SOLIT Safety of Life in Tunnels

Leitfaden zur ganzheitlichen Bewertung von Tunneln mit Brandbekämpfungs-anlagen sowie deren Planung

Wissenschaftlicher Abschlussbericht zum SOLIT² Forschungsvorhaben, erstellt durch das SOLIT² Forschungs-konsortium

Anhang 5:
Sicherheitsbewertung von Betriebstechnik

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Technologie unter dem Förderkennzeichen 19S9008 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Einordnung

Im Rahmen des Verbundprojektes zum Forschungsprojekt SOLIT² – Safety of Life in Tunnels, gefördert vom Bundesministerium für Wirtschaft und Technologie (BMWi) unter dem Förderkennzeichen 19S9008 aufgrund eines Beschlusses des Deutschen Bundestages, haben die Mitglieder des Forschungskonsortiums wissenschaftliche Einzelberichte zu den jeweils von ihnen bearbeiteten Arbeitspaketen erstellt. Wesentliche Ergebnisse der Einzelberichte wurden in dem vorliegenden Leitfaden zusammengefasst. Der Leitfaden wurde gemeinsam von den Konsortialmitgliedern erstellt und ist der gemeinsame wissenschaftliche Abschlussbericht des SOLIT²-Konsortiums im Sinne der Förderrichtlinien des BMWi. Daneben ist der Leitfaden Teil der Arbeitspakete. Die Einzelberichte sind über den Projektkoordinator erhältlich.

Impressum:
Leitfaden zur ganzheitlichen Bewertung von Tunneln mit Brandbekämpfungsanlagen sowie deren Planung

Für diesen Leitfaden sind die folgenden Anhänge verfügbar:
Anhang 1: Statusanalyse
Anhang 2: Ausgewählte Ergebnisse aus den Brandversuchen
Anhang 3: Planungsleitfaden für stationäre Brandbekämpfungsanlagen in Tunneln
Anhang 4: Beispielhafte Anwendung der Risikoanalyse
Anhang 5: Sicherheitsbewertung von Betriebstechnik
Anhang 6: Lebenszykluskosten von Betriebstechnik
Anhang 7: Brandszenarien zur Überprüfung der Wirksamkeit von BBA

An der Erstellung der Dokumente haben die folgenden Personen mitgewirkt:

BUNG AG, Beratende Ingenieure
Wolfgang Baltzer
Uwe Zimmermann

FOGTEC Brandschutz GmbH & Co KG
Tobias Hoffmann
Max Lakkonen
Dirk Sprakel
Sascha Wendland

Ruhr Universität Bochum – Lehrstuhl für Tunnelbau, Leitungsbau und Baubetrieb
Markus Thewes
Götz Vollmann

STUVA Studiengesellschaft für unterirdische Verkehrsanlagen e. V.
Frank Leismann
Roland Leucker
Antonio Piazolla

TÜV Süd Rail GmbH
Jürgen Heyn
Jakob Zaranek
Lutz Neumann

IFAB Institut für angewandte Brandschutzforschung GmbH
Stefan Kratzmeir
Rajko Rothe

Institut der Feuerwehr Sachsen Anhalt
Mario Koch
Horst Starke

Die Mitglieder des Forschungskonsortiums danken dem wissenschaftlichen Beirat für wertvolle Hinweise und Anregungen im Vorfeld der Durchführung der Brandversuche: Felix Amberg (ITA-COSUF), Frank Heimbecher, Jürgen Krieger (Bundesanstalt für Straßenwesen), Ingrid Ortlepp (Thüringer Innenministerium), Werner Thon (Feuerwehr Hamburg), Bernhard Koonen (Projektträger Mobilität und Verkehr), Robert Sauter (ADAC e. V.).

Herausgeber:
SOLIT² Forschungskonsortium, bestehend aus:
BUNG AG – Beratende Ingenieure
FOGTEC Brandschutz GmbH & Co. KG
Ruhr Universität Bochum – Lehrstuhl für Tunnelbau, Leitungsbau und Baubetrieb
STUVA Studiengesellschaft für unterirdische Verkehrsanlagen e. V.
TÜV Süd Rail GmbH

Druck und Verlag:

Die Dokumente erscheinen im Eigenverlag und sind über contact@SOLIT.info erhältlich.

Köln
Version: 2.0; Bearbeitungsstand: November 2012

Der Leitfaden wird durch das Forschungskonsortium weiter überarbeitet. Neue Bearbeitungsstände können über das Forschungskonsortium unter contact@SOLIT.info angefragt werden.

Projektkoordinator: FOGTEC Brandschutz GmbH & Co. KG, Schanzenstraße 19, 51063 Köln

Inhaltsverzeichnis

1. Einleitung

1.1 Vorwort

Der vorliegende Anhang „Sicherheitsbewertung der Betriebstechnik“ vervollständigt und präzisiert die im Hauptdokument „*Leitfaden zur ganzheitlichen Bewertung von Tunneln mit Brandbekämpfungsanlagen sowie deren Planung*“, Kapitel 3.3, beschriebene Methodik zum Nachweis des Sicherheitsniveaus von Tunnelausstattungsvarianten. Im Fokus liegt hierbei die Zuordnung von funktionalen und sicherheitsbezogenen Anforderungen an die Einzelkomponenten einer Brandbekämpfungsanlage (BBA), die als Bestandteil eines ganzheitlichen Tunnelsicherheitssystems agiert (nachfolgend als BBA bezeichnet), sowie deren Nachweis über ihren Lebenszyklus hinweg (vgl. DIN EN 61508-1:2011, Kapitel 7).

