Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Schutz kritischer Brücken und Tunnel

Schlussbericht

Zuwendungsempfänger:	**Bundesamt für Bevölkerungsschutz und Katastrophenhilfe** **Provinzialstraße 93** **53127 Bonn**
Förderkennzeichen:	**13N9637A**
Vorhabensbezeichnung:	**Operatives Krisenmanagement und Risikoanalyse Tunnelleitzentralen**
Projektleitung:	**Dr. Monika John-Koch**
Laufzeit:	**01.01.2012 – 31.12.2014, Verlängerung bis 31.03.2015**

Bundesministerium
für Bildung
und Forschung

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) im Rahmen des Programms „Forschung für die zivile Sicherheit“ gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Schlussbericht zu Nr. 3.2 (BNBest-BMBF98)

Bonn, 01.07.2015

Inhaltsverzeichnis

I. KURZDARSTELLUNG 4

I.1 Aufgabenstellung 4

I.1.1 Gesamtziel des Vorhabens 4

I.1.2 Ziel des Teilvorhabens „Operatives Krisenmanagement und Risikoanalyse Tunnelleitzentralen“ 4

I.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde 5

I.3 Planung und Ablauf des Vorhabens 5

I.3.1 Planung und Ablauf des AP3 „Operatives Krisenmanagement“ 6

I.3.2 Planung und Ablauf des AP4 „Risikoanalyse Tunnelleitzentralen“ 7

I.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde 7

I.5 Zusammenarbeit mit anderen Stellen 10

II. EINGEHENDE DARSTELLUNG 12

II.1 Darstellung erzielter Ergebnisse 12

II.1.1 Operatives Krisenmanagement 12

II.1.1.1 Strukturen des Notfall- und Krisenmanagements anderer Verkehrsträger 12

II.1.1.2 Workshop „Krisenmanagement bei Großschadenslagen in Straßentunneln“ 13

II.1.1.3 Ableitung der Maßnahmen (AP 5: Neue Maßnahmen) 16

II.1.1.4 Leitfaden Krisenmanagement (AP 7: Anwendungshilfen) 18

II.1.2 Risikoanalyse für Tunnelleitzentralen 19

II.1.2.1 Methodisches Vorgehen 19

II.1.2.2 Vorbereitung 21

II.1.2.3 Kritikalitätsanalyse / Feststellung des Schutzbedarfs 23

II.1.2.4 Gefahrenanalyse und Szenarienentwicklung 23

II.1.2.5 IT-Grundschutzanalyse 25

II.1.2.6 Detaillierte Risikoanalyse 25

II.1.2.7 Vorbeugende Maßnahmen und Strategien 28

II.2 Die Notwendigkeit und Angemessenheit der geleisteten Arbeit 33

II.3 Wichtigste Positionen des zahlenmäßigen Nachweises 33

II.4 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse im Sinne des fortgeschriebenen Verwertungsplans 33

II.5 Bekannt gewordene Entwicklungen in der Projektlaufzeit (Fortschritte anderer Stellen auf dem Gebiet des Vorhabens) 34

II.6 Erfolgte und geplante Veröffentlichungen der Ergebnisse 34

Abbildungen

Abbildung 1: Übersicht der Arbeitspakete 5

Abbildung 2: Vorgehensweise der Risikoanalyse 21

I. Kurzdarstellung

I.1 Aufgabenstellung

I.1.1 Gesamtziel des Vorhabens

Brücken und Tunnel sind exponierte und verwundbare Schlüsselelemente des Straßennetzes, da der Ausfall dieser Bauwerke meist erhebliche Verkehrsauswirkungen hat. Die Gründe für die Ausfälle können schwere Unfälle, z.B. in Verbindung mit dem Transport von Gefahrgütern, extreme Naturereignisse oder terroristische Angriffe sein.

Ziel des Projekts SKRIBT^{PLUS} war es, aufbauend auf den Innovationen und Erkenntnissen des Vorgängerprojekts SKRIBT, mit der (Weiter-) Entwicklung praxistauglicher Methoden und neuer Technologien den Einsatz innovativer Sicherheitssysteme für Brücken- und Tunnelbauwerke weiter voranzutreiben und die Sicherheit der Bauwerke und die der Nutzer zu erhöhen. Wie im Vorgängerprojekt lag auch SKRIBT^{PLus} ein ganzheitlicher Ansatz zugrunde, der den Belangen der Bauwerkseigentümer und –betreiber, der Nutzer und der Betriebs- und Einsatzdienste Rechnung trägt.

I.1.2 Ziel des Teilvorhabens „Operatives Krisenmanagement und Risikoanalyse Tunnelleitzentralen“

Das Teilvorhaben *„Operatives Krisenmanagement“* knüpfte an die Arbeiten des Vorgängerprojekts SKRIBT an, die sich mit den organisatorischen Aspekten zur Bewältigung von Schadensereignissen in Straßentunneln befassten. Entsprechende Empfehlungen für organisatorische Maßnahmen wurden unter dem Titel „Ereignismanagement für Straßentunnel – Empfehlungen für Betriebs- und Einsatzdienste“ in der BBK-Reihe „Praxis im Bevölkerungsschutz“ als Band 9 veröffentlicht. Sie umfassen vorbereitende Maßnahmen, wie z.B. Schulung der Einsatzdienste, Übungskonzepte und –szenarien, Struktur und Aufbau der Gefahrenabwehrpläne, sicherheitstechnische Einrichtungen zur Selbst- und Fremdrettung, Verhaltensanweisungen für Tunnelnutzer sowie Maßnahmen zur Einsatzunterstützung und Einsatznachbereitung.

Ziel des Teilvorhabens „Operatives Krisenmanagement“ war es zu prüfen, inwieweit die Alarm- und Gefahrenabwehrplanung für Straßentunnel in ihren Ereignisbewältigungskonzepten auch Extremereignisse in Straßentunneln einbeziehen und ob es zu den bestehenden Planungen auch weiterer zusätzlicher Maßnahmen bedarf.

Im Teilvorhaben *„Risikoanalyse Tunnelleitzentralen“* war es das Ziel, eine methodische Vorgehensweise zur Durchführung einer Risikoanalyse für Tunnelleitzentralen (TLZ) zu erarbeiten. Denn der Ausfall einer Tunnelleitzentrale hat erhebliche Konsequenzen für den Betrieb der überwachten Tunnel. Zwar führt dieser Ausfall – sei es durch Fehlfunktionen der technischen Komponenten, physische Einflüsse, wie z.B. Naturereignisse, oder durch vorsätzliche Handlungen etwa in Form von Hackerangriffen auf die Überwachungssoftware –, je nach Ausmaß, nicht zwingend zu einer Sperrung der überwachten Tunnel. Dennoch hat eine möglichst kurzfristige Wiederherstellung der Funktionsfähigkeit der TLZ allein aus betrieblicher bzw. Ressourcensicht hohe Priorität, da die Tunnel bei Ausfall der TLZ vor Ort mit Personal besetzt werden müssen. Im Rahmen einer Risikoanalyse sollten die Betreiber mögliche Gefährdungen, die zu einem Betriebsausfall führen können, analysieren, Verwundbarkeiten interner und externer Prozesse gegenüber bestimmten Gefahren abschätzen und darauf aufbauend Maßnahmen für ein im Vorfeld definiertes Schutzniveau ausarbeiten.

