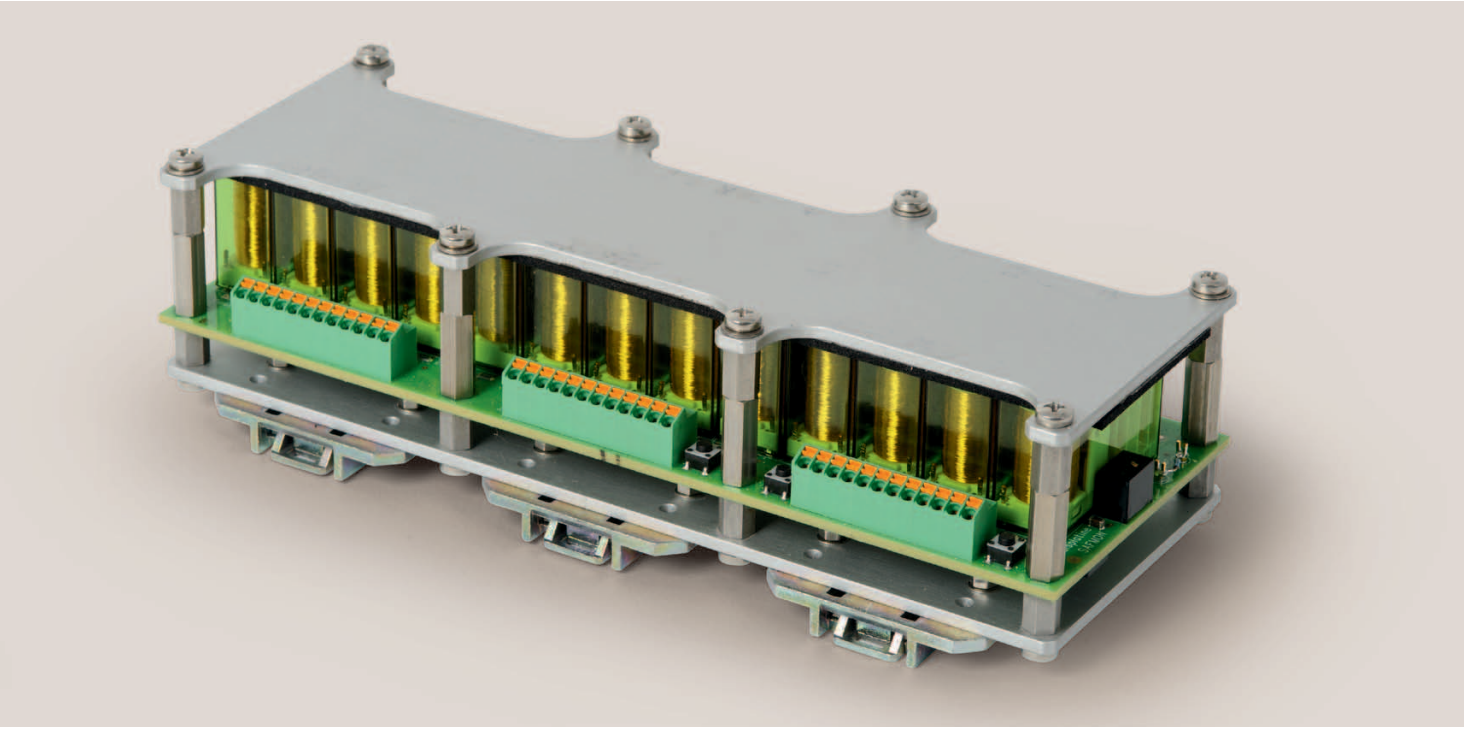
MTU SafeMon: Sicherheitskonzept für dieselmechanische und dieselhydrostatische Bahnantriebssysteme



Autor:

Ingo Lehmann
Manager Application Engineering Rail and Base Engineering Engine

Für Fahrzeughersteller und Bahnbetreiber steht die Sicherheit der Passagiere an oberster Stelle. Das Sicherheitssystem MTU SafeMon (Safety Monitor) hilft, Betriebsrisiken zu reduzieren und die vorgeschriebenen Sicherheitsziele zu erreichen. SafeMon ist ein Produkt zur Sicherheitsüberwachung, das aus einer zertifizierten Überwachungselektronik für sicherheitsrelevante Funktionen sowie der dazugehörigen sicherheits- und zulassungsbezogenen Dokumentation besteht. MTU SafeMon kann Schäden durch ungewollte Traktion oder Überdrehzahl verhindern. Dieser Artikel beschreibt Hintergrund, Funktionsweise und Nutzen des Sicherheitskonzepts..

1 | Motivation

Vor dem Hintergrund sich verschärfender europäischer Richtlinien und Verordnungen begann MTU im Jahr 2014, ein Sicherheitskonzept für die Bahn-PowerPacks zu entwickeln, die das Unternehmen herstellt. Dieses Sicherheitskonzept sollte den Fahrzeugherstellern langwierige Gefahren- und Risikoanalysen in Bezug auf den Antriebsstrang ersparen. Die von MTU spezifizierten Sicherheitsfunktionen müssen dann nur noch durch den Kunden bestätigt werden. Das daraus entstandene Produkt zur Sicherheitsüberwachung, der MTU SafeMon (Safety Monitor), kann nach den Vorgaben der sogenannten Sicherheitsbezogenen Anwendungsbedingungen (Englisch: safety application conditions, SAC) in das Fahrzeug integriert werden und regelt die sicherheitsrelevanten Funktionen des PowerPacks.

Die Verordnung 352/2009 der Europäischen Union legt eine gemeinsame Sicherheitsmethodik (Englisch: Common Safety Methods, daher auch als CSM-Verordnung bezeichnet) für die Evaluierung und Bewertung von Risiken fest.

