NeGSt

Neue Generation Signaltechnik

Sektorweite Initiative zur Sicherung der Zukunftsfähigkeit der Leit- und Sicherungstechnik

Teilbericht

AP 2100 – Signifikanzbewertung von Änderungen an technischen Systemen auf Grundlage Ausfallfolgen-Unsicherheits-Matrix

18.04.2013

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Laufzeit: 01.09.2011 – 31.08.2013

Projektträger: TÜV Rheinland Consulting GmbH

Änderungsverfolgung

Datum	Bearbeiter	Version	Inhalt
29.06.2012	Braband (Siemens AG)	V01	Erstellung
17.07.2012	Braband (Siemens AG)	V02	Einarbeitung von Anmerkungen nach dem AG-Treffen 2012-07-02
14.08.2012	Brinkmann (PINTSCH BAMAG GmbH)	V03	Änderung nach Inspektion
28.08.2012	Braband (Siemens AG)	V04	Abschließendes Review im AG-Treffen 2012-08-28
16.04.2013	Braband (Siemens AG)	V05	Einarbeitung weiterer Aspekte und Beispiele
18.04.2013	Beck (DB AG), Brinkmann (PINTSCH BAMAG GmbH), Schwencke (DLR)	V06	Einarbeitung von Korrekturen und Kommentaren

Inhaltsverzeichnis

1 Einleitung

Die Signifikanzbewertung von Änderungen hat bei der Umsetzung der EG Verordnung 352/2009 zu einigen Diskussionen geführt. Dies liegt unter anderem an teilweise den Sinn der Verordnung verändernden Übersetzungen aus dem englischen Original, aber auch an unklaren oder unvollständigen Formulierungen.

Hinderlich ist aber vor allem, dass es bisher kein einheitliches Verfahren zur Signifikanzbewertung gibt. Es gibt zwar allgemeine Vorschläge z. B. seitens ORR und darauf aufbauend Vorschläge des VDV bzw. der DB AG, ein ähnliches Verfahren, die sog. Ausfallfolgen-Unsicherheits-Matrix (AUM), insbesondere zur Bewertung organisatorischer, betrieblicher oder baulicher Änderungen einzusetzen, bisher gibt es aber keine Ausprägung der AUM zur Bewertung von Änderungen an signaltechnischen Systemen.

In diesem Bericht wird für eine Änderung an signaltechnischen Systemen diskutiert, ob und wie die Bewertung der Signifikanz mit einer AUM-Variante sinnvoll durchgeführt werden kann. Dies hätte den Vorteil, dass man dann im deutschen Eisenbahnsektor eine einheitliche Methode zur Signifikanzbewertung verabschieden könnte, die je nach Einsatzzweck mit unterschiedlichen Kriterien untersetzt werden könnte

Um das Ergebnis abzusichern, wird die Variante an typischen Beispielen pilotiert und mit den Ergebnissen einer bereits erarbeiteten qualitativen Signifikanzbewertung bei Durchführung von Änderungen auf Grundlage von Regelwerken abgeglichen.

2 Zum Begriff der Änderung

Bevor eine Signifikanzbewertung erfolgt, sollte zunächst überlegt werden, ob überhaupt eine Änderung im Sinne der EG Verordnung 352/2009 vorliegt. Leider wird in der Verordnung selbst der Begriff der Änderung nicht definiert, so dass man in einer weiten Auslegung des Begriffes auch davon ausgehen könnte, dass jede Änderung im Eisenbahnsystem auf Signifikanz zu bewerten wäre, z. B. Umlauf einer Weiche, Eingabe einer Langsamfahrstelle oder Änderung einer Projektierung. Dies ist aber sicherlich nicht Sinn der EG Verordnung 352/2009 und wurde auch von der ERA so bestätigt.

In EG Verordnung 352/2009 kann man aber unter Erwägung (4) implizit schließen, welche Änderungen überhaupt einer Signifikanzbewertung unterzogen werden sollten:

Gemäß Anhang III Ziffer 2 Buchstabe d der Richtlinie 2004/49/EG hat das Sicherheitsmanagementsystem Verfahren und Methoden für die Durchführung von Risikobewertungen und die Anwendung von Maßnahmen zur Risikokontrolle zu umfassen für den Fall, dass sich **aus geänderten Betriebsbedingungen oder neuem Material neue Risiken für die Infrastruktur oder den Betrieb ergeben.** Dieser wesentliche Bestandteil des Sicherheitsmanagementsystems ist Gegenstand dieser Verordnung.

Hieraus kann man insbesondere schließen, dass explizit geänderte Betriebsbedingungen oder neues Material Änderungen im Sinn der Verordnung sind, und dass es insbesondere um die Bewertung neuer Risiken geht, nämlich solche, die durch die Änderung hervorgerufen werden. Im weiteren Sinn sind also Änderungen nach EG Verordnung 352/2009 solche, bei denen neue Gefährdungen oder Risiken entstehen oder Risiken so verändert werden, dass diese Risiken die Anwendung eines Sicherheits- oder Risikomanagementverfahrens bedürfen. Diese Interpretation ist auch schlüssig in dem Sinne, dass die CSM VO ein harmonisiertes Risikomanagementverfahren beschreibt. Werden Risiken aber nicht verändert oder entstehen keine neuen Risiken, so ist auch kein Risikomanagementverfahren nötig, auch nicht nach CSM VO.