I.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Entsprechend dem ganzheitlichen Ansatz des Projektes wurde das Projektkonsortium, bestehend aus Industriepartnern, Bundesbehörden, einem Fraunhofer Institut und Hochschulen, interdisziplinär zusammengesetzt, die gemäß ihrer jeweiligen Expertise unterschiedliche Aspekte bearbeitet haben. Folgende Institutionen waren am Projekt beteiligt:

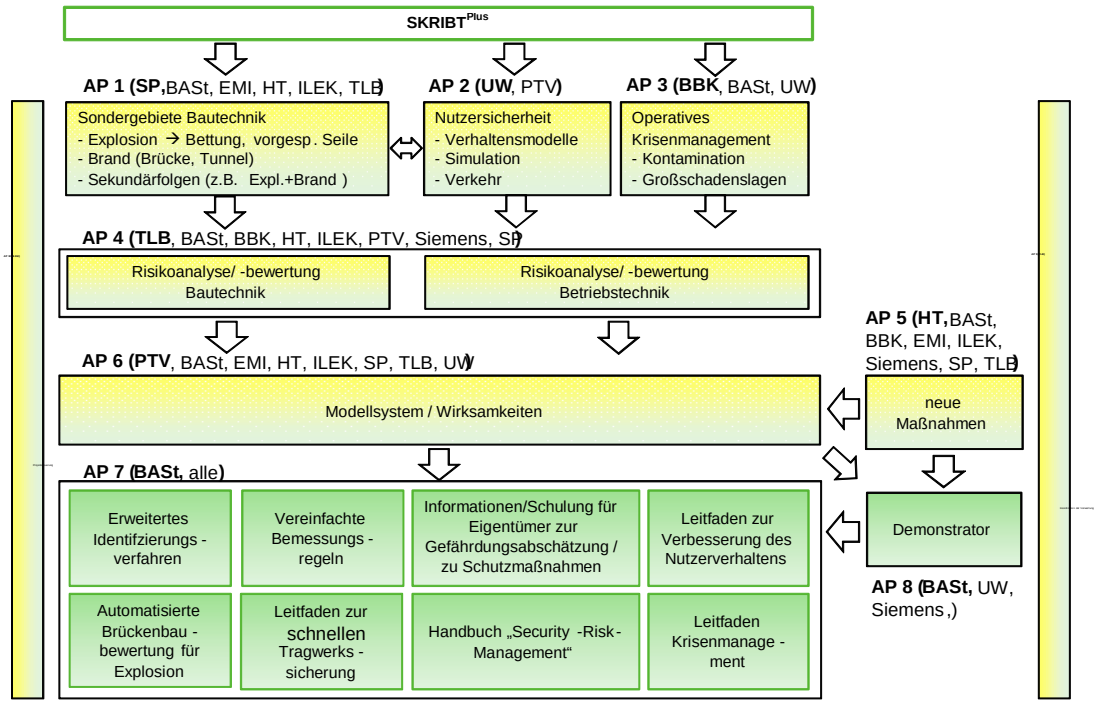
- Bundesanstalt für Straßenwesen (BASt), Abteilung für Brücken und Ingenieurbau
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Referat II.3 – Strategie KRITIS, Cyber-Sicherheit KRITIS
- Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut (EMI)
- HOCHTIEF PPP Solutions GmbH
- PTV Planung Transport Verkehr AG
- Ruhr-Universität-Bochum, Lehrstuhl für Tunnelbau, Leitungsbau und Baubetrieb (TLB)
- Schüßler-Plan Ingenieurgesellschaft mbH
- Siemens AG
- Universität Stuttgart, Institut für Leichtbau Entwerfen und Konstruieren (ILEK)
- Julius-Maximilians-Universität Würzburg, Lehrstuhl für Psychologie I

Das Projekt wurde durch die Bundesanstalt für Straßenwesen koordiniert.

I.3 Planung und Ablauf des Vorhabens

Das Projekt war in 10 Arbeitspakete gegliedert, die jeweils von einem Verbundpartner geleitet wurden. Die Projektstruktur und die jeweiligen Inhalte der Arbeitspakete sind der folgenden Abbildung zu entnehmen.

Abbildung 1: Übersicht der Arbeitspakete



Vom BBK wurde das Arbeitspaket 3 und im Arbeitspaket 4 der Themenbereich „Risikoanalyse Tunnelleitzentrale“ federführend bearbeitet. Die Ergebnisse aus diesen Arbeitspaketen wurden in Form von Empfehlungen im Arbeitspaket 5 „Neue Maßnahmen“ zusammengeführt und im Arbeitspaket 7 „Anwendungshilfen“ für die Publikation aufbereitet.

Die Projektlaufzeit betrug drei Jahre vom 01.01.2012 bis zum 31.12.2014 und wurde für den Zuwendungsempfänger BBK um weitere drei Monate bis zum 31.03.2015 kostenneutral verlängert. Für die Bearbeitung des Teilvorhabens wurde eine Mitarbeiterin mit einer Vollzeitstelle für die gesamte Projektlaufzeit beschäftigt, die administrativ-organisatorische Abwicklung sowie die Projektkoordination wurde durch fest angestelltes Personal wahrgenommen.

I.3.1 Planung und Ablauf des AP3 „Operatives Krisenmanagement“

Das Arbeitspaket wurde unter Federführung des BBK von den Verbundpartnern BASt und Universität Würzburg bearbeitet.

Im Zuge der Bearbeitung des Arbeitspakets wurden Literaturrecherchen über die Notfallkonzepte anderer Verkehrsträger (ÖPNV-Verkehrsbetriebe, DB AG, Flughäfen) durchgeführt, mit dem Ziel, bewährte Praktiken oder Instrumente bei der Krisenbewältigung zu identifizieren und eine Übertragbarkeit auf den Verkehrsträger „Straße“ zu prüfen.

Mit Blick auf die konkrete Lagebewältigung bei Extremereignissen in Straßentunneln wurde in Zusammenarbeit mit der BASt ein eintägiger Szenarien-Workshop unter Beteiligung der Einsatzdienste aus den Ländern Nordrhein-Westfalen sowie Thüringen durchgeführt. Ziel dieses Workshops war es, anhand von zwei Extremszenarien die Abläufe bei der Bewältigung einer Großschadenslage nachzuzeichnen und im Ergebnis die spezifischen Anforderungen an die Gefahrenabwehr bzw. an alle im Ereignisfall beteiligten Einsatzdienste zu formulieren.

Zudem wurden Forschungsprojekte im nationalen sowie internationalen Rahmen, die neue Technologien zur Einsatzunterstützung insbesondere bei Großschadenslagen entwickeln (z.B. Schutzkleidung, Kommunikation, Navigation), hinsichtlich ihrer Relevanz bei Einsätzen in Tunneln ausgewertet.

Als Ergebnis des Arbeitspakets wurden Empfehlungen abgeleitet, die in die Fortschreibung der Broschüre „Ereignismanagement für Straßentunnel“ eingegangen sind.

Die für die Einsatzdienste relevanten psychologischen Aspekte im Zusammenhang mit der Bewältigung von Großschadenslagen wurden vom Konsortialpartner Lehrstuhl für Psychologie I der Universität Würzburg näher untersucht. Hierzu wurde der aktuelle Status Quo bei psychologischen Aspekten des operativen Krisenmanagement in der Literatur gesichtet, aufbereitet und in Bezug zu den Interviewergebnissen mit den Einsatzdiensten aus dem Vorgängerprojekt SKRIBT gesetzt. Im Ergebnis wurden aus psychologischer Sicht Mindeststandards im Umgang mit Stress und potenziell belastenden Ereignissen erarbeitet.

Gemäß dem Projektzeitplan war für die Bearbeitung dieses Arbeitspakets ein Jahr vorgesehen. Da die Bearbeitung des Arbeitspakets später als geplant begann, ergab sich eine zeitliche Verschiebung bei dessen Bearbeitung, die allerdings aufgefangen werden konnte und keine Auswirkungen auf die weitere Bearbeitung der Thematik im Rahmen der nachfolgenden Arbeitspakete 5 und 7 hatte.

I.3.2 Planung und Ablauf des AP4 „Risikoanalyse Tunnelleitzentralen“

Im Arbeitspaket 4 sollte das System „Tunnelleitzentrale“ einer risikoanalytischen Betrachtung unterzogen werden. Im Rahmen dieser Risikoanalyse galt es, die kritischen Prozesse und die kritischen Elemente in den TLZ zu identifizieren, die für die Funktion und die Verlässlichkeit des Betriebs erforderlich bzw. unabdingbar sind, sowie das Risiko für die Tunnelleitzentralen zu bewerten.

Bei der Bearbeitung des Arbeitspakets gab es einen intensiven fachlichen Austausch insbesondere mit dem Konsortialpartner Siemens aber auch mit der BASt.

Im Zuge der Bearbeitung von AP 4 hat sich herausgestellt, dass entgegen dem Projektantrag die *Durchführung* einer Risikoanalyse einschließlich der Bewertung der bestehenden Maßnahmen sowie der Entwicklung weiterer Schutzmaßnahmen aus zeitlichen Gründen nicht realistisch war. Die Erarbeitung der Methode hat, bedingt durch einen längeren Ausfall der Projektmitarbeiterin, mehr Zeit in Anspruch genommen, als ursprünglich geplant. Zudem hätte eine ausführliche Risikoermittlung und Risikobewertung und die Betrachtung konkreter Maßnahmen anhand eines Referenzobjektes und damit standortbezogen durchgeführt werden müssen mit der Konsequenz, dass sich die Ergebnisse nicht ohne weiteres auf andere Objekte übertragen lassen. Der Schwerpunkt der Bearbeitung lag daher in der Ausarbeitung einer methodischen Vorgehensweise zur Durchführung einer Risikoanalyse.