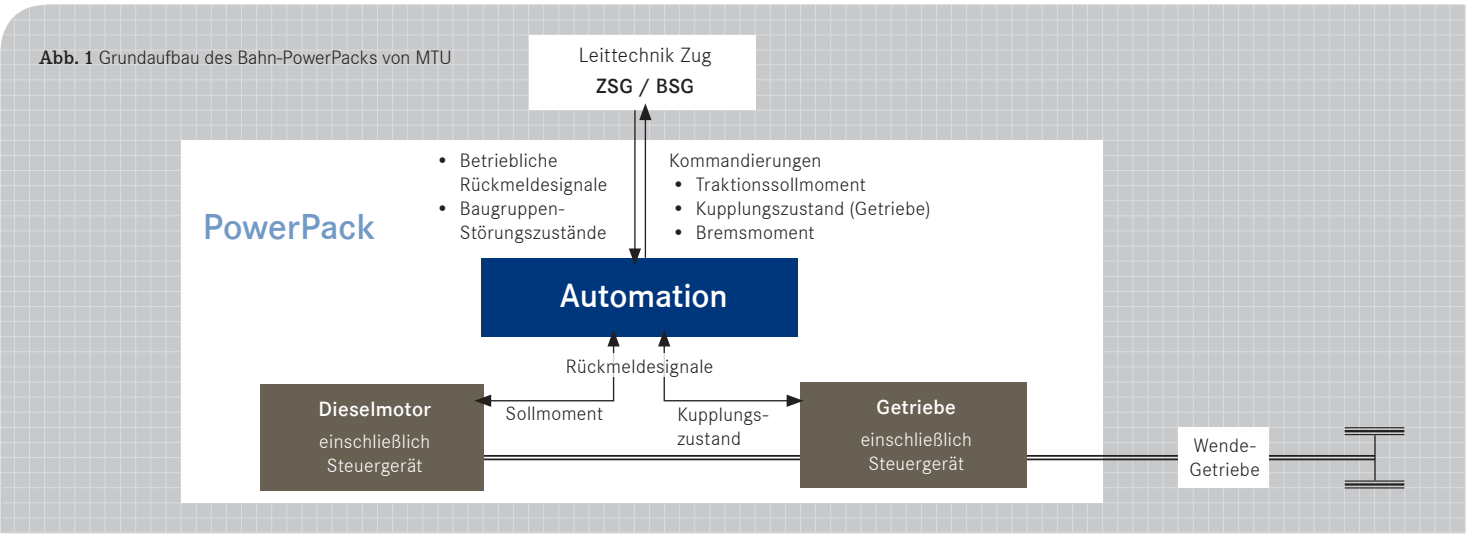


Abb. 1 Grundaufbau des Bahn-PowerPacks von MTU

Darauf basierend stellt die Sicherheitsrichtlinie Fahrzeuge (SIRF) eine Methodik zum Nachweis der funktionalen Sicherheit für Schienenfahrzeuge und der Erfüllung der CSM-Verordnung dar. Werden dessen Anforderungen korrekt umgesetzt und die Maßnahmen entsprechend angewendet, sind auch die Vorgaben der CSM-Verordnung erfüllt. Dies wird mit dem MTU SafeMon erreicht.

Basis für die MTU SafeMon zu grundlegenden Risikoanalysen war weder ein konkretes Fahrzeug noch ein konkretes Eisenbahnverkehrsunternehmen. Für den Einsatz des jeweiligen MTU-PowerPacks in einem konkreten Betriebsumfeld in einem konkreten Fahrzeug sind die Einstufungen und die Ergebnisse der Risikoanalyse durch den zuständigen Betreiber oder Integrator zu bestätigen, da die Ergebnisse sowohl vom betrieblichen Umfeld als auch von der jeweiligen Fahrzeugarchitektur abhängen und die Beurteilung der Risiken in Bezug auf die Anwendung eines Eisenbahnsystems im Verantwortungsbereich des Betreibers liegt.

Das in der SIRF beschriebene Risikoanalyseverfahren wird in der Funktionsliste des technischen Sicherheitsplans (TESIP) konkretisiert, welche Fahrzeugfunktionen und Gefährdungen identifiziert und entsprechende Sicherheitsziele in Form von Sicherheitsfunktionen und Sicherheitsanforderungsstufen formuliert.

Um sicherheitsrelvante und nicht sicherheitsrelevante Funktionen vom PowerPack zu trennen, wird das Bahn-PowerPack durch die zusätzliche Komponente MTU SafeMon ergänzt, welche die Sicherheitsfunktion mit entsprechendem Sicherheitsniveau ausführt.

Im Weiteren wird die grundlegende Sicherheitsarchitektur beschrieben und es wird dargestellt, mit welchen Maßnahmen das erforderliche Sicherheitsniveau erreicht wird.

2 | Grundsätzlicher Aufbau des MTU-PowerPacks ohne Sicherheitsfunktion und Einordnung in seine Umgebung

MTU-Bahn-PowerPacks sind kompakte Antriebssysteme, die neben Motor und Kraftübertragung alle für den Antrieb des Fahrzeugs benötigten Nebenaggregate, wie Kühlsystem und Abgasnachbehandlung, enthalten. Wesentliche Bestandteile sind Dieselmotor, Getriebe, Tragrahmen, Kühlanlage und Bordnetzgenerator sowie eine Automationseinheit zur Steuerung der PowerPack-Funktionen.

Abbildung 1 zeigt den grundsätzlichen Aufbau des PowerPacks mit einer Automation, welche das Zusammenwirken von Dieselmotor, Elektromotor und Getriebe koordiniert.