In der Regel handelt es sich daher bei wiederholter Anwendung von eingeführten Prozeduren nicht um Änderungen im Sinne der CSM VO, allenfalls bei Änderungen an den Prozeduren bzw. deren erstmaliger Anwendung.

3 Vorgaben der CSM VO

Die wesentlichen inhaltlichen Vorgaben der Verordnung sind die Folgenden:

(1) Wurde keine nationale Vorschrift notifiziert, anhand deren bestimmt werden kann, ob eine Änderung in einem Mitgliedstaat signifikant ist oder nicht, prüft der Vorschlagende die potenziellen Auswirkungen der betreffenden Änderung auf die Sicherheit des Eisenbahnsystems.

Hat die vorgeschlagene Änderung keinerlei Auswirkungen auf die Sicherheit, kann auf die Anwendung des in Artikel 5 beschriebenen Risikomanagementverfahrens verzichtet werden.

(2) Hat die vorgeschlagene Änderung Auswirkungen auf die Sicherheit, entscheidet der Vorschlagende auf der Grundlage eines Sachverständigenurteils über die Signifikanz der Änderung, wobei er folgende Kriterien berücksichtigt:

a) Folgen von Ausfällen: Szenario des schlechtesten anzunehmenden Falls („credible worst-case scenario“) bei einem Ausfall des zu bewertenden Systems unter Berücksichtigung etwaiger außerhalb des Systems bestehender Sicherheitsvorkehrungen;

b) innovative Elemente in der Implementierung der Änderung; dabei geht es nicht nur darum, ob es sich um eine Innovation für den Eisenbahnsektor als Ganzes handelt, sondern auch darum, ob es sich aus der Sicht der Organisation, die die Änderung einführt, um eine Innovation handelt;

c) Komplexität der Änderung;

d) Überwachung: Unmöglichkeit, die eingeführte Änderung über den gesamten Lebenszyklus des Systems hinweg zu überwachen und in geeigneter Weise einzugreifen;

e) Umkehrbarkeit: Unmöglichkeit, zu dem vor Einführung der Änderung bestehenden System zurückzukehren;

f) additive Wirkung: Bewertung der Signifikanz der Änderung unter Berücksichtigung aller sicherheitsrelevanten Änderungen des zu bewertenden Systems, die in jüngster Zeit vorgenommen und nicht als signifikant beurteilt wurden.

4 AUM-Verfahren

Hier soll ein kurzer Überblick über das Grundverfahren gegeben werden, dass in geringen Variationen den Vorschlägen von ORR, VDV und DB AG zugrunde liegt. Abbildung 1 zeigt die grundsätzliche Matrix, die auf den beiden Achsen eine Ausfallfolgenkategorisierung in Anlehnung an EN 50126 bzw. eine gemeinsame Einschätzung der Unsicherheit der Durchführung der Änderung auf Grundlage der Kriterien Innovation und Komplexität vorsieht