Entgegen der ursprünglichen Zeitplanung wurde der Bericht zur Risikoanalyse erst zum Ende der Projektlaufzeit fertiggestellt. Der Entwurf wurde im Februar 2015 Tunnelbetreibern in vier Bundesländern zur fachlichen Kommentierung zugesandt. Nach der Überarbeitung des Entwurfs wird die Methode zur Risikoanalyse als eigenständige Publikation in der BBK-Reihe „Praxis im Bevölkerungsschutz“, erscheinen.

I.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Thema „Operatives Krisenmanagement“

Die Bearbeitung dieser speziellen Thematik beruhte ganz wesentlich auf Experteninformationen. Dazu wurde ein Workshop durchgeführt sowie erforderliche Informationen bei den einzelnen Verkehrsträgern eingeholt.

Die für die Darstellung der Notfallkonzepte Verkehrsträger ÖPNV, DB AG sowie Flughäfen verwendete Literatur ist im Folgenden aufgelistet (Auswahl).

[1] Allgemeines Eisenbahngesetz vom 27. Dezember 1993 (BGBl. I S. 2378, 2396; 1994 I S. 2439), zuletzt geändert durch Artikel 7 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2542)

[2] Allgemeinverfügung der Eisenbahnuntersuchungsstelle des Bundes (EUB). Stand 01.01.2010 http://www.eba.bund.de/SharedDocs/Publikationen/EUB/DE/sonstige_Downloads/60_allgvfg_Unfallmeldung.pdf?__blob=publicationFile&v=1 (abgerufen am 18.10.2013)

[3] Arnold, Burkhard: Krisenmanagementplanung der Deutschen Bahn AG. In: Nationales Krisenmanagement im Bevölkerungsschutz. Hrsg.: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (= Reihe Praxis im Bevölkerungsschutz, Band 11). Bonn, Oktober 2008

[4] Betriebsanweisung für Notfälle (BA NOT). Hrsg.: Fraport AG Frankfurt Airport Services Worldwide, Traffic and Terminal Management 60547 Frankfurt am Main. Stand: Mai 2004 (unveröffentlicht / interne Planungsunterlage)

[5] Deutsche Bahn AG: Hilfeleistungseinsätze im Gleisbereich der DB AG. Stand März 2012

[6] Gertler, Ralph: Modell zur Organisation des Störungs-, Notfall- und Krisenmanagements innerhalb der Leipziger Verkehrsbetriebe. Vortrag im Rahmen der Fachtagung Sicherheits-, Notfall- und Störungsmanagement am 29.11/30.11.2012 in Hamburg. Veranstalter: breidenbach + frost GbR

[7] Kruse, K: Brand- und Katastrophenschutz in Eisenbahntunneln. Deutsche Bahn AG Notfallmanagement, Brandschutz. August 2003

[8] Luftverkehrsgesetz in der Fassung der Bekanntmachung vom 10. Mai 2007 (BGBl. I S. 698), zuletzt geändert durch das Gesetz vom 5. August 2010 (BGBl. I S. 1126)

[9] Luftverkehrs-Zulassungs-Ordnung in der Fassung der Bekanntmachung vom 10. Juli 2008 (BGBl. I S. 1229), zuletzt geändert durch Artikel 2 der Verordnung vom 18. Januar 2010 (BGBl. I S. 11)

[10] Puls, Jens: Risikobehaftete Infrastrukturen des öffentlichen Personenverkehrs aus Sicht der Deutschen Bahn AG. Vortrag im Rahmen des Symposiums „Risikobehaftete Infrastruktur öffentlicher Personenverkehr“ am 05. April 2006 in Wiesbaden. Veranstalter: Bundesverband Deutscher Wach- und Sicherheitsunternehmen

[11] Pundschuss, Tobias: Notfall- und Krisenmanagement am Flughafen Hannover. Vortrag im Rahmen einer Veranstaltung „Risikomanagement – Aktueller Stand 2010“ am 07.09.2010. Veranstalter: Medizinische Hochschule Hannover.
http://www.mh-hanno-ver.de/fileadmin/organisation/ressort_krankenversorgung/downloads/risikomanagement/RMAktuellerStand/2010/7-Pundschuss-SicherheitFlughafenHannover-2010.pdf
(abgerufen am 18.10.2013)

[12] Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung (Richtlinie über die Eisenbahnsicherheit)

[13] Till, Günter: Sicherheits- und Störungsmanagement bei moBiel. Vortrag im Rahmen der Fachtagung Sicherheits-, Notfall- und Störungsmanagement am 29.11/30.11.2012 in Hamburg. Veranstalter: breidenbach + frost GbR

[14] VDV-Sicherheitsleitfaden für ÖPNV-Unternehmen – Safety und Security. VDV Mitteilungen, Nr. 7018. Ausgabe Mai 2008

[15] Vereinbarung zwischen den Innenministern/-senatoren für Inneres der Länder und der Deutschen Bahn AG vom 7. August 1998, zur Zusammenarbeit im Rahmen der Gefahrenabwehr

[16] Verordnung über die Untersuchung gefährlicher Ereignisse im Eisenbahnbetrieb (Eisenbahn-Unfalluntersuchungsverordnung - EUV) vom 5. Juli 2007

[17] Vogt, Konrad: Das Notfallmanagement der Deutschen Bahn AG. In: Notfallvorsorge. Zeitschrift für Bevölkerungsschutz und Katastrophenhilfe. Heft 4, 2007

Thema „Risikoanalyse Tunnelleitzentralen“

Bei der Ausarbeitung der Methodik zur Durchführung einer Risikoanalyse für Tunnelleitzentralen wurden internationale und nationale Standards sowie branchenbezogene Leitfäden herangezogen. Da die Betriebsabläufe in der TLZ maßgeblich durch die Informationstechnologie unterstützt werden baut das zweistufige methodische Konzept in einem *ersten Schritt* auf dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf. Der IT-Grundschutz konkretisiert die allgemein gehaltenen Anforderungen der internationalen ISO-Standards 27001 und 27002 und hat sich als ganzheitliches Konzept für Informationssicherheit

als Standard etabliert. Die Durchführung einer detaillierten Risikoanalyse in einem *zweiten Schritt* orientierte sich sowohl am Leitfaden zum Risiko- und Krisenmanagement für Unternehmen und Behörden des Bundesministeriums des Innern (BMI) als auch an der Methode für die Risikoanalyse im Bevölkerungsschutz des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Die folgende Liste beinhaltet die verwendete Fachliteratur.

[18] Bierfert, Andreas: DIN EN 50518 – die „Leitstellen"-Norm. Auswirkungen auf die deutschen Feuerwehren. In: BRANDSchutz, Heft 5, 2013

[19] Bundesamt für Bevölkerungsschutz (Hrsg.): Katastrophen und Notlagen Schweiz. Risikobericht 2012. Bern, Februar 2013

[20] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Methode für die Risikoanalyse im Bevölkerungsschutz (= Reihe Wissenschaftsforum, Band 8). Bonn 2010

[21] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. Bonn 2008

[22] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS). Bonn 2008

[23] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. Bonn 2008

[24] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 Notfallmanagement. Bonn 2008

[25] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3 Risikoanalyse auf Basis von IT-Grundschutz. Bonn 2008

[26] Bundesamt für Sicherheit in der Informationstechnik: Gefährdungskatalog G 0 "Elementare Gefährdungen". 2011

[27] Bundesamt für Sicherheit in der Informationstechnik: Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. Bonn 2010 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?__blob=publicationFile (07.08.2014)

[28] Bundesamt für Sicherheit in der Informationstechnik: Leitfaden Informationssicherheit. 2012 https://www.bsi.bund.de/DE/Publikationen/publikationen_node.html (01.08.2014)

[29] Bundesamt für Sicherheit in der Informationstechnik: Register aktueller Cyber-Gefährdungen und Angriffsformen. In: BSI-Analysen zur Cybersicherheit. Version 1.00 vom 16.01.2012

[30] Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen. Berlin 2005

[31] Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. Berlin, 2011

[32] DIN EN 50518-1 (VDE 0830-5-6-1):2010-12, Alarmempfangsstelle – Teil 1: Örtliche und bauliche Anforderungen

[33] DIN EN 50518-2 (VDE 0830-5-6-2):2011-04, Alarmempfangsstelle – Teil 2: Technische Anforderungen

[34] DIN EN 50518-3 (VDE 0830-5-6-3):2011-09, Alarmempfangsstelle – Teil 3: Abläufe und Anforderungen an den Betrieb

[35] ISO/IEC 27001 Information technology – Security techniques – Information security management systems requirements specification, 2005