Wie im Hauptdokument, Kapitel 3.3, bereits angeführt, wird die Funktion „Brandbekämpfung“ als Haupt-Sicherheitsfunktion der BBA durch eine Reihe von Einzelfunktionen und Komponenten verwirklicht, die auf unterschiedlichen Technologien (zum Beispiel Mechanik/Hydraulik, Elektrik, programmierbare Elektronik) basieren. Bei der Ausrüstung einer Tunnelanlage mit einer BBA müssen daher alle Einzelkomponenten (z. B. Sensoren, Datenverarbeitung, Bereitstellung des Löschmediums, Leittechnik zur Ansteuerung der Bereichsventile bzw. der Tunnelbelüftungsanlage, etc.) sowohl einzeln als auch im Zusammenspiel zur Haupt-Sicherheitsfunktion betrachtet werden.

Die Ermittlung der quantitativen und qualitativen Anforderungen an die funktionale Sicherheit der relevanten Teilsysteme (Komponenten) folgt einem risikoorientierten Ansatz.

Bei der Nachweisführung ist der gesamte Sicherheitslebenszyklus der Komponenten zu betrachten, angefangen mit der Definition der Randbedingungen und dem Systemkonzept, über die Entwurfsphase, Einbau, Betrieb und Wartung bis zur Außerbetriebssetzung.

Für die Bestimmung der tolerierbaren Nichtverfügbarkeit (also der mittleren Wahrscheinlichkeit eines Ausfalls der BBA im Anforderungsfall) wird eine Methodik in Anlehnung an die DIN EN 61508 herangezogen. Der Nachweis der Erfüllung dieser Anforderung soll ebenfalls nach DIN EN 61508 erfolgen.

1.2 Zweck

Ziel dieses Anhangs ist die Konkretisierung der in DIN EN 61508 enthaltenen grundsätzlichen Anforderungen bezüglich der Errichtung und dem Betrieb von sicherheitsrelevanten elektrischen Systemen[1]. Insbesondere werden alle für die Funktion der BBA relevanten Einflussparameter identifiziert, welche im Rahmen einer Sicherheitsbewertung berücksichtigt werden müssen. Zudem wird dargestellt, wie die qualitativen und quantitativen Sicherheitsanforderungen in Abhängigkeit der notwendigen Risikoreduktion ermittelt werden können, auf die Einzelkomponenten aufzuteilen und schließlich nachzuweisen sind.

1.3 Anwendungsbereich

Die nachfolgend beschriebene Methodik kann grundsätzlich für alle sicherheitsbezogenen Funktionen der Anlagentechnik in Straßen- und Bahntunneln angewandt werden.

1.4 Abgrenzung

Das Einsatzpotenzial einer BBA hängt maßgeblich von den folgenden Faktoren ab:

- Der prinzipiellen Eignung der eingesetzten Technologien, Architektur und Komponenten (z. B. Messprinzip) unter den gegebenen Randbedingungen (z. B. Luftströmung),
- der physikalischen Wirksamkeit der Anlage bezüglich der verschiedenen anzunehmenden Brandkategorien und
- der sicherheitstechnischen Verfügbarkeit der BBA.

Eine hochwirksame BBA mit geringer Verfügbarkeit ist ebenso ungeeignet das Schadensausmaß und damit das Risiko zu senken wie eine schwach wirksame, jedoch hochverfügbare BBA.

1.4.1 *Eignung der Technologie*

In der nachfolgend dargestellten Methodik der Sicherheitsbewertung wird grundsätzlich die systematische Eignung der eingesetzten Technologie (hier insbesondere der notwendigen Komponenten der Sensorik) vorausgesetzt. Die Tauglichkeit der Komponenten muss hierzu in Form geeigneter Nachweise durch die Hersteller/Lieferanten im

[1] DIN EN 61508 bezieht sich auf elektrische, elektronische und programmierbare elektronische (E/E/PE) Systeme, viele Prinzipien sind jedoch auch auf nicht-elektrische Komponenten anwendbar.

Rahmen der Gesamtsicherheitsbewertung der Tunnelanlage aufgezeigt werden.

