OC-Point Risiko Analyse

Document Properties

Status: **draft**

Version: **1**

Owner: Ryf Urs (I-SR40-PMO-EXT)

Contributors: Sobel Jörg (I-NAT-SR40-PMO-EXT - Extern), Merk Andreas (I-NAT-SR40-PMO-FSP), Zaripov Yan (I-NAT-SR40-PMO-EXT - Extern), Ryf Urs (I-SR40-PMO-EXT)

Document history

Version (revision)	Changes	Document Owner	Approved
1 (455924)		Ryf Urs (I-SR40-PMO-EXT)	

Dieses Dokument ist ein Entwurf und Bedarf weiterer Formalisierungen und Präzisierungen.

Inhaltsverzeichnis

1 Informationen zum Dokument

1.1 Verwendungszweck und Zielgruppe

OCSR-1041 - Nach dem Prozess SPM-12894 - Safety Risk Assessement und Hazard Management und dem OC Safety Plan sind für die Gefährdungs-Identifikation und Risikoanalyse zwei Methoden anzuwenden:

1. STPA
2. FMEA, Risikoanalyse mit DIN VDE V 0831-103

STPA ist eine Top-Down-Methode, FMEA eine Bottom-Up-Methode. **[** draft **]**

OCSR-954 - Ziel der STPA Step 1 Analyse ist die Identifikation der unsicheren Kontrollaktionen: Unsafe Control Actions (UCAs). Die STPA-Methode ist beschrieben in: *SR40_Programm/STPA Hazard Analysis/STPA Hazard Analysis Plan DE* und wird für Leser dieses Dokuments als bekannt vorausgesetzt.
Die dieser Analyse zugrunde liegende Hierarchische Kontrollstruktur (HCS) ist beschrieben in STPA OC-Point HCS Fahrweg über Weiche
Auf Basis dieser HCS werden in der Step1 Analyse die Control Actions daraufhin analysiert, ob sie Sub-System Level Hazards verursachen können, d.h. ob sie unter bestimmten Bedingungen und in einem bestimmten Kontext als "Unsafe" Control Actions (UCA) auftreten können. Diese werden auf die Top System Level Hazards [*SR40_Programm/STPA Hazard Analysis/STPA Basic System Level Hazards EN*] gemappt. Die Analysen werden mit dem STPA-Tool SAHRA graphisch dokumentiert (Mind Map) und in Tabellen mit weiteren Erläuterungen ergänzt. **[** draft **]**

OCSR-1042 - Aus den identifizierten UCAs werden qualitative Sicherheitsanforderungen abgeleitet (sogenannte "Controller Constraints"). Die aus der vorliegenden Analyse abgeleiteten sind in Kapitel 4 zusammengefasst. **[** draft **]**

OCSR-955 - Ziel der DIN VDE V0831-103 [REF011] ist eine mit semi-quantitativen Verfahren Risiken technischer Funktionen in der Eisenbahnsignaltechnik zu analysieren und Sicherheitsanforderungen abzuleiten. Die in der HCS identifizierten Control Actions können auch auf Funktionen in der Sichtweise Norm der gemappt werden. Die Norm bezieht sich an verschiedenen Stellen auf die CSM-RA Verordnung EU/402/2013. Die Norm analysiert für gegebene Funktionen das Schutzziel, Ausfallarten, Auswirkungen (Worst Case Scenarios) und gibt jeweils Mitigations-Massnahmen und quantitative Sicherheitsanforderungen vor. Die aus der vorliegenden Analyse abgeleiteten sind in

Kapitel 4 zusammengefasst. **[** draft **]**

OCSR-1044 - Ziel STPA Step 2 Analyse ist Ursachen zu analysieren und Mitigations-Massnahmen festzulegen. Auf Basis der HCS werden Control Loops mit UCAs festgelegt und mögliche Ursachen analysiert. Die Analysen werden mit dem STPA-Tool SAHRA graphisch dokumentiert (Mind Map) und in Tabellen mit weiteren Erläuterungen ergänzt. Siehe Kapitel 6 **[** draft **]**

OCSR-1043 - Ziel STPA-Sec ist Ursachen aus dem Security Umfeld zu analysieren. Auf Basis der Control Loops erweitert mit physikalischen Netzwerk Nodes und Verbindungen werden Ursachen und Mitigations-Massnahmen anaysiert. Siehe Kapitel 7. **[** draft **]**

1.2 Stand der Bearbeitung

OCSR-957 -

Datum	Bearbeitung durch	Beschreibung Bearbeitungsstand
03.03.2020	Ryf, Urs	**Erstentwurf**
		Baseline für Safety Team Review
		Freeze
		Finale Ausarbeitung

Table 1 : Tabelle Stand der Bearbeitung

[draft **]**

Rollen und Verantwortlichkeiten sind im HCS Dokument STPA OC-Point HCS Fahrweg über Weiche festgelegt.

Eingangsdokumente und Referenzen sind im HCS Dokument festgelegt und definiert.

2 Gefährdungen und Unfälle auf Systemebene

OCSR-959 - Für die Analyse der Gefährdungen und Unfälle auf Systemebene OC-Point ist der Ausgangspunkt: **[** draft **]**

OCSR-960 - Grundlegenden Gefährdungen auf Systemebene SR40 aus dem Dokument *SR40_Programm/STPA Hazard Analysis/STPA Basic System Level Hazards EN* müssen auf den Kontext OC-Point heruntergebrochen werden. Nur Top Hazard TLH2 hat Sub-Hazards auf OC-Point Ebene, da der OC-Point keinerlei Informationen über Movable Objects (Fahrzeuge) hat.

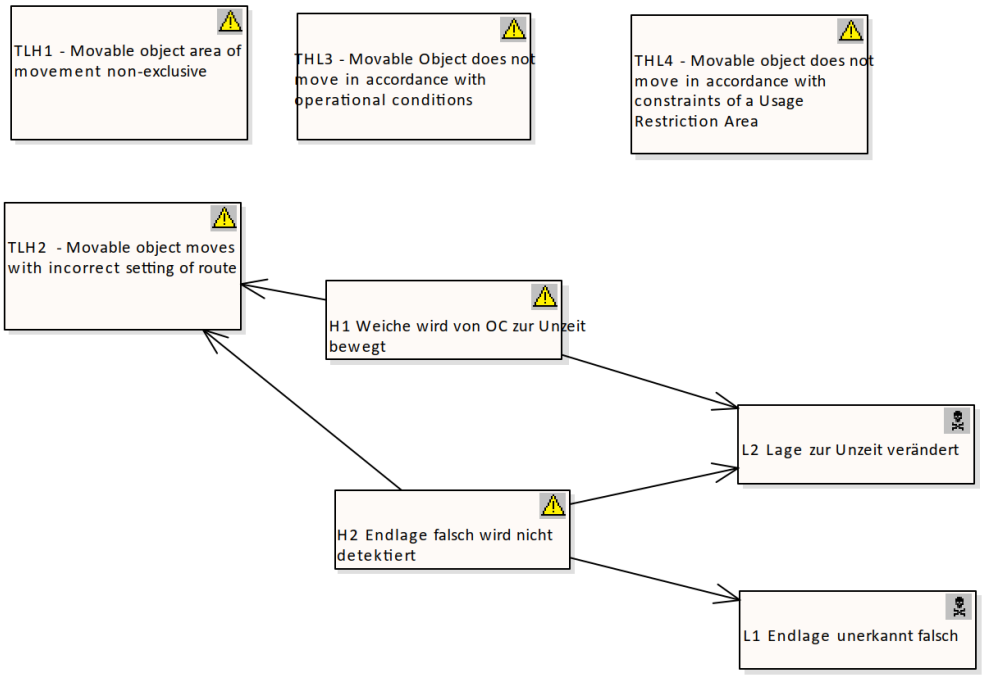


Figure 1 STPA Fundamentals

[draft **]**

OCSR-961 - Die Zusammenstellung von Unfällen aus ☐ SRP-14892 **[** draft **]**

OCSR-965 - Liste Sub System Level Hazards für "Fahrweg über Weiche bereitstellen": [draft **]**

OCSR-966 - *Sub-Hazard (H1) - Weiche wird von OC zur Unzeit bewegt*. Die Weiche wird umgestellt, wenn bereits ein Zug auf der Weiche ist oder demnächst darüber fahren wird, obwohl ein anderer Fahrweg geplant ist. Oder eine Schutzweiche wird zur Unzeit umgestellt und kann so ihre Schutzwirkung nicht mehr ausüben. **[** draft **]**

OCSR-967 - *Sub-Hazard (H2) - Endlage falsch wird nicht detektiert*. Die Endlage der Weiche in Realität entspricht nicht dem erwarteten Wert für die geplanten Fahrweg. **[** draft **]**

OCSR-969 - Liste der System Level Losses für "Fahrweg über Weiche bereitstellen" [draft **]**

OCSR-970 - *System Level Loss (L1).* Lage zur Unzeit verändert. **[** draft **]**

OCSR-971 - System Level Loss (L2). Endlage unerkannt falsch **[** draft **]**

3 Control Actions Analyse

OCSR-975 - In diesem Abschnitt werden die Analyse-Ergebnisse der Leitwort-Analyse für jede Control Action auf dem Analysemodell dokumentiert. Die Dokumentation für jede Control Action besteht aus folgenden Teilen: **[** draft **]**

OCSR-976 - Visualisierung der Gefährdungsanalyse für die Control Action. Dies ist ein Export aus "Enterprise Architect" von Sparx mit der Extension SAHRA von ZHAW. **[** draft **]**

OCSR-977 - Tabelle zur Leitwortanalyse mit verschiedenen Leitworten und verschiedenen Interpretationen. Diese enthält Control Action, Leitwort, eine passende Interpretation, Annahmen, daraus resultierend Fehlerart / Fehlermodus. **[** draft **]**

OCSR-1032 - Tabelle mit Verweis auf die Risikoanalyse nach VDE V 0831-103 [REFxxxx]. Diese enthält Schutzziel, Rahmenbedingungen, Ausfallarten der Funktion, Auswirkungen, Sicherheitsanforderung. **[** draft **]**