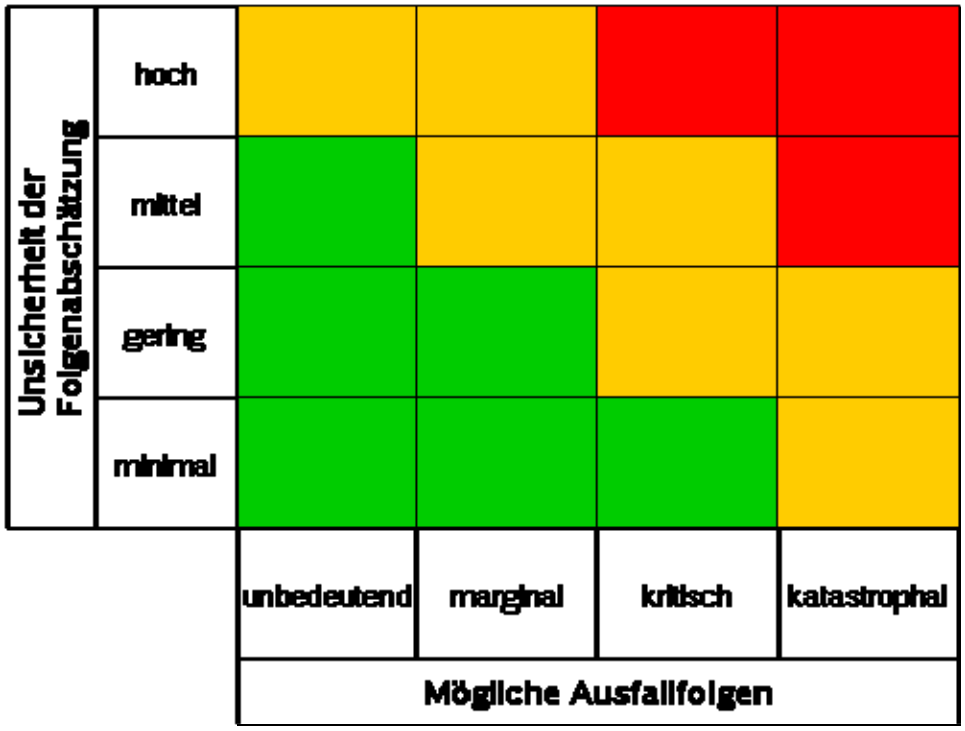

Abbildung 1: AUM

Wenn die beiden Einschätzungen vorgenommen werden, so erhält man folgende Entscheidungen

- Grün bedeutet „in jedem Fall nicht signifikant“
- Rot bedeutet „in jedem Fall signifikant“
- Gelb bedeutet, dass zusätzlich die Kriterien der Umkehrbarkeit und Überwachung zur abschließenden Beurteilung herangezogen werden müssen, die jeweils lediglich zwei Ausprägungen (gegeben/nicht gegeben) besitzen

Bei der Beschreibung der AUM fällt auf, dass statt einer Matrix auch alle Kriterien in Form von Tabellen (mit Punktbewertungen wie bei Risikoprioritätszahlen) beschrieben werden können und dass die Entscheidung von der Summe der Punkte abhängig gemacht werden kann. Dies beschreibt dasselbe Verfahren und führt zu identischen Entscheidungen, führt aber zu einer kompakteren Darstellung, insbesondere da man die beschreibenden Tabellen sowieso zusätzlich zur Matrix benötigt. Aus diesem Grund wird die Tabellendarstellung für dieses Dokument gewählt.

Bei der DB AG kommt das AUM-Verfahren mittels Matrix zur Bewertung organisatorischer, betrieblicher oder baulicher Änderungen zum Einsatz.

5 Diskussion der Signifikanzkriterien

5.1 Allgemeine Überlegungen

Bei der CSM VO geht es um einen risikoorientierten Ansatz, der immer bei signifikanten Änderungen anzuwenden ist. Die Signifikanzprüfung soll insbesondere sicherstellen, dass Änderungen, deren Durchführung bzw. fehlerhafte Durchführung ein erhöhtes oder zusätzliches Risiko mit sich bringen, durch ein harmonisiertes Risikomanagement-Verfahren abgesichert werden. D. h. generell ist bei einer summarischen Beurteilung der Änderung auch immer einzubeziehen, ob es sich um eine Änderung handelt, die ein großes Risikopotenzial beinhaltet.

5.2 Sicherheitsrelevanz

Es wird innerhalb dieser Betrachtung davon ausgegangen, dass die Änderung als sicherheitsrelevant eingestuft wird.

5.3 Folgen von Ausfällen

In der ERA Guidance heißt es dazu: „Das Kriterium der Folgenabschätzung von Ausfällen könnte beispielsweise eingesetzt werden, um zu prüfen, ob die Folgen eines sicherheitsrelevanten Fehlers der am zu bewertenden System vorgenommenen Änderung durch bestehende Maßnahmen außerhalb des zu bewertenden Systems gemindert werden. Dieses Kriterium kann dann in Kombination mit den anderen Kriterien zu der Beurteilung führen, dass eine sicherheitsbezogene Änderung sich ohne Verwendung der CSM noch in sicherer Weise verwalten ließe. Es liegt in der Verantwortung des Vorschlagenden, die Bedeutung der einzelnen Kriterien für die zu bewertende Änderung zu bestimmen."

Auch ist wichtig, zu berücksichtigen, dass es hier im engeren Sinn nicht die Folgen von Ausfällen des betrachteten Systems geht, sondern um Folgen von Fehlern bei der Durchführung der Änderung, vergleiche dazu auch die Ausführungen zu Erwägung (2) oben. Für LST ist beides als alleiniges Kriterium nicht sinnvoll, denn in der Regel können sicherheitsrelevante Systeme bzw. Änderungen an diesem in einem worst-case Szenario immer zu kritischen oder katastrophalen Folgen führen, d. h. Änderungen an LST wären immer signifikant.

Bei Änderungen an signaltechnischen Systemen könnte zur Bewertung der Ausfallfolgen der SIL zu Grunde gelegt werden (falls bekannt), da dieser in der Regel auf Grund einer Risikoanalyse ermittelt wurde, die sowohl die Ausfallfolgen als auch Risikoreduktionsfaktoren (Barrieren im Sinne von „etwaiger außerhalb des Systems bestehender Sicherheitsvorkehrungen") beinhaltet. Handelt es sich um ein neues System, so kann man eine Ausfallfolgenabschätzung nach EN 50126 vornehmen, muss sich aber bewusst sein, dass dies in der Regel immer zu sehr konservativen Abschätzungen führen wird.