1.4.2 *Physikalische Wirksamkeit*

Zur Ermittlung der physikalischen Wirksamkeit einer BBA wird auf die im Kapitel 3.6 des Hauptdokuments aufgezeigte Methodik verwiesen. Basis der Nachweisführung stellen z.B. empirische Versuchsreihen und die dabei ermittelten Messdaten dar (analog zur Vorgehensweise im Rahmen des SOLIT^2-Projekts). Diese dienen z. B. als Eingangsgrößen zum Aufbau von Simulationsmodellen (CFD-Analysen), wobei weitere Tunnelparameter (z. B. Tunnelgeometrie in Abhängigkeit des zu betrachtenden Objekts) sowie die angenommene Bemessungsbrandgröße berücksichtigt werden müssen. Je nach Auslösezeitpunkt und der abschätzbaren Wirksamkeit der Löschmaßnahme (unter Beachtung der möglichen Brandszenarien im Tunnel) können unterschiedliche Brandentwicklungen resultieren (vgl. Abb. 1).

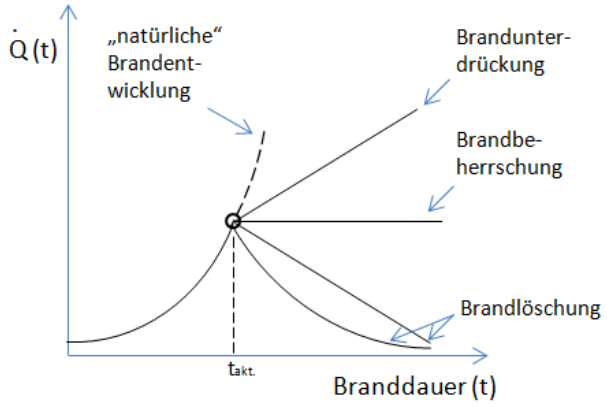

Abb. 1
Wirksamkeit einer Löschmaßnahmen auf die Wärmefreisetzung (Quelle: TÜV SÜD)

Im Weiteren wird daher auf die Wirksamkeit der BBA nicht näher eingegangen. Weitergehende Ausführungen können Kapitel 3.6 im Hauptdokument entnommen werden.

1.4.3 *Verfügbarkeit*

Die Ermittlung der notwendigen sicherheitstechnischen Verfügbarkeit ist Gegenstand der im Kapitel 2 dieses Anhangs beschriebenen Methodik.

Der Nachweis ist gemäß DIN EN 61508 zu führen, wobei bezüglich der Gesamt-Verfügbarkeit auch nicht-elektrische Komponenten zu berücksichtigen sind.

1.5 Begriffserklärungen

ALARP	As low as reasonably practicable (so niedrig wie vernünftigerweise möglich)
BBA	Brandbekämpfungsanlage
Bemessungsbrand	Brandgröße zur Dimensionierung von Brandschutzeinrichtungen. Dabei handelt es sich nicht um die maximal auftretende Brandgröße, sondern um eine zeitbezogene Brandentwicklung bzw. Brandintensität.
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch
FTA	Fehlerbaumanalyse (en. Fault Tree Analysis)
HFT	Hardware-Fehlertoleranz
HRR	Heat Release Rate (Energiefreisetzungsrate)
NFPA	National Fire Protection Association
PFD	Probability of Failure on Demand (Wahrscheinlichkeit eines Versagens bei Anforderung)
RABT	Richtlinien für die Ausstattung und den Betrieb von Straßentunneln
RAMS	Reliability, Availability, Maintainabilty, Safety
SFF	Anteil sicherer Ausfälle (en: safe failure fraction)
S-FMEA	System-Fehlermöglichkeits- und -Einflussanalyse (en: System-Failure Mode and Effects Analysis)
Sicherheit	Sicherheit von Tunnelnutzern, Einsatzkräften und der Infrastruktur
SIL	Sicherheits-Integritätslevel
spezifisches Sicherheitsniveau	Sicherheitsniveau, das durch das Erfüllen von bestimmten Schutzzielen erreicht wird
ZTV-ING	Zusätzliche Technische Vertragsbedingungen und Richtlinien für Ingenieurbauten

1.6 Normen und Regelwerke

- RABT: „Richtlinien für die Ausstattung und den Betrieb von Straßentunneln“, Aktuelle Ausgabe: 2006
- 2004/54/EG: Richtlinie des europäischen Parlaments über Mindestanforderungen an die Sicherheit von Tunneln im transeuropäischen Straßennetz, Aktuelle Ausgabe 2004
- Bewertung der Sicherheit von Straßentunneln, Heft B66, BASt
- Leitfaden für Sicherheitsbewertungen von Straßentunneln gemäß RABT 2006 (Abschnitt 0.5), BASt
- 2004/54/EC, Minimum safety requirements for tunnels in the Trans-European road network
- EN 54-4, Fire detection and fire alarm systems
- DIN 14675:2012-04, Brandmeldeanlagen – Aufbau und Betrieb
- VDE 0833-1, Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Allgemeine Festlegungen
- VDE 0833-2, Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Festlegungen für Brandmeldeanlagen
- Normreihe DIN EN 61508:2011, Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme
- DIN EN 50126-1, Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)

2. Methodik der Sicherheitsbewertung

2.1 Allgemeines

Die Nichtverfügbarkeit einer BBA hat unmittelbar negativen Einfluss auf die Personensicherheit und muss folglich hinreichend klein sein. Auf Grund der technischen Komplexität einer BBA einschließlich aller zur Sicherstellung der Wirkkette nötigen Komponenten (z. B. Branddetektion, Bereitstellung des Löschmediums, Steuerung der Lüftungstechnik) kann die Nichtverfügbarkeit nicht vernachlässigt werden. Dies gilt insbesondere aufgrund der Tatsache, dass eine BBA weder „inhärent sicher“, noch als „fail-safe“-System konzipiert und betrieben werden kann.

