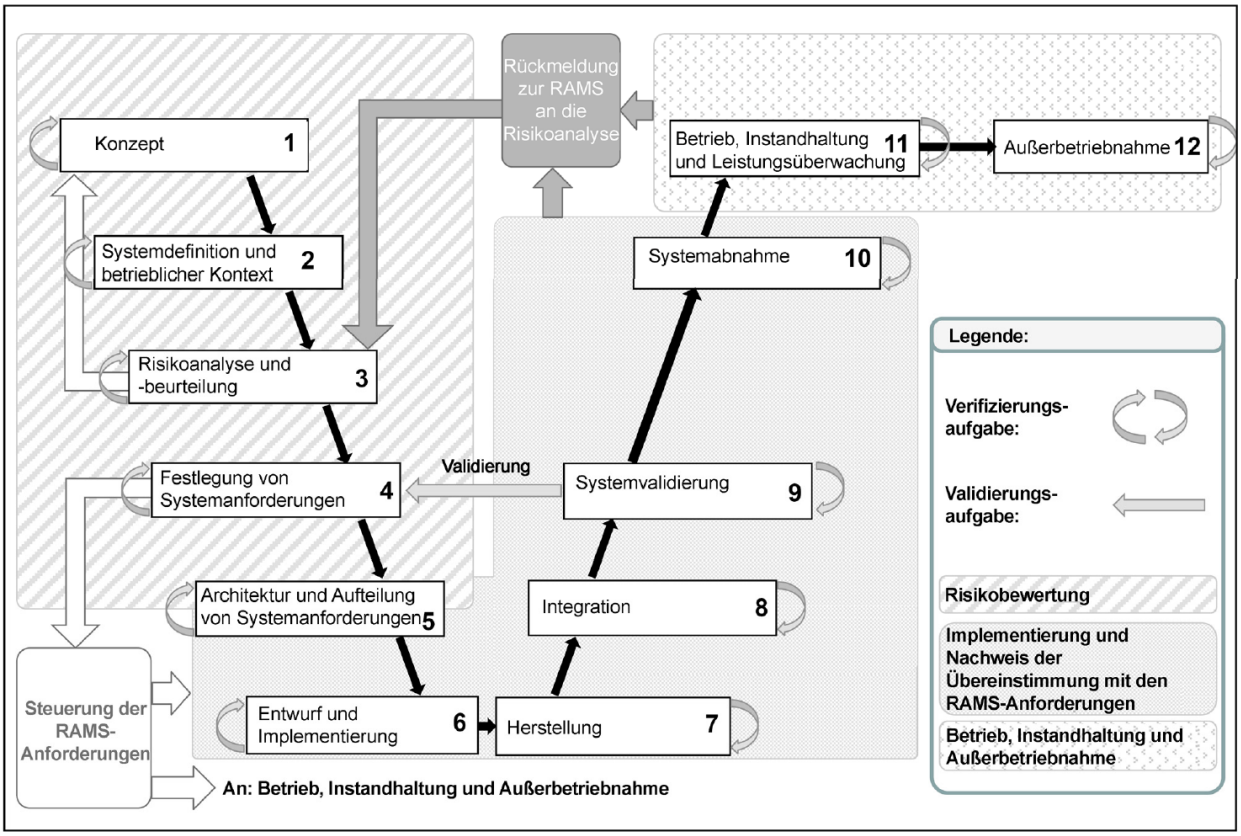


Figure 2: Lebenszyklus V-Darstellung (SN EN 50126)

Die RAM-Aktivitäten in den verschiedenen Lebenszyklusphasen werden im RAM-Plan festgeschrieben.

2.3 Anforderungen an den RAM-Plan gemäss SN EN 50126

SRP-20998 - Im RAM-Plan müssen die Aufgaben enthalten sein, die hinsichtlich der Erfüllung der RAM-Anforderungen für das betrachtete System als am wirkungsvollsten beurteilt werden. Im RAM-Plan müssen die Vorkehrungen für das Management zur Erfüllung der RAM-Anforderungen festgelegt werden. Dazu gehören Einzelheiten zur anzuwendenden Politik und Strategie, zum Anwendungsbereich des Plans und zur Planung der RAM-Aktivitäten.

SRP-21001 - Der RAM-Plan muss folgendes umfassen (SN EN 50126 Kap. 7.3.2.2):

1. Management einschliesslich Einzelheiten zu

    - Systemlebenszyklus und RAM-Aufgaben und -Prozesse, die innerhalb des Lebenszyklus durchgeführt werden müssen; (Verweis: Kapitel 4.5, 4.10)
    - System für die Berichterstattung bei Fehlern, die Fehleranalyse und entsprechende Korrekturmassnahmen (FRACAS), das ab Phase 7 des Lebenszyklus auf das betrachtete System anzuwenden ist, mit Aufzeichnungen z.B. zu folgenden Aspekten (Verweis: Kapitel 4.10, 5.3) :

        - Technische Daten des Systems,
        - Instandhaltungsmassnahmen,
        - Berichts- und Korrekturmassnahmen;

    - Alle RAM-bezogenen erforderliche Arbeitsergebnisse des Lebenszyklus; (Verweis: Kapitel 4.10, 6)
    - RAM-Abnahmeaufgaben; (Verweis: Kapitel 4.8, 4.9, 4.10, 5.2, 5.3)
    - Im RAM-Plan enthaltene Einschränkungen und Annahmen; (Verweis: Kapitel 1.2, 4.1, 4.2, 4.3, 4.7)
    - Festlegungen zur Einbindung von Unterauftragnehmern; (Verweis: Kapitel 4.4, 4.5, 4.10)

SRP-21000 -

2. Zuverlässigkeit, einschliesslich:

    - Zuverlässigkeitsanalyse und -prognose; (Verweis: Kapitel 4.1, 4.2, 4.7, 4.10, 5.1)
    - Zuverlässigkeitsplanung; (Verweis: Kapitel 4.1, 4.2, 4.10, 5.1, 5.2)

- Zuverlässigkeitsprüfung; (Verweis: Kapitel 4.8, 4.9, 5.2, 5.3)
- Erhebung und Bewertung von Zuverlässigkeitsdaten; (Verweis: Kapitel 4.10, 5.2, 5.3)

SRP-20997 -

3. Verfügbarkeit, einschliesslich:

- Verfügbarkeitsanalyse; (Verweis: Kapitel 4.1, 4.2, 4.7, 4.10, 5.1)
- Empfindlichkeitsanalyse; (Verweis: Kapitel 5.1.2)
- Erhebung und Bewertung von Verfügbarkeitsdaten; (Verweis: Kapitel 4.10, 5.2, 5.3)

SRP-20996 -

4. Instandhaltbarkeit, einschliesslich:

- Instandhaltbarkeitsanalyse und -prognose; (Verweis: Kapitel 4.1, 4.2, 4.7, 4.10, 5.1)
- Instandhaltbarkeitsplanung; (Verweis: Kapitel 4.2.3, 4.10, 5.4)
- Beurteilung der logistischen Unterstützung. (Verweis: Kapitel 4.2.2, 4.10, 5.4)

3 Grundlegende Systembeschreibung und Projektphasen

3.1 smartrail 4.0

SRP-21002 - Wichtige Systeme der Bahnproduktion erreichen in den nächsten Jahren das Ende ihrer Lebensdauer. Hinzu kommen aufgrund der technologischen Entwicklung neue Systemmöglichkeiten betreffend Zuglokalisierung und Automatisierung des Zugbetriebs. Die Handlungsbedarfe in der Bahnproduktion, denen die Schweizerische Bahnbranche gegenübersteht, umfassen:

- Rollout ETCS Level 2 bzw. Migration auf Level 3
- Wechsel und Vereinheitlichung der Stellwerktechnologie sowie netzweite Veränderung der Stellwerkinnenanlagen
- Umstellung des Bahnkommunikationssystem von GSM-R zu FRMCS (Future Railway Mobile Communication System)

- Automatisierung der Zugführung (Automatic Train Operation ATO)
- Einführung neuer Technologien zur Zuglokalisierung, mit denen sich eine grosse Menge an ungenutzten Automatisierungspotentialen, die Lösung ungelöster Sicherheitsprobleme sowie eine massive Reduktion der Aussenanlagen erzielen lassen
- Ersatz der bestehenden Fahrplan-, Dispositions- und Lenkungs- und Steuerungssysteme durch ein integrales Verkehrsmanagementsystem (Traffic Management System TMS) unter Ausnutzung des möglichen Automatisierungspotentials sowie als Basis für die Migration auf die neue Stellwerk-, ATO- und Lokalisierungstechnologien

SRP-23184 - Die entsprechenden Projekte zu Ersatz, Automatisierung und Digitalisierung werden im Programm smartrail 4.0 gebündelt, um mit einer abgestimmten Architektur ein optimiertes Gesamtsystem zu entwerfen. Die Entwicklung und Umsetzung der Projekte erfolgt in den Umsetzungsprogrammen TMS, APS (Advanced Protection System - ETCS Stellwerk), LCS (Lokalisierung, Connectivity & Security), ATO und COAT (CCS onboard application platform for trackside related functions).

SRP-23185 - Entwicklungsgegenstände in den Projekten sind Bahnanwendungen (generisch, spezifisch) oder Systeme, wobei für eine Anwendung ein oder mehrere Systeme notwendig sind. Ein System kann wiederum aus mehreren Subsystemen aufgebaut sein, welche wiederum für sich ein System darstellen. Die einer Anwendung zugeordneten Systeme können somit zu einem System zusammengefasst werden. Detailliertere Erläuterungen sind im SR40 Safety Plan enthalten.

SRP-21005 - Eine Systemübersicht SR40 ist im System Definition Document Deutsch gegeben. Die Systemarchitektur SR40 mit den verschiedenen Subsystemen und Software und deren Abhängigkeiten ist im Dokument System Architecture Description in Blockdarstellung aufgezeigt. Der RAM-Prozess SR40 stützt sich auf die Systemarchitektur SR40 ab. Nachfolgend wird als System SR40 die Gesamtheit der in der Systemarchitektur SR40 enthaltenen Subsysteme und Software bezeichnet.

SRP-23187 - Es werden folgende Definitionen verwendet:

- System: ein System besteht aus Hardware inklusive enthaltener Software oder aus reiner Hardware ohne Software
- Subsystem: Teil eines Systems, das selbst ein System darstellt
- Software: Teil eines Systems, das nur aus Software besteht
- Block: Subsystem oder Software
- Komponente: Hardware-Einheit. Subsysteme, die Hardware beinhalten, bestehen aus einzelnen Komponenten. Im Allgemeinen kann als Komponente ein Bauteil angesehen werden, welches im Rahmen einer Wartung oder Instandsetzung vor Ort auswechselbar ist (Line Replaceable Unit LRU).

SRP-23186 - Im RAM-Prozess SR40 werden jene Blöcke (Subsystem oder Software) identifiziert, die eine RAM-Relevanz aufweisen. Blöcke stellen eigene Entwicklungsgegenstände dar, können aber zusätzlich auch Teil eines Entwicklungsgegenstandes sein, der mehrere Blöcke umfasst (z.B. eine Bahnanwendung oder ein System mit mehreren Subsystemen). Enthält ein aus mehreren Blöcken bestehender Entwicklungsgegenstand einen oder mehrere RAM-relevante Blöcke, so ist auch der Entwicklungsgegenstand selbst RAM-relevant. Der vorliegende RAM-Plan SR40 richtet sich an Projekte, in denen die RAM-relevanten Entwicklungsgegenstände entwickelt werden.

3.2 Phasen des smartrail 4.0 Programm

SRP-21007 - Das Programm smartrail 4.0 umfasst übergeordnet drei Phasen, die in der nachfolgenden Abbildung dargestellt sind.

Figure 3: Phasen des SmartRail 4.0 Programm

SRP-21004 - Die Umsetzung erfolgt etappiert. Das System wird vorerst auf einem Teil des Netzes (z.B. eine Region) erprobt, bevor der schweizweite Rollout erfolgt.
Die RAM-Phasen im RAM-Management auf Ebene SR40 (Kap. 2.2.2) sind den Projektphasen wie folgt zuzuordnen:

- Projektierung: RAM-Phasen 1 bis 5
- Erprobung und Systementwicklung: RAM-Phase 6 des gesamten Systems, RAM-Phasen 7 bis 11 für die Probestrecken
- Industrialisierter Rollout inkl. Fertigung: RAM-Phasen 7 bis 11 für das gesamte System

SRP-23188 - Der Entwicklungsprozess der verschiedenen Entwicklungsgegenstände befindet sich in unterschiedlichen Lebensphasen des RAM-Prozesses. Es kann nicht immer vom gleichen Entwicklungsstand ausgegangen werden. Dies ist im übergeordneten RAM-Prozess auf Ebene SR40 zu berücksichtigen.

4 RAM Management

4.1 RAM-Politik

SRP-23190 - Um eine ausreichende RAM-Performance für das System SR40 und seine Entwicklungsgegenstände zu erreichen, werden vom RAM-Management SR40 folgende Grundsätze der RAM-Politik festgelegt:

SRP-23191 -

- Die Entwicklungsgegenstände werden konform zu den vorgeschriebenen Gesetzen und Normen entwickelt.

SRP-23193 -

- Alle RAM-relevanten Projekte müssen ein RAM-Management umsetzen.

SRP-23192 -

- Als RAM-relevant werden jene Entwicklungsgegenstände bezeichnet, die einen Einfluss auf die RAM-Performance des Systems SR40 haben. Die Bemessung der RAM-Performance erfolgt gemäss RAM-Strategie (siehe Kap. 4.2) anhand von Zugverspätungsminuten. Entsprechend gilt ein Entwicklungsgegenstand als RAM-relevant, wenn durch diesen Entwicklungsgegenstand Zugverspätungsminuten generiert werden können.

SRP-23195 -

- Die Verantwortung zur Einhaltung der RAM-Ziele der Entwicklungsgegenstände in der Entwicklung und Realisierung liegt in den einzelnen Projekten. Die Verantwortung zur Einhaltung der übergeordneten Ziele auf Ebene SR40 während der Entwicklung und Realisierung der Entwicklungsgegenstände liegt beim RAM-Management SR40.