Ausfallfolgen der Änderung	SIL 4	Katastrophal	4 Punkte
	SIL 3	Kritisch	3 Punkte
	SIL 2	Marginal	2 Punkt
	SIL 1	Unbedeutend	1 Punkt

Tabelle 1: Bewertung der Ausfallfolgen

Es muss dabei unbedingt beachtet werden, dass diese Tabelle NICHT aussagt, dass SIL und Ausfallfolgen nach EN 50126 gleichgesetzt werden können. Die adäquate Einschätzung ist der SIL, ersatzweise kann die Kategorie nach EN 50126 gewählt werden, wenn kein SIL bekannt ist.

5.4 Innovative Elemente in der Implementierung der Änderung

Die Innovation muss nicht nur auf die Technik bezogen werden, sondern auch auf die Erfahrung des Vorschlagenden bzw. dessen Organisation mit der Durchführung der Änderung. Dabei spannt sich ein Bogen auf zwischen Änderungen, die z. B. mittels spezifischen Regelwerks durchgeführt werden können bis zu Änderungen, bei denen der Vorschlagende keine Erfahrung hat.

Innovation der Änderung	Der Vorschlagende hat keine Erfahrung mit Technik bzw. Prozess zur Durchführung der Änderung	2 Punkte
	Der Vorschlagende hat in einzelnen Aspekten keine Erfahrung mit Technik bzw. Prozess zur Durchführung der Änderung	1 Punkt
	Der Vorschlagende hat Erfahrung mit Technik bzw. Prozess zur Durchführung der Änderung, oder es gibt spez. Regelwerke für die Durchführung der Änderung	0 Punkte

Tabelle 2: Bewertung der Innovation

Formal wird mit der mittleren Kategorie eine abweichende Bewertungsmöglichkeit im Vergleich zu Abbildung 1 eingeführt, diese bleibt in der Gesamtklassifikation aber kompatibel dazu, vgl. Tabelle 4.

5.5 Komplexität der Änderung

Bei Änderungen an technischen Systemen spielt insbesondere die Anzahl der betroffenen Teilsysteme bzw. Schnittstellen (auch organisatorisch) eine Rolle.

Komplexität der Änderung	Die Änderung bezieht sich auf mehrere Systeme mit vielen Schnittstellen und vielen Abhängigkeiten zu anderen Systemen	1 Punkt
	Die Änderung bezieht sich auf ein einzelnes System mit wenigen Schnittstellen und es gibt wenige Abhängigkeiten zu anderen Systemen	0 Punkte

Tabelle 3: Bewertung der Komplexität

Zum Vergleich mit der AUM ist es sinnvoll, als Zwischenschritte die Kombination der Bewertung der Innovation und Komplexität zu betrachten (Summer der Punkte).

Unsicherheit der Folgenabschätzung	Hoch	3 Punkte
	Mittel	2 Punkte
	Gering	1 Punkt
	Minimal	0 Punkte

Tabelle 4: Bewertung der Innovation und Komplexität

Im Ergebnis der Tabelle 4 erkennt man insbesondere die Kompatibilität der Punktebewertung mit der AUM, siehe Abbildung 1.

5.6 Überwachung

Bei Änderung an technischen Systemen ist das System bereits erfolgreich implementiert und in Betrieb gesetzt worden, dazu gehört auch die Betrachtung aller Aspekte über den gesamten Lebenszyklus, der für die Änderung relevant ist. Insbesondere bei Neuzulassungen und großen Änderungszulassungen werden die neuen Komponenten in einer Sicherheits- und Betriebserprobung intensiv überwacht. Abweichungen werden entweder über technische Diagnoseeinrichtungen oder betrieblich über das Instandhaltungs- bzw. Sicherheitsmanagement des Betrei-

bers entdeckt und behandelt. Diese Prozesse greifen grundsätzlich auch bei neuen Systemen, so dass in der Signaltechnik in der Regel von ausreichender Überwachung ausgegangen werden kann.

Überwachbarkeit der Änderung	Die Erfüllung sicherheitsrelevanter Eigenschaften der Änderung ist mit bewährten Prozessen bzw. Methoden der Qualitätssicherung möglich	0 Punkte
	Zur Überwachung müssen Prozesse oder Methoden der Qualitätssicherung neu geschaffen werden oder es sind Teilaspekte der Änderung nicht überwachbar	1 Punkt

Tabelle 5: Bewertung der Überwachung

5.7 Umkehrbarkeit

Bei Änderungen an technischen Systemen ist das System bereits erfolgreich eingeführt worden, d. h. es ist als sehr unwahrscheinlich einzustufen, dass die durchgeführten Änderungen in ihrer Gesamtheit rückgängig gemacht werden müssen. Außerdem ist bei LST-Anwendungen in der Regel schon aus Verfügbarkeitsgründen eine Rückfallebene definiert, die zumindest temporär eingesetzt werden könnte, wenn ein Rückbau o. ä. notwendig wäre. Nach einer erfolgten Typzulassung kann bei Änderungen häufig mit vertretbarem Aufwand zu dem vorherigen Zustand zurückgekehrt werden oder es können betriebliche Ersatzmaßnahmen festgelegt werden. Nur bei neuen Systemen bei denen es keine sinnvollen betrieblichen oder technischen Rückfallebenen gibt, wäre die Umkehrbarkeit der Änderung nicht gegeben.