Agiert die BBA als Bestandteil eines ganzheitlichen Tunnelsicherheitssystems, so muss eine hinreichend hohe Verfügbarkeit der eingesetzten Komponenten nachweislich erzielt und aufrecht erhalten werden. Die Sicherheitseinstufung orientiert sich dabei maßgeblich an dem Wert des Bemessungsrisikos einer Tunnelanlage (vgl. Kap. 2.6 im Hauptdokument) in Korrelation mit dem ggf. notwendigen Kompensationserfordernis unter Berücksichtigung tunnelspezifischer, risikorelevanter Parameter.

Als Verfügbarkeit wird grundsätzlich die Fähigkeit einer Ausrüstung oder von deren Teilen verstanden, die ihnen zugedachte Funktion unter festgelegten Bedingungen zu einem bestimmten Zeitpunkt, hier im Anforderungsfall, zu erfüllen.

Die Gesamtsicherheitsfunktion der BBA wird definiert werden als *die Beaufschlagung eines Bereichs mit einem Löschmedium in vorgesehener Art und Weise (Menge, Ort, Zeit), ausgelöst durch ein Initialereignis wie Brand oder Rauchentwicklung im Tunnel (nach Überschreitung eins vordefinierten Schwellenwertes).*

Die Gesamtsicherheitsfunktion kann auch Komponenten oder Maßnahmen beinhalten, die nicht der BBA direkt zugeordnet sind, z.B. die Alarmierung des Betriebspersonals, die Steuerung der Lüftung oder der Lichtzeichenanlagen, wenn dies für eine ordnungsgemäße Funktion der BBA notwendig ist.

2.2 Gesamtsicherheitslebenszyklus

Bei der Beurteilung der System-Sicherheit ist grundsätzlich der gesamte Lebenszyklus des Sicherheitssystems zu berücksichtigen, vgl. DIN EN 61508-1. Die Abb. 2 zeigt den dort definierten Lebenszyklus. Begleitend fordert die DIN EN 61508 zu jeder Phase des Gesamtsicherheitslebenszyklus oder kontinuierlich folgende vier Aktivitäten:

- Verifikation,
- Beurteilung der funktionalen Sicherheit,
- Management der funktionalen Sicherheit sowie
- Dokumentation.

Aufgrund der zu erwartenden Bedingungen im vorliegenden Fall (hier mit Verweis auf die im Rahmen des SOLIT^2-Projekts eingesetzte Technologie) sowie den typischen Eigenschaften einer BBA im Allgemeinen, sind insbesondere folgende Faktoren zu berücksichtigen:

- Projektspezifische Randbedingungen insbesondere klimatischer Art
- Ausfälle während des Betriebs bzw. durch Alterung und deren rechtzeitige Erkennung
- Fehler des Personals bei Wartungs- und Instandhaltungsmaßnahmen

- Unvollständige Diagnostizierbarkeit und Testbarkeit bestimmter Komponenten oder Teilfunktionen
- Zuvor nicht erkennbare Ausfälle im Anforderungsfall
- Abkündigungen von Komponenten und damit Notwendigkeit des Austauschs durch Ersatzkomponenten bzw. Nachentwicklung von Hard- und Software (Modifikation/Nachrüstung)
- Betrieblichen Randbedingungen, wie z. B. Maßnahmen bei Störungen, Reparaturzeiten etc.