3.1 Control Action "CA1 DPS bereitstellen"

OCSR-981 - *Step1 CA-Analyse: "CA1 DPS bereitstellen"*

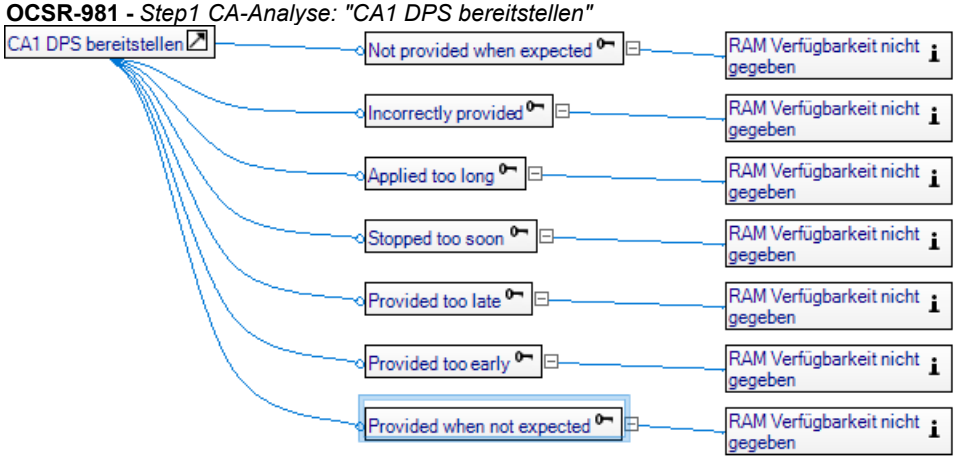


Figure 2 : CA1 Analyse

[draft **]**

OCSR-984 - *UCA1 aus "CA1 DPS bereitstellen"*

Sender	TMS
Receiver	APS
Control Action	CA1 DPS bereitstellen
Key Word	siehe Figure oben
Interpretation of Key Word	"Not provided when expected", "Incorrectly provided", "Applied too late", "Stopped too soon", "Provided too late", "Provided too early", "Provided when not expected": Wenn DPS nicht rechtzeitig bereitsteht, wird Produktionskapazität beeinflusst.
UCA Description	Safety: keine RAM, Security: DPS wird nicht rechtzeitig bereitgestellt, Verspätungen entstehen.
Analysis Result Safety	**safe**
Analysis Result RAM, Security	beeinflussbar
List of Hazards	keine
List of Threats	Direkt: Keine (T1) Indirekt: Das anfragende System (TMS) ist nicht autorisiert. (T2)
List of Potential Losses	Safety: keine Security: keine RAM:
Worst Case Scenario	Safety: keine RAM, Security: keine DPS werden an OC übermittelt. Kein Fahrweg wird bereitgestellt und kann befahren werden. Keine Produktionskapazität verfügbar.
Mitigation Measures	Safety: keine Security: Nur Security-zertifizierte TMS dürfen mit APS kommunizieren (T2) RAM:

[draft]

OCSR-1019 - Ergebnis der Analyse: keinen Anhaltspunkt für Gefährdungen

Grund: warum keine UCAs gefunden werden konnten -> siehe Analyse Figure oben

[draft]

OCSR-1031 - Risikoanalyse nach VDE V 0831-103 [REF011]

Funktion nach Ziffer	B.2.1 "Fahrstrasse einstellen"
Schutzziel	sicherstellen, dass entsprechend der Stellvorgabe die beabsichtigte Fahrstraße einläuft
Rahmenbedingungen	- die Funktion wird als Schutzfunktion benötigt, wenn entsprechend der Kompatibilität des Fahrzeuges zum Fahrweg (z.B. für Züge mit Lademaßüberschreitung) nicht alle Fahrwege geeignet sind - die Sicherung der Fahrstraße ist nicht betroffen; diese Funktion wird separat betrachtet
Ausfallarten der Funktion	a) nicht der Stellvorgabe entsprechender Fahrweg eingestellt
Auswirkungen (Worst Case Szenarien)	a1) bei Reisezügen mit übergroßen Fahrzeugen, wenn der Fahrweg hier für nicht geeignet ist: Aufprall auf bauliche Anlagen neben dem betroffenen Gleis (=Unfallklasse B, da davon ausgegangen werden darf, dass die durchgehenden Hauptgleise geeignet sind und somit ein Aufprall bei Fahrt durch ein nicht durchgehendes Hauptgleis nur mit geringer Geschwindigkeit erfolgt) a2) wenn haltender Reisezug in Gleis ohne Bahnsteig eingelassen wird: Aussteigeunfall(=Unfallklasse C, da mehrere Reisende betroffen sein können) a3) bei Güterzügen mit Lademaßüberschreitung, wenn der Fahrweg hierfür nicht geeignet ist: Aufprall auf bauliche Anlagen neben dem betroffenen Gleis (=Unfallklasse B)
Schutzobjekt	siehe Norm
Bewertung von Barrieren	siehe Norm
Risiko Score Matrix	siehe Norm
Sicherheitsanforderung an Schutzfunktion	10 E-5/h Diese Sicherheitsanforderung gilt auch für das Einstellen eines Fahrweges durch Einzelumstellung der betreffenden Weichen (im Störungsfall), da die Abläufe bei Ausfallart a) analog sind. -> Issue: Unterschiedliche Bewertung aus STPA und VDE 0831-103 ist weiter zu analysieren. -> Gemäss System Konzept sind Zugkontrolleinrichtungen (Ladegut, Lichtraumprofil, etc.) nicht Bestandteil des Projekts OC

[draft]

3.2 Control Action "CA2 Move Point"

OCSR-1018 -

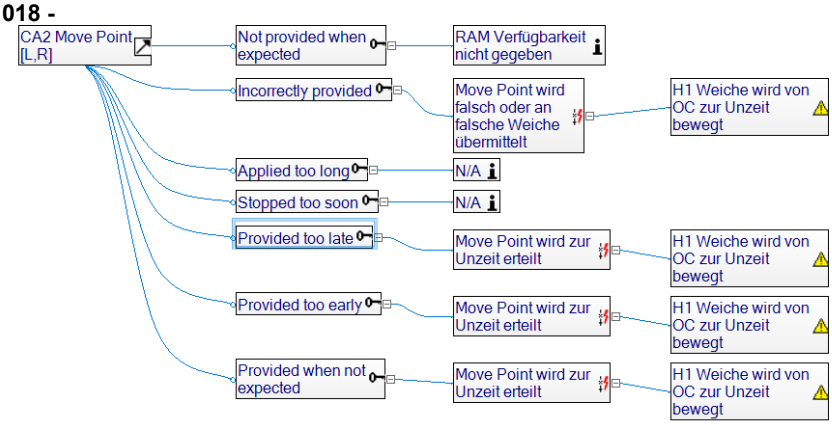


Figure 3 CA2 Analyse

[draft]

OCSR-985 - Worst Case Scenario: UCA-AS-aus Move Point

Eine Weiche wird während einer Zugfahrt umgestellt. Wenn der Zug direkt über der Weiche ist, wird ein Teil links und

der andere rechts weiterfahren, was den Zug zum Entgleisen bringen wird. Oder es kommt zu einem Zusammenstoss mit einem Zug auf einem anderen Fahrweg oder einer Kollision mit Objekten neben den Geleisen. **[** draft **]**

OCSR-1029 - *UCA2-aus CA2 Move Point*

Sender	APS
Receiver	OC-Point
Control Action	CA2 Move Point
Key Word	siehe Figure oben
Interpretation of Key Words	"Not provided when expected" Die Weiche wird nicht umgestellt, die Bahnproduktion kann nicht ausgeführt werden. Setzt voraus, dass APS die Endlage überprüft. "Incorrectly provided": Die Weiche erhält verfälschte Aufträge, in welche Richtung sie umgestellt werden soll oder die falsche Weiche wird andressiert. "Applied too long", "Stopped too soon": N/A da Kommando zu einem diskreten Zeitpunkt gesendet wird. "Provided too early", "Provided when not expected": Die Weiche wird umgestellt, obwohl noch kein Kommando erteilt wurde. "Provided too late": Die Weiche wird umgestellt, obwohl kein Kommando mehr erwartet wurde.
UCA Description	Move Point wird zur Unzeit ausgeführt
Analysis Result Safety	**unsafe**
Analysis Result RAM, Security	beeinflussbar
List of Hazards	siehe Figure oben
List of Threats	APS: • CST1 Eine Integritätsverletzung von Software und Daten führt zu falschen Entscheidungen und SF1 wird erzwungen und/oder SRAC1 manipuliert Kommunikation APS->FOT->OC: • CST2 Es werden nicht vom APS autorisierte Kommandos (inject) zur Weiche gesendet (SF1) • CST3 Autorisierte Kommandos werden in ihrer zeitlichen Abfolge manipuliert (z.B. nach der Endlageauswertung) Kommunikation OC->FOT->APS: • CST4 Die Information der Weichenlage wird manipuliert (SRAC1)
List of Potential Losses	siehe Figure oben
Worst Case Scenario	siehe oben
Mitigation Measures	Safety: SF1 Weiche zur Unzeit umstellen verhindern. Unzeit = Erlaubnis von APS zur Umstellung liegt nicht vor. SRAC1 APS muss Endlage der Weiche überwachen und bei Abweichungen Zugfahrten verhindern. Security:

	MCST1: Sicherung und Überwachung des APS mit geeigneten Massnahmen
	• Prevent: Trusted and Protected Computing Environment
	• Detect: Intrusion Detection System, Regular system plausibility checks
	• Respond: Nothalt des Systems und gesamten kontrollierten Bereiches
	MCST2: Kommandos werden mit Autorisierungsinformationen angereichert
	• Prevent: Signatur oder Verschlüsselung des Kommandos
	• Detect: Empfänger (OC) meldet jegliche Verletzung der Signatur oder der Verschlüsselung
	• Respond: Überprüfung und Erhöhung der Kommunikationsüberwachungsmassnahmen bei Vorfall und Wiederaufnahme der Kommunikation
	MCST3: Die Kommunikation muss an zeitliche parameter gebunden und überprüft werden
	• Prevent:
	  • L1 Kommandos werden Zeitgebunden und mit CST2 gesichert (Secure Time)
	  • L2 Kommandos erzeugen einen direkten Feedback so das eine zeitliche Abweichung/Manipulation erkannt wird.
	• Detect:
	  • L1/L2 Kommandos weichen von der tolerierten Zeitfenstern ab
	• Respond: Überprüfung und Erhöhung der Kommunikationsüberwachungsmassnahmen bei Vorfall und Wiederaufnahme der Kommunikation
	MCST4: Die Kommunikation (Das Feedback) wird mit Autorisierungsinformationen angereichert
	• Prevent: Signatur oder Verschlüsselung des Feedbacks
	• Detect: Empfänger (APS) meldet jegliche Verletzung der Signatur oder der Verschlüsselung
	• Respond: Überprüfung und Erhöhung der Kommunikationsüberwachungsmassnahmen bei Vorfall und Wiederaufnahme der Kommunikation
	RAM:

[draft **]**

OCSR-1023 - Ergebnis der Analyse: Gefährdungen sind vorhanden, Mitigations Massnahmen sind zu planen **[** draft **]**

OCSR-1037 - Risikoanalyse nach VDE V 0831-103 [REF011]

Funktion nach Ziffer	Die Norm sieht nicht vor die Funktion Fahrstrasse einstellen auf APS und OC zu verteilen, deshalb Analyse siehe 3.3 - Control Action "CA3 Weiche umstellen"
Schutzziel	
Rahmenbedingungen	
Ausfallarten der Funktion	
Auswirkungen (Worst Case Szenarien)	
Schutzobjekt	
Bewertung von Barrieren	
Risiko Score Matrix	
Sicherheitsanforderung an Schutzfunktion	

[draft]

3.3 Control Action "CA3 Weiche umstellen"

OCSR-1017 -

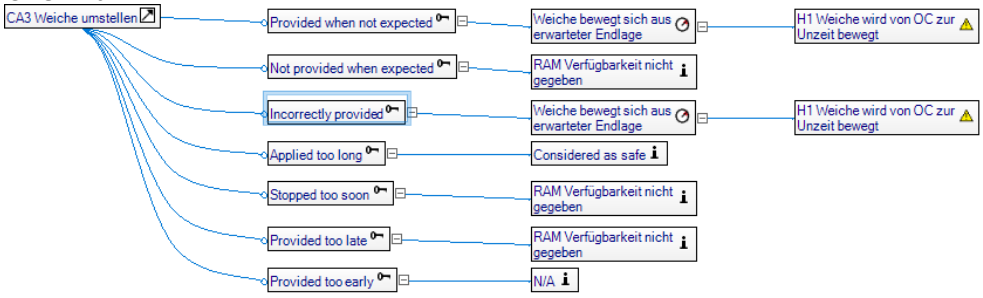


Figure 4 CA3 Analyse

[draft]

OCSR-1013 - Worst Case Scenario: UCA-AS-aus Weiche umstellen

Eine Weiche wird während einer Zugfahrt umgestellt. Wenn der Zug direkt über der Weiche ist, wird ein Teil links und der andere rechts weiterfahren, was den Zug zum Entgleisen bringen wird. Oder es kommt zu einem Zusammenstoss mit einem Zug auf einem anderen Fahrweg oder einer Kollision mit Objekten neben den Geleisen. [draft]

OCSR-1028 - *UCA2 aus CA3 Weiche umstellen*

Sender	OC-Point
Receiver	Prozesse "Fahrweg über Weiche x bereitstellen"
Control Action	CA3 Weiche umstellen
Key Word	siehe Figure oben
Interpretation of Key Word	"Not provided when expected": Die Weiche wird nicht umgestellt, die Bahnproduktion kann nicht ausgeführt werden. Setzt voraus, dass APS die Endlage überprüft. "Incorrectly provided": Die Weiche erhält verfälschte Aufträge, in welche Richtung sie umgestellt werden soll oder die falsche Weiche wird andressiert. "Applied too long": Die Endlage ist erreicht und der Weichen-Antrieb erhält weiterhin Energie. Die Endlage bleibt unverändert. "Stopped too soon": Die Weiche wird nicht vollständig umgestellt, die Bahnproduktion kann nicht ausgeführt werden. Setzt voraus, dass APS die Endlage überprüft. "Provided too late": Die Weiche wird zu spät umgestellt, die Bahnproduktion kann nicht ausgeführt werden. Setzt voraus, dass APS die Endlage überprüft. "Provided too early": N/A Kommando wird erst ausgeführt wenn dieses eintrifft, ansonsten siehe ""Provided when not expected":

	"Provided when not expected": Die Weiche wird umgestellt wenn dies nicht erwartet wird.
UCA Description	Die Weiche wird zur Unzeit umgestellt.
Analysis Result Safety	**unsafe**
Analysis Result RAM, Security	beeinflussbar
List of Hazards	siehe Figure oben
List of Threats	OC: • CST5 Der OC bewegt die Weiche ohne ein autorisiertes Kommando • impliziert CST2 und CST3
List of Potential Losses	siehe Figure oben
Worst Case Scenario	siehe oben
Mitigation Measures	Safety: SF1 Weiche zur Unzeit umstellen verhindern. Unzeit = Erlaubnis von APS zur Umstellung liegt nicht vor. SRAC1 APS muss Endlage der Weiche überwachen und bei Abweichungen Zugfahrten verhindern. Security: MCST5: Der OC muss in der Lage sein die Autorisierung des Kommandos festzustellen (exklusiv MCST3.L2) • Prevent: Die Überprüfung der Autorisierung, sowie die anschliessende Ausführung des Kommandos, muss in vertrauenswürdig und integritätsgeschützt erfolgen • MCST3.L1 Die Autorisierung ist gegen eine sichere Zeit zu prüfen. • Detect: MCST2 • Respond MCST2 RAM:

[draft **]**

OCSR-1022 - Ergebnis der Analyse: Gefährdungen sind vorhanden, Mitigations Massnahmen sind zu planen **[** draft **]**

OCSR-1036 - Risikoanalyse nach VDE V 0831-103 [REF011]

Funktion nach Ziffer	B.2.11 Fahrstraße sichern(Zugstraße)
Schutzziel	(-> bei SR40 ist die Funktionen verteilt auf APS und OC) - sicherstellen, dass die Fahrwegelemente nach dem Einstellen der Fahrstraße (SR40 WI-1082 - Fahrweg) als Voraussetzung für das Erteilen der Fahrterlaubnis (SR40 WI-1975 - Bewegungserlaubnis) gegen Beanspruchung durch eine andere Fahrstraße bzw. gegen Einzelbedienung gesichert (>>verschlossen) sind. - überwachen, dass die vorstehend genannten Bedingungen solange eingehalten sind, bis die betreffende Fahrt die Fahrwegelemente geräumt hat
Rahmenbedingungen	- die Auflösung der einzelnen Fahrwegelemente erfolgt zugbewirkt nach dem Grundsatz der kontinuierlichen Belegung oder durch Bedienung - die Auflösung des Durchrutschweges erfolgt durch Bedienung oder zeitbewirkt - die hier beschriebene Funktionalität wird bei bestimmten Stellwerksarchitekturen bereits teilweise mittels der Funktion ››Zulassungsprüfung<< gewährleistet; letztere umfasst jedoch nicht die vollständige und kontinuierliche Sicherung aller Fahrwegelemente

	und wird daher nicht separat betrachtet
Ausfallarten der Funktion	a) Fahrwegelement nicht verschlossen oder überwacht b) Fahrwegelement vorzeitig aufgelöst c) Element im Durchrutschweg vorzeitig aufgelöst
Auswirkungen (Worst Case Szenarien)	a1) Entgleisung durch fehlenden Umstellschutz an beweglichen Fahrwegelementen (=Unfallklasse G, da ohne weitere Einschränkung der Rahmenbedingungen davon ausgegangen werden muss, dass das Fahrwegelement von einem Reisezug bei hoher Geschwindigkeit befahren wird) a2) Wie al) bei Regionalstrecken, wenn von mittlerer Geschwindigkeit des betroffenen Zuges ausgegangen werden darf (=Unfallklasse E) a3) Bei Weichen mit Vorzugslage: Entgleisung durch fehlenden Umstellschutz und automatisches Rückstellen in die Vorzugslage (=Unfallklasse E, da die Vorzugslage für Fahrten in den durchgehenden Hauptgleisen eingerichtet ist und ein Rückstellen in die Vorzugslage daher nur erforderlich ist, wenn die Weiche in abzweigender Stellung und damit mit mittlerer Geschwindigkeit befahren wurde) a4) Zusammenstoß mit anderen Fahrzeugen durch fehlenden Umstellschutz und resultierender Fahrt in falschen Fahrweg oder fehlender direkter Flankenschutz (=Unfallklasse G, da ohne weitere Einschränkung der Rahmenbedingungen davon ausgegangen werden muss, dass ein mit hoher Geschwindigkeit fahrender Reisezug betroffen ist) a5) Wie a4) bei Regionalstrecken, wenn von mittlerer Geschwindigkeit des betroffenen Zuges ausgegangen werden darf (=Unfallklasse F) b) Für die zu schützende Fahrt ist davon aus zugehen, dass die Schutzfunktion ebenfalls nicht mehr sichergestellt ist. Die Auswirkungen sind dann analog zu a). Insofern wird auf eine separate Analyse von Ausfallart b) verzichtet. c1) Wenn der Durchrutschweg in Anspruch genommen wird: Flankenfahrt(=Unfallklasse F, da zwar davon ausgegangen werden muss, dass ein Reisezug betroffen ist - der Zusammenstoß wegen des bereits eingeleiteten Bremsvorgangs jedoch nicht mit hoher Geschwindigkeit erfolgt). c2) Wenn der Durchrutschweg in Anspruch genommen wird: Entgleisung durch fehlenden Umstellschutz an beweglichen Fahrwegelementen (=Unfallklasse F, da zwar davon ausgegangen werden muss, dass ein Reisezug betroffen ist - die Entgleisung wegen des bereits eingeleiteten Bremsvorgangs jedoch nicht mit hoher Geschwindigkeit erfolgt).
Schutzobjekt	siehe Norm
Bewertung von Barrieren	siehe Norm
Risiko Score Matrix	siehe Norm
Sicherheitsanforderung an Schutzfunktion	SF4: 3 x 10E-9 (allgemein) -> SIL 4

[draft]

3.4 Control Action "CA4 Lage prüfen"

OCSR-1016 -

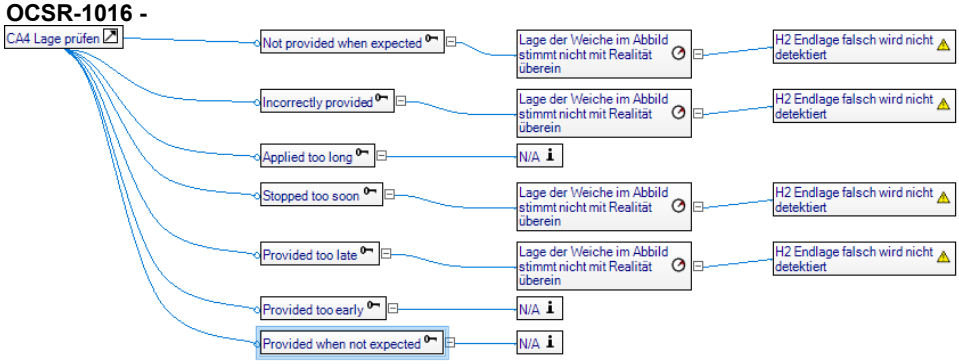


Figure 5 CA4 Analyse

[draft]