[36] ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management, 2005

[37] ISO/IEC 27005 Information technology – Security techniques – Information security risk management. 2011

[38] Krings, Susanne: Verwundbarkeit Kritischer Infrastruktur gegenüber Hochwasserereignissen. In: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Indikatoren zur Abschätzung von Vulnerabilität und Bewältigungspotenzialen am Beispiel von wasserbezogenen Naturgefahren in urbanen Räumen. (= Schriftenreihe Forschung im Bevölkerungsschutz, Band 13). Bonn 2011

[39] Lenz, Susanne: Vulnerabilität Kritischer Infrastrukturen. (= Schriftenreihe Forschung im Bevökerungsschutz, Band 4). Bonn 2009

[40] Richtlinien für die Ausstattung und den Betrieb von Straßentunneln - RABT, FGSV-Nr. 339, Forschungsgesellschaft für Straßenwesen. Köln 2006

[41] VdS 3137:2013-09 (2), Zertifizierung von Alarmempfangsstellen gemäß DIN EN 50518

I.5 Zusammenarbeit mit anderen Stellen

Die projektinterne Zusammenarbeit war gekennzeichnet durch einen intensiven Informationsaustausch mit regelmäßigen Treffen des Projektkonsortiums sowie Arbeitstreffen im Rahmen der Bearbeitung der einzelnen Arbeitspakete.

Die Kooperation mit Dritten im Rahmen eines Workshops war Voraussetzung für die Bearbeitung des Arbeitspakets 3. Folgende Institutionen, in ihrer Funktion als Tunnelbetreiber, Sicherheitsbeauftragte für Tunnel, Feuerwehren und Polizei, haben am Workshop teilgenommen:

- Autobahnpolizeiinspektion Thüringen
- Freistaat Thüringen
  Landesamt für Bau und Verkehr, Zella-Mehlis
- KREBS UND KIEFER
  Beratende Ingenieure für das Bauwesen GmbH
- Landesbetrieb Straßenbau NRW
- Polizeipräsidium Köln, Direktion Verkehr
- VIA Beratende Ingenieure, Berlin
- Stadt Köln
  Berufsfeuerwehr, Amt für Feuerschutz, Rettungsdienst und Bevölkerungsschutz
- Stadt Bonn
  Feuerwehr und Rettungsdienst
- Stadtverwaltung Suhl
  Amt für Brand- und Katastrophenschutz
- SW Ingenieurbüro Brandschutz GmbH, Ichtershausen

Bezüglich der Empfehlungen zur Aus- und Fortbildung der Feuerwehren bei Einsätzen in Tunneln fand ein intensiver Austausch mit dem Leiter des Didaktik- und Entwicklungsteams der International Fire Academy (Schweiz) und Mitglied des Arbeitskreises Tunnel der baden-württembergischen Feuerwehren statt.

Im Zuge der Recherchen und der erforderlichen inhaltlichen Abstimmungen zum Thema Risikoanalyse für Tunnelleitzentralen wurde mit folgenden Institutionen zusammengearbeitet:

- Autobahndirektion Südbayern, München
- Bundesamt für Sicherheit in der Informationstechnik
- Landesbetrieb Straßen, Brücken und Gewässer, Freie und Hansestadt Hamburg
- Landesbetrieb Straßenbau NRW
- Freistaat Thüringen
  Landesamt für Bau und Verkehr, Zella-Mehlis

II. Eingehende Darstellung

II.1 Darstellung erzielter Ergebnisse

II.1.1 Operatives Krisenmanagement

II.1.1.1 Strukturen des Notfall- und Krisenmanagements anderer Verkehrsträger

Die Untersuchung der Notfallkonzepte anderer Verkehrsträger orientierte sich an folgenden Fragestellungen:

- Welche Eskalationsstufen hinsichtlich der Reaktion / Ereignisbewältigung gibt es?
- Welche Szenarien / Ereignisse werden betrachtet?
- Von welchen worst-case-Szenarien wird ausgegangen?
- Wie sieht die interne Notfall- und Krisenorganisation aus?
- Welche Vorbereitungen organisatorischer Art werden für Großschadenslagen bzw. Krisenszenarien getroffen?

Die Recherchen bezogen sich auf Betriebe des ÖPNV, auf Flughäfen sowie auf die DB AG.

Die Untersuchungen haben gezeigt, dass bei den betrachteten Verkehrsträgern je nach Ereignisklassifikation (Störung, Notfall, Krise) entsprechende Notfallkonzepte existieren und im Großschadens- bzw. Krisenfall unternehmensinterne Sonderstrukturen in Form von Krisenstäben greifen, die im Aufbau an die kommunalen Verwaltungs- bzw. Krisenstäbe angepasst sind. Gleichwohl sind derartige Strukturen für den Krisenfall – wie sich aus einigen Gesprächen mit Vertretern von Verkehrsbetrieben ergab –, keineswegs Standard, was insbesondere auch an der mangelnden Sensibilisierung der Verantwortlichen in Bezug auf Extremereignisse läge.

Die Aufgabe der unternehmensinternen Krisenstäbe besteht u.a. darin, eine Lagebewertung vorzunehmen und diese fortzuschreiben, alle erforderlichen Maßnahmen zur internen Gefahrenabwehr einzuleiten und zu koordinieren, die Einsatzleitung und die Einsatzdienste vor Ort zu unterstützen, mit externen Beteiligten zu kommunizieren sowie die Öffentlichkeitsarbeit und Krisenkommunikation wahrzunehmen. Kennzeichnend für die Krisenorganisation der betrachteten Verkehrsträger ist, dass im Krisenfall eigene Mitarbeiter vor Ort (z.B. Notfallmanager der DB AG, lokale Teams bei Verkehrsbetrieben oder die Technischen Einsatzleitung beim Flughafen bestehend aus dem Technischen Einsatzleiter und Fachführern der Einsatzgruppen) zur Bewältigung der Krise und Unterstützung des Einsatzleiters / der Einsatzdienste zur Verfügung stehen. Ihre Aufgabe ist es, die vor Ort eingesetzten eigenen Mitarbeiter zu führen sowie die Einsatzleitung und den eigenen Krisenstab zu informieren.

Die Abläufe im Krisenfall (Erreichbarkeiten, Alarmierungs- und Meldewege) sowie die Aufbauorganisation mit den jeweiligen Verantwortlichkeiten und Zuständigkeiten sind in sogenannten „Krisenhandbüchern“, beim Flughafen Frankfurt z.B. in internen Betriebsanweisungen für Notfälle (BA NOT) dokumentiert. Wesentlicher Bestandteil der Vorbereitung auf Krisenfälle sind Schulungen der Mitarbeiter sowie Krisenstabsübungen auch gemeinsam mit den kommunalen Krisenstäben.

Im Rahmen des operativen Krisenmanagements bedarf es neben einer funktionierenden Krisenorganisation auch entsprechender Hilfsmittel. Besonders interessant und ggf. auch als Vorbereitung auf (Groß-) Schadensereignisse in Straßentunneln übertragbar wäre das in der BA NOT festgelegte Vorgehen mit vordefinierten Notfallverfahren, die standardisierte - also wiederkehrende - Maßnahmen mit den jeweiligen Zuständigkeiten, Aufgaben und Führungsfunktionen beschreiben, und das es erlaubt, dem Anwender zielgruppenspezifisch und dienststellenbezogen

einen Alarmplan für das jeweilige Ereignis zu erstellen. Auch die Entwicklung von Checklisten für Krisenszenarien, wie bei den Leipziger Verkehrsbetrieben, ist ein probates Mittel, um im Ereignisfall einen reibungslosen Kommunikationsablauf zwischen allen beteiligten Einsatzdiensten zu gewährleisten.

Eine wesentliche Bedeutung in der Krisenbewältigung wird der Presse- und Öffentlichkeitsarbeit bzw. der Krisenkommunikation beigemessen. Damit keine sich widersprechende Informationen in die Öffentlichkeit gelangen, müssen die Vorgehensweisen abgestimmt und die Zuständigkeiten festgelegt sein.

In der Alarm- und Gefahrenabwehrplanung für Straßentunnel sind betreiberinterne Krisenmanagementstrukturen im Fall von Großschadensereignissen vergleichbar den beschriebenen Verkehrsträgern nicht vorhanden. Im Ereignisfall wird die Einsatzleitung vor Ort durch die zuständige Tunnelleitzentrale mit Lageinformationen, Steuerung der Betriebstechnik und Informationsvermittlung zu weiteren Diensten unterstützt.