SRP-23194 -

- Durchführung des Lebenszyklus nach Norm SN EN 50126 für die RAM-relevanten Entwicklungsgegenstände.

SRP-23200 -

- Anzuwendende Normen bei RAM-relevanten Entwicklungsgegenständen:

SRP-23199 -

- Die Ausführungsbestimmungen der Eisenbahnverordnung (AB-EBV) schreiben für Sicherungsanlagen und Telematikanwendungen, welche am operativen Eisenbahnbetrieb direkt beteiligt sind (z.B. Steuerungs- und Automatisierungstechnik) und die in direktem Zusammenhang mit der Sicherheit und Zuverlässigkeit des Eisenbahnbetriebs stehen, vor, dass für die Spezifikation und den Nachweis der Erfüllung der Zuverlässigkeits-, Verfügbarkeits-, Instandhaltbarkeits- und Sicherheitsanforderungen (RAMS-Anforderungen) die Cenelec Norm SN EN 50126 anzuwenden ist. Diese Norm ist daher auch anzuwenden, wenn es sich um eine nichtsicherheitskritische Bahnanwendung handelt. Die Norm ist entsprechend für alle RAM-relevanten Entwicklungsgegenstände, deren Ausfall sich direkt negativ auf den Bahnbetrieb auswirkt, anzuwenden.

SRP-23202 -

- Ausserhalb des Geltungsbereichs der Norm sind z.B. Anwendungen, welche der Planung oder der Disposition des Eisenbahnbetriebs dienen. Im RAM-Management SR40 wird festgelegt, dass auch für solche Systeme, sofern sie RAM-relevant sind, die Cenelec Norm SN EN 50126 anzuwenden ist (z.B. TMS-Pas).

SRP-23201 -

- Das RAM-Management SR40 legt somit fest, dass der Lebenszyklus nach SN EN 50126 mit sämtlichen RAM-relevanten Aktivitäten für die RAM-relevanten Entwicklungsgegenstände durchzuführen ist. Insbesondere bei komplexeren Systemen mit unterschiedlichen Hierarchieebenen (z.B. Anwendungen mit mehreren RAM-relevanten Blöcken) kann der Vertiefungsgrad der einzelnen Lebenszyklusphasen stufengerecht angepasst werden. Für RAM-relevante Entwicklungsgegenstände, deren Einfluss auf die übergeordnete RAM-Performance des Systems SR40 sehr gering oder vernachlässigbar ist, kann der Lebenszyklus in vereinfachter, reduzierter Form durchlaufen werden (selektive

Anpassung der Aktivitäten bzw. Phasen). Dies wird zwischen RAM-Management SR40 und Projekt abgestimmt und ist im RAM-Plan des Entwicklungsgegenstandes festzuhalten.

SRP-23197 -

- Um systematische Software-Fehler im Griff zu haben, ist für RAM-relevante Software folgendes Vorgehen vorgesehen:
  - Software, die sowohl Safety- als auch RAM-relevant ist: Es ist die Norm SN EN 50128 anzuwenden. Für Teile der Software, die nur RAM-relevant und nicht Safety-relevant sind, sind mindestens die SIL0-Anforderungen der Norm zu erfüllen. Für Teile der Software, die sowohl RAM- als auch Safety-relevant sind, gelten die sicherheitsbezogenen Anforderungen.
  - Software, die nur RAM- und nicht Safety-relevant ist: Es ist grundsätzlich das gleiche Vorgehen vorgesehen: Erfüllung der SIL0-Anforderungen gemäss SN EN 50128 für RAM-relevante Software. Die Aktivitäten können jedoch selektiv aufwandgerecht angepasst werden (SN EN 50128 reduziert). Dies wird zwischen RAM-Management SR40 und Projekt abgestimmt und ist im RAM-Plan des entsprechenden Entwicklungsgegenstandes festzuhalten.
  - Die Software-Entwicklung ist Teil der Cenelec Lebenszyklusphasen 6 (Design) und 7 (Fertigung). In der Phase 8 (Installation) werden Software und Hardware zu einem System integriert.

SRP-23196 -

- Common Cause Failures (CCF) sind in den Zuverlässigkeits- und Verfügbarkeitsberechnungen zu berücksichtigen. Bei der Verwendung von beta-Faktoren ist die Methodik gemäss SN EN 61508-6 anzuwenden.

SRP-23198 -

- Bei Neuentwicklungen sind die Vorgaben zur MTTF-Ermittlung gemäss MTTF-Berechnungsstandard Siemens Norm SN29500 anzuwenden.

SRP-23210 -

- Sofern ein Entwicklungsgegenstand den RAM-Lebenszyklus durchläuft, ist ein RAM-Plan zu erstellen. Der RAM-Plan ist durch den RAM-Manager SR40 zu reviewen und freizugeben.

SRP-23209 -

- Im RAM-Plan werden Methoden und Verfahren für jede Phase des Lebenszyklus festgelegt, die geeignet sind, um die in der jeweiligen Phase vorgesehenen Tätigkeiten erfolgreich durchzuführen.

SRP-23212 -

- Alle gemäss RAM-Plan zu erstellenden Dokumente sind einem Review zu unterziehen.

SRP-23211 -

- Zur Durchführung des Prozesses gemäss SN EN 51026 müssen diverse Rollen besetzt werden. In den Projekten ist der Projektleiter dafür verantwortlich, dass diese Stellen im Projekt festgelegt und mit kompetenten Mitarbeitern besetzt werden.

SRP-23206 -

- Der erfolgreiche Durchlauf des Lebenszyklus oder Teilen davon ist in einem RAM-Nachweis (Phasen 1-x) für die RAM-relevanten Entwicklungsgegenstände nachzuweisen. Auf Ebene SR40 wird ebenfalls ein RAM-Nachweis (Phasen 1-x) vom RAM-Management SR40 erstellt.

SRP-23205 -

- Verifikation: Phasenaktivitäten und Resultate sind am Ende einer jeden Phase zu verifizieren.

SRP-23208 -

- Validierung: Die Festlegung der RAM-Anforderungen ist in der Phase 4 zu validieren. Die Erfüllung der Anforderungen ist in der Phase 9 zu validieren.

SRP-23207 -

- Die Vorgaben an das SR40-Programm betreffend Qualitätsmanagement sind

umzusetzen. Die Projekte müssen ein Qualitätsmanagement anwenden, das konform oder äquivalent zur EN ISO 9001 ist

SRP-23250 -

- Systemgrenzen und Schnittstellen der Entwicklungsgegenstände müssen eindeutig definiert werden. Bei Entwicklungsgegenständen, die den Lebenszyklus sowohl für RAM als auch für Sicherheit durchlaufen, müssen Systemgrenzen und Schnittstellen in beiden Prozessen (RAM und Sicherheit) identisch sein.

SRP-23249 -

- RAM- und Sicherheitsanforderungen sind miteinander abzustimmen.

SRP-23204 -

- An das System SR40 (auf Basis der Systemarchitektur SR40) und die RAM-relevanten Entwicklungsgegenstände sind eindeutige und überprüfbare RAM-Ziele festzulegen. RAM-Ziele für das System SR40 werden vom RAM-Management SR40 vorgegeben und auf die RAM-relevanten Blöcke gemäss Systemarchitektur runtergebrochen. Die Entwicklungsgegenstände werden in den Projekten definiert. Besteht ein Entwicklungsgegenstand aus mehreren Blöcken, ergeben sich die RAM-Anforderungen an den Entwicklungsgegenstand aus den RAM-Anforderungen an die enthaltenen RAM-relevanten Blöcke. Die Festlegung dieser RAM-Anforderungen an die Entwicklungsgegenstände erfolgt im Austausch zwischen RAM-Management SR40 und den Projekten. Die Projekte geben die Entwicklungsgegenstände vor, das RAM-Management SR40 formuliert die RAM-Anforderungen an diese Entwicklungsgegenstände basierend auf den durch das RAM-Management SR40 festgelegten RAM-Anforderungen an die einzelnen Blöcke.

4.2 RAM-Strategie

SRP-21023 - Grundsätzlich wird mit der Durchführung des RAM-Prozesses die Strategie verfolgt, die durch das System smartrail 4.0 verursachten Verspätungen zu minimieren und anfallende Kosten zu optimieren. Im Fokus des RAM-Prozesses steht die betriebliche Leistungsfähigkeit (RAM-Performance). Die Thematik Personensicherheit ist nicht Betrachtungsgegenstand des RAM-Prozesses und wird im SR40 Safety Plan behandelt. Die gegenseitigen Abhängigkeiten, die es zu berücksichtigen gilt, werden an den relevanten Schnittstellen koordiniert.

4.2.1 Zulassung

SRP-21034 - Da die Zulassung von SR40-Anwendungen, -Systemen und -Produkten (Entwicklungsgegenstände) primär Safety betrifft, ist der Zulassungsprozess im SR40 Safety Plan beschrieben. Das RAM-Management ordnet sich diesem unter. Im RAM-Plan wird nicht weiter auf den Zulassungsprozess eingegangen.

4.2.2 RAM-Ziele

SRP-21033 - Die übergeordneten Zielvorgaben auf Ebene SR40 an das System SR40 und die Blöcke bzw. Entwicklungsgegenstände werden als Zugverspätungsminuten (ZVmin) quantifiziert. Die Zugverspätungsminuten berücksichtigen Personen- und Güterverkehr und beinhalten sowohl primäre als auch sekundäre Verspätungsminuten. Die RAM-Zielherleitung sowie die Ableitung der RAM-Anforderungen basiert auf der Datenanalyse und den Einsparzielen/Ambitionen im SBB-Netz. Es wird davon ausgegangen, dass damit ebenfalls die Bedürfnisse und Anforderungen der weiteren Bahnbetreiber im Branchenprogramm abgedeckt sind, dies wird jedoch noch abgestimmt.

SRP-23215 - Die genaue Herleitung der Zielvorgabe an das System SR40 ist in RAM Targets SR40 erläutert. Die Ziele lassen sich wie folgt zusammenfassen:

- Es wird ein konkretes Einsparziel festgelegt, welches mit SR40 erreicht werden soll.
- Weiter werden Einsparpotentiale identifiziert, die nach Möglichkeit mit SR40 erreicht werden sollen (Ambitionen). Mit dem RAM-Prozess SR40 wird die Ausschöpfung dieser Einsparpotentiale angestrebt.
- Anhand des Einsparziels und der Einsparpotentiale wird die Anzahl ZVmin festgelegt, die maximal durch das System SR40 verursacht werden darf (Zielvorgabe SR40).

SRP-23216 - Diese Anzahl ZVmin für das System SR40 wird anhand von Expertenschätzungen

unterschiedlichen Störungsursachen zugeteilt. Ein Teil dieser ZVmin bleibt technischen Störungen vorbehalten. Diese beinhalten Hardware-Fehler (zufällige Fehler) und Software-Fehler (systematische Fehler). Die restlichen ZVmin werden zum einen menschlich/prozessual bedingten Störungen sowie nicht quantifizierbaren Störungen (Cyber-Attacken, Fail-Safe-Situationen, …), zum anderen den mit den Schätzungen verbundenen Unsicherheiten (Reserve) zugeordnet.

SRP-23214 - Die durch technische Störungen (Hardware- und Software-Fehler) verursachten ZVmin pro Jahr bilden die Ausgangsbasis zur Ableitung der quantitativen RAM-Anforderungen an die Blöcke gemäss Systemarchitektur. Dieser Betrag an ZVmin wird anteilsmässig den verschiedenen, berücksichtigten, RAM-relevanten Blöcken zugeordnet. Die Verteilung und die Methodik zu deren Herleitung sind in RAM Targets - Projects (in Bearbeitung) beschrieben. Die RAM-Anforderungen an die Blöcke werden von den ZVmin abgeleitet und als quantifizierte Zuverlässigkeits- (MTTF) und Instandhaltbarkeitswerte (MTTR) für Hardware und als Verfügbarkeitsziele (A) für Software formuliert. Auf Basis dieser Anforderungen an die Blöcke werden ebenfalls die entsprechenden quantifizierten RAM-Anforderungen an Entwicklungsgegenstände definiert, welche mehrere Blöcke enthalten (z.B. Bahnanwendungen). Diese Entwicklungsgegenstände mit den enthaltenen Blöcken werden in den Entwicklungsprojekten festgelegt, die quantifizierten Anforderungen (MTTF, MTTR, A) vom RAM-Management SR40 bestimmt. Die Zielvorgaben sind definierten Störungsklassen zugeordnet, d.h. dieEntwicklugsgegenstände erhalten je Störungsklasse eine Zielvorgabe. Die verschiedenen Störungsklassen beinhalten die ZVmin, die im netzweiten Schnitt pro Ausfallminute bei der entsprechenden Störung auftreten (Details siehe RAM Targets - Projects (in Bearbeitung)). Die weiteren oben erwähnten Störungen (menschlich/prozessual bedingt, Cyber-Attacken, ...) sind nicht oder nur schwer quantifizierbar, weshalb eine sinnvolle Zuteilung an die Subsysteme nur schwer möglich ist. Für diese Störungen werden keine quantitativen RAM-Anforderungen an die Entwicklungsgegenstände gestellt.

SRP-23217 - Es gilt anzumerken, dass betreffend Verfügbarkeit von Elementen (Subsysteme, Komponenten, Software) nur die korrektive Instandhaltung berücksichtigt wird (störungsbedingte Ausfälle). Die präventive Instandhaltung ist eine geplante Tätigkeit und fliesst nicht in die Berechnung der (Nicht-)Verfügbarkeit ein.

SRP-21664 - Verschiedene Blöcke bzw. Entwicklungsgegenstände verursachen nur einen vernachlässigbaren Beitrag zu den ZVmin, da z.B. Rückfallebenen bestehen oder allenfalls weitere Störungen anderer Blöcke gleichzeitig auftreten müssten. In der übergeordneten Analyse zur Ableitung der RAM-Anforderungen an die Blöcke aus den ZVmin werden diese Blöcke nicht berücksichtigt. Diese erhalten eine allgemeine RAM-Anforderung (z.B. ein Verfügbarkeitsziel).