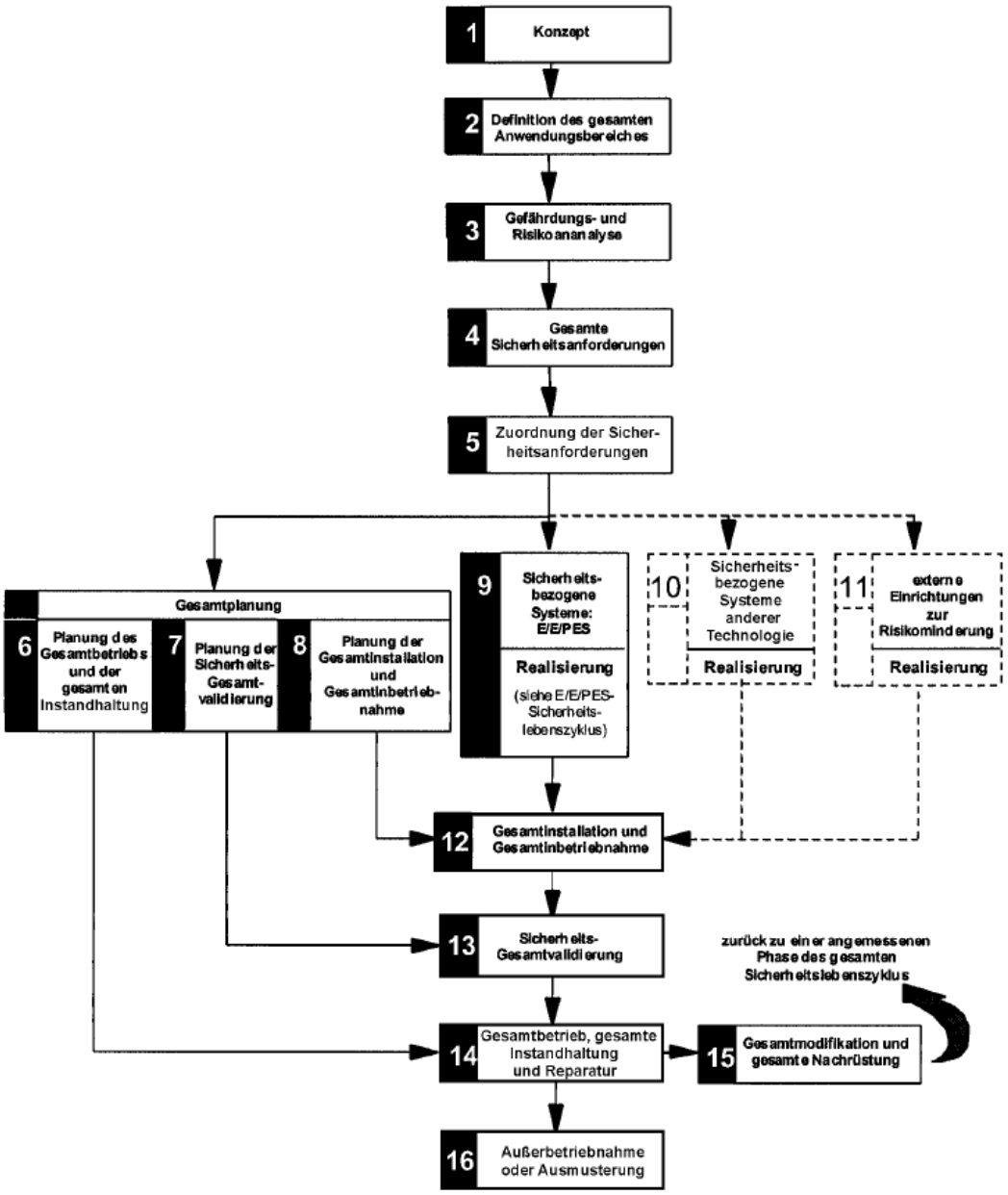

Abb. 2
Gesamt-Sicherheitslebenszyklus (Quelle: DIN EN 61508-1)

2.3 Risikoanalyse und Gefährdungsanalyse

Gemäß DIN EN 61508-1 ist eine Gefährdungs- und Risikoanalyse durchzuführen (Schritt 3 in der Abb. 2). Während im Maschinen- und Anlagenbau eine Unterscheidung hierbei häufig schwer fällt und nicht sinnvoll ist, ist im Fall der Betrachtung einer BBA eine klare Trennung möglich und notwendig.

Das Risiko ergibt sich allgemein aus der Häufigkeit einer Gefährdung (hier eines Brandes), deren Auswirkung/Schaden (hier Verletzte oder Tote) sowie der Wahrscheinlichkeit, dass die erwartete Auswirkung eintritt. Gibt es sehr unterschiedliche Gefährdungen (z. B. sehr verschiedene Brandlasten/Szenarien) und/oder unterschiedliche Auswirkungen, sind diese zunächst separat zu betrachten und entsprechend ihrer Häufigkeit bzw. Wahrscheinlichkeit gewichtet zu addieren. Aufgabe der Risikoanalyse ist es, die Sicherheit zu bewerten und im Falle des Überschreitens eines zuvor festgelegten Risikoakzeptanzkriteriums risikomindernde Maßnahmen zu definieren. Die Installation einer BBA kann eine solche risikomindernde Maßnahme sein, ihre Funktion ist dann eine „Sicherheitsfunktion“. Die sicherheitsrelevanten Anforderungen an diese Sicherheitsfunktion ergeben sich aus dem Maß der notwendigen Risikominderung.

Es wird davon ausgegangen, dass das Initialereignis „Brand oder Rauchentwicklung oberhalb eines zuvor festgelegten Schwellenwerts“ seltener als einmal pro Jahr und Anlage eintritt. Somit ist gemäß DIN EN 61508 die Definition einer tolerierbaren Nichtverfügbarkeit im Anforderungsfall („Probability of Failure on Demand“, PFD_{tol}) erforderlich.

Somit gilt:

$$PFD_{tol} = \frac{Risiko_{tol}}{Risiko_{orig}}$$

mit dem Risiko ohne BBA $Risiko_{orig}$.

Gleichermaßen fordert die RABT in Kapitel 0.5 eine explizite Risikobewertung für Tunnelanlagen, die eine besondere Charakteristik aufweisen bzw. abweichend zu den RABT Vorgaben ausgeführt werden (dies betrifft folglich auch die Implementierung einer BBA als kompensatorische Maßnahme in der Tunnelsicherheitstechnik). Eine ausführliche Beschreibung zur Methodik der Risikobewertung ist dem Kapitel 3.3 des Hauptdokuments zu entnehmen.