II.1.1.2 Workshop „Krisenmanagement bei Großschadenslagen in Straßentunneln“

Für die erweiterte Fragestellung des operativen Krisenmanagements bei der Bewältigung von Großschadenslagen in Straßentunneln im Rahmen von SKRIBT^{PLus} war es ebenso wichtig, Experten hinzuzuziehen und basierend auf deren Praxiserfahrungen mögliche Defizite im Ablauf der Rettungskette zu identifizieren bzw. Maßnahmenvorschläge zur deren Optimierung zu erarbeiten. Im Februar 2013 wurde ein eintägiger Expertenworkshop durchgeführt, zu dem Vertreter der Feuerwehr, der Polizei, der Tunnelleitzentralen, der Tunnelbetreiber sowie Sicherheitsbeauftragte für Straßentunnel aus Nordrhein-Westfalen und Thüringen eingeladen waren. Der Teilnehmerkreis wurde zunächst auf zwei Bundesländer begrenzt, um die inhaltliche Diskussion stärker auf die Thematik und weniger auf die länderspezifische Verfahren zu fokussieren.

Ziel des Workshops

Ziel des Workshops war es, anhand zweier Szenarien die Abläufe bei der Bewältigung einer Großschadenslage in einem Tunnel nachzuzeichnen und im Ergebnis die spezifischen Anforderungen an die Gefahrenabwehr bzw. an alle im Ereignisfall involvierten Einsatzdienste zu formulieren. Es sollte diskutiert werden, welche Abläufe bei den Einsatzkräften vor Ort, den Krisenstäben sowie den Behörden zur Bewältigung einer derartigen Großschadenslage nötig und sinnvoll sind und welche Maßnahmen zur Vorbereitung auf ein solches Ereignis im Vorfeld getroffen werden sollten. Die Diskussion im Workshop diente dazu zu überprüfen, ob die bereits bestehenden Konzepte in der Alarm- und Gefahrenabwehrplanung für Tunnelbauwerke auch Extremereignisse abdecken.

Szenarien

Grundlage der Diskussion waren zwei Extremereignisse „Großexplosion/Brand“ und „Freisetzung von Chlorgas“ mit einem Massenanfall von Verletzten (MANV) und im Fall des Szenarios Explosion/Brand einer erheblichen Zerstörung der im Tunnel verfügbaren Sicherheits- und Betriebstechnik. Ziel war es, komplexe Szenarien zu vorzustellen, deren Bewältigung deutlich an die Grenzen der verfügbaren Bewältigungskapazitäten und vorhandenen Strukturen gehen. Dabei war es für die Diskussion zunächst unerheblich, ob das Ereignis auf menschliches Versagen oder einen gezielten Anschlag zurückzuführen ist.

Die vorgestellten Szenarien wurden anhand der folgenden Leitfragen diskutiert.

- Was ist nach dem Ereigniseintritt zu tun und welche Maßnahmen werden eingeleitet?
- Wer muss alarmiert und benachrichtigt werden?
- Auf welcher Ebene werden Krisenstäbe einberufen?
- Was passiert bei einer Großschadenslage in den Krisenstäben, Behörden sowie bei den Einsatzkräften vor Ort?
- Wie geht man bei unklaren Ereignissen vor? (terroristischer Anschlag)
- Welche personellen und materiellen Ressourcen werden benötigt?
- Wie wird reagiert, wenn im Fall eines Kontaminationsereignisses nicht eindeutig ist, welcher Stoff ausgetreten ist?

Ergebnisse

Eine Bewertung der Einsatzgrenzen bei der Bewältigung der vorgestelllten Szenarien durch die Teilnehmer läßt sich wie folgt zusammenfassen:

- Bei derartigen Ereignissen sind beim Eintreffen der Einsatzkräfte nur noch wenige Menschen zu retten. Im Ereignisfall tragen die Tunnelnutzer eine hohe Eigenverantwortung. Falsches Verhalten der Nutzer kann durch die Betriebs- und Einsatzdienste nicht kompensiert werden.
- Die Bewältigung solcher Großschadensereignisse im Tunnel wird nicht allein durch das Einsatzkräfteaufgebot bestimmt. Aus der Sicht der Feuerwehr gäbe es zwischen der RABT[1]-konformen Ausstattung des Tunnels und der Ausstattung der Feuerwehr eine Lücke. Die vorgestellten Szenarien sind grenzwertig (der Aufwand für Standard-Szenarien ist bereits sehr hoch) und nicht deckungsgleich mit den Möglichkeiten der Feuerwehr, so
  - reichen Chemikalienschutzanzüge nur für die Einsatzdauer von 20 Minuten,
  - sind die Einsatzzeiten für Atemschutzträger begrenzt und erlauben eine Eindringtiefe von max. 80 m bis 100 m,
  - ist im Tunnel ist nur Löschwasser verfügbar, Schaumrohre sind selten.

Somit bestimmen sowohl die persönliche Schutzausrüstung der Feuerwehrkräfte als auch die Tunnelausstattung (z.B. zu großer Abstand der Notausgänge) die Einsatzgrenzen der Rettungskräfte.

Bei der Besprechung der Szenarien wurden verschiedene Aspekte aufgezeigt, die für die Lagebewältigung von Bedeutung sind. Dies betrifft insbesondere

- die Kommunikation der Einsatzdienste untereinander gerade in der Anfangsphase bei der Erstellung eines gemeinsamen Lagebilds. Vorgeschlagen wurde, entsprechende Checklisten für Abfragen des Lagebildes zu erstellen, an denen sich die Leitstellen orientieren sollen;
- die Verbesserung Lageinformation durch Übertragung der Videobilder aus der TLZ auch zu den Leitstellen der Feuerwehr und Polizei;
- die Möglichkeit der Direktkommunikation zwischen TLZ und Feuerwehr über digitalen Funk;

[1] Abkürzung für: Richtlinien für die Ausstattung und den Betrieb von Straßentunneln

- die Erarbeitung von Vorgaben für Tunnelbelüftung bei Gefahrgutunfällen, da im Ereignisfall schnelles Handeln gefragt ist. Derartige Konzepte gibt es bisher nicht. Es sollten entsprechende Handlungsanweisungen für den Kontaminationsfall für die Operatoren erstellt werden.

In der abschließenden Diskussion, in der die Teilnehmer nach ihren Wünschen / Vorstellungen zur besseren Vorbereitung auf (Groß-) Schadenslagen gefragt worden sind, wurde darüber hinaus folgender Handlungsbedarf aufgezeigt:

- Automatische Anrufweiterleitung von Notrufen 112 und 110 mittels Mobiltelefon an die Tunnelleitzentrale (ermöglicht eine genaue Ortung des Ereignisorts).
- Höhere Standardisierung und Vereinheitlichung der Abläufe und Verfahren zwischen den Einsatzdiensten (Standards für Sicherheitsübungen, Standards für Alarm- und Gefahrenabwehrpläne, Verfahrensweisen im Ereignisfall vor Ort, z.B. Bedienung der Feuerwehrbedienfelder).
- Realitätsnahe Schulung der Operatoren am Tunnelsimulator.
- Definition / Konkretisierung der Aufgaben des Tunnelüberwachungspersonals (z.B. in den RABT).
- Erarbeitung von Schulungsmodulen für Operatoren mit Blick auf den Informationsaustausch zwischen den Einsatzdiensten oder auch Verhaltensanweisungen für Operatoren im Fall einer Bombendrohung.
- Einrichtung von zentralen Ausbildungsstätten für die Feuerwehr mit Spezialausbildung für Tunneleinsätze.
- Mehr Forschung zum Thema „Tunnelbrand“.
- Novellierung der FwDV-Vorschriften (Stichwort Atemschutz, Chemikalienschutzanzüge).
- Berücksichtigung der Einsatzbedingungen vor Ort, insbesondere ausreichende Aufstell- und Bewegungsflächen, Notzufahrten für die Rettungskräfte sowie leicht zu öffnende Mittelstreifenüberfahrten zum Wechseln in die andere Röhre.
- Mehr Unterstützung der Kommunen bei der Sicherstellung der Gefahrenabwehr durch entsprechende Ausstattung (z.B. Atemschutz, Tunnellöschfahrzeuge).
- Stärkere Sensibilisierung der Tunnelnutzer durch Information / Aufklärung. Dabei wurde die ehemals sehr erfolgreiche Sendung „Der 7. Sinn“ als eine Möglichkeit zur Aufklärung über das richtige Verhalten in Tunneln genannt.