OCSR-1012 - Worst Case Scenario: UCA4 aus Lage prüfen

Die Endlage einer Weiche stimmt nicht mit dem Abbild überein. APS nimmt dann eine korrekte Endlage der Weiche an und lässt einen Zug fahren. Der Zug kann Entgleisen und im schlimmsten Fall mit einem Zug kollidieren. [draft]

OCSR-1027 - *UCA4 aus CA4 Lage prüfen*

Sender	OC-Point
Receiver	Prozesse "Fahrweg über Weiche x bereitstellen"
Control Action	CA4 Lage prüfen
Key Word	siehe Figure oben
Interpretation of Key Word	"Not provided when expected" "Incorrectly provided": "Applied too long": "Stopped too soon": "Provided too late": "Provided too early": "Provided when not expected":
UCA Description	Lage prüfen liefert nicht das korrekte Ergebnis (Feedback)
Analysis Result Safety	**unsafe**
Analysis Result RAM, Security	beeinflussbar
List of Hazards	siehe Figure oben
List of Threats	OC: • CST6 Der OC ist durch Manipulation nicht in der Lage den wahren Status der Weiche zu melden. • impliziert CST4
List of Potential Losses	siehe Figure oben
Worst Case Scenario	siehe oben
Mitigation Measures	Safety: SF2 Sicherstellen, dass die Lage der Weiche korrekt ermittelt und übertragen wird. Security: MCST6: Der OC muss in der Lage sein die Lageinformation unverfälscht zu melden und authentisieren können • Prevent: Die Auswertung und Authentisierung der Lageinformation hat in integritätsgeschützt und vertrauenswürdig zu erfolgen • Detect: Die Integrität des zu verarbeitenden Prozesses ist regelmässig zu prüfen. APS meldet jegliche Verletzung der Signatur oder der Verschlüsselung • MCST4 RAM:

[draft]

OCSR-1021 - Ergebnis der Analyse: Gefährdungen sind vorhanden, Mitigations Massnahmen sind zu planen

[draft]

OCSR-1035 - Risikoanalyse nach VDE V 0831-103 [REF011]

Funktion nach Ziffer	B.2.3 Endlage überwachen (Fahrwegweiche, Zugstraße)
Schutzziel	sicherstellen,dass die Weiche die richtige Stellung und Endlage hat
Rahmenbedingungen	- Weiche spitz befahren - Weiche in Fahrstraßenabhängigkeit(Zugstraße) (-> bei SR40 APS-SL abhängig)
Ausfallarten der Funktion	a) Weiche unerkannt in falscher Stellung b) Weiche unerkannt nicht in Endlage
Auswirkungen (Worst Case Szenarien)	a1) Entgleisung durch Überschreiten der zulässigen .....
Schutzobjekt	siehe Norm
Bewertung von Barrieren	siehe Norm
Risiko Score Matrix	siehe Norm
Sicherheitsanforderung an Schutzfunktion	SF5: 10*E-9/h (allgemein) -> SIL 4

[draft]

3.5 Control Action "CA5 Topologie konfigurieren"

OCSR-1015 -

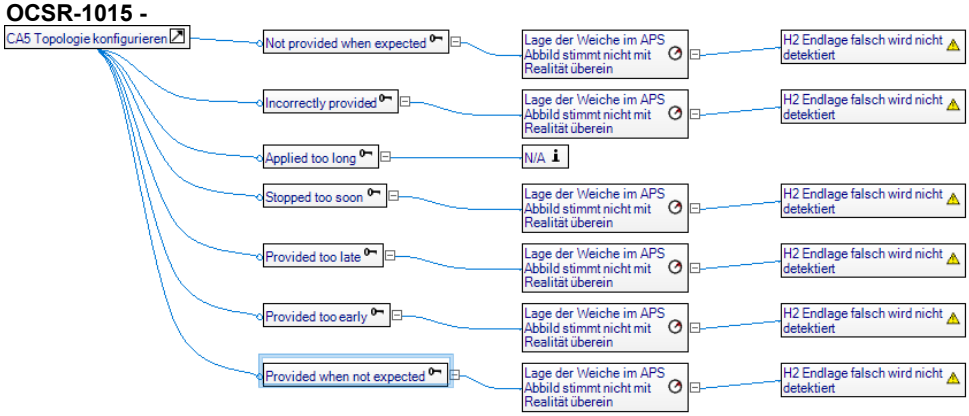


Figure 6 CA5 Analyse

[draft]

OCSR-1011 - Worst Case Scenario: UCA5 Topologie konfigurieren

Die Topologie von APS stimmt nicht mit der Realität überein und falsche Weichen werden umgestellt oder deren Lage interpretiert. Züge können Entgleisen oder mit anderen Zügen kollidieren. [draft]

OCSR-1026 - *UCA5 aus CA5 Topologie konfigurieren*

Sender	DCM
Receiver	APS
Control Action	CA5 Topologie konfigurieren
Key Word	siehe Figure oben
Interpretation of Key Word	"Not provided when expected", "Incorrectly provided", "Stopped too soon", "Provided

	too late":, "Provided too early", "Provided when not expected": Die Topologie im APS stimmt nicht mit der Realität oder Konfiguration des OC überein. "Applied too long": N/A Topologie wird durch Kommando ausgeführt.
UCA Description	Topologie wird nicht identisch zur Konfiguration der Weiche und Realität übermittelt
Analysis Result Safety	**unsafe**
Analysis Result RAM, Security	beeinflussbar
List of Hazards	siehe Figure oben
List of Threats	CST7: Die Konfigurationsdaten werden mutwillig manipuliert.
List of Potential Losses	siehe Figure oben
Worst Case Scenario	siehe oben
Mitigation Measures	Safety: SF3 Topologie in APS muss mit Konfiguration in OC und der Realität übereinstimmen Security: MCST7: Die Konfigurationsdaten sind gegen Manipulation zu schützen • Prevent: Konfigurationsdaten müssen ab dem Erstellungsereignis authentisiert und integritätsgeschützt werden. Konfigurationsdaten dürfen nur von autorisierten Entitäten verarbeitet und eingespielt werden. (Trusted Chain & Traceability) • Detect: Bei einer Verletzung von Authentizität und Integrität, sowie bei unautorisierten Vorgängen ist eine weitere Verarbeitung oder Benutzung der Daten zu stoppen und zu melden. • Respond: Überprüfung und Behebung der Ursache via Trace Log RAM:

[✏ draft **]**

OCSR-1020 - Ergebnis der Analyse: Gefährdungen sind vorhanden, Mitigations Massnahmen sind zu planen **[**✏ draft **]**

OCSR-1034 - Risikoanalyse nach VDE V 0831-103 [REF011]

Funktion nach Ziffer	keine Entsprechung
Schutzziel	
Rahmenbedingungen	
Ausfallarten der Funktion	
Auswirkungen (Worst Case Szenarien)	
Schutzobjekt	
Bewertung von Barrieren	
Risiko Score Matrix	
Sicherheitsanforderung an Schutzfunktion	

Issue: Analyse "CA5 Topologie konfigurieren" nach VDE V 0831-103 [REF010] planen oder verweisen. **[**✏ draft **]**

3.6 Control Action "CA6 Weiche konfigurieren"

OCSR-1014 -

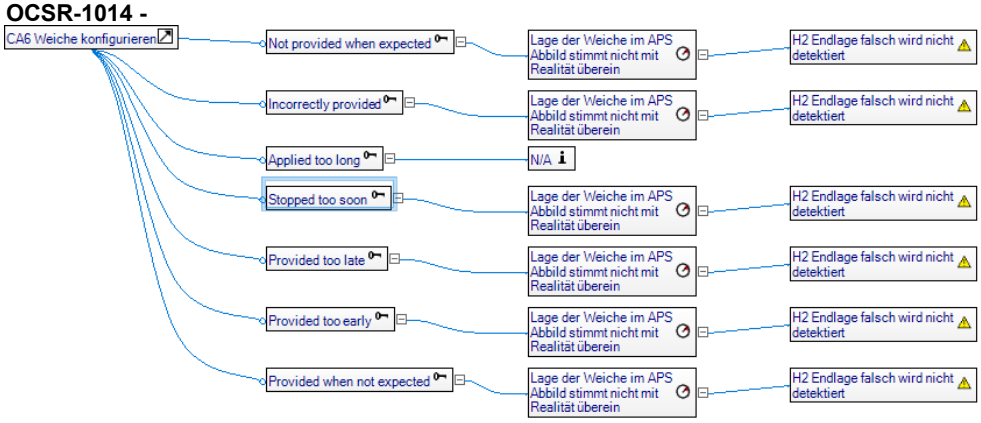


Figure 7 CA6 Analyse

[draft **]**

OCSR-1010 - Worst Case Scenario: UCA6 aus Weiche konfigurieren

Die Konfiguration von OC stimmt nicht mit der Realität überein und falsche Weichen werden umgestellt oder deren Lage falsch gemeldet. Züge können Entgleisen oder mit anderen Zügen kollidieren. **[** draft **]**

OCSR-1024 - *UCA6 aus CA6 Weiche konfigurieren*

Sender	DCM
Receiver	OC-Point
Control Action	CA6 Weiche konfigurieren
Key Word	siehe Figure oben
Interpretation of Key Word	"Not provided when expected", "Incorrectly provided", "Stopped too soon", "Provided too late":, "Provided too early", "Provided when not expected": Die Konfiguration im OC stimmt nicht mit der Realität oder Topologie im APS überein. "Applied too long": N/A Topologie wird durch Kommando ausgeführt.
UCA Description	Konfiguration der Weiche wird nicht identisch zur Topologie im APS und Realität übermittelt
Analysis Result Safety	**unsafe**
Analysis Result RAM, Security	beeinflussbar
List of Hazards	siehe Figure oben
List of Threats	CST7
List of Potential Losses	siehe Figure oben
Worst Case Scenario	siehe oben
Mitigation Measures	Safety: SRAC2: Topologie in APS muss mit Konfiguration in OC und der Realität übereinstimmen.