Die übergeordnete Leittechnik des Fahrzeugs kommandiert die Traktionsvorgabe in Form von einem Sollmoment oder einer Solldrehzahl. Darüber hinaus kommandiert sie den Kupplungsstatus und für den Fall, dass eine dynamische Bremse zum Einsatz kommt, ein Bremsmoment. Die Automation wird mit SIL 0 realisiert. Das Sicherheits-Integritäts-Level (SIL) ist ein Maß der Sicherheitsanforderung. SIL 0 stellt das kleinste Level dar, SIL 4 ist die maximale Sicherheitsanforderung.

3 | Resultierendes Sicherheitskonzept

3.1 | Grundgedanke

Es wird ein Getriebe eingesetzt, das in Bezug auf die korrekte Umsetzung der Kupplungsvorgabe das Sicherheitsniveau SIL 2 erreicht. SIL 2 reicht für die sichere Traktionsunterbrechung des Antriebsstrangs jedoch nicht aus. Im energiefreien Zustand befindet sich die Kupplung im Status "ausgekuppelt".

Aus diesem Grund wird zusätzlich zu den Komponenten, welche für die Realisierung der Funktionalität des PowerPacks verantwortlich sind, die Überwachungseinheit SafeMon definiert, welche

a) im Fall der Aktivierung der Sicherheitsfunktion
b) im Fall eines erkannten Ausfalls oder Fehlers einer der beteiligten Komponenten

eine entsprechende Sicherheitsreaktion erzeugt. Es wird das Ziel verfolgt, die Funktionen mit hohem Sicherheitsniveau durch eine einfache Hardware-Schaltung zu realisieren. Die Automation befindet sich nicht im sicherheitskritischen Pfad.

3.2 | Festlegung zusätzlicher Eingabeschnittstellen

Da die Anforderung sicherer Traktionstrennung von den Achsen für unterschiedliche Szenarien mit unterschiedlichen Sicherheitsanforderungsstufen zu erfüllen ist, werden dafür unterschiedliche Eingabesignale festgelegt, siehe Abbildung 2.