Einige der aufgezeigten Handlungsfelder (z.B. Schulungskonzepte für Operatoren, Spezialausbildung der Feuerwehren bei Tunneleinsätzen, Einsatzbedingungen vor Ort) wurden bereits im Rahmen von SKRIBT behandelt und in der Broschüre „Ereignismanagemnt für Straßentunnel – Empfehlungen für Betriebs- und Einsatzdienste“ berücksichtigt.

Fazit

Die Szenariendiskussion hat gezeigt, dass der Fremdrettung bei derartigen Extremereignissen objektive Grenzen – sei es die Ausrüstung der Feuerwehr oder die bauwerksspezifischen Gegebenheiten des Tunnels – gesetzt sind. Im Rahmen der Vorbereitung auf Ereignisse im Tunnel wird der Aus- und Fortbildung der Feuerwehren und der Operatoren sowie der Nutzerschulung und -information große Bedeutung beigemessen. Darüber hinaus sind entsprechende Vorkehrungen / Konzepte vor Ort für einen Massenanfall von Verletzten zu treffen.

Auch wenn das Szenario „Gefahrgutunfall“ in den derzeitigen Alarm- und Gefahrenabwehrplänen berücksichtigt ist, zeigte die Diskussion, dass im Fall des Austritts von Gefahrstoffen, wie in dem vorgestellten Szenario der Stoff Chlor, keine Konzepte zur Tunnellüftung existieren. Im Ereignisfall würde die Feuerwehr vor Ort entscheiden, wie die Lüftung zu steuern ist. Da dies unter Stress geschieht und ggf. auch Auswirkungen auf das Umfeld haben kann, wurde empfohlen, im Vorfeld entsprechende Belüftungskonzepte zu erstellen.

Im Ergebnis lässt sich auch feststellen, dass Kommunikation und Information der Einsatzdienste untereinander eine der tragenden Säulen im Zuge der Ereignisbewältigung ist. Dies betrifft sowohl die Informationsinhalte zum Lagebild als auch die Informationswege, wie z.B. Kommunikation über Digitalfunk oder die Übertragung des Lagebildes über Video auch an Feuerwehr und Polizei.

Im Ereignisfall unterstützt die TLZ die Einsatzleitung vor Ort mit Lageinformationen sowie auf Anweisung der Einsatzleitung durch Steuerung der Betriebstechnik und Information der Tunnelnutzer. Eine Präsenz des Betreibers vor Ort als Fachberater wurde auch aus pragmatischen Gründen (Entfernungen zum Tunnel) nicht als notwendig erachtet.

Im Bericht zu Arbeitspaket 3 sind die Ergebnisse der Bearbeitung ausführlich dokumentiert.

II.1.1.3 Ableitung der Maßnahmen (AP 5: Neue Maßnahmen)

Im Arbeitspaket 5 wurden über die in SKRIBT entwickelten Maßnahmen hinaus, weitere neue bauliche, betriebliche und organisatorische Maßnahmen erarbeitet und untersucht.

Das BBK hat basierend auf den Ergebnissen des Arbeitspakets 3 für den organisatorischen Bereich die im Folgenden beschriebenen Maßnahmenempfehlungen formuliert.

Erarbeitung von Tunnelbelüftungskonzepten bei Freisetzung von giftigen Gasen

Unfälle mit Beteiligung von Gefahrgut zählen zu den Gefahrenlagen, für die im Rahmen der Alarm- und Gefahrenabwehrplanung für Tunnel entsprechende Vorbereitungen zu treffen sind. Allerdings sind nicht alle Tunnel für Gefahrguttransporte freigegeben. Je nach Tunnelkategorie kann der Transport bestimmter Gefahrgüter eingeschränkt oder Gefahrguttransporte gänzlich verboten sein. Die Zuweisung zu einer Tunnelkategorie, die sich auf risikoanalytische Verfahren stützt, erfolgt durch die zuständige Verwaltungsbehörde.

Kommt es zu einem Unfall und Austritt von Gefahrstoffen, so ist es entscheidend, die Art und die Eigenschaften des Stoffes möglichst schnell zu identifizieren und geeignete Einsatzmaßnahmen einzuleiten. Die Feuerwehr-Dienstvorschrift 500 „Einheiten im ABC-Einsatz“ regelt die taktischen Vorgehensweisen im Umgang mit Gefahren durch radioaktive, biologische und chemische Stoffe.

Es gehört zum Standard der sicherheitstechnischen Ausstattung im Tunnel, dass ein Brand im Tunnel automatisch detektiert wird. Gasdetektionsanlagen hingegen, die beispielsweise bei chemischen Anlagen standardmäßig eingesetzt werden, sind in Straßentunneln unüblich und werden auch in den RABT nicht gefordert. Im Rahmen des Vorgängerprojekts SKRIBT wurde empfohlen, solche Anlagen, deren Investitions- sowie die laufenden Unterhalts- und Wartungskosten gering sind, je nach Risikobewertung des Tunnels und abgestimmt auf das für den Tunnel zugelassene Gefahrgut einzusetzen. Bei einer schnellen Detektion kann ggf. verhindert werden, dass die ausgetretenen Gase sich entzünden oder explodieren. Eine solche Anlage bietet auch die Möglichkeit, Lüftungsszenarien bei Gasaustritt speziell für die jeweilige Situation zu regeln.

Für den Brandfall in einem Tunnel sind spezielle Lüftungsprogramme vorgesehen, die entweder automatisch durch die Brandmeldeeinrichtung oder durch das Tunnelüberwachungspersonal

ausgelöst werden. Entsprechende standardisierte Konzepte bzw. Programme zur Steuerung der Tunnellüftung bei Freisetzung von giftigen Gasen gibt es nicht. So kann bei brennbaren Gasen und Flüssigkeiten, die explosionsfähige Gas-Luft-Gemische bilden können, die richtige Maßnahme darin bestehen, die Lüftung abzuschalten.

Die Alarm- und Gefahrenabwehrpläne sollten Handlungsoptionen für Gasaustritts-Szenarien aufzeigen, die neben der Lüftungssteuerung für jedes Tunnelportal auch Pläne zur Sperrung und Sicherung des betroffenen Umfelds sowie zur Warnung der Bevölkerung beinhaltet. Die Operatoren sollten Handlungsanweisungen erhalten, wie die Lüftungssteuerung bei entsprechenden Ereignissen betrieben werden soll. Die Szenarien sollten auch Gegenstand regelmäßiger Übungen sein.

Kommunikation zwischen den Einsatzdiensten im Ereignisfall

Lagebild – Kommunikation der Leitstellen untereinander

Im Ereignisfall können die Meldungen auf unterschiedlichen Wegen (Notrufstation, Mobiltelefon, Stör- und Alarmmeldungen der Tunnelbetriebstechnik) in verschiedene Leitstellen, so der Tunnelleitzentrale oder den Leitstellen der Feuerwehr bzw. der Polizei, eingehen. Die Leitstellen sind verpflichtet, sich gegenseitig zu informieren, die Informations- und Alarmierungswege sind in den Alarm- und Gefahrenabwehrplänen festgelegt und können je nach Ereignisart (z.B. Unfall oder Brand) unterschiedlich sein. Insbesondere bei langen Anfahrtswegen sollte mit den zuständigen Feuerwehren im Hinblick auf Tunnelbrände abgestimmt werden, wie frühzeitig ihre Alarmierung erfolgen soll. Mögliche relevante Ereignisse können etwa die Entnahme eines Feuerlöschers aus seiner Halterung im Tunnel oder irgendeine Form von Rauchentwicklung sein.

Um die Lage bewerten zu können, sind der Informationsaustausch sowie eine enge Kooperation zwischen den Leitstellen besonders wichtig. Eines der Hauptprobleme ist, dass in den Leitstellen aufgrund der unterschiedlichen Informationsquellen verschiedene Lagedarstellungen existieren, die zu einem gemeinsamen Lagebild zusammengeführt werden müssen. Bei der Erstellung eines Lagebildes sind folgende Faktoren zu berücksichtigen: Welche Informationen werden benötigt und wie werden diese Informationen allen Beteiligten zur Verfügung gestellt (z.B. über Telefon, Einsatzleitsystem, gemeinsame Lagekarte).

Generell wird bei der Informationsweitergabe als wichtig erachtet, die Lageinformationen objektiv und unabhängig vom Schadensausmaß, möglichst sachlich und weitgehend emotionsfrei zu übermitteln. Des Weiteren ist zu berücksichtigen, dass insbesondere bei einer Großschadenslage neben grundlegenden einsatzrelevanten Informationen (Wo ist es passiert?, was ist passiert?, wie viele verletzte Personen?, welche Art von Verletzungen? etc.) im Zuge der Ereignisbewältigung von den Einsatzkräften weitere kleinteiligere Lageinformationen erwartet werden.