	SRAC3: APS muss Konfiguration in OC auf Übereinstimmung mit der Topologie im APS überprüfen. SF3: OC darf nur durch APS freigegebene Konfigurationen verwenden. Security: MCST7 RAM:

[draft **]**

OCSR-1025 - Ergebnis der Analyse: Gefährdungen sind vorhanden, Mitigations Massnahmen sind zu planen **[** draft **]**

OCSR-1033 - Risikoanalyse nach VDE V 0831-103 [REF011]

Funktion nach Ziffer	keine Entsprechung
Schutzziel	
Rahmenbedingungen	
Ausfallarten der Funktion	
Auswirkungen (Worst Case Szenarien)	
Schutzobjekt	
Bewertung von Barrieren	
Risiko Score Matrix	
Sicherheitsanforderung an Schutzfunktion	

Issue: Analyse "CA6 Weiche konfigurieren" nach VDE V 0831-103 [REF010] planen oder verweisen. **[** draft **]**

4 Security Analyse

4.1 Control Layer

4.1.1 Logical Structure

OCSR-1087 - The logical structure analysis maps the security constraints, defined in STPA OC-Point HCS Fahrweg über Weiche to the individual logical components.
Important note: This mapping isn't investigated of its real impact yet, it show only the possibilities out of the previous defined generic threats.

	Command Injection (CSTR-I-1)	Command Drop (CSTR-I-2)	Command Manipulation (CSTR-I-3)	Command Delay (CSTR-I-4)	Feedback Injection (CSTR-I-5)	Feedback Drop (CSTR-I-6)	Feedback Manipulation (CSTR-I-7)	Feedback Delay (CSTR-I-8)	Communication Delay (CSTR-A-1)	Communication Drop (CSTR-A-2)	Node Overloaded (delay)(CSTR-A-3)	Node Overload (drop)(CSTR-A-4)
CTRL-N-1	X	X	X	X	X	X	X	X	X	X		
CTRL-N-2	X	X	X	X					X	X		
CTRL-N-3												
CTRL-N-4					X	X	X	X	X	X		
CTRL-C-1	X	X	X	X					X	X	X	X
CTRL-C-2	X	X	X	X					X	X	X	X
CTRL-C-3					X	X						
CTRL-C-4					X	X	X	X	X	X	X	X

[draft]

4.1.2 Security Constraints analysis

OCSR-1088 - Now we define (filter out) the resulting Security Constraints based on the identified hazards (Info: Control actions are currently excluded).

The UCAs Analysis shows that we have 2 final Hazards which leads to the 2 final system losses. In the next step we iterate thru the possible security constraints and check which of them would produce which hazard:

"H1 - Die Weiche wird zur Unzeit bewegt":
Based on the Safety-analysis we can exclude following security constraints:

- CSTR-I-2 Command drop is not issue since we will detect a non-move at the end of the process by checking the state and keeps the area safe
- CSTR-I-3 Command manipulation is not an issue, moving the blade into the wrong direction will detected at the end of the process and the area stays safe.
- CSTR-I-4 Command delay is on the first view not an issue, because the final state check will show the missing execution or the still in movement, but we know that even in a perfect safety world without security help we are able to delay a command until after the sensor is read, so we may miss the detection of the command state. **This constraint not be excluded**.
- CSTR-I-5 till CSTR-I-8 are feedback constraints, they may help us to detect H1, but does not prevent the move. Further the system does not check every second of its lifecycle the state of the point. The check becomes important when the system is used - a train runs over the point.
- CSTR-A-1 and CSTR-A-3 Delay due to communication or system overload leads into the same behavior as CSTR-I-4 and **will be not excluded.**
- CSTR-A-2 and CSTR-A-4 Drop due to communication and overload lead into the same behavior as constraint CSTR-I-8

"H2 - Endlage falsch wird nicht detektiert":

Based on the Safety-analysis we can exclude following security constraints:

- CSTR-I-1 till CSTR-I-4 since these are command issues, they are not valid for the feedback
- CSTR-I-6 Feedback drop is not an issue, without an answer the system stays safe, it declares the process as not finished
- CSTR-I-8 Feedback delay is not an issue, because having not the status due to a delay leads into the same issue like Feedback drop. The system will not conclude a finish of the process.
- CSTR-A-1 and CSTR-A-2 Communication delay or node overload delays will lead into the same clause as CSTR-I-8
- CSTR-A-2 and CSTR-A-4 Communication drop or a node overload drop leads into the same clause as CSTR-I-6

This leads into the following for system important Security constraints and first high level requirements:

- CSTR-I-1 Command injection and CSTR-I-5 Feedback Injection
  - Security Requirement 1: The system has to prevent injections of commands and sensor statuses at any time
- CSTR-I-4 Command Delay/CSTR-A-1 Communication Delay/CSTRA-A-3 Node overload delay (A Safety not covered attack, delay till after sensor read)
  - Security Requirement 2: The system has to prevent a delay of commands after the feedback transmission
- CSTR-I-7 Feedback Manipulation
  - Security Requirement 3: The System has to prevent any manipulation of the feedback information

[draft **]**

4.2 Component Layer

4.2.1 Mapping and Labeling

OCSR-1117 - The first analysis was done in PowerPoint following the Ivo Friedberg thesis. This lead into slightly different models. We do first a mapping between both models.
Note: may be solved later differently

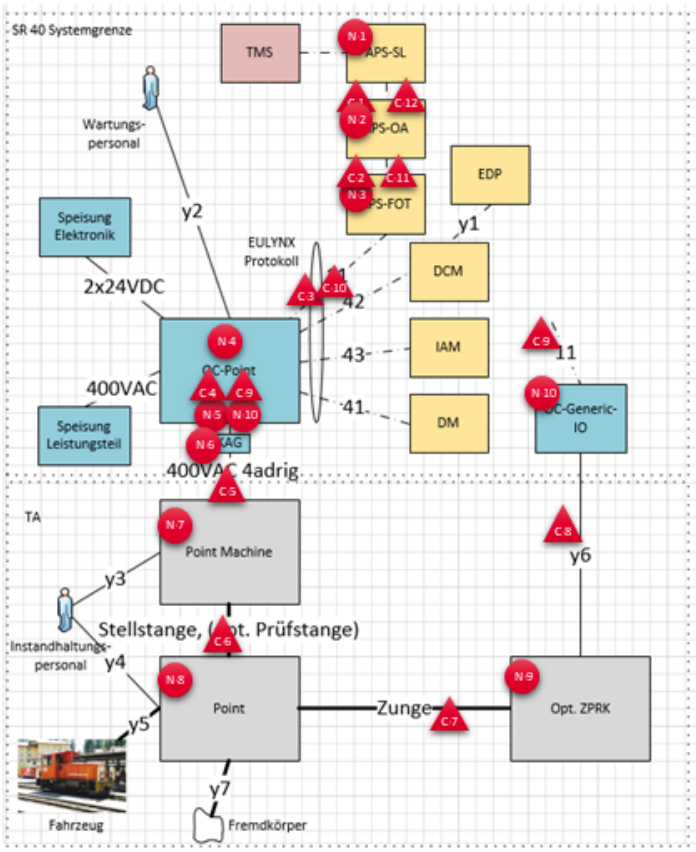


Figure 8 Model Safety Analysis

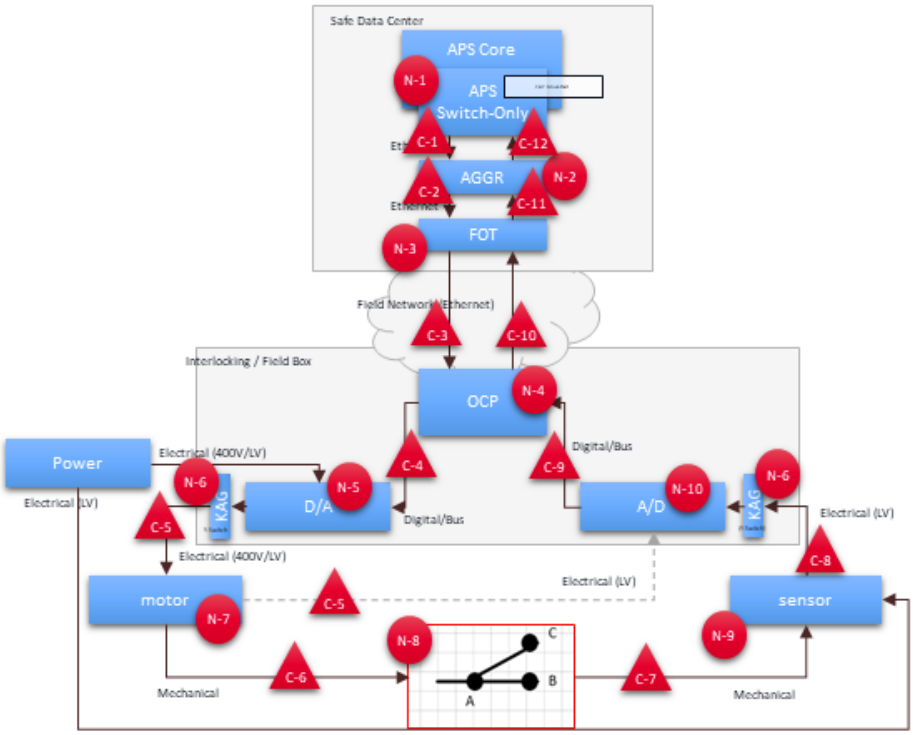


Figure 9 Modell Security Analysis

[draft]

4.2.2 Resulting constraints/hazards from control layer

OCSR-1118 - Note: Everything below KAG (Component N6/CPT-N-6) is out of scope (grandfathered) of this investigation.