In der Gefährdungsanalyse werden alle Möglichkeiten, welche sich auf die Sicherheitsfunktion auswirken könnten, identifiziert und bewertet. Dies sind alle Ereignisse (insbesondere technische oder menschliche Fehler, aber ggf. auch Umwelteinflüsse), welche zum Ausfall der sicherheitsbezogenen (risikomindernden) Funktion und damit letztlich zu einem (größeren) Schaden führen können.

Sowohl Risiko- als auch Gefährdungsanalysen können nur unter definierten Randbedingungen durchgeführt werden. Die für eine Risikoanalyse benötigten Randbedingungen sind oft unabänderbar (z. B. vom Gesetzgeber oder Auftraggeber definiert), die Risikoanalyse wird daher einmalig zu Projektbeginn durchführt oder sogar projektunabhängig erstellt.

Die für die Durchführung einer Gefährdungsanalyse zusätzlich erforderlichen Randbedingungen und Parameter hingegen sind praktisch immer projektspezifisch, weil sie der eingesetzten Technik und Architektur entspringen. Da die Technik zu Projektbeginn in der Regel noch nicht feststeht, muss die Gefährdungsanalyse zumeist während der Entwicklung regelmäßig überarbeitet und detailliert werden.

3. Systemdefinition

3.1 Anforderungen an die Gesamt-Sicherheitsfunktion

Wird eine BBA als kompensatorische Maßnahme in der Tunnelsicherheitsausrüstung (vgl. Abb. 46 im Hauptdokument) eingesetzt, darf die Nichtverfügbarkeit der Gesamtsicherheitsfunktion der BBA einen Wert von $PFD_{tol} = 10^{-1}$ nicht überschreiten, unabhängig vom dort ermittelten Wert.

Der erforderliche Sicherheitsintegritätslevel als Maß für die Freiheit des Systems von systematischen Fehlern (z. B. Softwarefehler, Auslegungsfehler etc.) muss hierbei entsprechend mindestens mit SIL 1 festgelegt werden.

Im Rahmen der Systemdefinition wird eine Architektur geplant, die mit Hilfe geeigneter Werkzeuge, i. d. R. einer FTA oder S-FMEA, qualitativ und quantitativ auf Schwachstellen untersucht wird. Daraus werden Maßnahmen zur Risikominderung abgeleitet. Die Anhänge zu den Teilen 2 und 3 der DIN EN 61508 liefern hierfür umfangreiche Anforderungstabellen in Abhängigkeit vom angestrebten Sicherheitsintegritätslevel.

Weitere Schritte zur Planung, Implementierung, Betrieb und Wartung der eingesetzten Systeme sind den anwendbaren Anforderungen gemäß DIN EN 61508 zu entnehmen.

3.2 Anforderungen an Teil-Sicherheits-funktionen

Die Gesamtsicherheitsfunktion muss in Teil-Sicherheitsfunktionen zerlegt werden, welche den einzelnen Komponenten der BBA, angefangen von der Erkennung des Brandes (ab einer festgelegten Leistung bzw. Rauchentwicklung), über das Bereitstellen des Löschmediums bis zur Verteilung desselben über den vorgesehenen Bereich, zugeordnet werden können.

Die Aufteilung der Sicherheitsanforderungsspezifikation in einen Hardware- und einen Software-Anteil – wie im Punkt „Leittechnik“ angedeutet – folgt der Hierarchie der DIN EN 61508. Im Systemtest wird an späterer Stelle die erfolgreiche Integration nachgewiesen.

Entsprechend sind aus der Spezifikation der Anforderungen an das Gesamtsystem BBA mehrere Teilspezifikationen für die jeweiligen sicherheitsgerichteten Komponenten der BBA abzuleiten.

Wie bereits in Abschnitt 2.1 angedeutet, kann die Sicherheitsfunktion der BBA in ihrer Gesamtheit im Allgemeinen in folgende Teil-Sicherheitsfunktionen zerlegt werden:

- Erkennung eines Brandereignisses (Sensorik/Branddetektion)
- Informationsübertragung (z. B. Bussystem)
- Informationsverarbeitung/Leittechnik (Hardware und Software)
- Aktivierung/Bereitstellung des Löschmediums (z. B. Pumpen und deren Steuerung/Energieversorgung)
- Steuerung/Führung des Löschmediums (z. B. Rohrleitungen, Ventile und deren Ansteuerung)
- Verteilung des Mediums über den definierten Bereich (z. B. durch Düsen)

Der Zielwert für die Nichtverfügbarkeit PFD_{tol} der BBA bezieht sich auf den gesamten Wirkweg, der für die Realisierung der Gesamt-Sicherheitsfunktion notwendig ist. Er muss also auf die einzelnen Komponenten aufgeteilt werden. Eine erfahrungsgemäß sinnvolle Aufteilung der PFD_{tol} der Gesamtfunktion auf die Teil-Sicherheitsfunktionen ist in Abb. 3 dargestellt.