SRP-21030 - Die Zielvorgaben an die Entwicklungsgegenstände müssen in den

Entwicklungsprojekten nachgewiesen werden (Prognoseberechnungen und -abschätzungen). Grundsätzlich vorhersagbar und damit im Rahmen der Projektierung auch nachweisbar sind diese RAM-Kennwerte nur für zufällige Hardware-Fehler, da nur diese auf die Komponente bezogen statistisch ermittelt bzw. anhand von Wahrscheinlichkeitswerten berechnet werden können. Software-Fehler sind systematische Fehler und grundsätzlich mittels qualitätssichernder Massnahmen zu beherrschen, die in den Prozessen des Qualitätsmanagements abzubilden sind (QM-Plan, Q-Lenkungsplan etc.). Die Praxis zeigt aber, dass systematische Fehler in der Regel nicht komplett zu verhindern sind. Deshalb werden quantitative Verfügbarkeitsanforderungen an die Software gestellt, welche in den Entwicklungsprojekten mittels Expertenschätzungen überprüft werden müssen. Nachweisbar ist die Einhaltung der Software-Verfügbarkeitsziele schlussendlich erst im Betrieb, d.h. erstmals in der Erprobung. Letzteres gilt grundsätzlich auch für die Hardware, nur lassen die Prognoseberechnungen in der Entwicklung eine Vorhersage mit geringerer Unsicherheit zu.

SRP-23220 - Die quantitativen RAM-Zielvorgaben an die Blöcke bzw. Entwicklungsgegenstände betreffen nur technische Störungen. Die RAM-Analysen in den Entwicklungsprojekten beschränken sich jedoch nicht nur auf die technischen Fehler, sondern umfassen alle relevanten Störungsursachen, d.h. auch jene Störungsursachen, für die übergeordnet ein Anteil der gesamten ZVmin vorgesehen ist (mehr zur Analyse der Störungen im Kap. 4.7 Risiko-Management RAM).

SRP-23219 - Das Gesamtziel auf übergeordnete Ebene wird anhand der Prognosen in den Entwicklungsprojekten der Entwicklungsgegenstände überprüft.

SRP-23221 - Grundsätzlich sind die RAM-Zielvorgaben an die Entwicklungsgegenstände einzuhalten. Wenn jedoch aufgrund von Kosten/Nutzen-Überlegungen eine Nichteinhaltung der Zielvorgaben sinnvoll erscheint, ist dies mit dem RAM-Management SR40 abzustimmen. Die Einhaltung des übergeordneten Ziels muss gewährleistet sein und wird vom RAM-Management SR40 überprüft, unter Berücksichtigung des Spielraums, den die vorgesehene Reserve bietet.

SRP-21029 - Das Dokument RAM Targets - Projects (in Bearbeitung) enthält nur die aus den übergeordneten Zielvorgaben abgeleiteten Zielvorgaben an die Blöcke bzw. Entwicklungsgegenstände (quantifizierte RAM-Kennwerte für Zuverlässigkeit und Instandhaltbarkeit betreffend Hardware sowie Verfügbarkeit betreffend Software). Neben diesen Vorgaben werden jedoch weitere RAM-relevante Anforderungen an die Entwicklungsgegenstände definiert, z.B. in Bezug auf Organisation und Ressourcen (Stichwort Instandhaltungsvermögen), Instandhaltungsstufen (Maintenance Levels), Schulung, Konfigurationsmanagement, Zustandsüberwachung, Fehlererkennung und -diagnose, Reaktionszeit bei Störung, SW-Upgrades etc. Diese Anforderungen können sowohl qualitativer als auch quantitativer Natur sein (z.B. MTBM und MTTM für Instandhaltung, oder systemspezifische Anforderungen an die MFDT, MLD oder MRT bei der Instandhaltbarkeit). Die Erarbeitung dieser Anforderungen erfolgt nicht durch das RAM-Management SR40, sondern im

Projekt des Entwicklungsgegenstandes und/oder in Abstimmung mit bzw. nach Vorgaben von DMDC sowie OCT (übergeordnete Schnittstellen).

SRP-21032 - Eine weitere wichtige übergeordnete Schnittstelle besteht zur Sicherheit (S). Obwohl RAM und S organisatorisch getrennt behandelt werden, sind sie nicht isoliert zu betrachten, sondern die gegenseitigen Abhängigkeiten sind zu berücksichtigen und abzustimmen. RAM-beeinflussende Randbedingungen oder RAM-Anforderungen aus S müssen im Koordinationsprozess RAM und S ermittelt und im RAM-Prozess zwingend berücksichtigt werden.

4.2.3 Prinzipien zur Erfüllung der RAM-Ziele

SRP-21031 - Die RAM-Strategie sieht folgende Prinzipien zur Erfüllung der RAM-Ziele vor:

1. Keine isolierte Betrachtung der RAM(S)-Elemente Zuverlässigkeit, Verfügbarkeit, Instandhaltung (und Sicherheit), sondern Berücksichtigung der gegenseitigen Abhängigkeit

SRP-21025 -

2. Potentielle Fehlzustände (Fehler oder Ausfälle) von Systemen, Subsystemen und Komponenten werden systematisch analysiert, unter Berücksichtigung von Technik, Mensch und Umwelt, und Auswirkungen auf die RAM-Performance bewertet. Fehlzustände können zufällig oder systematisch auftreten.

SRP-21026 -

3. Erreichung eines hohen Grades an Zuverlässigkeit durch

    - Einsatz robuster, den Umweltbedingungen angepasster Komponenten
    - Systemtoleranzen sind so auszulegen, dass geringfügige Abweichungen der betreffenden Parameter von ihren Nennwerten nicht zu einem gestörten Betrieb führen
    - Komponenten sind so auszulegen, dass sie möglichst nicht nahe an ihren Grenzwerten betrieben werden
    - bei der Beschaffung von Materialien und bei der Lenkung von Herstellungs- und Installationsprozessen sind gute Qualitätsmanagementpraktiken anzuwenden
    - Identifikation kritischer Komponenten für die Zuverlässigkeit der Entwicklungsgegenstände und Definition limitierender Massnahmen

(Zuverlässigkeitsanforderungen an Komponenten, auf Entwicklungsgegenstände zugeschnittene Redundanzkonzepte, Überwachungsmassnahmen, Instandhaltungsmassnahmen, …)

- Kompatibilität:
    - es muss sichergestellt sein, dass Regionen auf unterschiedlichen Softwareständen (Versionen) miteinander kommunizieren können
    - Aufbau COAT: verschiedene Versionen / Produkte der Plattform (unterschiedliche Hersteller) müssen kompatibel mit den zum Einsatz kommenden Applikationen sein
- Zusammenarbeit mit befähigten Zulieferern / Herstellern (Präqualifikation)

SRP-21024 -

4. Erreichung eines hohen Grades an Verfügbarkeit durch:

- Zuverlässige Komponenten
- Zuverlässige Strukturen / Architekturen (u.a. Redundanzkonzept)
- Teilsysteme können autark weiterlaufen
- Optimierte Instandhaltungsstrategie (mittels RCM)
- Hohe Verfügbarkeit der logistischen Unterstützung (inkl. hohe Verfügbarkeit von Ersatzteilen)
- Minimierung von Instandsetzungszeiten
- Dokumentation sämtlicher Wartungstätigkeiten
- Ausreichende Schulung des Unterhaltspersonals
- Ausreichende Massnahmen zur Reduktion menschlicher Fehler (bei Instandhaltungstätigkeiten, SW-Upgrades etc.)
    - Checklisten
    - nur geschultes Personal für wichtige / kritische Tätigkeiten
    - Bediener müssen richtig geleitet werden (HMI, Betriebs- und Instandhaltungsdokumentation, ...)
- Software-Konzept
    - Regionalisierung, um Ausmass systematischer Software-Fehler zu verringern
    - Schatten- und Testbetrieb von Software-Upgrades (regional über längere Zeit)
    - Schweizweiter Roll-out von Software-Upgrades gestaffelt nach

Regionen

- Downgrade-Möglichkeit in ausreichend schneller Zeit

SRP-21028 -

5. Erreichung eines hohen Grades an Instandhaltbarkeit durch:

   - zielgerichtete Fehlerdiagnose / Eigendiagnose
   - Zugänglichkeit von Komponenten
   - einfacher Ausbau bzw. Austausch von Komponenten
   - modularer Aufbau
   - Standardisierung
   - Testmöglichkeiten / Prüffreundlichkeit
   - SLA: Vorgaben an Lieferanten/Hersteller betreffend Reaktionszeiten, insb. bei Software-Fehlern

4.3 RAM-relevante Blöcke

SRP-21051 - Sämtliche Blöcke, die eine RAM-Relevanz aufweisen (d.h. Blöcke, die bei Fehlfunktion Verspätungsminuten generieren können), sind in nachfolgender Tabelle aufgeführt. Basis bildet die Systemarchitektur SR40. Weiter ist angegeben, welche Normen in der Entwicklung der Blöcke gemäss RAM-Politik (Kap. 4.1) anzuwenden sind. Die Anforderungen betreffend anzuwendender Normen bei aus mehreren Blöcken bestehenden Entwicklungsprojekten ergeben sich aus den Mindestanforderungen der enthaltenen Blöcke. Dies wird mit dem RAM-Management SR40 abgestimmt und im RAM-Plan des entsprechenden Entwicklungsgegenstandes festgelegt. Unter „SN EN 50126 reduziert" ist die Anwendung des Lebenszyklus gemäss SN EN 50126 in reduziert Form für RAM-Aktivitäten zu verstehen. Dies gilt für Blöcke, die nur einen vernachlässigbaren Beitrag zu den ZVmin verursachen. Diese werden in der übergeordneten Analyse der ZVmin nicht berücksichtigt und erhalten eine allgemeine RAM-Anforderung (siehe auch Kap. 4.2.2). Das Vorgehen wird abgestimmt mit dem RAM-Management SR40 im RAM-Plan der Entwicklungsgegenstände festgelegt. Für Blöcke bzw. Entwicklungsgegenstände, die nicht Safety-relevant sind, können die Aktivitäten bezüglich Software-Entwicklung (SIL0-Anforderungen) aufwandgerecht selektiv festgelegt werden ("SN EN 50128 reduziert"). Auch hier wird das Vorgehen abgestimmt mit dem RAM-Management SR40 im RAM-Plan der Entwicklungsgegenstände festgelegt.

SRP-23273 -

Block	Programm	SN EN 50126	SN EN 50126 reduziert	SN EN 50128	SN EN 50128 reduziert	Safety-relevant (05.11.2019)
Safe Data Center Application	APS	X		X		X
Enterprise Application Platform	TMS	X			X	
Control IP Network	LCS	X			X	
Enterprise IP Network	LCS	X			X	
FRMCS	LCS	X			X	
OC	APS	X		X		X
COAT (Platform)	COAT	X		X		X
GLAT Tag	LCS	X		X		X
APS Safety Manager	APS	X		X		X
APS Safety Logic	APS	X		X		X
APS Object Aggregation	APS	X		X		X
APS Movement Authority Transactor	APS	X		X		X
APS Mobile Object Transactor	APS	X		X		X
APS Fixed Object	APS	X		X		X

Transactor						
APS Safe Topology System	APS		X	X		X
ATO Transactor	ATO		X		X	
TMS-Pas	TMS	X			X	
TMS-Com	TMS		X		X	
TMS-Topo	TMS		X		X	
TMS-Ordering Portal	TMS		X		X	
TMS ATO Execution	TMS		X		X	
TMS-ARS-ILTIS	TMS	X			X	
TMS Plan Execution	TMS	X		X		X
TMS Workbench	TMS		X		X	
TMS Analysis	TMS		X		X	
Identity & Access Management	GLAT	X			X	
Vehicle Supervisor	APS	X			X	
Vehicle Locator	GLAT	X			X	
ATO Vehicle	COAT		X		X	
MTC On-Board	APS		X	X		X
MTC	APS		X	X		X

Trackside						
DM	APS		X		X	
DC	APS		X	X		X

Table 1 : RAM-relevante Blöcke

4.4 Organisation

SRP-21047 - Nachfolgende Ausführungen beschränken sich auf die RAM-Phasen 1 bis 10. Die detaillierten Organisationsformen für die Phasen 11 bis 12 sind noch auszuarbeiten.

4.4.1 Organisationsstruktur

SRP-21046 - Die Aufbauorganisation des Programms SR40 ist im Programmhandbuch smartrail 4.0 aufgezeigt. Das RAM-Management ist im Bereich Fachliche Querschnittsthemen (FQT) angesiedelt.