Umkehrbarkeit der Änderung	Gegeben, z. B. wenn ein Vorzustand wieder hergestellt werden kann oder es eine angemessene betriebliche Rückfallebene gibt	0 Punkte
	Nicht gegeben, z. B. wenn ein neues System eingesetzt wird, ohne das der Betrieb nicht durchgeführt werden kann	1 Punkt

Tabelle 6: Bewertung der Unkehrbarkeit

5.8 Additive Wirkung

Die additive Wirkung ist bei einer Änderung an einem technischen System bei der Beurteilung aller der o. a. Kriterien zu betrachten, d. h. als Änderung ist immer die Änderung im Vergleich mit der letzten als signifikant beurteilten Änderung aufzufassen. Ist das technische System neu oder hat es noch keine signifikante Änderung gegeben, so sind die o. a. Kriterien so auszulegen wie für ein neues System.

5.9 Gesamtbewertung

Die Gesamtbewertung besteht darin, die Summe der Punkte der Einzelbewertungen zu bilden und mit einem Grenzwert zu vergleichen, den man durch Vergleich mit der AUM, siehe Abbildung 1, gewinnen kann. Z. B. führt dort die Kombination „katastrophal“ und „mittlere Unsicherheit“ zur Grenze, dies entspricht nach Tabelle 1 und Tabelle 4 genau 6 Punkten, d. h. ab diesem Wert sind Änderungen signifikant, darunter nicht signifikant.

Gesamtbewertung	6 oder mehr Punkte	Änderung signifikant
	Weniger als 6 Punkte	Änderung nicht signifikant

Tabelle 7: Gesamtbewertung

Bei der Beurteilung spielen die Kriterien Umkehrbarkeit und Überwachung keine Rolle mehr, wenn die Beurteilung aufgrund der anderen Kriterien schon 6 oder mehr Punkte ergibt (da es keine negativen Punktzahlen gibt) oder weniger als 4 Punkte (da die Kriterien höchstens 2 Punkte beitragen). Aus Gründen der Vereinfachung der Vorgehensweise und der Vergleichbarkeit der Ergebnisse wird jedoch empfohlen, diese Bewertung immer mit durchzuführen.

6 Beispielanwendungen

6.1 Typische Beispiele aus der Praxis

In Tabelle 8 sind einige beispielhafte Signifikanzbewertungen vorgenommen worden, insbesondere um Plausibilität und Praktikabilität der Methode an bekannten Beispielen zu testen.

	Änderungen an technischen Systemen		Signifikanzbewertung								
	Technik	Art der Änderung	LH-Änderung	RA-Änderung	Ausfallfolgen	Innovation	Komplexität	Umkehrbahrkeit	Überwachung	Summe	Signifikanz
1	ESTW	Fehlerbehebung	nein	nein	4	0	0	0	0	4	NEIN
2		geänderte Technik	nein	nein	4	2	0	0	0	6	JA
3		geänderte Funktion	ja	nein	4	0	1	0	0	5	NEIN
4		geänderte Funktion	ja	ja	4	2	1	0	0	7	JA
5		neue Funktion	ja	ja	4	2	0	0	0	6	JA
6	BÜSA	Fehlerbehebung	nein	nein	3	0	0	0	0	3	NEIN
7		geänderte Funktion	ja	nein	3	0	1	0	0	4	NEIN
8		geänderte Funktion	ja	ja	3	2	1	0	0	6	JA
9		neue Funktion	ja	ja	3	2	0	0	0	5	NEIN
10	Rangiertechnik	neue Funktion	ja	ja	2	2	0	0	0	4	NEIN
11	PZB	neue Funktion	ja	ja	1	2	1	1	0	5	NEIN
12	BÜ-Fzg-Schleife	geänderte Funktion	ja	ja	3	2	0	0	0	5	NEIN
13	Signale	geänderte Technik	ja	ja	4	2	0	0	0	6	JA

Tabelle 8: Beispielhafte Signifikanzbewertungen

Natürlich ist jede konkrete Bewertung ein Einzelfall, aber es lassen sich auch aus den generischen Bewertungen einige Erkenntnisse gewinnen.

Betrachtet man z. B. ein ESTW, das nur SIL 2 Anforderungen erfüllen muss, was z. B. im Einsatzgebiet Industrie- oder Regionalbahnen oder bei Rangierstellwerken vorkommen kann, so kann man aufgrund der Abschätzung in Tabelle 9 erkennen, dass Änderungen an einem solchen ESTW in der Regel nicht signifikant sind, es sei denn, es gäbe anderslautende nationale Vorschriften.