Müssen zum Erreichen der angenommenen Wirksamkeit der Brandbekämpfung weitere Bedingungen geschaffen werden (z. B. Eingriff in die Be-/Entlüftung etc.), sind auch diese Funktionen bzw. Komponenten zu betrachten.

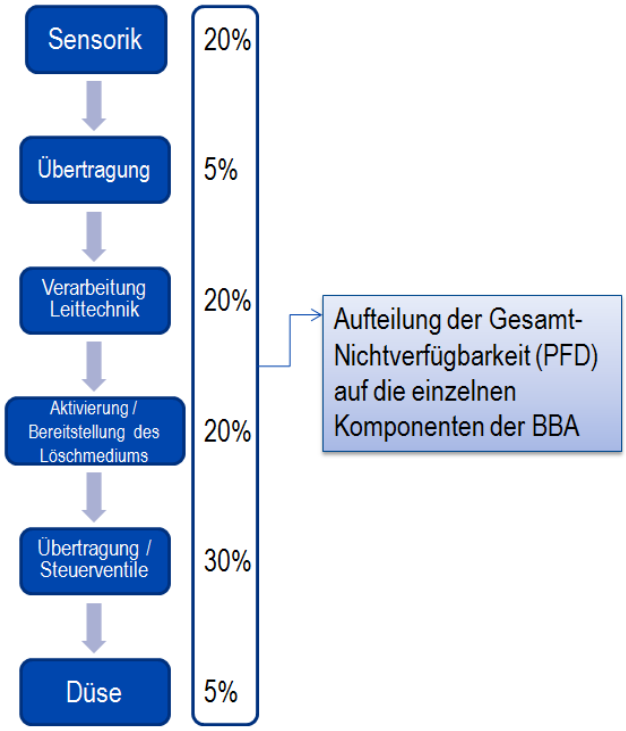

Abb. 3
Beispielhafte Aufteilung der Gesamt-Nichtverfügbarkeit einer BBA auf die Komponenten der Wirkkette

3.3 Hinweise zur Nachweisführung

Das Erreichen der den Teil-Sicherheitsfunktionen und somit den einzelnen Komponenten zugeteilten Grenzwerten $PFD_{tol,Komp}$ ist geeignet nachzuweisen. Für E/E/PE-(Teil-)Systeme soll der Nachweis gemäß DIN EN 61508 erfolgen. Für andere Komponenten (z. B. Ventile, Pumpen etc.) muss hingegen der Nachweis über einschlägige Normen oder Erfahrungswerte erfolgen. In jedem Fall sind alle relevanten Randbedingungen (insbesondere Umweltparameter) sowie betrieblichen Parameter (Ausfalldetektion, Reaktions-/Reparaturzeiten etc.) in der Komponenten- bzw. Gesamtsystemdokumentation zu berücksichtigen.

Zum Nachweis, dass die mit der Realisierung tatsächlich erreichte Nichtverfügbarkeit PFD_{ist} kleiner ist als die tolerierbare Nichtverfügbarkeit PFD_{tol}, muss genau eine komplette Wirkkette gemäß Abschnitt 3.2 betrachtet werden. D. h. es ist anzunehmen, dass im Bereich X ein Initialereignis vorliegt, welches von dem/den diesem Bereich zugeordneten Sensor(en) erkannt werden muss, ggf. die für diesen Bereich nötigen Randbedingungen geschaffen werden müssen und in diesem Bereich

das Löschmedium ausgebracht werden muss. Unterscheiden sich die einzelnen Bereiche bezüglich der an der Wirkkette beteiligten Elemente (z. B. Ventilanzahl), so ist der „worst-case“-Bereich zu betrachten, also der mit den meisten oder kritischsten Komponenten.

Um den hohen Anforderungen und der notwendigen Planungssicherheit gerecht zu werden, ist die Entwicklung und kontinuierliche Anpassung einer für die Nachweisführung verbindlichen Prüfspezifikation unerlässlich. Diese muss alle, zur Implementierung der BBA in das ganzheitliche Tunnelsicherheitskonzept erforderlichen Prüfaktivitäten beinhalten und von der zuständigen Abnahmebehörde geprüft und bestätigt werden.

Der gesamte Entwicklungsprozess, spätestens angefangen in der Lebenszyklusphase 3, muss gutachterlich (unabhängig und sachkundig) begleitet werden (siehe hierzu z.B. DIN EN 61508-1, Kap. 8).

4. Randbedingungen zur Validierung

Einen wichtigen Gesichtspunkt zur Festlegung der quantitativen Anforderungen an eine Sicherheitsfunktion gemäß DIN EN 61508 stellt die Anforderungsrate der Sicherheitsfunktion dar. Es wird zwischen folgenden Arten unterschieden:

- **niedrige Anforderungsrate**
  wenn die Häufigkeit von Anforderungen der Sicherheitsfunktion nicht größer als einmal je Jahr ist;
- **hohe Anforderungsrate**
  wenn die Häufigkeit von Anforderungen der Sicherheitsfunktion größer als einmal je Jahr ist;
- **kontinuierliche Anforderung**
  wenn die Anforderung an die Sicherheitsfunktion kontinuierlich vorhanden ist.