Nachfolgende Abbildung zeigt die Gliederung der RAM-Organisation im Programm SR40 gemäss vorliegendem RAM-Plan:

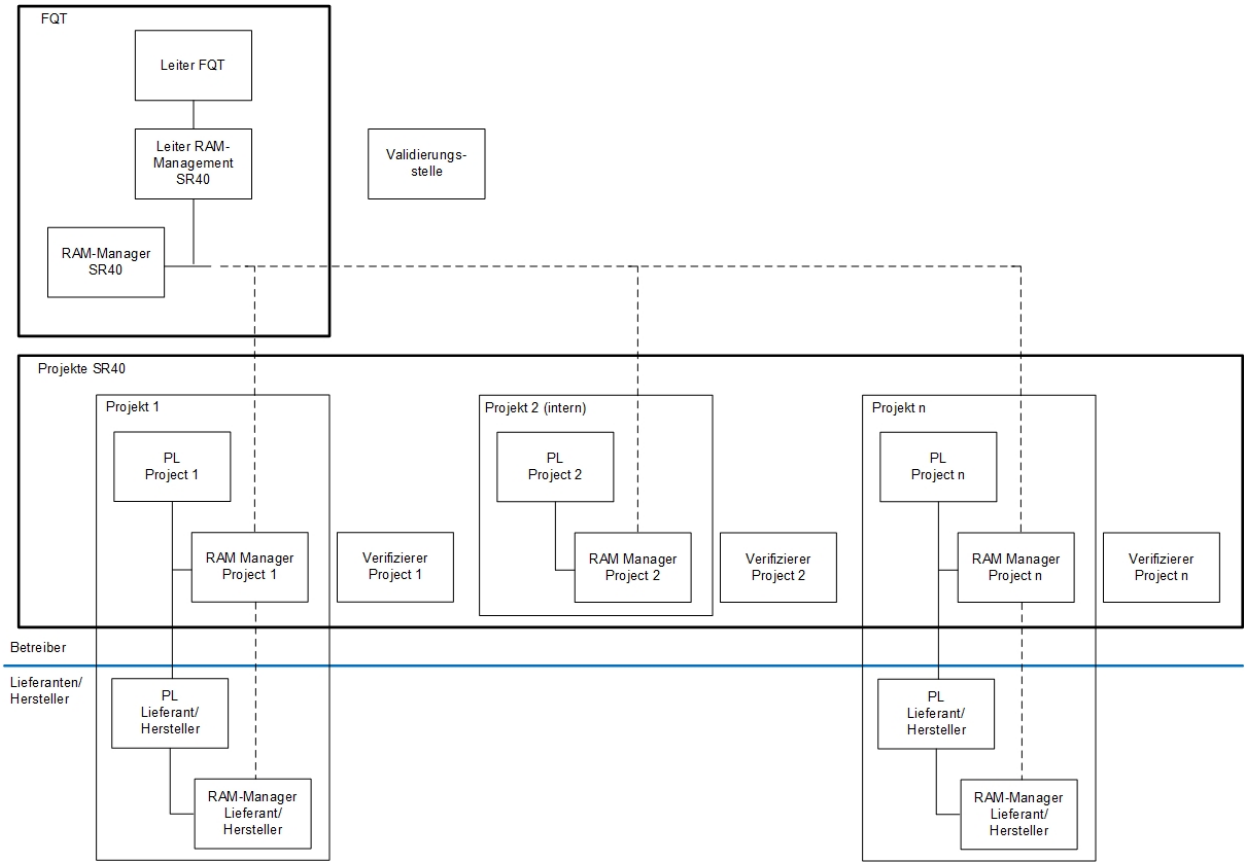


Figure 4 : RAM-Organisation

4.4.2 Rollen in der Organisation

SRP-21049 - Der Leiter RAM-Management SR40 ist verantwortlich für:

- Erstellung und Aktualisierung des übergeordneten RAM-Plans, des übergeordneten RAM-Nachweises (Phasen 1-x) und aller einhergehender Analysen und Berichte
- Sicherstellung, dass sämtliche RAM-Anforderungen in den entsprechenden Projektphasen behandelt und umgesetzt werden, und dass die entsprechenden Ressourcen an Personal, Werkzeugen und Methoden zur Verfügung stehen
- Sicherstellung, dass die Dokumentation und Nachvollziehbarkeit aller RAM-bezogenen Entscheidungen gewährleistet ist
- Herleitung des übergeordneten RAM-Zieles SR40 und Zuteilung an Blöcke bzw. Entwicklungsgegenstände
- Koordination der RAM-Aktivitäten zwischen den Projekten und Management der RAM-bezogenen Schnittstellenthemen zwischen den Projekten
- Koordination mit den übergeordneten Schnittstellen OCT, DMDC und Safety
- Einhaltung der relevanten RAM-Normen
- Kontrolle der RAM-Aktivitäten der Projekte
- Freigabe von RAM-relevanten Dokumenten in den Projekten

SRP-21042 - Die Tätigkeiten der RAM-Manager SR40 umfassen:

- Unterstützung des Leiters RAM-Management SR40 in all seinen Tätigkeiten
- Unterstützung der RAM-Manager Project in den RAM-Analysen der Entwicklungsgegenstände
- Vorlagen für die Projekte erstellen (RAM-Plan, FMECA etc.)
- Reviews der RAM-bezogenen Berichte der Projekte

SRP-21064 - Die RAM-bezogenen Aufgaben der Entwicklungsprojektleiter umfassen:

- Bestimmung eines RAM-Managers im Projekt (RAM-Manager Project)
- Beauftragung eines Verifizierers mit der Durchführung der Verifikation im Projekt
- Bereitstellung der erforderlichen Ressourcen zur Erfüllung der RAM-Aufgaben im Projekt
- Koordination der RAM-Aktivitäten mit den weiteren Projektaktivitäten
- Sicherstellung des Qualitätsmanagements im Projekt und der Durchführung der einhergehenden Kontrollen und Prüfungen

SRP-21068 - Der RAM-Manager Project ist verantwortlich für:

- Erstellung und Aktualisierung des RAM-Plans sowie des RAM-Nachweises (Phasen 1-x) auf Stufe des Entwicklungsgegenstandes und aller einhergehender Analysen und Berichte in enger Zusammenarbeit mit den Projektingenieuren
- Sicherstellung, dass sämtliche RAM-Aktivitäten in den entsprechenden Projektphasen behandelt und umgesetzt werden
- Einhaltung der relevanten RAM-Normen
- Sicherstellung, dass die Dokumentation und Nachvollziehbarkeit aller RAM-bezogenen Entscheidungen gewährleistet ist
- Herleitung systemspezifischer RAM-Anforderungen der Entwicklungsgegenstände, die nicht von der übergeordneten Zielstellung auf Ebene SR40 vorgegeben sind
- Zuteilung RAM-Anforderungen an Komponenten und Teilsysteme der Entwicklungsgegenstände, abgeleitet von den übergeordneten Zielen an den Entwicklungsgegenstand (sofern nicht konkret von der übergeordneten Zielstellung vorgegeben)
- Massnahmen einleiten zur Überwachung und Verbesserung des Entwicklungsgegenstandes im Betrieb
- Beaufsichtigung und Kontrolle sämtlicher RAM-Aktivitäten der Lieferanten und Hersteller

SRP-21066 - Der Lieferant / Hersteller ist verantwortlich für:

- Durchführung der vertraglich geschuldeten RAM-Aktivitäten
- Einhaltung der relevanten RAM-Normen
- Sicherstellung, dass die gelieferten Produkte und Komponenten allen spezifischen und normativen Anforderungen sowie dem aktuellen Stand der Technik entsprechen
- Erstellung und Aktualisierung der RAM-Analysen des gelieferten Produkts / Systems und Zusammenstellung der einhergehenden Berichte und Dokumente
- Durchführung der qualitätssichernden Massnahmen
- Dokumentation aller RAM-Aktivitäten
- Koordination der RAM-Aktivitäten mit dem Kunden sowie den Zulieferern

SRP-21058 - Diverse Verantwortlichkeiten des RAM-Manager Project auf Seite SR40 können auf den RAM-Verantwortlichen auf Seite Lieferant / Hersteller übertragen werden, insbesondere wenn von einem Lieferanten / Hersteller das vollständige Produkt / System geliefert wird. Der RAM-Verantwortliche auf Seite SR40 ist aber nach wie vor für die Beaufsichtigung und Kontrolle sämtlicher RAM-Aktivitäten des Lieferanten / Herstellers verantwortlich, und hat sicherzustellen,

dass sämtliche zugeteilten RAM-Anforderungen im Projekt erfüllt werden. Die Verantwortlichkeiten sind im RAM-Plan des Entwicklungsgegenstandes festzulegen und im Pflichtenheft des Lieferanten / Herstellers aufzunehmen. Die Verantwortlichkeiten können je nach Anforderungen in den verschiedenen Entwicklungsgegenständen erweitert werden.

SRP-23222 - Ergänzend gibt es noch die Rollen Verifizierer, Validierer und Reviewer, welche im Kap. 4.9 erläutert werden.

4.4.3 RAM-Schnittstellen und Koordinationsaufgaben

SRP-21056 - Auf übergeordneter Ebene SR40 werden die RAM-Aktivitäten mit den Sicherheitsaktivitäten sowie mit OCT und DMDC (insbesondere Instandhaltungsthemen) abgeglichen. Dazu finden in regelmässigen Abständen Sitzungen zwischen RAM-Manager SR40 und entsprechenden Vertretern statt. Beschlüsse mit Auswirkungen auf RAM bzw. Safety werden protokolliert, Aufgaben mittels Pendenzenlisten verwaltet.

SRP-21061 - Die RAM-Koordination der Projekte wird durch die RAM-Manager SR40 wahrgenommen. Dies erfolgt in den regelmässigen RAM-Sitzungen mit den RAM-Managern der Projekte (siehe Kap. 4.14).

SRP-21060 - Die RAM-Koordination mit den Lieferanten/Herstellern liegt im jeweiligen Verantwortungsbereich des Projekts und wird vom entsprechenden RAM-Manager Project wahrgenommen. Für die Lieferanten/Hersteller gelten grundsätzlich die gleichen übergeordneten Vorgaben wie an die Entwicklungsprojekte. Die RAM-Anforderungen an die Blöcke bzw. Entwicklungsgegenstände werden auf übergeordneter Ebene zugeteilt. Das weitere Herunterbrechen von RAM-Anforderungen an Komponenten und Teilsysteme von Lieferanten/Herstellern liegt im Verantwortungsbereich der einzelnen Projekte. Abstimmungssitzungen zwischen den RAM-Managern der Projekte und Vertretern der Lieferanten/Herstellern liegen im Verantwortungsbereich der Projekte und sind durch diese zu organisieren. An den RAM-Sitzungen zwischen übergeordnetem RAM-Management SR40 und RAM-Management der Projekte ist eine Teilnahme der Lieferanten/Hersteller nach Absprache mit dem RAM-Manager SR40 möglich.

SRP-21071 - Bem.: Der Prozess der Schnittstellenkoordination wird derzeit für das Programm SR40 definiert.

4.5 Projekt-/Lebenszyklus

SRP-21070 - Bezüglich Lebenszyklen auf unterschiedlichen Hierarchieebenen werden im vorliegenden RAM-Plan zwei Ebenen betrachtet: Ebene SR40 und Ebene der Entwicklungsgegenstände. Weitere Ebenen innerhalb der Entwicklungsgegenstände sind, falls vorgesehen, in den RAM-Plänen der Entwicklungsgegenstände zu behandeln. Anhand des in der SN EN 50126 (§ 6.5.2) beispielhaft festgelegten Vertiefungsgrades der durchzuführenden RAM-Aktivitäten in den verschiedenen RAM-Phasen, werden in vorliegendem Dokument aus Sicht des übergeordneten RAM-Managements folgende Vertiefungsstufen in den Lebenszyklen auf Ebene SR40 und der Entwicklungsgegenstände festgelegt. Diese sind ebenfalls anhand des Schattierungsgrades in Figure 6 erkennbar. Phase 12 steht nicht im Projektfokus und ist deshalb nicht aufgeführt.

SRP-21055 -

- Ebene SR40: Auf der Ebene SR40 erfolgt keine Entwicklung eines Systems oder einer Anwendung. Nichtsdestotrotz wird auf Ebene SR40 ein Lebenszyklus in Anlehnung an die Norm SN EN 50126 durchlaufen, um zu gewährleisten, dass die erforderlichen RAM-Aktivitäten auf übergeordneter Ebene SR40 Berücksichtigung finden. Die RAM-Phasen 1 bis 5 sowie 9 bis 11 kommen dabei vollständig zur Anwendung, während die Phasen 6 bis 8 nur mit niedrigem Vertiefungsgrad durchlaufen werden.

SRP-21043 -

- Entwicklungsgegenstände: Bei den Entwicklungsgegenständen kommen im Allgemeinen die RAM-Phasen 1 bis 11 vollständig zur Anwendung kommen. Der Vertiefungsgrad kann unter Berücksichtigung einer verfeinerten Betrachtung mit zusätzlichen Hierarchieebenen angepasst werden. Dies ist in den RAM-Plänen der Entwicklungsgegenstände zu dokumentieren.

SRP-21041 - Nachfolgende Abbildung zeigt den Lebenszyklus in der V-Darstellung auf beiden berücksichtigten Ebenen SR40 und Entwicklungsgegenstand (Projektebene), und zeigt die wichtigsten Verbindungen und Wechselwirkungen zwischen den Ebenen in Bezug auf Zuteilung der Anforderungen und Systemvalidierung auf. Der Übersichtlichkeit halber sind die RAM-Phasen 6 bis 8 mit niedrigem Vertiefungsgrad auf Ebene SR40 nicht dargestellt.