Es gilt demnach zu definieren, welche Informationen im Einzelnen die Feuerwehr, die Polizei und der Rettungsdienst benötigen, um daraus eine Checkliste bzw. einen Kriterienkatalog zu erstellen, an denen sich die Leitstellen und insbesondere die Operatoren in der Tunnelleitzentrale, bei Abfragen und Informationsweitergabe orientieren können. Diese Definition kann für einige ausgewählte (Extrem-) Szenarien (Brand, Explosion, Freisetzung von giftigen Gasen) erfolgen.

Für Brandereignisse in Straßentunneln sind z.B. folgende spezifische Informationen besonders wichtig:

- Betroffene Röhre
- Nicht betroffene Röhre (diese muss explizit festgestellt werden, weil diese Röhre dann als sicherer Raum zu betrachten ist, z.B. für die Einfahrt des Rettungsdienstes, der nicht über Atemschutz verfügt)
- Genauer Brandort
- Strömungsrichtung (ggf. in beiden bzw. allen Röhren, weil die Gefahr der Rauchumkehr aus der betroffenen in die nicht betroffene Röhre möglich ist)
- Stabilität der Strömungsrichtung: Ist eine Umkehr möglich oder sogar im Lüftungsregime vorgesehen oder aktuell beabsichtigt?
- Auf welcher Portalseite tritt Rauch aus?
- Personenlast (z.B. Reisebusse etc.)
- Gefahrgutfahrzeuge

Als Vorbereitung auf Schadensereignisse in Tunnelbauwerken wird empfohlen, eine Checkliste zu erstellen, die als Grundlage für eine unmissverständliche Kommunikation und Lagebewertung für die Einsatzdienste dienen soll. Dazu gehört insbesondere die Vereinbarung eindeutiger, einheitlich verwendeter Bezeichungen (beispielsweise "Röhre Süd" statt "linke Röhre"). Zur Sicherstellung, dass die Kommunikation im Ereignisfall auch funktioniert, sollten regelmäßig Kommunikationsübungen zwischen Leitstellen und Einsatzdiensten stattfinden.

Lagebild – Übertragung der Videobilder zur Feuerwehr / Polizei

Ein Aspekt, der im Zusammenhang mit der Lagebilderfassung in Tunneln diskutiert wird, ist die Übermittlung der Lagebilder aus dem Tunnel über Video zu den Leitstellen der Feuerwehr und Polizei. Noch ist es nicht die Regel, dass die Führungskräfte der eingesetzten Feuerwehren selbst direkten Zugang zu den Videoinformationen haben. Aus der Sicht der Einsatzkräfte wird jedoch die Bildinformation als hilfreicher angesehen als nur der telefonische Kontakt mit der Tunnelleitzentrale bzw. die verbale Lagebeschreibung. Da diesbezüglich keine datenschutzrechtlichen Hürden im Wege stehen, sollte geprüft werden, ob im Ereignisfall eine Livebildübertragung aus dem Tunnelraum zur Feuerwehr / Polizei realisierbar wäre. Wichtig für die Lagebewertung wären auch Videoaufzeichnungen, die die Situation im Tunnelraum in den letzten Minuten vor der Ereignismeldung wiedergeben, um z.B. die Anzahl der Fahrzeuge und der Personen in den inzwischen verrauchten Bereichen abschätzen zu können.

II.1.1.4 Leitfaden Krisenmanagement (AP 7: Anwendungshilfen)

Im Arbeitspaket 7 wurden die Ergebnisse der Untersuchungen aus den vorangegangenen Arbeitspaketen zielgruppenspezifisch, also für Bauwerkseigentümer, Betreiber, Nutzer sowie Betriebs- und Einsatzdienste, in Form von Bemessungsregeln, Schulungstools, Leitfäden etc. aufbereitet.

Entgegen der ursprünglichen Planung hat das BBK zum Thema „Organisation“ keinen separaten „Leitfaden Krisenmanagement“ erstellt. Vielmehr erwies es sich als sinnvoll, die neuen Maßnahmen und Empfehlungen in einer Fortschreibung der im Vorgängerprojekt SKRIBT erstellten Broschüre „Ereignismanagement für Straßentunnel – Empfehlungen für Betriebs- und Einsatzdienste“ zu integrieren.

Inhaltlich erweitert wurde die Broschüre um die im Arbeitspaket 5 beschriebenen Empfehlungen zur Kommunikation der Einsatzdienste im Ereignisfall sowie zum Thema Tunnelbelüftungskonzepte bei Freisetzung von giftigen Gasen.

Ein besonderes Augenmerk galt der Krisenkommunikation und insbesondere den sozialen Medien, die heutzutage eine nicht zu unterschätzende Rolle in der Krisenkommunikation und der Katastrophenhilfe einnehmen.

Darüber hinaus wurden auch die aktuellen Projektergebnisse der Universität Würzburg zu den Themen Psychosoziale Notfallversorgung der Einsatzdienste (Empfehlungen für Mindeststandards) und Verhaltensanweisungen für Tunnelnutzer in die Empfehlungen integriert und auf aktuelle Literatur sowie aktuelle Forschungsprojekte mit direktem Bezug auf das Ereignismanagement in Straßentunneln verwiesen.

Die inhaltlich erweiterte Fassung der Broschüre ist im Mai 2015 erschienen.

II.1.2 Risikoanalyse für Tunnelleitzentralen

Für die Aufrechterhaltung des Betriebs in Straßentunneln sind die Tunnelleitzentralen zuständig. Sie übernehmen die Überwachung, Steuerung und Sicherung des Verkehrs sowie die Steuerung der technischen Betriebseinrichtungen im Normal-, Störungs- und im Ereignisfall. Dabei ist gemäß den RABT bei Tunneln ab 400 m Länge eine 24-stündige Überwachung sicherzustellen [1]. Diese Aufgaben werden in einigen Bundesländern, wie z.B. in Bayern, von Verkehrs- und Betriebszentralen wahrgenommen, die neben der Tunnelüberwachung auch für die Verkehrsüberwachung und -steuerung auf Bundesautobahnen zuständig sind. Auch wenn der Tunnelbetrieb grundsätzlich automatisch gesteuert wird, ist die ständige Überwachung der Tunnel eine wesentliche Voraussetzung, um das Sicherheitsniveau für die Tunnelnutzer zu gewährleisten. Im Sinne der Aufrechterhaltung eines zuverlässigen Verkehrssystems „Straße“ können Straßentunnel und die zugehörigen Tunnelleitzentralen je nach ihrer Bedeutung Kritische Infrastrukturen darstellen.

Im Folgenden werden die einzelnen Schritte zur Durchführung einer Risikoanalyse für Tunnelleitzentralen kurz beschrieben. Im Bericht zu Arbeitspaket 4 ist methodische Vorgehensweise ausführlich dargestellt.

II.1.2.1 Methodisches Vorgehen

Es existiert eine Reihe von methodischen Ansätzen zur Durchführung einer Risikoanalyse, die sich auf quantitative oder qualitative Verfahren stützen. Quantitative Berechnungen setzen allerdings voraus, dass entsprechendes Datenmaterial zur Verfügung steht. In aller Regel fehlen aber die erforderlichen Daten und Statistiken, auf deren Basis Eintrittswahrscheinlichkeiten für Gefahren oder auch das zu erwartende Schadensausmaß berechnet werden können.

Unabhängig davon, ob ein quantitativer oder qualitativer Ansatz für die Risikobewertung gewählt wird, ist die Durchführung einer Risikoanalyse mit Arbeitsaufwand und folglich auch mit Kosten verbunden. Um diesen Aufwand zu begrenzen, bietet sich für die Durchführung einer Risikoanalyse für TLZ eine zweistufige Vorgehensweise an, die auf bewährten Methoden beruht:

1. Erstellung / Überprüfung des Sicherheitskonzepts auf Basis von IT-Grundschutz
2. Durchführung einer detaillierten Risikoanalyse

Die Betriebsabläufe bzw. die einzelnen Prozesse in der TLZ werden maßgeblich durch die Informationstechnologie unterstützt. Daher ist die Gewährleistung der Informationssicherheit, die

auf den Grundwerten Verfügbarkeit, Vertraulichkeit und Integrität beruht, ein ganz wesentlicher Bestandteil der Risikoanalyse und des darauf aufbauenden Sicherheitskonzepts für Tunnelleitzentralen. Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bietet eine praxiserprobte qualitative Methode zur Risikobewertung in der Informationssicherheit, welche in einem ***ersten Schritt*** zur Überprüfung des vorhandenen Schutzniveaus angewendet werden sollte. Die Methodik ist eingebunden in ein ganzheitliches Konzept eines Informationssicherheitsmanagements, das als Bestandteil eines allgemeinen Risikomanagements im BSI-Standard 100-1 „Managementsysteme für die Informationssicherheit (ISMS)“ [2] ausführlich erläutert wird.