Ausgehend aus dem zu erwartenden Einsatzprofil der BBA (bezogen auf die Funktion der Brandbekämpfung und der hierzu erforderlichen Systemansteuerung) unter Berücksichtigung der statistisch ermittelten Tunnelbrandfälle, wird die Anforderungsrate als **niedrig** eingestuft.

Die Komponenten der Brandmeldeanlage (BMA) als wesentlichem Teilsystem der BBA müssen grundsätzlich den Anforderungen der Normen DIN EN 54 Teile 1 bis 25; DIN VDE 0833 Teile 1, 2 und 4 sowie der DIN 14675 zum Aufbau und Betrieb von BMA entsprechen.

Für die sicherheitsbezogenen Systeme der Brandbekämpfungstechnik wie Informationsverarbeitung, Bereitstellung von Löschmedium unter Beachtung des notwendigen Systemdrucks sowie Ansteuerung von Bereichsventilen liegen bisher vergleichsweise wenig Erfahrungswerte vor.

Generell werden zur Steigerung der Zuverlässigkeit und Verfügbarkeit der BBA folgende Maßnahmen als zielführend erachtet:

- Unabhängige Prüfung von Planungs-, Projektierungs-, Test- und Wartungs-/ Instandhaltungsunterlagen, Komponenten (einschließlich Software), sowie Vor-Ort-Prüfung der Installation
- Einfehlersichere, fehleroffenbarende Anbindung der Peripherieelemente
- Einfehlersichere, fehleroffenbarende Vernetzung der unterschiedlichen Auswerte- und Steuereinheiten sowie abgesetzten Bedieneinheiten
- Möglichst weitreichende Selbstüberwachung aller Komponenten des Systems zwecks schneller Fehleroffenbarung
- Redundanzen in Sensorik, Verarbeitung und Aktorik (z. B. Doppelrechner in bestimmten Baugruppen)
- Vom Standard-Wirkpfad unabhängiger Not-Wirkpfad für den Fall nicht diagnostizierter Fehler
- Regelmäßige Funktionsprüfung der an der Sicherheitsfunktion beteiligten Komponenten (insbesondere solcher ohne oder mit nur geringem Diagnosedeckungsgrad)
- Regelmäßige fachgerechte Instandhaltungsmaßnahmen
- Präventiver Austausch bestimmter Komponenten

5. Zusammenfassung

Wird eine BBA als integraler Bestandteil eines ganzheitlichen Tunnelsicherheitssystem eingesetzt, so muss die gesamte Anlagentechnik als ein sicherheitsbezogenes System betrachtet werden. Darin eingeschlossen sind sowohl Komponenten der Hardware und Software wie auch ggf. existierende menschliche Faktoren, die zur Ausführung von einer oder mehreren Sicherheitsfunktionen erforderlich sind. Ein möglicher Ausfall der Sicherheitsfunktion führt zu einer signifikanten Zunahme des Sicherheitsrisikos für Personen und damit zur Nichterfüllung der definierten Schutzziele (vgl. Kap. 2.2 im Hauptdokument).

Folglich ist die „Funktionale Sicherheit“ einer BBA grundsätzlich dann gegeben, wenn jede spezifizierte Sicherheitsfunktion der Anlage ausgeführt und die für jede Sicherheitsfunktion geforderte Verfügbarkeit nachweislich erreicht wird.

Basierend auf Gefährdungs- und Risikoanalysen müssen hierzu tolerierbare Grenzwerte für die Nichtverfügbarkeit von sicherheitsbezogenen Funktionen einer BBA definiert werden (z. B. ausgedrückt in Form des PFD_{tol} gemäß DIN EN 61508).

Im Bezug auf die Spezifikation, Entwicklung und Implementierung von Softwareapplikationen (z. B. für die Leit- und Steuerungstechnik einer BBA) müssen insbesondere systematische Fehler der sicherheitsbezogenen Funktionen hinreichend ausgeschlossen werden. Um dies zu erreichen, werden in DIN EN 61508 dem Sicherheitsziel (ausgedrückt durch den SIL) entsprechende Methoden gefordert.

Hardwarekomponenten können zudem zufällig ausfallen (z. B. infolge von Alterung), was zu einer Nichtverfügbarkeit einer BBA im Anforderungsfall führt. Diese Ausfälle können durch Ausfallraten und andere statistische Werte numerisch beschrieben und somit berechnet werden.

Die Beurteilung der Funktionalen Sicherheit erfolgt im Rahmen einer entwicklungsbegleitenden Begutachtung, an deren Ende die Bewertung des vom Hersteller der BBA erstellten Sicherheitsnachweises steht. Alle Tätigkeiten müssen von Personen durchgeführt werden, die für die auszuführende Tätigkeiten nachweislich kompetent sind. Der Gutachter muss den gemäß DIN EN 61508 geforderten Unabhängigkeitsgrad besitzen.