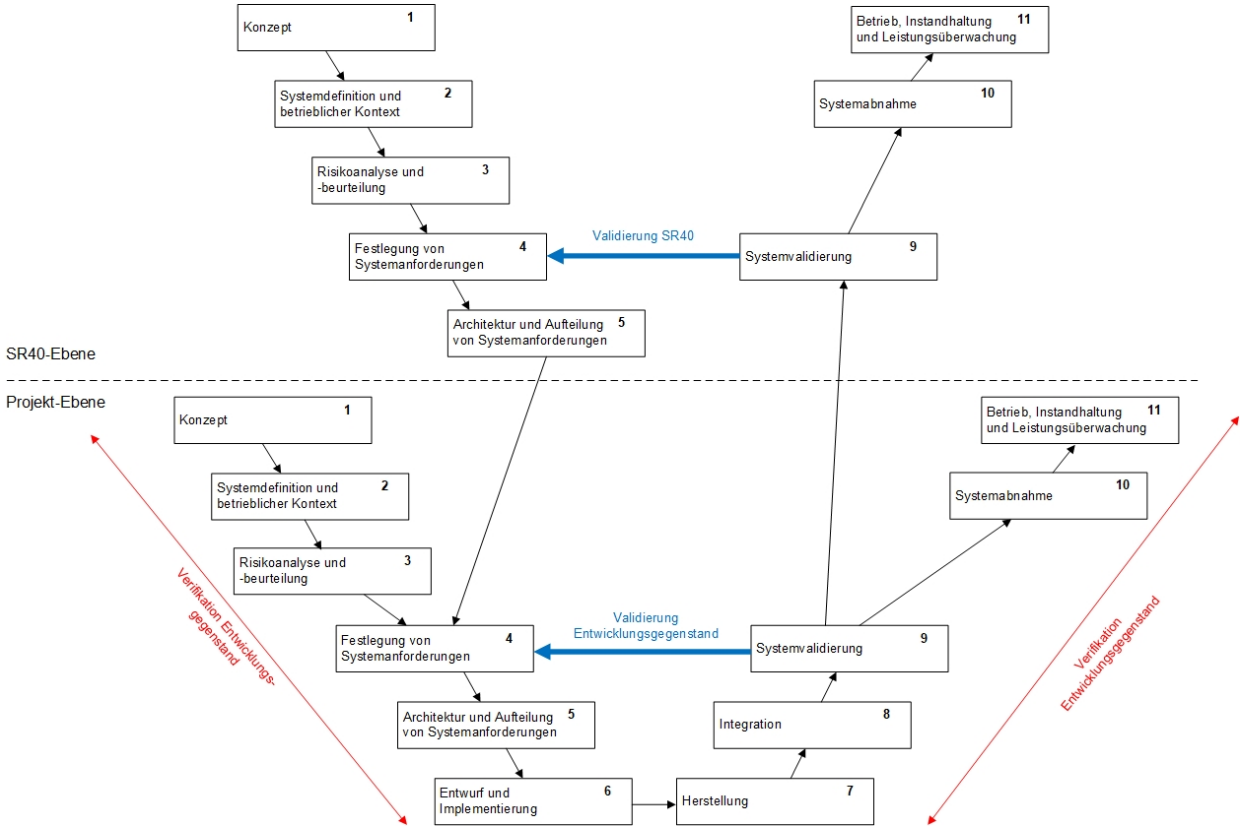
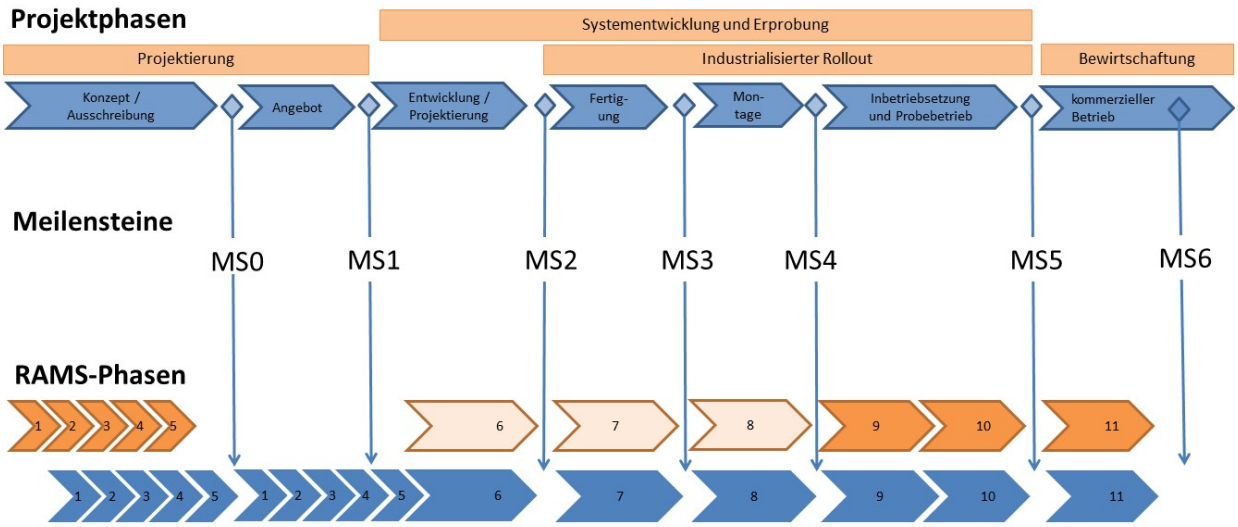


Figure 5 : Lebenszyklus in V-Darstellung für die Hierarchieebenen SR40 und Entwicklungsgegenstand

SRP-21045 - Der Zusammenhang und exemplarische zeitliche Ablauf zwischen Projektphasen und RAM-Phasen der Ebene SR40 (orange hinterlegt) und der Entwicklungsgegenstände (blau hinterlegt) sind in der nachfolgenden Abbildung dargestellt. Beispielhaft sind Projektmeilensteine der Entwicklungsgegenstände aufgeführt, die jedoch individuell in den einzelnen Projekten zu bestimmen sind. Die Projektphasen und der zeitliche Ablauf der Projekte können je nach Entwicklungsgegenstand von der Darstellung und in Relation zur Ebene SR40 abweichen, insbesondere in der übergeordneten Phase der Projektierung.

SRP-23385 -



MS0	Ausschreibung
MS1	Angebot
MS2	Freigabe Fertigung
MS3	FAT
MS4	SAT
MS5	Abnahme
MS6	Nachweis im kommerziellen Betrieb

Figure 6 : Projekt- und RAM-Phasen für die Ebenen SR40 und Entwicklungsprojekte

SRP-21038 - Auf Ebene SR40 werden vorerst die Phasen 1 bis 5 durchlaufen. In Phase 4 werden die RAM-Anforderungen (Zuverlässigkeits-, Verfügbarkeits- und Instandhaltungsanforderungen) an das System SR40 (gemäss Systemarchitektur) festgelegt, in Phase 5 erfolgt die Zuteilung an die einzelnen Blöcke bzw. Entwicklungsgegenstände als Eingangsgrösse für die Phase 4 der Entwicklungsgegenstände. Dies erfolgt anhand einer ersten Prognose auf Basis von Erfahrungswerten und typischer (Hersteller-)Werte. Auf Ebene des Entwicklungsprojektes werden die Analysen mit Fokus auf die Teilsysteme und Komponenten des jeweiligen Entwicklungsgegenstandes durchgeführt. Die Phasen 1 bis 5 werden auf Ebene des Entwicklungsprojektes bis zur Ausschreibung des Entwicklungsgegenstandes durchlaufen (je nach Entwicklungsgegenstand evtl. nur Phasen 1 bis 4), und werden anschliessend vom Lieferanten/Hersteller erneut untersucht. Die Aktivitäten der Phasen 6 bis 8 sind schwerpunktmässig auf Entwicklungsprojektebene angesiedelt. Die Validierung erfolgt auf Ebene der Entwicklungsprojekte und auf Ebene SR40 (siehe Kap. 4.9). Die Performance im Betrieb wird auf Ebene der Entwicklungsgegenstände aufgezeichnet und ausgewertet und auf Ebene SR40 anhand der betrieblichen Auswirkungen (ZVmin) überprüft.

4.6 RAM-Plan

SRP-23225 - Für sämtliche RAM-relevanten Entwicklungsgegenstände ist ein RAM-Plan gemäss Norm SN EN 50126 zu erstellen.

SRP-23224 - Die RAM-Pläne der Entwicklungsgegenstände werden in den jeweiligen Entwicklungsprojekten erstellt, wobei der RAM-Plan SR40 (vorliegendes Dokument) eine Richtlinie für die Erstellung darstellt. Es kann auf die Angaben in diesem Dokument verwiesen werden, sofern diese Angaben die Aktivitäten, Prozesse, Ressourcen, Methoden etc. auf Entwicklungsprojektebene ausreichend beschreiben. Insbesondere sind die Aktivitäten und Verantwortlichkeiten mit Bezug zu den Lieferanten/Herstellern in den RAM-Plänen der Entwicklungsgegenstände vertiefter zu beschreiben. Im RAM-Plan des Entwicklungsgegenstandes sind die zu erstellenden Dokumente und auch die Projektmeilensteine mit Datum aufzuzeigen. Die Dokumente müssen einem Review unterzogen werden.

SRP-23227 - Wenn Vorgaben aus dem RAM-Plan SR40 in den Projekten nicht angewendet werden sollen, ist das im RAM-Plan des Entwicklungsgegenstandes zu begründen und mit dem RAM-Management SR40 abzustimmen.

SRP-23226 - Der Prozess zur Erstellung ist im SPM (12899 RAM Plan erstellen) festgehalten.

4.7 Risk Management RAM

SRP-23235 - In Phase 3 des Lebenszyklus ist eine Risikobewertung durchzuführen. Diese umfasst Risikoanalyse und -beurteilung. Im RAM-Prozess sind RAM-Äquivalente zu Gefährdungen zu identifizieren und zu klassifizieren. Dies erfolgt grundsätzlich nach dem in der RAM-Strategie aufgestellten Prinzip: Potentielle Fehlzustände (Fehler oder Ausfälle) von System, Subsystem und Komponenten werden systematisch analysiert, unter Berücksichtigung von Technik, Mensch und Umwelt, und Auswirkungen auf die RAM-Performance bewertet. Als RAM-Äquivalente zu Gefährdungen sind Fehlzustände (Faults) anzusehen, die sich negativ auf die RAM-Performance bzw. betriebliche Leistungsfähigkeit auswirken können. Bevor die Risikoanalyse durchgeführt wird, ist die Kenntnis der Systemgrenzen des Betrachtungsgegenstands von grosser Wichtigkeit. Erst dann kann die Identifikation von Fehlzuständen korrekt erfolgen.

SRP-23234 - Sämtliche potentiellen Fehlzustände (Faults) und ihre Beurteilung werden systematisch in einem Störungsprotokoll erfasst. Das Störungsprotokoll wird als FMECA (System-FMECA und Konstruktions-FMECA) erstellt und enthält unter anderem die

identifizierten Störungen (Fehlzustände), ihre Risikobewertung und -beurteilung (Kritizität) und allfällige Massnahmen zur Minderung der Risiken.

SRP-23237 - Ein Störungsprotokoll wird sowohl auf Ebene SR40 erstellt als auch für jeden RAM-relevanten Entwicklungsgegenstand. Für Entwicklungsgegenstände auf unterschiedlichen Hierarchieebenen (z.B. Entwicklungsgegenstand "Block" innerhalb Entwicklungsgegenstand "Bahnanwendung") sind die Störungsprotokolle vom Vertiefungsgrad und vom Umfang her der Hierarchieebene entsprechend zu erstellen (z.B. prozessual bedingte Störungen im Zusammenhang mit der Bahnanwendung im Störungsprotokoll der Bahnanwendung, Störung einer Einzelkomponente im Störungsprotokoll des entsprechenden Blocks). Einzelstörungen auf einer unteren Ebene können als gesammelter Eintrag im Störungsprotokoll der höheren Ebene aufgenommen werden.
Die erstmalige Durchführung der FMECA erfolgt in der Phase 3. Das Störungsprotokoll ist über den gesamten Lebenszyklus zu pflegen. Im Projekt sind die Resultate und Informationen der Phasen 5 bis 10 jeweils mit dem Störungsprotokoll abzugleichen. Bei Identifikation zusätzlicher Störungen oder bei Änderung von Eingangswerten der Risikobewertung (Ausmasseinstufung, Häufigkeit, …), ist die Risikobeurteilung erneut vorzunehmen und, falls notwendig, sind Massnahmen zu definieren und umzusetzen.

SRP-23236 - Das Störungsprotokoll Ebene SR40 umfasst die Störungen der einzelnen Blöcke (sämtliche Blöcke gemäss Systemarchitektur) gesamthaft und ihre Auswirkungen. Damit werden zwei Ziele verfolgt:

- Identifikation der RAM-relevanten Blöcke
- Überprüfung der RAM-Ziele an die einzelnen Blöcke und an das System SR40. Die in den Entwicklungsprojekten ermittelten Prognosewerte werden für die verschiedenen Störungsklassen zusammengeführt und die betrieblichen Auswirkungen (ZVmin) quantifiziert.

SRP-23231 - Im Störungsprotokoll des Entwicklungsgegenstands ist die Analyse von der Bearbeitungstiefe bis auf die Ebene der einzelnen Elemente des Entwicklungsgegenstands entsprechend der Hierarchieebene durchzuführen. Je nach Hierarchieebene und Kenntnis der Systemarchitektur des Entwicklungsgegenstandes wird die FMECA als System-FMECA oder Konstruktions-FMECA durchgeführt (siehe Kap. 5.1.1). Als Störungsursachen sind zu berücksichtigen:

- Hardware
- Software

- Schnittstellen zu anderen Systemen
- Betriebliche Faktoren
- Faktoren der Instandhaltung
- Menschliche Faktoren
- Umwelt (mechanische, elektrische, natürliche Ursachen)

SRP-23230 - Nicht zu berücksichtigen sind bewusster Missbrauch sowie aussergewöhnliche oder seltene und gravierende Umweltereignisse, die zu Fehlern oder Ausfällen führen können (Naturkatastrophen, Unfallereignisse (z.B. Kollisionen), Brandereignisse, …).

SRP-23233 - Um eine Risikobeurteilung vornehmen zu können sind Risikoakzeptanzprinzipien (RAP) und Risikoakzeptanzkriterien (RAC) festzulegen. Aus den gemäss Norm drei möglichen, anzuwendenden RAP wird vorliegend die explizite Risikoabschätzung (qualitativ oder quantitativ) angewendet. RAC werden anhand des übergeordneten RAM-Ziels an den Entwicklungsgegenstand (gemäss Kap. 4.2.2) vom RAM-Management SR40 abgeleitet. Die Akzeptanz eines Risikos erfolgt immer unter der Betrachtung folgender Aspekte:

- Einhaltung definierter Risikogrenzwerte
- Kosten/Nutzen-Wirksamkeit von Massnahmen zur Risikominderung

SRP-23232 - Für Hardware oder Software sind die identifizierten Störungen zwingend zu quantifizieren bzw. einer vorgegebenen Klasse mit quantitativen Angaben zur Klassenbreite zuzuordnen. Für andere Störungsursachen sind die Risiken wenn möglich auch zu quantifizieren, wenn entsprechende Grundlagen (Statistiken, …) vorliegen, die eine Quantifizierung ermöglichen. Ansonsten können diese Risiken auch qualitativ bestimmt werden.