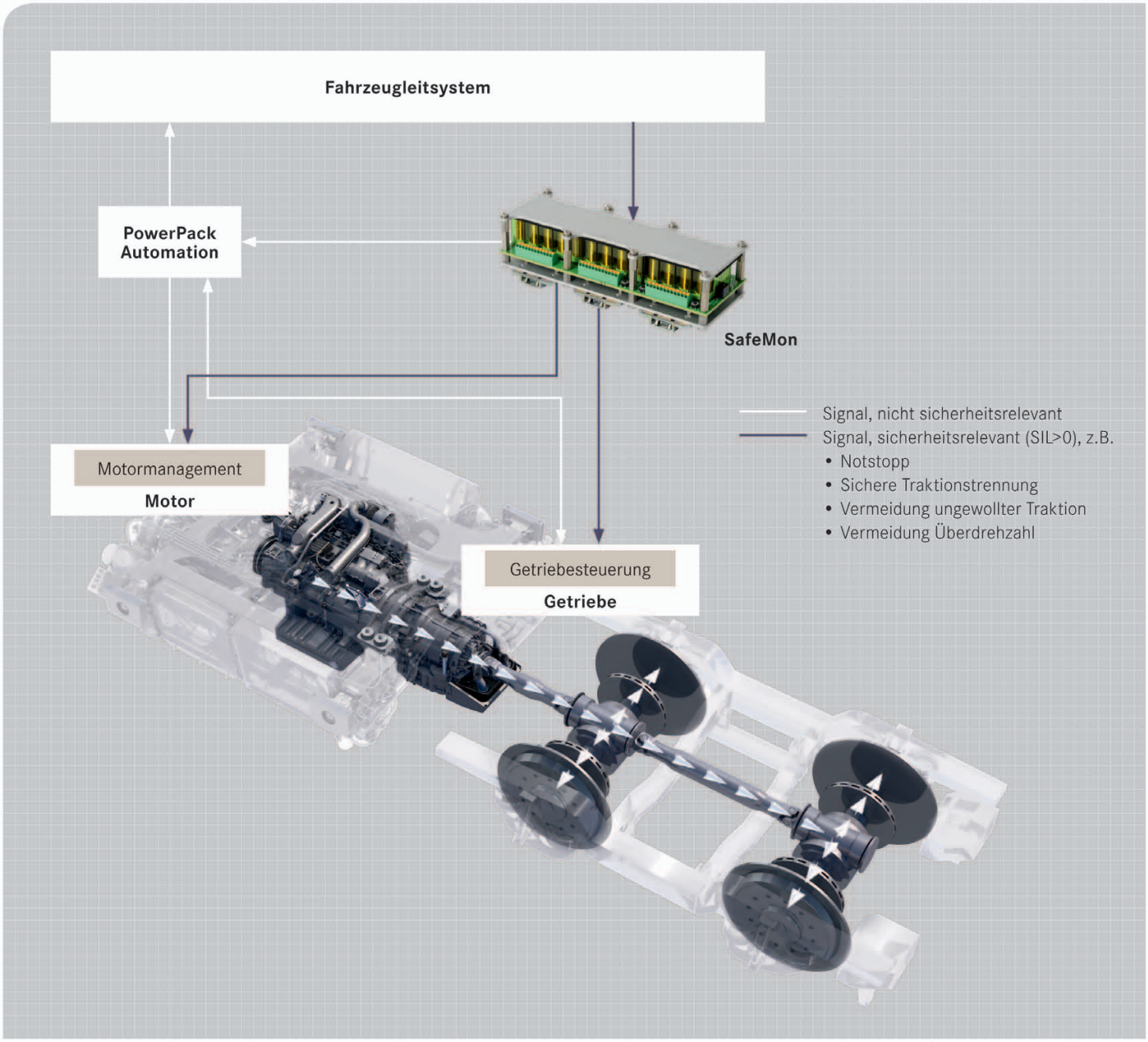
a) Sichere Unterbrechung Antriebsstrang (zweikanalig, antivalent): Über dieses Signal wird die Unterbrechung des Antriebsstrangs kommandiert, wenn die Sicherheitsbremse aktiv ist. Dabei wird in Kauf genommen, dass die Steuergeräte abgeschaltet werden.

b) Aktivierung Kupplung: Über dieses Signal lässt sich die Kupplung im ausgekuppelten Zustand verriegeln, wenn der Zug abgestellt wird. Ein Fehler bei der Auswertung der Kupplungsvorgabe kann daher nicht zum ungewollten Einkuppeln führen.

c) Kupplungsvorgabe: Dieses Signal wird mit der geringsten Sicherheitsanforderungsstufe ausgewertet.

3.3 | Funktion und grundsätzlicher Aufbau des Safety Monitors (MTU SafeMon)

Wenn der Befehl "Sichere Unterbrechung Antriebsstrang" kommandiert ist, dann unterbricht der MTU SafeMon den Durchtrieb des Getriebes. Damit lässt sich die Unterbrechung mit einem Sicherheitsniveau realisieren, welches das des Getriebesteuergerätes übersteigt. In Abbildung 2 ist zusätzlich eine Drehzahlüberwachung enthalten. Der MTU SafeMon überwacht neben den Signalen zur Antriebsstrangunterbrechung und der Kupplung auch die Drehzahlwerte der Motoren und unterbricht deren Spannungsversorgung für den Fall, dass er erhöhte Drehzahlwerte erkennt.



Umgesetzte Sicherheitsfunktionen

SIL 1	SIL 2	SIL 3
• Vermeiden von ungewollter Traktion • Schutz vor Überdrehzahlen	• Sicheres Abschalten des PowerPacks, falls erforderlich (Not-Stopp) • Sicheres Auskuppeln	• Sicheres Abtrennen der Antriebskraft (Traktion)

Optional: Überwachen von Druck und Temperatur für weitere Sicherheitsfunktionen

Die Safety Integrity Levels wurden gemäß der CSM-Verordnung (Common Safety Methods) ermittelt und durch unabhängige Gutacher bestätigt.