Constraints	N1	N2	N3	N4	N5	N10	C1/C12	C2/C11	C3/C10	C4/C9
CSTR-I-1	H1	H1	H1	H1	H1		H1	H1	H1	H1
CSTR-I-4	(H1)	(H1)	(H1)	(H1)	(H1)		(H1)	(H1)	(H1)	(H1)
CSTR-I-5	H2	H2	H2	H2		H2	H2	H2	H2	H2
CSTR-I-7	H2	H2	H2	H2		H2	H2	H2	H2	H2
CSTR-A-1	(H1)	(H1)	(H1)	(H1)	(H1)		(H1)	(H1)	(H1)	(H1)
CSTR-A-3	(H1)	(H1)	(H1)	(H1)	(H1)		(H1)	(H1)	(H1)	(H1)

[draft **]**

4.2.3 Security constraints analysis

OCSR-1131 - Detailierte, per Komponente Security-Constraints

- N1 APS
  - CSTR-I-1 Das APS muss sicherstellen das Schaltkommandos nicht ohne Grund und Überprüfung erzeugt werden können.
  - CSTR-I-4 Das APS muss sicherstellen das es einen Mechanismus gibt der extreme Schaltkommandoverzögerungen unterbindet oder erkennt.
  - CSTR-I-5 Das APS muss sicherstellen das es keine fremden Feedbacks der Weichenlage entgegen nimmt
  - CSTR-I-7 Das APS muss sicherstellen das die Feedbacks der Weichenlage nicht manipuliert werden können
  - CSTR-A-1 Siehe CSTR-I-4
  - CSTR-A-3 Siehe CSTR-I-4
- N2 AGGR
  - CSTR-I-1 Der Aggregator muss sicherstellen das Schaltkommandos nur vom Stellwerk erzeugt werden können und das sie an den richtigen FOT weitergeleitet werden.
  - CSTR-I-4 Der Aggregator muss sicherstellen das es einen Mechanismus gibt der extreme Schaltkommandoverzögerungen unterbindet oder erkennt.
  - CSTR-I-5 Der Aggregator muss sicherstellen das es keine fremden Feedbacks der Weichenlage entgegen nimmt
  - CSTR-I-7 Der Aggregator muss sicherstellen das die Informationen zur Weichenlage nicht manipuliert werden können
  - CSTR-A-1 Siehe CSTR-I-4
  - CSTR-A-3 Siehe CSTR-I-4
- N3 FOT
  - CSTR-I-1 Der Fixed Object Transactor muss sicherstellen das Schaltkommandos nur vom Aggregator erzeugt werden können und das sie an den richtigen OCP weitergeleitet werden.
  - CSTR-I-4 Der Fixed Object Transactor muss sicherstellen das es einen Mechanismus gibt der extreme Schaltkommandoverzögerungen unterbindet oder erkennt.
  - CSTR-I-5 Der Fixed Object Transactor muss sicherstellen das es keine fremden Feedbacks der Weichenlage entgegen nimmt

    - CSTR-I-7 Der Fixed Object Transactor muss sicherstellen das die Informationen zur Weichenlage nicht manipuliert werden können
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4
- N4 OCP
    - CSTR-I-1 Der Object Controller Point muss sicherstellen das Schaltkommandos nur vom FOT erzeugt werden können und das die richtige Weiche geschalten wird.
    - CSTR-I-4 Der Object Controller Point muss sicherstellen das es einen Mechanismus gibt der extreme Schaltkommandoverzögerungen unterbindet oder erkennt.
    - CSTR-I-5 Der Object Controller Point muss sicherstellen, dass das Feedback der Weichenlage immer dem Ursprungs des Sensor (A/D Wandler) entstammt
    - CSTR-I-7 Der Object Controller Point muss sicherstellen das die Informationen zur Weichenlage immer dem Zustandes des Sensors (A/D Wandler entspricht
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4
- N5 D/A Wandler
    - CSTR-I-1 Der D/A Wandler muss sicherstellen, dass das Schaltkommando vom OC stammt
    - CSTR-I-4 Der D/A Wandler muss sicherstellen das er das Schaltkommando nicht verzögert ausführt
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4
- N10 A/D Wandler
    - CSTR-I-5 Der A/D Wandler muss sicherstellen das die erzeugten Daten aus den Sensordaten stammen
    - CSTR-I-7 Der A/D Wander muss sicherstellen das die erzeugten Daten den Sensordaten entsprechen
- C1/C12
    - CSTR-I-1 Die Datenverbindung muss sicherstellen das zwischen APS und Aggregator keine fremden Daten eingefügt (injected) werden können
    - CSTR-I-4 Die Datenverbindung muss Verzögerungen in der Übermittlung möglichst verhindern und bei Auftreten offenbaren
    - CSTR-I-5 Die Datenverbindung muss sicherstellen das beide Gegenstellen authentisch sind.
    - CSTR-I-7 Die Datenverbindung muss sicherstellen das zu übertragende Daten nicht verändert werden können und Veränderungen erkannt werden können
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4
- C2/C11
    - CSTR-I-1 Die Datenverbindung muss sicherstellen das zwischen Aggregator und Fixed Object Transactor keine fremden Daten eingefügt (injected) werden können
    - CSTR-I-4 Die Datenverbindung muss Verzögerungen in der Übermittlung möglichst verhindern und bei Auftreten offenbaren
    - CSTR-I-5 Die Datenverbindung muss sicherstellen das beide Gegenstellen authentisch sind.
    - CSTR-I-7 Die Datenverbindung muss sicherstellen das zu übertragende Daten nicht verändert werden können und Veränderungen erkannt werden können
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4
- C3/C10
    - CSTR-I-1 Die Datenverbindung muss sicherstellen das zwischen Fixed Object Transactor und Object Controller Point keine fremden Daten eingefügt (injected) werden können
    - CSTR-I-4 Die Datenverbindung muss Verzögerungen in der Übermittlung möglichst verhindern und bei

Auftreten offenbaren
    - CSTR-I-5 Die Datenverbindung muss sicherstellen das beide Gegenstellen authentisch sind.
    - CSTR-I-7 Die Datenverbindung muss sicherstellen das zu übertragende Daten nicht verändert werden können und Veränderungen erkannt werden können
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4
- C4/C9
    - CSTR-I-1 Die Datenverbindung muss sicherstellen das zwischen Object Transactor Point und den AD/DA Wandlern keine fremden Daten eingefügt (injected) werden können
    - CSTR-I-4 Die Datenverbindung muss Verzögerungen in der Übermittlung möglichst verhindern und bei Auftreten offenbaren
    - CSTR-I-5 Die Datenverbindung muss sicherstellen das beide Gegenstellen authentisch sind.
    - CSTR-I-7 Die Datenverbindung muss sicherstellen das zu übertragende Daten nicht verändert werden können und Veränderungen erkannt werden können
    - CSTR-A-1 Siehe CSTR-I-4
    - CSTR-A-3 Siehe CSTR-I-4

[✏ draft **]**

4.2.4 Analysis notes

Security for Safety in this example can be done at different layers, probably the same for Safety. We could already implement measures at the control layer to solve the Security4Safety issues completely independent of almost any underlaying realization structure. The protection at the highest level will make the Security lifecycle with its security operation component much easier and cheaper.

4.3 RAM issues due to Security constraints

Todo - Andreas

5 Zusammenfassung UCAs Analyse

5.1 Executive Summary

Kurze Beschreibung der Hauptbefunde die zu Sicherheitsrisiken führen. todo

5.2 Vorläufige Sicherheitsanforderungen

OCSR-989 - Dieser Abschnitt enthält die Vorschläge für Sicherheitsanforderungen. Jede Sicherheitsanforderung bezieht sich auf eine UCA. **[**✏ draft **]**

OCSR-990 - Allgemein gültige Sicherheitsanforderung: Das Eintreten eines UCA während operativen Einsatz von SR40 ist zu vermeiden. **[**✏ draft **]**

5.2.1 Sicherheitsfunktionen und sicherheitsrelevante Anwendungsbedingungen aus STAP Step 1

(SFx = Sicherheitsfunktion / Safety Constraint; SRACx = Sicherheitsrelevante Anwendungsbedingung an übergeordnetes System)

OCSR-1067 - SF1: Weiche zur Unzeit umstellen verhindern. Unzeit = Erlaubnis von APS zur Umstellung liegt nicht vor. **[**draft **]**

OCSR-1066 - SRAC1: APS muss Endlage der Weiche überwachen und bei Abweichungen Zugfahrten verhindern. **[**draft **]**

OCSR-1065 - SF2: Sicherstellen, dass die Lage der Weiche korrekt ermittelt und übertragen wird. **[**draft **]**

OCSR-1064 - SF3: OC darf nur durch APS freigegebene Konfigurationen verwenden. **[**draft **]**

OCSR-1063 - SRAC2: Topologie in APS muss mit Konfiguration in OC und der Realität übereinstimmen. **[**draft **]**

OCSR-1062 - SRAC3: APS muss Konfiguration in OC auf Übereinstimmung mit der Topologie im APS überprüfen. **[**draft **]**

5.2.2 Sicherheitsfunktionen und sicherheitsrelevante Anwendungsbedingungen aus FMEA (VDE V 0831)

OCSR-1061 - SF4: Fahrwegelemente während erteilter Bewegungserlaubnis nicht bewegen (Fahrstraße sichern) 3 x 10E-9 (allgemein) -> SIL 4 (Aufgabe gemeinsam durch APS und OC zu lösen) **[**draft **]**

OCSR-1060 - SF5: Endlage überwachen der Weiche 10*E-9/h (allgemein) -> SIL 4 **[**draft **]**

5.3 Vorläufige Security/Informationssicherheitsanforderungen

OCSR-1100 - Dieser Abschnitt enthält Vorschläge für Informationssicherheitsanforderungen. Jede Informationssicherheitsanforderung bezieht sich auf eine UCA. **[**draft **]**

OCSR-1099 - Allgemeingültige Informationssicherheitsanforderung Bedrohungen die das Eintreten einer UCA ermöglichen sind mit geeigneten Massnahmen durch den gesamten SR40 Lebenszyklus behandeln (d.h. Risikominimierung) und deren Wirkung zu überwachen. **[**draft **]**

5.3.1 Sicherheitsfunktionen und sicherheitsrelevante Anwendungsbedingungen aus STAP Step 1

OCSR-1129 - MCST1: Sicherung und Überwachung des APS mit geeigneten Massnahmen

- Prevent: Trusted and Protected Computing Environment
- Detect: Intrusion Detection System, Regular system plausibility checks
- Respond: Nothalt des Systems und gesamten kontrollierten Bereiches

[draft **]**

OCSR-1128 - MCST2: Kommandos werden mit Autorisierungsinformationen angereichert

- Prevent: Signatur oder Verschlüsselung des Kommandos
- Detect: Empfänger (OC) meldet jegliche Verletzung der Signatur oder der Verschlüsselung
- Respond: Überprüfung und Erhöhung der Kommunikationsüberwachungsmassnahmen bei Vorfall und Wiederaufnahme der Kommunikation

[draft **]**

OCSR-1127 - MCST3: Die Kommunikation muss an zeitliche parameter gebunden und überprüft werden

- Prevent:
  - L1 Kommandos werden Zeitgebunden und mit CST2 gesichert (Secure Time)
  - L2 Kommandos erzeugen einen direkten Feedback so das eine zeitliche Abweichung/Manipulation erkannt wird.
- Detect:
  - L1/L2 Kommandos weichen von der tolerierten Zeitfenstern ab
- Respond: Überprüfung und Erhöhung der Kommunikationsüberwachungsmassnahmen bei Vorfall und Wiederaufnahme der Kommunikation