Kriterium	Bewertungsgrenzen	Bewertung für SIL2 Stellwerk
Ausfallfolgen	2	Bewertung = 2
Innovation	0 – 2	
Komplexität	0 – 1	
Überwachung	0	In der Regel Bewertung für LST-Anwendung = 0
Umkehrbarkeit	0	In der Regel Bewertung für LST-Anwendung = 0
Summe	2 – 5	

Tabelle 9: Signifikanzbewertung für typische SIL2 Stellwerke

6.2 Beispiel Schnittstellenänderung

Weiter wurde das Beispiel „Schnittstellenänderung“, das sich z. B. bei der Standardisierung von Schnittstellen – wie von DB Netz AG vorgeschlagen- ergeben kann, im Detail betrachtet. Allgemein sieht die Aufgabenstellung wie in Abbildung 2 aus. Dabei ist insbesondere anzumerken:

1. Vorschlagender im Sinne CSM VO ist die DB Netz AG
2. Die Schnittstellen SCI-x selber enthalten keine Funktion, sondern nur die Telegrammdefinitionen.
3. Diese ermöglichen der Anwendung, die Dienste des Sicherheitsprotokolls anwendungsspezifisch zu nutzen.
4. Das Sicherheitsprotokoll RaSTA ist eine herstellerunabhängige Fortschreibung des SAHARA-Protokolls, mit dem die DB Netz AG, aber auch die Herstellerfirmen, die es implementiert haben, jahrelange Erfahrung besitzen. Die Spezifikation und deren Implementierung wurden bereits mehrfach geändert.
5. Für RaSTA gelten dieselben Sicherheitsanforderungen wie für SAHARA. Diese Änderung kann ohne Änderung einer Risikoanalyse implementiert werden.
6. Das Sicherheitsprotokoll erfüllt die DIN EN 50159 und ist unabhängig vom jeweiligen Transportmedium

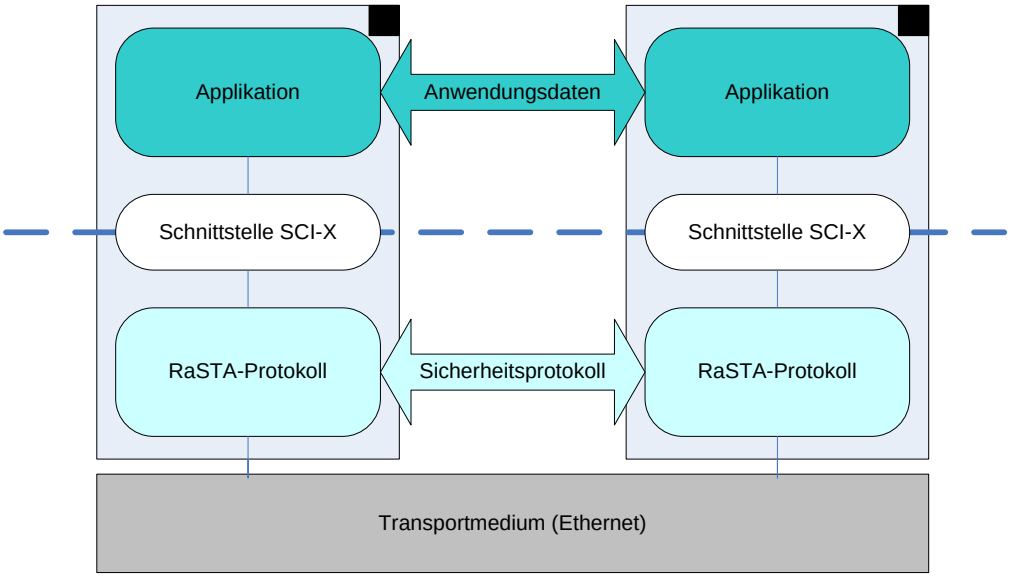

Abbildung 2: Beispiel Schnittstellenänderung

Für die Signifikanzbewertung wird die generische Schnittstelle SCI-x inkl. der darunter liegenden Implementierung betrachtet, unabhängig von der Applikation wie z. B. ILS, RBC oder LX. Für die Signifikanzbewertung mit AUM bedeutet dies:

- Ausfallfolgen: in der Regel handelt es sich um Daten, die mit Integrität SIL 4 transportiert werden müssen -> 4 Punkte
- Innovation: Der Vorschlagende hat Erfahrungen mit der Durchführung der Änderung und es gibt relevantes Regelwerk -> 0 Punkte
- Komplexität: Die Änderung besteht in einer Delta-Implementierung und ist damit wenig komplex ->0 Punkte
- Überwachbarkeit: Es stehen bewährte Prozesse und QM-Methoden zur Überwachung bereit ->0 Punkte
- Umkehrbarkeit: Es gibt betriebliche Rückfallebenen und es kann ggf. auf Vorgängerversionen zurückgegriffen werden. Außerdem kann das System komplett in Labortests auf Einsatztauglichkeit getestet werden->0 Punkte
- Additivität: nicht gegeben, da erste Änderung nach CSM VO