SRP-23229 - Die Methodik ist näher in Kap. 5.1 beschrieben. Der Prozess des Risikomanagements RAM ist im SPM (RAM Risiko Management - in Bearbeitung) festgehalten.

4.8 RAM-Nachweis (Phasen 1-x)

SRP-21037 - Zentrales Dokument des RAM-Nachweiskonzepts ist der RAM-Nachweis (Phasen 1-x), der sowohl auf Ebene SR40 als auch für die Entwicklungsgegenstände erstellt wird. Hierin werden im Sinne der SN EN 50126 alle Aktivitäten und Ergebnisse der RAM-Phasen 1-x dokumentiert oder anhand entsprechender Verweise referenziert. Der RAM-Nachweis wird mit Abschluss einer jeden Lebenszyklusphase (x) aktualisiert. Nach der RAM-Phase 10 gehen die RAM-Nachweise in den Verantwortungsbereich des Betreibers über.

SRP-23239 - Die Nachweisführung in den Entwicklungsprojekten erfolgt gegenüber den festgelegten, zugeteilten RAM-Zielen (MTTF, MTTR etc.), während im übergeordneten

Nachweis die betrieblichen Auswirkungen (ZVmin) einbezogen werden.

SRP-21040 - Der Prozess zum RAM-Nachweis ist im SPM (13088 RAM Nachweis Phasen 1-X erstellen) festgehalten.

4.9 Verifikation und Validierung, Reviews

SRP-21039 - Verifikations- und Validierungsaufgaben werden gemäss SN EN 50126 durchgeführt.

SRP-23238 - Die **Verifikation** wird am Ende einer jeden Lebenszyklusphase eines Entwicklungsgegenstandes durchgeführt. Das Ziel der Verifikation ist es nachzuweisen, dass die gelieferten Ergebnisse dieser Phase in jeder Hinsicht die Anforderungen dieser Phase erfüllen.

SRP-23240 - Das Projekt muss einen Verifizierer mit der Durchführung der Verifikation beauftragen. Der Verifizierer darf nicht selbst in der Entwicklungsphase des Projekts mitgearbeitet haben, kann aber ein Mitarbeiter eines anderen Projekts von smartrail 4.0 sein. Die Prüfprozesse und die damit verbundenen Tätigkeiten werden im Verifikationsplan festgeschrieben. Die Prüfergebnisse werden in einem RAM-Verifikationsbericht dokumentiert.

SRP-23241 - Jede Entwicklungsphase kann nur mit einer Verifikation abgeschlossen werden. Befunde aus der Verifikation sind vom Projekt auf Relevanz zu prüfen. Relevante Befunde sind zu beheben und vom Verifizierer erneut zu bewerten. Die Verifikation kann nur abgeschlossen werden, wenn keine relevanten Befunde mehr offen sind.

SRP-23242 - Der Prozess zur Verifikation ist im SPM (13215 Phase nach 50126 abschliessen und verifizieren - in Bearbeitung) festgehalten.

SRP-23243 - Die **Validierung** wird in den Lebenszyklusphasen 4 und 9 durchgeführt.
In Lebenszyklusphase 4 "Festlegung von Systemanforderungen" hat die Validierung das Ziel, sicherzustellen, dass die Systemanforderungen (einschliesslich der RAMS-Anforderungen) richtig und unter Anwendung der in Norm SN EN 50126 festgelegten Anforderungen sowie aller sonstigen speziellen durch den gesetzlichen Rahmen festgelegten Anforderungen festgelegt wurden.
In Lebenszyklusphase 9 "Systemvalidierung" hat die Validierung das Ziel, sicherzustellen, dass das betrachtete System die für den vorgesehenen Verwendungszweck oder die vorgesehene Anwendung festgelegten Anforderungen erfüllt.

SRP-21073 - Die Validierung erfolgt auf Ebene der Entwicklungsgegenstände und auf Ebene SR40. Die Mehrzahl der Anforderungen sind auf Ebene der Entwicklungsgegenstände definiert

und werden dort validiert. Auf der Ebene SR40 werden die Festlegung und Erfüllung der übergeordneten RAM-Anforderungen validiert. Für die Durchführung der Validierung ist eine unabhängige Validierungsstelle von smartrail 4.0 benannt worden. Der Validierungsprozess (Tätigkeiten und Prüfprozess, Verantwortlichkeiten, Bewertungskategorien, Massnahmen, Dokumentation) wird im Validierungsplan festgeschrieben. Die Prüfergebnisse werden in einem RAM-Validierungsbericht dokumentiert.

SRP-23245 - Befunde aus der Validierung sind vom Projekt auf Relevanz zu prüfen. Relevante Befunde sind zu beheben und vom Validierer erneut zu bewerten. Die Validierung kann nur abgeschlossen werden, wenn keine relevanten Befunde mehr offen sind.

SRP-23244 - Alle gemäss RAM-Plan zu erstellenden Dokumente sind einem **Review** zu unterziehen. Die vom RAM-Manager Project erstellten RAM-Dokumente werden vom übergeordneten RAM-Management SR40 einem Review unterzogen (formelles und technisches Review). Die von den Lieferanten / Herstellern erstellte RAM-Dokumentation wird sowohl vom RAM-Manager Project als auch vom übergeordneten RAM-Management geprüft und bewertet.

SRP-23247 - Relevante Befunde sind zu beheben und vom Reviewer erneut zu bewerten. Das Review kann nur abgeschlossen werden, wenn keine relevanten Befunde mehr offen sind.

SRP-23246 - Nachfolgend sind die erwähnten Rollen in einer Tabelle gegenüber gestellt:

SRP-23386 -

Aktivität	Reviewer	Verifizierer	Validierer
Phasenbezug der Prüfung	innerhalb Phase	Abschluss Phase	phasenübergreifend
Prüfung Normvorgaben und Prozesse	×	✓ Einhaltung	✓ adäquate Definition Prozesse sowie Stichproben der Einhaltung
Prüfung Arbeitsmethodik	×	✓ adäquate Auswahl+Einhaltung	✓ adäquate Methodensequenz
Materielle Prüfung der Arbeitsergebnisse	✓	✓ Stichproben (nach Ermessen Verifizierer)	✓ Stichproben (nach Ermessen Validierer)
Prüfung Review	×	✓	✓ Stichproben
Prüfung Gebrauchstauglichkeit in order to allow the system under consideration to serve the intended use or application	×	×	✓
Prüfung Verifizierung	×	×	✓

Table 2 : Abgrenzung der Rollen, mit "x" bezeichnete Felder zeigen an, dass die Aktivität von der Rolle nicht durchgeführt wird.

4.10 Aktivitäten der RAM-Aufgaben während des Lebenszyklus

SRP-21131 - Nachfolgende Tabelle zeigt die wichtigsten RAM-Aktivitäten im Programm SR40 auf Ebene der Entwicklungsprojekte auf. Grundsätzlich sind sämtliche Aktivitäten gemäss SN EN 50126 in den jeweiligen RAM-Phasen durchzuführen. Für die Phasen 1 bis 5 können die Entwicklungsarbeiten parallel erfolgen. Der Abschluss aller Entwicklungsphasen muss aber in der vorgegebenen Reihenfolge erfolgen. Für die Aktivitäten auf Projektebene wird i.d.R. in nachfolgender Tabelle der RAM-Manager Project als verantwortlich angesehen, unter Mitwirkung des Lieferanten/Herstellers bei extern erbrachten Leistungen. Wie bereits in Kap. 4.4.2 erwähnt, können diverse Verantwortlichkeiten auf den Lieferanten/Hersteller übertragen werden. Dies ist in den RAM-Plänen der Entwicklungsgegenstände festzuschreiben. Diese sind auch detaillierter auszuarbeiten im Hinblick auf durch den Lieferanten/Hersteller auszuführenden Aktivitäten, die spezifisch für die jeweiligen Entwicklungsgegenstände vorzusehen sind.

SRP-21133 -

RAM Phasen	RAM-Aktivitäten	Verantwortlich	Dokument
1 bis 5	Systemumfang, Zweck, Kontext des Entwicklungsgegenstands definieren	System Analyst	RAM-Nachweis Ph. 1-x
	Systemdefinition: • Einsatzprofil inkl. funktionale Anforderungen, Lebensdauer, Langzeitbetriebsstrategien und -bedingungen, Instandhaltungsbedingungen • Systemgrenze und Schnittstellen (Technik, Mensch, Umwelt) • Beeinflussung des Systems durch Umgebung / Schnittstellen	tbd	RAM-Nachweis Ph. 1-x
	RAM-Plan erstellen: • RAM-Politik und -	RAM-Manager Project	RAM-Plan Entwicklungsgegenstand

	Strategie festlegen • RAM-Management • Festschreiben der Organisation und Verantwortlichkeiten betreffend RAM • Anforderungen SN EN 50126-1 erfüllen • Aktivitäten und Werkzeuge im Lebenszyklus zur Sicherstellung ausreichender Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit bestimmen		
	RAM-Anforderungen und -Leistungsmerkmale des bestehenden Systems analysieren	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Identifikation und Bewertung von Fehlern / Ausfällen (RAM-Äquivalente zu Gefährdungen)	RAM-Manager Project	Störungsprotokoll (FMECA des Entwicklungsgegenstands)
	RAM-Anforderungen der Entwicklungsgegenstände festlegen, die nicht von der übergeordneten SR40 Ebene vorgegeben sind	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	vorläufige RAM-Analyse (Zuverlässigkeitsblockdiagramm, systematische SW-Fehler)	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Nachweis- und Abnahmeprozess definieren	RAM-Manager Project Validierungsstelle	RAM-Nachweis Ph. 1-x RAM-Plan Entwicklungsgegenstand Validierungsplan
	Verifikationsplan erstellen	Verifizierer Project	Verifikationsplan Project
	Verifikation, Verifikationsbericht erstellen	Verifizierer Project	Verifikationsbericht Project
	Validierungsplan erstellen	Validierungsstelle	Validierungsplan

	Validierung, Validierungsbericht erstellen	Validierungsstelle	Validierungsbericht
	Zuteilung der RAM-Anforderungen unter Berücksichtigung der Systemarchitektur: • Spezifikation der RAM-Anforderungen an Subsysteme und Komponenten • Vorgaben betreffend Instandhaltung und Instandhaltbarkeit • Festlegung der RAM-Abnahmekriterien und -prozesse für Subsysteme und Komponenten	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Übertragung der RAM-Anforderungen an UN	RAM-Manager Project	Pflichtenheft UN (Bem.: die Phasen 1 bis 5 sind auch vom UN zu untersuchen)
	Lebenszykluskostenanalyse	RAM-Manager Project	LCC sheet
6	Durchführen RAM-Analyse und -Vorhersage im Rahmen des Entwurfs und der Konstruktion von Entwicklungsgegenständen und Komponenten • Design Analyse und finale Festlegung Design	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Verifikation	Verifizierer Project	Verifikationsbericht Project
	Planen der RAM-Aufgaben für weitere Phasen: • Herstellung (Qualitätssicherung,	RAM-Manager Project	RAM-Nachweis Project

	Prüfprozess, Environmental Stress Screening) • Integration (Prüfung der Subsysteme und Komponenten auf RAM-Konformität, Verfahrensweisen für Installation und IBN, Prüfbarkeit eingebauter Teilsysteme und Komponenten) • Betrieb und Instandhaltung (Betriebs- und Instandhaltungsverfahren festlegen und vorbereiten, Bereitstellung von Ersatzteilen und Logistik-Support planen, Schulungsmassnahmen festlegen und vorbereiten) • Leistungsüberwachung (FRACAS)		
	Aktualisieren RAM-Plan	RAM-Manager Project	RAM-Plan Entwicklungsgegenstand
	Aktualisieren Validierungsplan	Validierungsstelle	Validierungsplan
	Aktualisieren LCC-Analyse	RAM-Manager Project	LCC sheet
7	Qualitätssicherungsmassnahmen	tbd	RAM-Nachweis Ph. 1-x
	RAM-Verbesserungsprüfung	tbd	RAM-Nachweis Ph. 1-x
	Environmental Stress Screening	tbd	RAM-Nachweis Ph. 1-x
	RAM-bezogene Inspektions- und Prüfberichte	tbd	RAM-Nachweis Ph. 1-x
	Verifikation	Verifizierer	Verifikationsbericht Project

		Project	
	Vorbereitung FRACAS	tbd	RAM-Nachweis Ph. 1-x
8 - 10	RAM-bezogene Inspektions- und Prüfberichte	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Verifikation	Verifizierer Project	Verifikationsbericht Project
	Vorkehrungen für den Systemsupport: • Mitarbeiterschulung • Verfügbarmachung von Verfahren für den Systemsupport • Erstellen von Ersatzteilvorgaben • Erstellen von Werkzeugvorgaben • Anwenderbedingungen an den Betreiber	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Validierung durchführen und abschliessen, Validierungsbericht erstellen	Validierungsstelle	Validierungsbericht
	Prozess für die Erhebung und Beurteilung von Betriebsdaten für die Betriebsphase einleiten	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	RAM-Nachweis Phasen 1 - 10 erbringen und abschliessen	RAM-Manager Project	RAM-Nachweis Ph. 1-x
	Aktualisieren LCC-Analyse	RAM-Manager Project	LCC sheet
11	Implementierung und Pflegen des FRACAS-Prozesses für die Erhebung und Aufzeichnung von Daten zur RAM-bezogenen Leistung	Betreiber (Unterscheidung zw. Erprobung und def. Betrieb)	
	Pflegen des FRACAS und	Betreiber	

	regelmässiges Überprüfen der FRACAS-Aufzeichnungen	(Unterscheidung zw. Erprobung und def. Betrieb)	
	Berichte zur Analyse und Beurteilung der RAM-Leistungsmerkmale	Betreiber (Unterscheidung zw. Erprobung und def. Betrieb)	
	Leistungsüberprüfung im Betrieb (HW- und insb. auch SW-Vorgaben)	Betreiber (Unterscheidung zw. Erprobung und def. Betrieb)	
	Aktualisieren LCC-Analyse mit nachgewiesenen Werten aus Betrieb	Betreiber (Unterscheidung zw. Erprobung und def. Betrieb)	
	Beurteilung der RAM-Implikation auf Änderungen und Nachrüstungen	Betreiber (Unterscheidung zw. Erprobung und def. Betrieb)	
12 (nicht im Projektfokus)	Ermitteln der RAM-bezogenen Auswirkungen von Ausserbetriebsetzung und Entsorgung	Betreiber	

SRP-23855 - Die RAM-Aktivitäten auf Ebene SR40 werden noch ergänzt.