Abb. 2 Ergänzung des Bahn-PowerPack-Aufbaus um sicherheitsrelevante Anteile

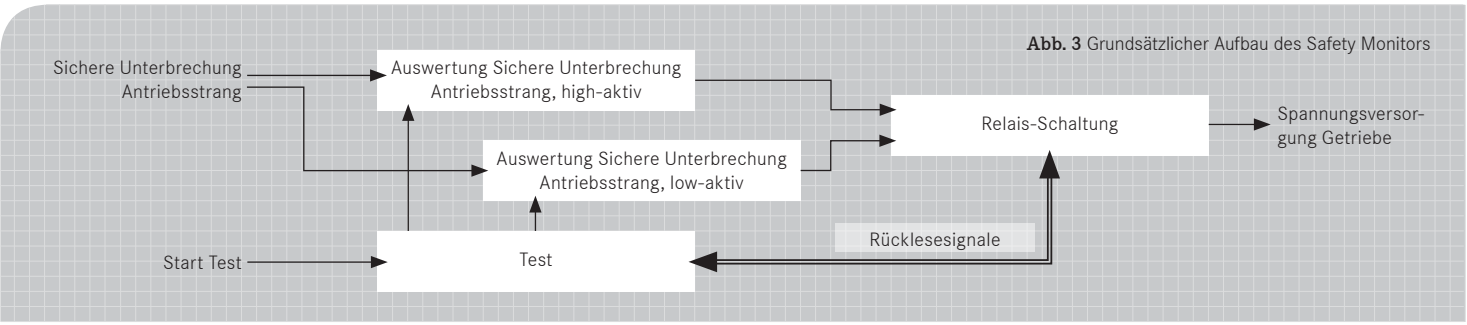


Abb. 3 Grundsätzlicher Aufbau des Safety Monitors

Abbildung 3 zeigt den grundsätzlichen Aufbau des Safety Monitors. Die beiden Signale, über welche die sichere Unterbrechung des Antriebsstrangs kommandiert wird, werden jeweils in eine Auswerteschaltung geführt, welche eine Schutzschaltung gegen Überspannungen und ungewollte elektromagnetische Effekte (EMV-Störungen) enthält. Die Ausgabesignale dieser Auswerteschaltung dienen als Eingabesignale für eine Relaisschaltung, welche als UND-Verknüpfung dient und ein Relais mit zwangsgeführten Kontakten enthält. Die Spannungsversorgung für das Getriebesteuergerät ist nur dann aktiv, wenn über beide Eingabesignale keine Unterbrechung kommandiert wird.

4 | Zulassungsprozess für Schienenfahrzeuge

Allgemeine Basis für die Zulassung stellen auf europäischer Ebene die Interoperabilitätsrichtlinie 2008/57/EG und die CSM-Verordnung 352/2009/EG dar. Die Interoperabilitätsrichtlinie definiert die grundlegenden Anforderungen, die jedes Teilsystem, also auch etwa ein Fahrzeug, erfüllen muss. Die technischen Anforderungen, die diese grundlegenden Anforderungen spezifizieren und die Schnittstellen definieren, sind in den sogenannten „technischen Spezifikationen für Interoperabilität" (TSI) hinterlegt.

Die Fahrzeugkonstruktion wird auf regelbasiertem Ansatz bezüglich Erfüllung der Anforderungen durch die sogenannte Benannte Stelle (im Englischen „Notified Body", kurz NoBo) geprüft. Darüber hinaus kann es für spezifische nationale Aspekte (zum Beispiel für offene Punkte in den TSI) weitere nationale Vorschriften, die sogenannten NNTR (im Englischen „Notified National Technical Rules") geben. Deren konforme Erfüllung wird durch die sogenannte Beauftragte Benannte Stelle (im Englischen „Designated Body", kurz DeBo) bestätigt. Die CSM-Verordnung definiert den einheitlichen Prozess zur Identifikation und Beherrschung von Gefährdungen im Eisenbahnsystem. Eine unabhängige Sicherheitsbewertung wird für signifikante, sicherheitsrelevante Änderungen am Eisenbahnsystem durch den AsBo (im Englischen „Assessment Body“) als unabhängige Bewertungsstelle für Sicherheit durchgeführt.