Zur Überprüfung wurde noch eine qualitative Signifikanzbewertung durchgeführt. Diese ist statthaft, da die Änderung komplett auf Grundlage bestehenden und relevanten Regelwerk wie DIN EN 50128, 50129 und 50159 durchgeführt wird:

- Fordert das Regelwerk für die Änderung die Durchführung einer expliziten Risikoanalyse? Nein, die Sicherheitsanforderungen können direkt von SAHARA übernommen werden
- Besitzt die Organisation Erfahrung mit der Durchführung der Änderung bzw. Anwendung des Regelwerks? Ja, sowohl DB Netz AG als auch die beteiligten Hersteller haben eine solche Änderung bereits auf Basis dieses Regelwerks durchgeführt.

Beide Analysen ergeben übereinstimmend, dass die Standardisierung dieser Schnittstellen nicht signifikant nach CSM VO ist. Es muss allerdings angemerkt werden, dass diese Bewertung nur die Schnittstellen und nicht die jeweilige Anwendung betrachtet hat. Änderungen in den Anwendungen müssen ggf. gesondert bewertet werden.

6.3 Diskussion

Die Bewertung der Ausfallfolgen mittels SIL ist praktikabel und führt zu eindeutigen Zuordnungen. Wo kein expliziter SIL ausgewiesen ist, kann man diesen aus Empfehlungen substituieren (z. B. wird SIL 4 für Entwicklungen nach Mü8004 in der Regel angenommen) oder man benutzt die Einstufung der Schadensfolgen nach EN 50126.

Ein guter Indikator für weitere Kriterien ist, ob das Lastenheft oder die Risikoanalyse zur Durchführung der Änderung geändert werden muss. Muss weder Lastenheft noch Risikoanalyse angepasst werden, z. B. bei Fehlerbehebung (Zeile 1 und 6), so spricht dies häufig für geringen Innovationsgrad und geringe Komplexität, d. h. in der Regel resultiert keine signifikante Änderung. Es gibt jedoch Einzelfälle, z. B. wenn eine bestehende Komponente durch eine neue ersetzt wird, für die der Vorschlagende weder Erfahrungen mit der Technik noch den Prozessen hat, in denen hohe Ausfallfolgen im Zusammenspiel mit hoher Innovation sofort zu einer signifikanten Änderung führen (Zeile 2). Wird dagegen eine Funktion geändert (in der Regel mit Änderung des Lastenhefts verbunden, aber ohne Anpassung der Risikoanalyse), so kann dies auch bei komplexen Änderungen, aber in der Regel geringem Innovationsgrad, zu nicht signifikanten Änderungen führen (Zeile 3 und 7). Muss dagegen die Risikoanalyse angepasst werden, weil eine Funktion radikal geändert wird oder neu dazukommt, führt dies in der Regel bei SIL 4 immer zu signifikanten Änderungen (Zeile 4 und 5), während bei geringerem SIL die Entscheidung von den weiteren Kriterien abhängt, z. B. Komplexität (Zeile 9-11).

Es bleibt abschließend zu diskutieren, ob eine mittlere Einstufung für den Innovationsgrad sinnvoll ist. Dafür spricht, dass sonst jede Innovation bei SIL4 sofort zu einer signifikanten Änderung führt. Insbesondere im Fall von technischen Änderungen ohne funktionale Änderungen könnte eine mittlere Einstufung sinnvoll sein, z. B. wenn eine Standardtechnik eingesetzt werden soll, die für die Eisenbahnsignaltechnik zwar neu ist, die aber in anderen Bereichen schon eingesetzt wird. Hier könnte es nachvollziehbar sein, dass man nur bei Vorliegen weiterer Indikatoren wie z. B. hohe Komplexität, auf eine signifikante Änderung entscheidet.

7 Zusammenfassung

In diesem Bericht wird das allgemeine AUM-Verfahren zur Signifikanzbewertung um konkrete Interpretationen der Kriterien für Änderungen an technischen Systemen ergänzt. Es wird dabei eine alternative tabellarische Beschreibung benutzt, die eine vereinfachte und kompaktere Darstellung erlaubt, aber voll kompatibel zum allgemeinen AUM-Verfahren bleibt. Insbesondere wird dasselbe Entscheidungskriterium bez. Signifikanz benutzt. Daher wird vorgeschlagen, diese Variante als AUM-T zu bezeichnen.

Weiter wird AUM-T anhand von typischen Beispielen plausibilisiert und getestet und mit anderen Vorschlägen verglichen. Es zeigt sich, dass man mit AUM-T zu konsistenten und differenzierten Signifikanzbewertungen gelangt

Dies stellt im Vergleich zu den originalen Signifikanzkriterien der CSM VO und alternativen Vorschlägen zur allgemeinen Signifikanzprüfung einen erheblichen Fortschritt dar, insb. da insgesamt mit diesem Vorschlag eine Reihe von schon vorhandenen Vorschlägen zu Signifikanzbewertungsmethoden zu einer einheitlichen Familie von Methoden zur Signifikanzbewertung für den Eisenbahnsektor komplettiert werden könnte.