[✏ draft **]**

OCSR-1126 - MCST4: Die Kommunikation (Das Feedback) wird mit Autorisierungsinformationen angereichert

- Prevent: Signatur oder Verschlüsselung des Feedbacks
- Detect: Empfänger (APS) meldet jegliche Verletzung der Signatur oder der Verschlüsselung
- Respond: Überprüfung und Erhöhung der Kommunikationsüberwachungsmassnahmen bei Vorfall und Wiederaufnahme der Kommunikation

[✏ draft **]**

OCSR-1125 - MCST5: Der OC muss in der Lage sein die Autorisierung des Kommandos festzustellen (exklusiv MCST3.L2)

- Prevent: Die Überprüfung der Autorisierung, sowie die anschliessende Ausführung des Kommandos, muss in vertrauenswürdig und integritätsgeschützt erfolgen
  - MCST3.L1 Die Autorisierung ist gegen eine sichere Zeit zu prüfen.
- Detect: MCST2
- Respond MCST2

[✏ draft **]**

OCSR-1124 - MCST6: Der OC muss in der Lage sein die Weichenlageinformation unverfälscht zu melden und authentisieren können

- Prevent: Die Auswertung und Authentisierung der Weichenlageinformation hat in integritätsgeschützt und vertrauenswürdig zu erfolgen
- Detect: Die Integrität des zu verarbeitenden Prozesses ist regelmässig zu prüfen. APS meldet jegliche Verletzung der Signatur oder der Verschlüsselung
- MCST4

[✏ draft **]**

OCSR-1123 - MCST7: Die Konfigurationsdaten sind gegen Manipulation zu schützen

- Prevent: Konfigurationsdaten müssen ab dem Erstellungsereignis authentisiert und integritätsgeschützt werden. Konfigurationsdaten dürfen nur von autorisierten Entitäten verarbeitet und eingespielt werden. (Trusted Chain & Traceability)
- Detect: Bei einer Verletzung von Authentizität und Integrität, sowie bei unautorisierten Vorgängen ist eine weitere Verarbeitung oder Benutzung der Daten zu stoppen und zu melden.
- Respond: Überprüfung und Behebung der Ursache via Trace Log

[draft **]**

5.3.2 Ein System das die Informationssicherheitsanforderungen erfüllt

OCSR-1130 - Die Security-Anforderungen lassen sich mit einem einfachen System wie folgt umsetzten.
MCST1: wird umgesetzt wie angegeben

MCST2: Das APS sendet zusätzlich zum Weichenschaltkommando einen Autorisationscode, der nur von dem bestimmten OC interpretiert werden kann. Der Autorisationscode enthält nur die Freigabe zum Schalten, nicht die Richtung.

MCST3: Option L1 Der Autorisationscode enthält eine sichere Zeit und der OC schaltet nur wenn die Schaltfreigabezeit nicht abgelaufen ist. Option L2 Der OC kann die Zeit nicht auswerten und schaltet bedingungslos mit dem Autorisationscode. Der OC sendet eine gesicherte Quittierung (z.B. durch einen zusätzlichen Zufallscode erstellt vom APS) des Schaltkommandos. Das Stellwerk muss sicherstellen das eine Überprüfen der Lage erst geschieht wenn auch die überprüfte Quittierung des Schaltkommandos vorhanden ist (Plausibilisierung). Eine Verletzung stellt einen Security-Vorfall dar und muss untersucht werden.

MCST4: Die Weichenlageinformation erhält eine auf den OC bezogene Signatur, die das Stellwerk überprüfen muss. Nebenbedingung Zeit: die Signatur enthält Informationen die Wiederholen und Verzögerungen (Siehe MCST3) offenbaren.

MCST5: Da der OC ein Feldelement mit updatefähiger Software ist, wird die Überprüfung des Kommandos in eine unabhängige Hardwareeinheit, in der Form eines Arduino/ESP32 (tamper proofed), implementiert. Die Hardwareeinheit schaltet den Strom zur Ausführung des Kommandos frei. Eine Alternative ist die Unterbrechung der Weiterleitung des nur noch elektrischen Schaltkommandos (Signal vor dem D/A Wandler) zur ausführenden externen Einheit.

MCST6: Da der OC ein Feldelement mit updatefähiger Software ist, werden die Sensordaten der Lage von einem Hardwaremodul (Arduino/ESP32, tamper proofed) ausserhalb des OC angereichert und signiert.

MCST7: Die Konfigurationsdaten des APS, welche die Information zur Autorisierungsgenerierung enthalten sind besonders zu schützen. Ein vertiefter Schutz der Konfigurationsdaten auf dem OC ist nicht nötig. Das Stellwerk kann seine Konfiguration über die Überprüfung der Autorisationscode (z.B. durch einmal hin und her schalten oder Nullkomandos) abgleichen.

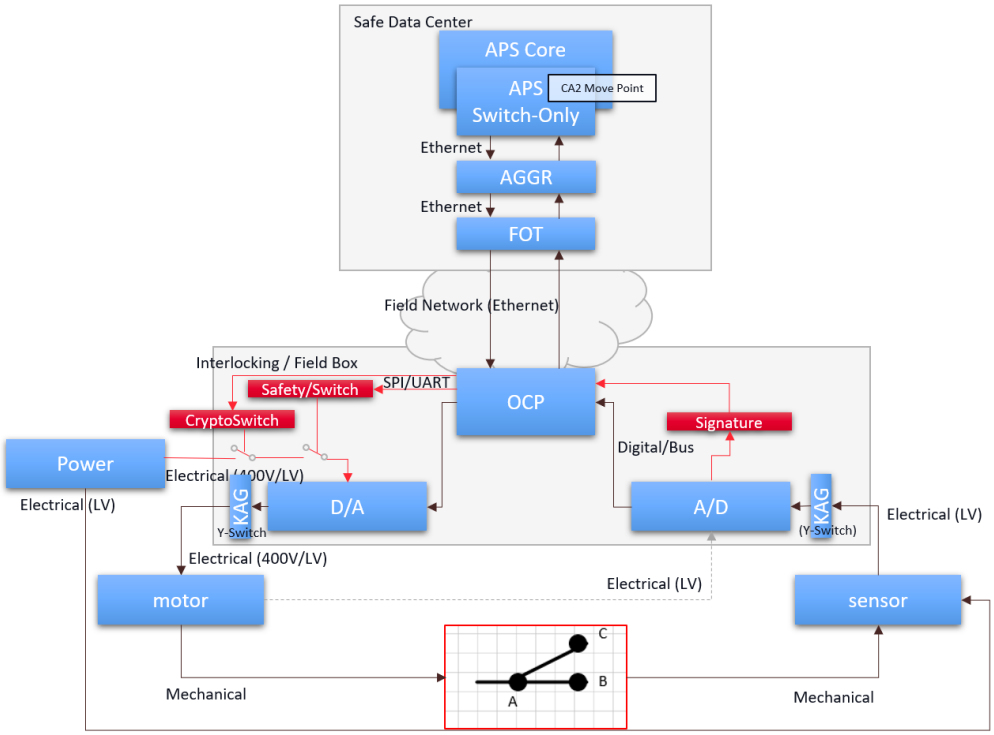


Figure 10 Security and Safety Solution Proposal

Beschreibung des Sicherheitssystems

Die roten Boxen (Figure 10) sind die zu hinzuzufügenden Elemente (Hardwareeinheiten) zum OC. Die Security-Elemente CryptoSwitch und Signature werden von eigenständigen sicheren MCU (Microcontroller Unit) ausgeführt.
Die MCU CryptoSwitch hat nur die Funktion den Strom zum Motor freizuschalten wenn sie ein für sie verschlüsseltes Autorisationskommando enthält. Erhält der OC nun Schaltkommandos ohne Autorisationscodes verläuft die Schaltung ins Leere, da kein Strom am Weichenmotor anliegt, auch eine Manipulation des OC Betriebsystems hat keinen Erfolg mehr. Der Datenpfad zwischen OC und dem CryptoSwitch ist auf das reine Austauschen des verschlüsselten Autorisationscodes beschränkt. Das Schlüsselmaterial zum erzeugen des Autorisationscodes liegt dazu nur im APS vor und wird beim Installieren des CryptoSwitches mit dem APS ausgetauscht.
Die MCU Signature signiert die Sensordaten des Weichenlagesensors bevor eine Bearbeitung in Software auf dem OC passiert. Der Datenpfad vom Signaturmodul zum OC überträgt nur das Datenpaket und die zugehörige Signatur. Die Schlüsseldaten zur Signatur wurden bei der Installation im APS hinterlegt. Der OC sendet dann seine Weichenlagedaten zusammen mit dem vom Signaturmodul erzeugten Daten zum APS. Das APS überprüft die Daten und Signatur auf Richtigkeit. Bei Abweichung deklariert das APS das Gebiet zum OC als "Unsafe" und eine Intervention durch Security Operation und RailOP ist nötig.

Sicherheitssystem ohne Zeitbezug

Ohne weitere Logiken braucht das System eine sichere Zeit, welche im gesamten System und auf dem MCUs anliegt.
Begründung: Ohne Zeit lässt sich zwar in jede Richtung die Authentizität überprüfen jedoch nicht wann welche Daten erzeugt wurden. Es fehlt dazu eine gemeinsame Referenz.
Um den SR40 Gedanken "Ohne Zeit auszukommen können" zu folgen lässt sich zumindest die Safety mit einer gerichteten Verbindung vom CryptoSwitch zum Signaturmodul informationssicherheitstechnisch absichern. Das Stellwerk reichert den Autorisationscode mit eigenen Daten an, welche nun beide Module durchlaufen und zum Stellwerk zurück gesandt werden. Das Stellwerk überprüft nun ob die angereicherten Daten den Erwartungen der Dauer des Umlaufs und der Integrität des Inhalts entsprechen. Bei Abweichungen wird das Gebiet zum OC als "Unsafe" markiert und eine Intervention durch Security Operation und RailOP ist nötig. **[** draft **]**

6 Offene Punkte UCAs Analyse

OCSR-994 - Dieses Kapitel soll analog zu *SR40_Programm/STPA Analyse Workspace Vorlage/Vorlage_HCS* mit offenen Punkte in Form von "Issue" Work Items befüllt werden **[** draft **]**

OCSR-1030 - Prozess "Hazard Verwalten" inkl. Darstellung des "Hazards Log" (Gefährdungslogbuch) ist noch nicht vollständig festgelegt. **[** draft **]**