4.11 Qualitätsmanagement

SRP-21069 - Für die RAM-Aktivitäten und -Dokumente gelten die Bedingungen und Anforderungen an die Qualitätspolitik im Programm SR40. Das Prozessmanagement ist im SPM definiert: SPM Management & Organisation.

4.12 Requirements Management

SRP-23259 - Das Requirements Management ist im Requirements Management Plan v2 beschrieben. Ein Prozess für das RAM Requirements Management wird erstellt (in Bearbeitung).

4.13 Konfigurations- und Änderungsmanagement

SRP-21067 - Die RAM-Nachweise der Realisierung beziehen sich jeweils auf einen bestimmten Konfigurationsstand einer Software oder Hardware, und, falls zutreffend, der dazugehörigen Software (embedded). Dokumentation und Bezeichnung von Hard- und Software müssen eindeutig einer Version zugeordnet werden können.

SRP-21059 - Bei späteren Änderungen an Hardware oder Software ist die Gültigkeit von früher durchgeführten Prüfungen und Nachweisen neu zu beurteilen und, falls notwendig, muss sie durch zusätzliche Prüfungen wiederhergestellt werden. Das Änderungsmanagement muss eine lückenlose Dokumentation der Änderungen sicherstellen. Der Prozess ist von den Verantwortlichen noch zu beschreiben.

4.14 Reporting

SRP-21063 - In regelmässigen, terminierten Sitzungen mit den RAM-Managern SR40 und dem RAM-Manager Project werden unter Leitung des übergeordneten RAM-Managements SR40 alle wichtigen RAM-Punkte abgestimmt. Bei Bedarf nehmen weitere Vertreter der Projekte an den Sitzungen teil. Die Sitzungsresultate werden protokolliert. Mittels Pendenzenlisten werden terminierte Aufgaben an Projekte und an das übergeordnete RAM-Management SR40 verwaltet.

SRP-21057 - Das Reporting auf Ebene der Entwicklungsprojekte ist in den entsprechenden Projekten festzulegen.

4.15 Allgemeine Anforderungen an zu verwendende Methoden

SRP-21087 - Für die Durchführung der RAM-Analysen sind auf allen Stufen möglichst einheitliche Werkzeuge zu verwenden.

SRP-21091 - Die Analyse für jede Betrachtungseinheit (System / Subsystem / Komponente) beinhaltet soweit zweckmässig und stufengerecht:

- Vollständiges Mengengerüst des Betrachtungsperimeters
- Berücksichtigung von Betriebsaufgaben, Umweltbedingungen, Lebenserwartung

- Anwendungsbedingungen
- Ermittlung von Einzel- und Mehrfachausfällen
- Berücksichtigung von Common Cause Failures (CCF), z.B. mittels beta-Faktoren
- RAM-Analysen zur Überprüfung der quantitativen RAM-Anforderungen
- Abhängigkeiten zu internen und externen Schnittstellen
- Quellenangaben zu RAM-Kennwerten
- Nachweisbarkeit, dass die für die RAM-Analysen angenommenen RAM-Kennwerte im architektonischen Systemzusammenhang realistische Werte darstellen (z.B. mittels FRACAS über einen aussagekräftigen Beobachtungszeitraum)

5 Methodik / Verfahren

5.1 RAM-Analyse

SRP-21090 - Für die Durchführung der RAM-Analysen auf SR40 Ebene und Projektebene ist eine einheitliche Vorgehensweise unter Anwendung bestimmter Werkzeuge vorzusehen. Für die Ermittlung der ZVmin gesamt auf Ebene SR40 kommt das **Verursacherprinzip** zur Anwendung, d.h. Störungen im Betrieb (Ereignisfolge) werden dem Entwicklungsgegenstand zugerechnet, bei dem der Fehlzustand auftritt (Ereignisursache). Dies wird bei der Zuteilung der RAM-Anforderungen auf die Entwicklungsgegenstände berücksichtigt. In der RAM-Analyse eines jeden einzelnen Entwicklungsgegenstands werden entsprechend nur die innerhalb des Entwicklungsgegenstands auftretenden Störungen zur Berechnung der RAM-Kennwert betrachtet. Dadurch werden Mehrfachzählungen von Störungen vermieden.

5.1.1 Failure Mode, Effects and Criticality Analysis (FMECA)

SRP-23854 - Grundsätzlich werden vorliegend zwei Arten der FME(C)A berücksichtigt:

- System-FMECA: Hierbei wird das System bzw. der Entwicklungsgegenstand auf Erfüllung von definierten Funktionen untersucht und Störungsarten, die zur Nichterfüllung der Funktion führen, identifiziert und bewertet. Diese Art wird verwendet, wenn die Systemstruktur nicht oder nicht detailliert bekannt ist.
- Konstruktions-FMEA: Ist die Struktur des Systems bzw. Entwicklungsgegenstand gut bekannt, erfolgt die Analyse auf Komponentenebene, wobei ebenfalls die Analyse mit Bezug zur definierten Funktion der Komponente erfolgt. Im Rahmen der Analyse können jedoch mehrere Komponenten zu einer Hauptkomponente zusammengefasst werden.

SRP-21084 - Auf Ebene SR40 wird ein Störungsprotokoll als System-FMECA SR40 geführt. In diesem werden alle Störungen unter Berücksichtigung des erwähnten Verursacherprinzips (Schnittstellenthematik), die Störungshäufigkeiten (ω), die Ausfalldauern sowie die Verfügbarkeiten pro Subsystem und Störungsklasse zusammengeführt und die betrieblichen Auswirkungen (ZVmin) quantifiziert und beurteilt.

SRP-23275 - Die FMECA SR40 enthält:

- als Systemelemente die Blöcke gemäss System-Architektur SR40
- eine Funktionsbeschreibung des Systemelements
- eine Störungsanalyse mit
    - möglicher Störungsursache (z.B. Hardware- oder Software-Fehler ohne nähere Untersuchung, wo die Ursache des Fehlers liegt oder wie dieser zustande kommt - dies erfolgt in der Analyse des Entwicklungsgegenstandes in den Projekten), und
    - der Auswirkung auf den Betrieb
- eine Klassifizierung der Schwere: es kommen die Störungsklassen zur Anwendung, die auch bei der Ziele-Herleitung verwendet werden (siehe Kap. 4.2.2). Diesen Störungsklassen sind quantifizierte Werte hinterlegt (Anzahl ZVmin pro Minute Ausfall). Zusätzlich wird eine Störungsklasse "0" definiert ohne Auswirkung auf den Betrieb.
- die RAM-Kennwerte der Blöcke (MTTF, MTTR und/oder Verfügbarkeit A): in einem ersten Schritt entsprechen diese Werte den auf übergeordneter Ebene bestimmten Kennwerten zur Herleitung der Ziele an die Blöcke, anschliessend werden die Werte durch die in den Analysen der Projekte ermittelten Werte ersetzt und kontinuierlich nachgeführt.
- die durch die Störung verursachten ZVmin
- als Akzeptanzkriterium das übergeordnete RAM-Ziel an den Block
- eine Beurteilung der verursachten ZVmin anhand des Akzeptanzkriteriums (Kritizität).

SRP-23276 - Weiter ist im Störungsprotokoll eine Aggregation sämtlicher durch die Blöcke verursachten ZVmin enthalten zur Überprüfung des Gesamtziels an SR40.

SRP-23277 - Ebenfalls im Störungsprotokoll enthalten ist eine Entscheidliste, die Entscheide zu den in den Projekten durchgeführten Analysen enthält, die zu einer Nicht-Einhaltung der übergeordnet an den Entwicklungsgegenstand vorgegebenen Ziele führt (z.B. aufgrund von Kosten/Nutzen-Erwägungen).

SRP-23302 - Ausgangspunkt der RAM-Analysen der Entwicklungsprojekte ist jeweils ein

Störungsprotokoll auf Ebene der Entwicklungsprojekte, unter Berücksichtigung allfälliger Hierarchieebenen innerhalb der Entwicklungsgegenstände (Anwendungen, Systeme, Blöcke, ...). Dieses Störungsprotokoll besteht jeweils aus einer FMECA des Entwicklungsgegenstandes (System- oder Konstruktions-FMECA), die folgendes beinhaltet:

- für die Betrachtung und Hierarchieebene zweckmässige Systemelemente. Dies können Teil-/Subsysteme, Funktionseinheiten (Hardware oder Software) oder Komponenten sein. Betreffend Hardware muss die FMECA der Blöcke schlussendlich bis auf Ebene der einzelnen Komponenten erstellt werden (Konstruktions-FMECA, erfolgt voraussichtlich beim Lieferanten/Hersteller). Es muss ein vollständiges Mengengerüst abgebildet sein.
- eine Funktionsbeschreibung des Systemelements
- eine Störungsanalyse mit
    - Störungsart (failure mode)
    - Störungsursache (failure cause)
    - Auswirkung im Subsystem
    - Auswirkung auf Funktionsweise der Umsysteme
    - Betriebliche Auswirkung (relevant für Bestimmung der ZVmin)
- Erkennungs- / Detektionsmodus
- eine Klassifizierung der Schwere: es kommen die Störungsklassen zur Anwendung, die auch bei der übergeordneten Ziele-Herleitung verwendet werden (siehe Kap. 4.2.2). Diesen Störungsklassen sind quantifizierte Werte hinterlegt (Anzahl ZVmin pro Minute Störung). Zusätzlich wird eine Störungsklasse "0" definiert ohne Auswirkung auf den Betrieb.
- Quantitative oder qualitative Angaben zu Eintretenswahrscheinlichkeit, quantitative Angaben zu Ausfalldauern:
    - für Hardware sind MTTF- und MTTR-Werte anzugeben
    - für Software sind Häufigkeiten und Ausfalldauern abzuschätzen und die Verfügbarkeit zu bestimmen
    - für andere Störungsursachen sind Häufigkeiten quantitativ zu bestimmen, falls entsprechende Methoden, Statistiken, Datenbankwerte o.ä. vorliegen. Andernfalls ist eine qualitative Abschätzung zu treffen. Zu diesem Zweck werden Häufigkeitsklassen vorgegeben (z.B. unwahrscheinlich / selten / gelegentlich / wahrscheinlich / häufig) mit quantifizierten Klassenbreiten (z.B. 1 mal pro Jahr bis 1 mal pro 10 Jahre). Für die Berechnungen des Risikos wird die Klassenmitte verwendet. Die Klassen werden in RAM Targets - Projects (in Bearbeitung) vorgegeben.

    - Allenfalls ist auch eine qualitative Bewertung nicht möglich. Diese Störungen müssen als nicht bewertbar gekennzeichnet werden. Wichtig ist, dass die möglichen Störungen zumindest identifiziert werden. Eine Einstufung lässt sich evtl. in einer späteren Projektphase vornehmen (Resultate und Informationen der Phasen 5 bis 10 sind jeweils mit dem Störungsprotokoll abzugleichen).
- das Risiko: dieses wird vorliegend ermittelt aus der Kombination der durchschnittlichen Ausfalldauer pro Jahr und der Störungsklasse. Die Einheit des Risikos ist ZVmin pro Jahr.
- Risikoakzeptanzkriterien (RAC): es werden zwei Grenzwerte definiert, die einem Bruchteil der übergeordneten Zielvorgabe an den Entwicklungsgegenstand entsprechen (z.B. unterer Grenzwert von 1% der ZVmin pro Jahr und oberer Grenzwert von 10% der ZVmin pro Jahr in der entsprechenden Störungsklasse). Die RAC werden in RAM Targets - Projects (in Bearbeitung) festgehalten.
- Risikobeurteilung (Kritizität) und Massnahmendefinition
    - Liegt das Risiko oberhalb des oberen Grenzwertes (roter Bereich) sind Massnahmen zu identifizieren und die Risikobeurteilung erneut vorzunehmen. Die Massnahmen sind auf Kosten/Nutzen-Wirksamkeit zu prüfen. Ist die Kosten/Nutzen-Wirksamkeit gegeben, so ist die entsprechende Massnahme umzusetzen. Die Massnahme fliesst als Anforderung an das Subsystem in die Phase 4 (Festlegung von Systemanforderungen) ein. Ist die Kosten/Nutzen-Wirksamkeit nicht gegeben, so ist das weitere Vorgehen mit dem RAM-Management SR40 abzustimmen. Die weitere Beurteilung erfolgt unter Berücksichtigung der Zielvorgabe an den Entwicklungsgegenstand sowie an das System SR40.
    - Liegt das Risiko zwischen den beiden Grenzwerten (gelber Bereich), sind Massnahmen zu identifizieren. Eine Kosten/Nutzen-Bewertung und allfällige Umsetzung ist vorerst in einem ersten Schritt noch nicht notwendig. Erst wenn die Zielvorgabe an den Entwicklungsgegenstand, die mittels Zuverlässigkeits-/Verfügbarkeitsberechnung überprüft wird (siehe Kap. 5.1.2), nicht eingehalten wird, sind für die Massnahmen Kosten/Nutzen-Bewertungen vorzunehmen. Kosten/Nutzen-wirksame Massnahmen sind umzusetzen (Systemanforderung).
    - Liegt das Risiko unterhalb des unteren Grenzwertes (grüner Bereich), ist vorerst keine Identifikation von Massnahmen erforderlich. Sollte jedoch die Zielvorgabe an den Entwicklungsgegenstand überschritten werden, und es können keine Kosten/Nutzen-wirksame Massnahmen bei rot- oder gelb-

klassifizierten Störungen identifiziert werden (sofern derart klassifizierte Störungen überhaupt vorliegen), sind auch für die grün-klassifizierten Störungen Massnahmen zu identifizieren und auf Kosten/Nutzen-Wirksamkeit zu prüfen. Kosten/Nutzen-wirksame Massnahmen sind umzusetzen (Systemanforderung).