8 Anhang

8.1 Vergleich mit qualitativen Signifikanzkriterien

Im NeGSt-Ergebnisbericht „Signifikanz von Änderungen auf Grundlage relevanter Regelwerke“ wurde versucht, einfache qualitative Signifikanzkriterien zu finden. Dabei wird die Signifikanzprüfung auf zwei Fragen reduziert

- „Fordert das Regelwerk für die Änderung die Durchführung einer expliziten Risikoanalyse?“
- „Besitzt die Organisation Erfahrung mit der Durchführung der Änderung bzw. Anwendung des Regelwerks?“

Allerdings muss man dazu sagen, dass diese Vorgehensweise voraussetzte, dass relevante Regelwerke vorhanden sind und damit schon eine große Einschränkung der Änderungen z. B. bezüglich Innovationsgrad macht. Außerdem besteht bei einer einfachen qualitativen Vorgehensweise immer die Gefahr, dass die zu konservativ ist, d. h. Änderungen als signifikant klassifiziert, die es bei genauerer Betrachtung evt. nicht sind.

Im Vergleich zur AUM-Vorgehensweise betrachtet die qualitative Signifikanzprüfung nur Fälle, bei denen das Regelwerk, d. h. auch das Lastenheft nicht geändert wird, d. h. nur die Fälle 1, 2 und 6 aus Tabelle 7. Die Fälle 1 und 6 würden auch als nicht signifikant klassifiziert werden und Fall 2 immer als signifikant, da die Organisation keine ausreichenden Erfahrungen mit der innovativen Technik hat. In der AUM könnte z. B. Fall 2 bei niedrigem SIL auch als nicht signifikant klassifiziert werden, d. h. die qualitative Signifikanzprüfung ist wie erwartet konservativer, aber die Ergebnisse sind konsistent.

Betrachtet man umgekehrt die Fälle, die qualitative Signifikanzprüfung als signifikant klassifiziert, d. h. Änderungen, mit denen die Organisation keine ausreichende Erfahrung hat oder bei denen eine (Änderung der) Risikoanalyse erforderlich ist, so ergeben sich ebenfalls konsistente Resultate. Bei hohem SIL führt ein hoher Innovationsgrad, der auch bei Änderung der Risikoanalyse in der Regel unterstellt wird, bei der AUM-Vorgehensweise immer zu einer signifikanten Änderung, aber es sind Abstufungen und eine genauere Differenzierung mittels der anderen Parameter möglich.

8.2 Referenzen

DB AG	Signifikanzprüfung, Foliensatz, DN Netz AG, 18.04.2012
EN 50 126	DIN EN 50 126: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS). 2000 - 03
CSM VO	VERORDNUNG (EG) Nr. 352/2009 DER KOMMISSION vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates, Amtsblatt der Europäischen Union, L 108/4, 29.4.2009
CSM GUI	ERA: Leitlinie zur Anwendung der Verordnung der Kommission über die Festlegung einer Gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Eisenbahnsicherheitsrichtlinie, ERA/GUI/01-2008/SAF
CSM EX	ERA: Sammlung von Beispielen für Risikobewertungen und möglicher Werkzeuge zur Unterstützung der CSM-Verordnung, ERA/GUI/02-2008/SAF
Mü8004	Mü8004: Technische Grundsätze für die Zulassung von Sicherungsanlagen, Eisenbahn-Bundesamt, Ausgabe vom 01.02.2007

NeGSt	Ergebnisbericht „Signifikanz von Änderungen auf Grundlage relevanter Regelwerke“
ORR	ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation, ORR, 2010
VDV	Anwendung der Verordnung (EG) Nr. 352/2009 – CSM – gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG bei der Änderung betrieblicher Prozesse und Verfahren, Ausschuss für Eisenbahnbetrieb (AEB), VDV, Februar 2009

8.3 Abkürzungen

Abk.	Langform / Erläuterung
AUM	Ausfallfolgen-Unsicherheits-Matrix
AUM-T	AUM-Technik
BÜ	Bahnübergang
BÜSA	Bahnübergangs-Sicherungsanlage
CSM	Common Safety Method
DB AG	Deutsche Bahn AG
DIN	Deutsches Institut für Normung
EG	Europäische Gemeinschaft
EN	Europäische Norm
ERA	European Railway Agency
ESTW	Elektronisches Stellwerk
Fzg	Fahrzeug
ILS	Interlocking System
LST	Leit- und Sicherungstechnik
LX	Level Crossing
NeGSt	Neue Generation Signaltechnik
ORR	Office of the Rail Regulator
PZB	Punktförmige Zugbeeinflussung
QM	Qualitätsmanagement
RaSTA	Rail Safe Transport Application
RBC	Radio Bock Center
SAHARA	Safe High Available and Redundant Communication Protocol
SCI	Standard Communication Interface
SIL	Safety Integrity Level