OCSR-1107 - Prozess "Threats Verwalten" inkl. Darstellung des "Threat Log" (Bedrohungslogbuch) ist noch nicht vollständig festgelegt. **[** draft **]**

7 Ursachenanalyse Safety

OCSR-1049 - Ziel der STPA Step 2 Analyse ist Einflussfaktoren auf die Aktoren und Sensoren zu analysieren, die den gleichen Effekt wie die UCA (Unsafe Control Action) haben.
Die Control Loops werden so modelliert, das in einem ersten Schritt nur die Control Actions (CA) und Feedbacks (FB) zwischen zwei Controllern oder einem Controller und einem Prozess dargestellt werden. In einem zweiten Schritt werden die Aktoren auf dem Pfad der Control Actions und die Sensoren auf dem Pfad der Feedbacks ergänzt. Die Aktoren und Sensoren sollen soweit bekannt der physikalischen Architektur entsprechen.
Für die Ursachen Analyse wird eine Bottom-Up Methode verwendet, hier FMEA.
Im Control Loop kann gut dargestellt werden, was die Abhängigkeiten zwischen Ursache und Wirkung ist, die Folgen wurden bereits im Kapitel 3 - Control Actions Analyse analysiert. **[** draft **]**

FMEA folgende Key Words werden für die Ursachenanalyse verwendet:
"Not provided when expected" -> "Nicht sichergestellt."
"Incorrectly provided": -> "falscher Wert"
"Applied too long": -> "Zuviel .."
"Stopped too soon": -> "Zuwenig .."
"Provided too late": "Provided too early": "Provided when not expected": -> "Zur Unzeit"

7.1 Control Loop CL1 APS - OC-Point

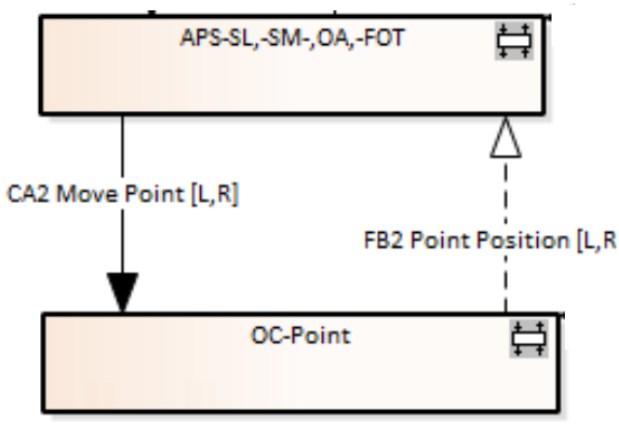


Figure 11 CL1 Diagramm

7.2 Control Loop CL1.1 APS - OC-Point mit Aktoren und Sensoren

Wird nicht weiter detailliert, da nur Netzwerk Elemente für die CA und FB verwendet werden.

Anforderungen aus Safety Plan OC:

SF5: EN50159 ist zu erfüllen für Kategorie 2 Netzwerke und Kategorie 3 Netzwerke.

Nr.	Funktion (CA, FB, ..)	Mögliche Fehlfunktion	Mögliche Ursache	Massnahme aktuell	Massnahme empfohlen
1	CA2, FB2	falscher Wert wird übertragen	EMV-Störung, Übertragungsfehler	SF5 Eulynx Sicherheitscode MD4	-
2	CA2, FB2	Information wird zur Unzeit übertragen	Netzwerk-Verzögerung, -Duplizierung	SF5 Eulynx Sequenz-Nr. Zeitstempel	-
3	CA2, FB2	Information wird verfälscht	Netzwerk-Manipulation in Kat. 3 Netzwerken	-	Kryptographische Massnahmen um Manipulation zu verhindern/entdecken
4	CA2, FB2	Adressierung falsch	Falsche Konfiguration von Netzwerk Komponenten	SF5 Eulynx Sender, Empfänger Adressen	Security Massnahmen um falsche Identitäten zu verhindern/entdecken
5					

7.3 Control Loop CL2 OC-Point - Prozess

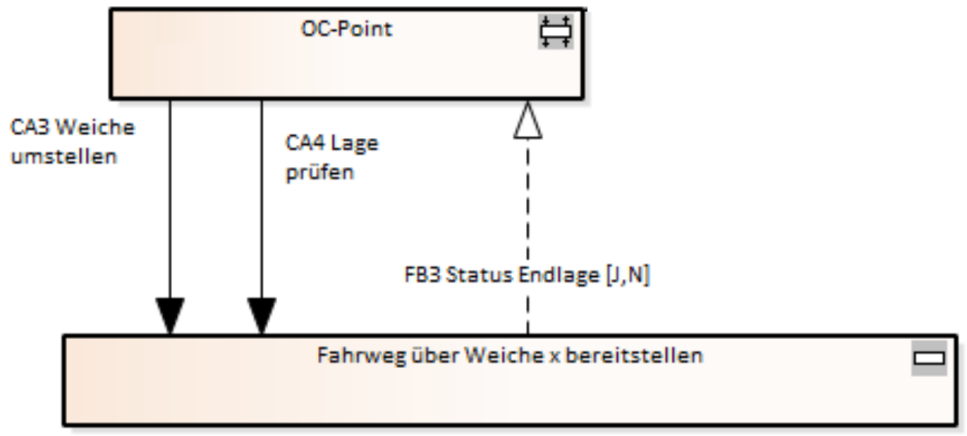
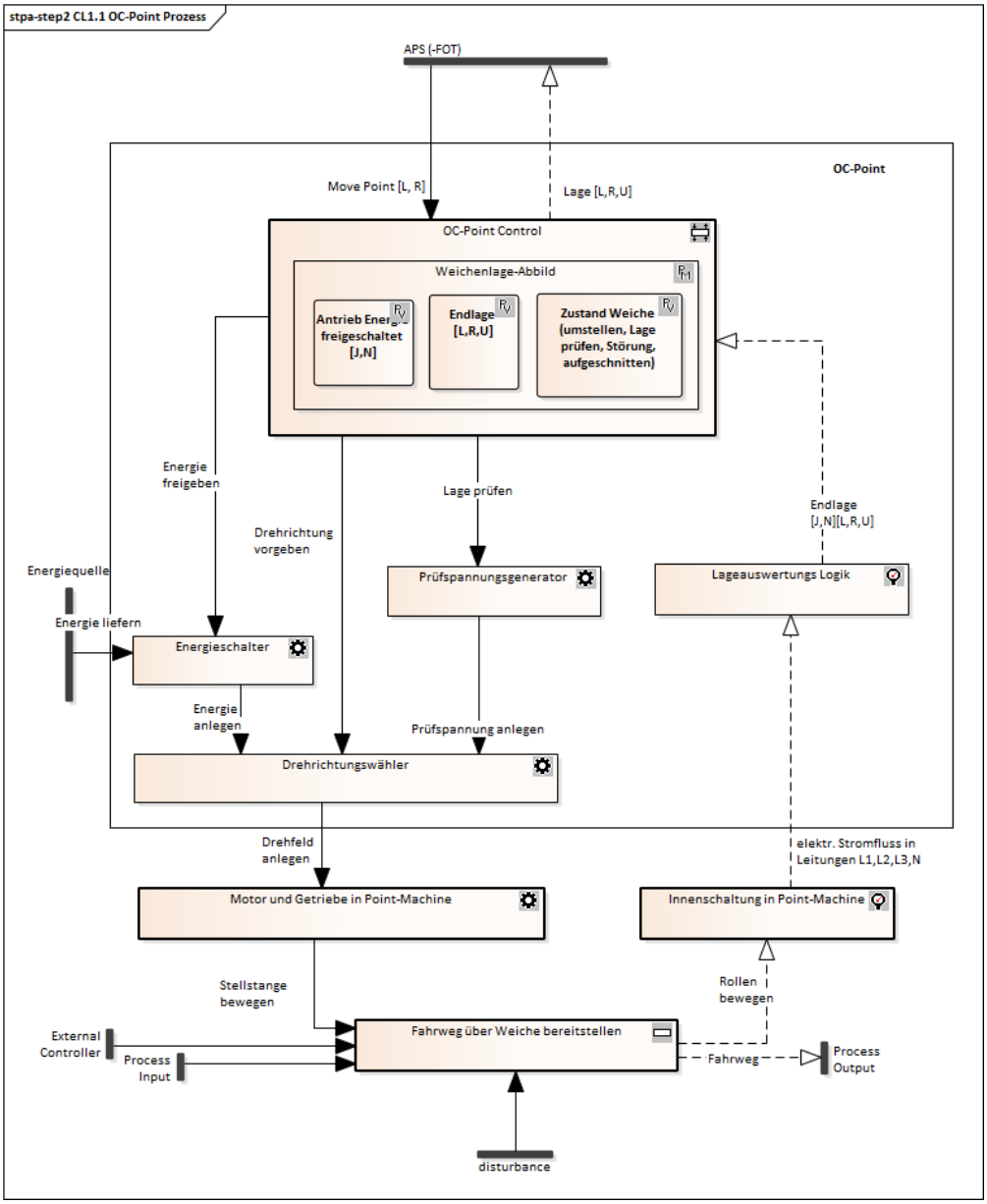


Figure 12 CL2 Diagramm

7.4 Control Loop CL2.1 OC-Point - Prozess mit Aktoren und Sensoren



7.4.1 FMEA CL2.1

Nr.	Funktion (CA, FB, ..)	Mögliche Fehlfunktion	Mögliche Ursache	Massnahme aktuell	Massnahme empfohlen
1	Move Point, Lage	wie Kap. 6.2	wie Kap. 6.2	wie Kap. 6.2	wie Kap. 6.2
2	Drehfeld bereitstellen	Zuwenig (Energieschalter hochohmig)	HW Fehler		
2.1		Zuviel (Energieschalter "verklebt")	HW Fehler		
2.2.1		Zur Unzeit	HW Fehler		
2.2.2			EMV-Störung		
2.2.3			SW-Fehler in OC-Point Control		

3	Drehrichtung vorgeben				
4	Energie liefern				
5	Energie freigeben	wie 2			
6	Lage prüfen				
7	Prüfspannung anlegen				
8	Energie anlegen	zu wenig Energie, Motor dreht nicht	Energiequelle zu schwach		
9	Endlage	falscher Wert			
10	Stellstange bewegen Rollen bewegen	bewegen nicht, falsche Richtung	Motor defekt, Mechanik gebrochen, Motor falsch angeschlossen, ...	out of Scope da bestehende TA	
11	Fahrweg	nicht sichergestellt	Schienenbruch	out of Scope da bestehende TA	

todo