Der Zulassungsprozess ist dementsprechend gegliedert. Der Antragsteller beantragt die Inbetriebnahmegenehmigung bei der jeweiligen nationalen Sicherheitsbehörde für das Eisenbahnsystem. Der Antragsteller führt die notwendigen Untersuchungen durch und erstellt die erforderlichen Nachweise, die dann durch die drei genannten Bewertungsstellen NoBo, DeBo und AsBo bewertet werden. Die Ergebnisse dieser drei Stellen sind die wesentliche Grundlage, auf der die nationale Eisenbahnsicherheitsbehörde die Inbetriebnahmegenehmigung ausspricht. Mit diesem formalen Akt ist die Zulassung abgeschlossen.

Durch die klare Trennung von Sicherheitsverantwortungen in Antriebssystem PowerPack wird ein separater Sicherheitsnachweis gemäß der EN 50129 erstellt. Dieser kann dann direkt in den Sicherheitsnachweis des gesamt Fahrzeuges eingebunden werden und dem AsBo vorgelegt werden. Das vereinfacht den Zulassungsprozess für das Gesamtfahrzeug deutlich.

5 | Zusammenfassung

MTU SafeMon bietet Kunden vielfältigen Nutzen: MTU liefert mit diesem Produkt ein fertiges Sicherheitskonzept für den gesamten Antriebsstrang. Alle Sicherheitsfunktionen werden entsprechend dem gewünschten Sicherheitslevel gesteuert – komplett dokumentiert und bereits von externen Stellen begutachtet. Der Kunde erhält ein komplettes Antriebssystem aus einer Hand, zertifiziert nach der Europäischen Norm für Sicherheitsnachweise (EN 50129). MTU liefert auch die dazugehörige Dokumentation und vereinfacht somit den Zulassungsprozess.

Mit SafeMon sind Sie jederzeit sicher unterwegs

- Die Sicherheitsanalysen nach etablierten Regeln sind durchgeführt
- Ergebnisse der Analyse müssen durch den Kunden bestätigt werden.
- Sicherheitsbericht gemäß EN 50129 für das PowerPack wird durch MTU erstellt
- Kunde bettet den Bericht in den Sicherheitsbericht des Gesamtfahrzeugs ein

Sicherheitsfunktionen, welche der SafeMon umsetzt:

– Sichere Traktionstrennung SIL 3
– Sicheres Auskuppeln SIL 2
– Sicherer Not-Stopp SIL 2
– Vermeidung Überdrehzahl SIL 1
– Vermeidung ungewollte Traktion SIL 1

MTU Friedrichshafen GmbH
A Rolls-Royce Power Systems Company

www.mtu-online.com

September 2016

MTU ist eine Marke der Rolls-Royce Power Systems AG. Schnellaufende MTU-Motoren und Antriebssysteme sind in Schiffen, Schienenfahrzeugen, Landwirtschafts-, Industrie- und Bergbaufahrzeugen, militärischen Fahrzeugen, in Energiesystemen und in der Öl- und Gasindustrie im Einsatz. Das Portfolio umfasst Dieselmotoren mit Leistungen bis 10.000 Kilowatt sowie Gasmotoren bis 2.530 Kilowatt. Für die Steuerung und Überwachung der Motoren und Antriebsanlagen entwickelt und produziert das Unternehmen maßgeschneiderte Elektroniksysteme.

Power. Passion. Partnership.

10 079 (54 2D)