- Für Risiken, die sich nicht einstufen lassen, sind vorkehrende Massnahmen gegen die Störung zu identifizieren. Handelt es sich dabei um aufwandgerechte, einfach umzusetzende Massnahmen (z.B. Checklisten), sind sie als Systemanforderung weiter zu berücksichtigen.

SRP-23281 - Mit diesem Vorgehen wird folgendes gewährleistet:

- Störungen werden systematisch erfasst und bewertet.
- Störungen, die zu einem hohen Grad zur Nicht-Verfügbarkeit des Entwicklungsgegenstandes beitragen, werden identifiziert und das Risiko nach Möglichkeit reduziert.
- Massnahmen werden auf ihre Kosten/Nutzen-Wirksamkeit geprüft.

SRP-23280 - Die Überprüfung der Zielvorgabe an den Entwicklungsgegenstand erfolgt mittels Zuverlässigkeits-/Verfügbarkeitsberechnungen (siehe Kap. 5.1.2). FMECA und Zuverlässigkeits-/Verfügbarkeitsberechnung sind sich ergänzende Instrumente und erfordern allenfalls ein iteratives Vorgehen in den RAM-Analysen. Der Nutzen von in der FMECA identifizierten Massnahmen kann allenfalls nur über die Zuverlässigkeits-/Verfügbarkeitsberechnung ermittelt werden.

5.1.2 Zuverlässigkeits- und Verfügbarkeitsberechnung, Sensitivitätsanalyse

SRP-21097 - Das Mengengerüst und die quantifizierten RAM-Kennwerte der einzelnen Elemente in der Subsystem-FMECA bilden die Grundlage für die **Zuverlässigkeits-/Verfügbarkeitsberechnungen**, anhand derer die Zielvorgaben der Entwicklungsgegenstände (MTTF, MTTR, A) je Störungsklasse überprüft werden. Die Berechnungen beinhalten Einzel- und Mehrfachausfälle unter Berücksichtigung der Systemstruktur, des Mengengerüsts, der Systemlogik und von Common Cause Failures (CCF). Für die CCF können beta-Faktoren gemäss SN EN 61508-6 hergeleitet und verwendet werden. Im Rahmen des Programms SR40 werden i.d.R. Zuverlässigkeitsblockdiagramme (RBD, SN EN 61078) zur Berechnung verwendet, andere Methoden wie Fehlerbaumanalysen (FTA, IEC 61025) sind jedoch auch zulässig.

SRP-23283 - Die in den Berechnungen verwendeten RAM-Kennwerte können Streuungen unterliegen. Dies betrifft vor allem jene Werte, welchen keine statistische Grundlage zugrunde liegt und abgeschätzt worden sind (wie z.B. Störungen infolge Software-Fehler). Es empfiehlt sich deshalb eine Sensitivitätsanalyse durchzuführen, um den Einfluss infolge Änderungen der RAM-Kennwerte auf die Zuverlässigkeit / Verfügbarkeit des Entwicklungsgegenstands aufzuzeigen. Es soll ein pessimistisches Szenario modelliert werden, für das jene RAM-Kennwerte verschlechtert werden, welche die grössten Unsicherheiten enthalten.

5.1.3 Redundanzen

SRP-23287 - In den RAM-Analysen können Redundanzen in der Architektur eines Entwicklungsgegenstandes in verschiedenen Fällen bereits als vorausgesetzt angesehen werden, z.B. wenn eine entsprechende Anforderung aus Safety-Sicht notwendig ist, oder aufgrund von normativen Vorgaben, oder falls die standardisierte Lösung dies ohnehin vorsieht. In diesen Fällen ist in der FMECA als Systemelement das redundanten Teilsystem aufzunehmen.

SRP-23286 - Bei Komponenten oder Systemelementen mit hoher Kritizität kann als Massnahme zur Erhöhung der Verfügbarkeit eine erhöhte Redundanz in der FMECA aufgenommen werden. Der Nutzen ist mittels Verfügbarkeitsberechnung, in der die Architektur des Entwicklungsgegenstandes abgebildet ist, zu überprüfen, die Bewertung in der FMECA vorzunehmen.

SRP-23288 - Wenn als Massnahme eine Redundanz identifiziert wird, ist es wichtig anzumerken, um welche Art von Redundanz (kalte, heisse, passive Redundanz) es sich handelt und welche Umschaltzeit von einem Kanal auf den anderen erwartet wird.

SRP-23285 - Grundsätzlich sind Redundanzen immer auf Kosten/Nutzen-Wirksamkeit zu prüfen. Auch vorausgesetzte Redundanzen sollten dahingehend hinterfragt werden, solange sie nicht aus Safety-Sicht notwendig sind.

5.1.4 Schnittstellen

SRP-23291 - Schnittstellen sind ebenfalls in der System-FMECA zu berücksichtigen und zu analysieren. Es gilt, wie erwähnt, das Verursacherprinzip.

SRP-21099 - Dabei ist zwischen SR40-internen Schnittstellen zwischen den Entwicklungsgegenständen, Schnittstellen zu Gewerken des Bahnbetreibers, aber ausserhalb der SR40-Systemgrenze, sowie Schnittstellen zu externen Dritten zu unterscheiden:

SRP-21094 -

- Schnittstellen SR40-intern: Berücksichtigung RAM-relevanter Einflüsse von Schnittstellenpartnern. Über den Schnittstellenprozess (in Erarbeitung) werden die Fehler und ihre Auswirkung beim Verursacher eingespeist. Die Risikobeurteilung erfolgt beim Verursacher (Verursacherprinzip).

SRP-21093 -

- Schnittstellen zu Betreiber-Gewerken (z.B. Gebäudeinfrastruktur): auf Ebene des Entwicklungsgegenstandes werden quantifizierte Anforderungen an die Zuverlässigkeit / Verfügbarkeit der Schnittstellenpartner gestellt (z.B. Stromversorgung oder HLK-Anlage), die vom Schnittstellenpartner zu erfüllen sind und im weiteren RAM-Prozess SR40 als gegeben angesehen werden (keine Überprüfung oder Nachweisführung im SR40).

SRP-21096 -

- Schnittstellen zu Dritten (z.B. externe Energieversorgung): die quantifizierte Zuverlässigkeit / Verfügbarkeit der Leistung des Drittanbieters muss ermittelt werden (Abschätzung anhand Erfahrungswerten, statistische Auswertung oder Angaben beim Drittanbieter einholen) und in der Gestaltung der Systemarchitektur des Entwicklungsgegenstandes berücksichtigt werden (z.B. USV mit n+1- oder 2n-Redundanz), sodass die Zuverlässigkeit / Verfügbarkeit der extern erbrachten Dienstleistung möglichst keine Verschlechterung der Verfügbarkeit des Entwicklungsgegenstandes zur Folge hat. Diese Analyse erfolgt mittels RBD oder FTA.

5.1.5 Instandhaltbarkeitsanalyse

SRP-21100 - In der Instandhaltbarkeitsanalyse wird überprüft, ob die Vorgaben betreffend MTTR des Entwicklungsgegenstandes (bzw. MFDT / MLD / MRT der Komponenten, falls erforderlich) eingehalten werden. Anhand des Mengengerüsts und der MTTF-Werte in der FMECA ist zudem die Anzahl an Instandsetzungseinsätzen (korrektive Instandhaltung) zu bestimmen. Falls diese betriebsseitige Vorgaben überschreitet (Abstimmung mit OCT), sind entsprechende Gegenmassnahmen vorzusehen.

5.2 Nachweis- und Abnahmeverfahren

SRP-21095 - Der Nachweis der Erfüllung der RAM-Anforderungen erfolgt durch Validierung nach Validierungsplan. Das Nachweiskonzept wird im Validierungsplan festgelegt.

SRP-21102 - Die RAM-Abnahmekriterien sind in den jeweiligen RAM-Nachweisen der Phasen 1-x (Ebene SR40 und Entwicklungsgegenstände) dokumentiert oder referenziert und im Polarion (requirements management) erfasst.

SRP-21101 - Der Nachweis der RAM-Anforderungen wird ebenfalls in den jeweiligen RAM-Nachweisen der Phasen 1-x dokumentiert. Der Nachweis, dass die angenommenen RAM-Kennwerte der Komponenten und Subsysteme erfüllt werden, wird mit Hilfe eines implementierten FRACAS durchgeführt (siehe Kap. 5.3). Mit dem FRACAS werden die in der Analyse angenommenen RAM-Kennwerte im Betrieb regelmässig überprüft und bei signifikanten Abweichungen Verbesserungs- oder Anpassungsmassnahmen vorgesehen.

SRP-21092 - Die Plattform und die konkreten Prozesse für den Nachweis der Wirksamkeit der präventiven und korrektiven Instandhaltung bzw. der Einhaltung der RAM-Anforderungen im Betrieb (FRACAS) sind noch zu definieren. Dies erfolgt in Abstimmung mit DMDC.

SRP-21080 - Weitere für die Entwicklungsgegenstände erforderliche, spezifische Nachweis- und Abnahmeverfahren sind in den jeweiligen RAM-Plänen festzuschreiben (z.B. Verfahren zum Nachweis der MRT im Rahmen der Abnahme).

5.3 FRACAS

SRP-21078 - FRACAS (Failure Reporting, Analysis, and Corrective Action System) ist ein System für die Berichterstattung bei Fehlern, die Fehleranalyse und entsprechende Korrekturmassnahmen. Es dient primär zur Überwachung und Sicherstellung der RAM-Anforderungen des Systems. Der Prozess kann in die vier Stufen Datenerfassung (Erfassung von technischen Daten, Instandhaltungsmassnahmen, Berichts- und Korrekturmassnahmen), Auswertung, Verbesserungsmassnahmen und Überprüfung eingeteilt werden.

SRP-21082 - Der Prozess wird bereits in der Phase der Erprobung angewendet, zum einen als Nachweis, dass die bis zum industrialisierten Rollout gewonnenen Felddaten den RAM-Prognosen nicht widersprechen, zum anderen um Korrekturen und Verbesserungsmassnahmen bereits in den industrialisierten Rollout einfliessen zu lassen.
Der Prozess sowie die Vorgaben an die Datenerfassung, -Auswertung und Berichterstattung sind mit DMDC abzustimmen.

5.4 Ersatzteile und Instandhaltungsmanagement

SRP-21081 - Als Methode zur Bestimmung der Instandhaltungsstrategie ist RCM (Reliability Centered Maintenance, SN EN 60300-3-11) vorgesehen. Es handelt sich um einen systematischen Ansatz zur Implementierung eines kosteneffektiven Instandhaltungsprogramms, das eine zuverlässigen und sicheren Betrieb des Systems gewährleistet. Die FMECA bildet dabei den ersten Schritt des RCM ab zur Identifikation kritischer Störungen und ihrer Auswirkungen.

SRP-21075 - Der RCM-Prozess stellt sicher, dass die effizienteste Instandhaltungsaufgabe für jede Komponente bzw. Entwicklungsgegenstand definiert wird basierend auf der Kritikalitätsrangfolge der Störungen. Um eine hohe Qualität der RCM-Analyse zu gewährleisten, ist der Prozess und die notwendigen Instandhaltungsplanungen und -tätigkeiten (Instandhaltungsorganisation, -prozesse und -planung, Ersatzteilekonzept und -listen, …) in enger Zusammenarbeit der Lieferanten/Hersteller mit dem Betreiber zu erstellen. Das Ersatzteilekonzept muss die RAM-Anforderungen an Instandsetzungszeiten und Verfügbarkeiten berücksichtigen. Die Analyse zur Bestimmung der Ersatzteilvorhaltung erfolgt auf Basis der vorgesehenen Nutzungsdauern, Ausfallraten, Lieferzeiten und Anzahl verbauter Komponenten. Weiter sind die Betreibervorgaben betreffend Ersatzteillagern und Logistikkette zu berücksichtigen.

5.5 Requirements Management

SRP-21074 - Die Methodik ist im Requirements Management Plan v2 beschrieben.

5.6 Konfigurations- und Änderungsmanagement

SRP-21077 - Die Methodik ist von den Verantwortlichen noch zu beschreiben.

5.7 LCC, Kosten/Nutzen-Analysen

SRP-21076 - In den Kosten/Nutzen-Analysen betreffend Massnahmenumsetzung sind nicht nur die Investitionskosten relevant, sondern auch jene Kosten, welche während der Lebensdauer (LCC) anfallen (Betriebskosten, Instandhaltungskosten, ...). Im Rahmen der Analyse wird die monetarisierte Risikominderung (Nutzen = Reduktion ZVmin) den LCC gegenübergestellt und auf Wirksamkeit überprüft. Die zu berücksichtigenden Kosten je ZVmin werden den Projekten mitgeteilt.

SRP-23294 - Die Methodik für die LCC-Ermittlung inkl. der Diskontierung der Kosten auf den Zeitpunkt null ist von den Verantwortlichen noch zu beschreiben.

6 Dokumente der RAM-Aktivitäten

SRP-21089 - Übergeordnet auf Ebene SR40 (nicht abschliessend):

- RAM-Plan SR40
- RAM-Nachweis SR40 (Phasen 1-x)
- Störungsprotokoll (FMECA SR40)
- RAM-Ziele SR40 und Störungsklassen
- RAM-Ziele Projects (Herleitung und Zuteilung der Anforderungen an die Blöcke bzw. Entwicklungsgegenstände)

SRP-21104 - Auf Ebene der einzelnen Entwicklungsgegenstände (nicht abschliessend):

- RAM-Plan
- RAM-Nachweis (Phasen 1-x)
- Störungsprotokoll (FMECA des Entwicklungsgegenstandes)

Es ist anzumerken, dass für die Ausschreibung ergänzende RAM-Dokumente erstellt werden (z.B. RAM-Pflichtenheft für Lieferanten / Hersteller).

SRP-21103 - Die Dokumente werden jeweils phasengerecht aktualisiert.