Die Methode des IT-Grundschutzes basiert auf dem BSI-Standard 100-2 [3], der die Vorgehensweise zur Anwendung des IT-Grundschutzes beschreibt, und den IT-Grundschutzkatalogen. In den nach dem Baukastenprinzip aufgebauten Grundschutzkatalogen, bestehend aus Baustein-, Gefährdungs- und Maßnahmenkatalogen, werden für IT-Systeme, Anwendungen, Netze, *aber auch für die Bereiche der Infrastruktur, Organisation, Personal und Notfallvorsorge,* wie es im Basisschutzkonzept des Bundesministeriums des Inneren (BMI) 2005 veröffentlicht wurde [4], Standardsicherheitsmaßnahmen empfohlen. Folglich deckt der IT-Grundschutz nicht nur Aspekte der Informationssicherheit ab, sondern bezieht auch andere Werte, wie z.B. Gebäude, technische Versorgungsinfrastruktur etc., mit ein. Dabei werden typische Gefährdungen betrachtet (z.B. Feuer, Überflutung, Computer-Viren etc.), die eine hohe Eintrittswahrscheinlichkeit haben oder erheblichen Schaden anrichten können, die Schutzmaßnahmen erfordern. Da es sich bei den Maßnahmen um einen Basisschutz handelt, der mögliche Verwundbarkeiten bzw. Schwachstellen sowie die Eintrittswahrscheinlichkeiten mit berücksichtigt, bedarf es bei der IT-Grundschutz-Vorgehensweise ohne weiteren Analyseaufwand zunächst nur eines Soll-Ist-Abgleichs zwischen den in den IT-Grundschutzkatalogen empfohlenen und den bereits realisierten Maßnahmen. Auf diese Weise soll eine Basis-Sicherheit gegenüber Standard-Gefährdungen erreicht werden.

Der IT-Grundschutz konkretisiert die allgemein gehaltenen Anforderungen der ISO-Standards 27001 [5] und 27002 [6] und hat sich als ganzheitliches Konzept für Informationssicherheit als Standard etabliert. Eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz erfolgt durch das BSI.

Die Durchführung einer detaillierten Risikoanalyse in einem ***zweiten Schritt*** erweist sich dann als sinnvoll, wenn es sehr kritische Bereiche / Systeme gibt, die im IT-Grundschutz nicht behandelt werden, d.h. zusätzliche Maßnahmen zu ergreifen sind. Dies gilt vor allem, wenn Szenarien herangezogen werden, die in ihrer Intensität über den ggf. realisierten Schutz gegenüber der betrachteten Gefahr deutlich hinausgehen. Dabei orientiert sich die Risikoanalyse-Methodik sowohl am Leitfaden zum Risiko- und Krisenmanagement für Unternehmen und Behörden des Bundesministeriums des Innern (BMI) [7] als auch an der Methode für die Risikoanalyse im Bevölkerungsschutz des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) [8].

Die Vorgehensweise der Risikoanalyse lässt sich anhand der folgenden Fragestellungen erläutern:

- *Vorbereitung:* Woran muss man denken, wenn man eine Risikoanalyse durchführen möchte?
- *Kritikalitätsanalyse / Schutzbedarfsfeststellung:* Welche Bereiche der Einrichtung sind für den Betriebsablauf besonders wichtig und folglich kritisch?
- Gefahrenanalyse und Szenarienentwicklung: Welche Gefahren drohen?
- *IT*-Grundschutzanalyse*:* Welche Schutzmaßnahmen gibt es bereits?

- *Detaillierte Risikoanalyse:* Reichen diese Maßnahmen gegenüber den betrachteten Szenarien aus?
  - Wie wahrscheinlich sind diese Szenarien?
  - Gibt es besonders verwundbare Bereiche?
  - Wie hoch ist der Schaden beim Ausfall bestimmter Prozesselemente?
  - Wie hoch ist das Risiko?

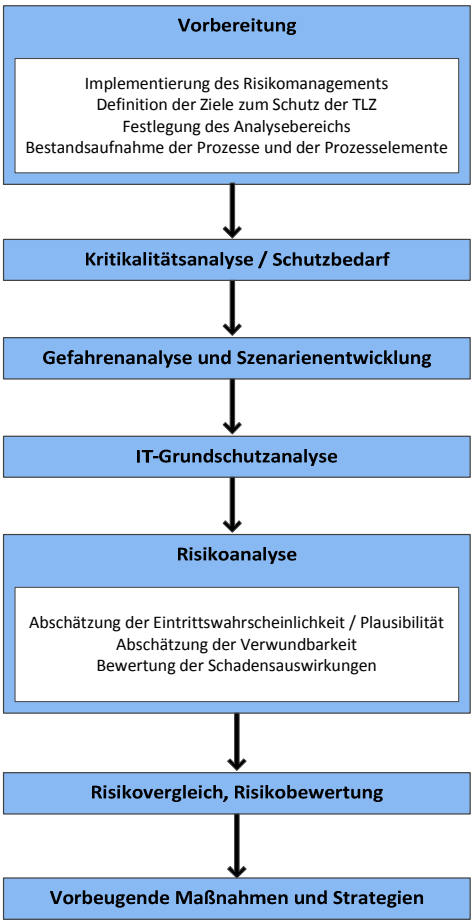


Abbildung 2: Vorgehensweise der Risikoanalyse

II.1.2.2 Vorbereitung

Implementierung des Risikomanagements

Die Durchführung einer Risikoanalyse muss gut vorbereitet sein, indem im Vorfeld grundsätzliche Fragen zur Etablierung eines Risikomanagements in der Einrichtung geklärt und die erforderlichen organisatorischen Voraussetzungen geschaffen werden. Hierzu zählen insbesondere die Implementierung des Projekts durch die Leitungsebene in die bestehenden Strukturen, die Festlegung der Zuständigkeiten im Rahmen der Umsetzung sowie die Bereitstellung notwendiger Ressourcen.

Die Durchführung einer Risikoanalyse in einer TLZ sollte durch die zuständige Verwaltungsbehörde für Straßentunnel, in der Regel durch die Straßenbauverwaltung der Länder, initiiert und getragen werden. Es liegt in der Verantwortung der zuständigen Verwaltungsbehörde, den

Untersuchungsbereich im Rahmen der Risikoanalyse festzulegen, die Ziele des Risikomanagements zu definieren sowie grundlegende Entscheidungen, welche Schutzmaßnahmen zu ergreifen sind, zu treffen. Darüber hinaus ist die Verwaltungsbehörde auch für die Bereitstellung der personellen sowie finanziellen Ressourcen zuständig. Es sollte eine Projektgruppe eingerichtet werden, die die Risikoanalyse durchführt und geeignete Maßnahmenvorschläge erarbeitet.

Alle Entscheidungen, Begründungen und Ergebnisse im Verlauf des Risikoanalyse-Prozesses sind sorgfältig zu dokumentieren, um die Nachvollziehbarkeit von Vorgängen und getroffenen Maßnahmen für alle Beteiligten zu gewährleisten.

Definition der Schutzziele und Festlegung des Analysebereichs

Im Vorfeld der Risikoanalyse sind zunächst die Ziele festzulegen, die das erwünschte Schutzniveau bzw. den Sollzustand für die Einrichtung bzw. für die zu schützenden Bereiche der Einrichtung beschreiben und an denen sich die Untersuchung orientieren kann. Anhand dieser Ziele lassen sich kritische Prozesse und die zugehörigen Elemente ermitteln sowie die identifizierten Risiken bewerten. Sie bilden somit die Entscheidungsgrundlage, ob zusätzliche Maßnahmen im Rahmen des Risikomanagements zu ergreifen sind.

Die ständige Tunnelüberwachung durch eine Tunnelleitzentrale ist ein wesentlicher Baustein des Sicherheitssystems für Straßentunnel. Zwar hat der Ausfall der TLZ nicht zwingend eine Sperrung der überwachten Tunnel mit den entsprechenden verkehrlichen Auswirkungen zur Folge, solange die Überwachung der Tunnel vor Ort gewährleistet ist. Dies wird jedoch umso kritischer, je mehr Tunnel von einer Stelle aus überwacht werden. Deshalb hat eine möglichst kurzfristige Wiederherstellung der Funktionsfähigkeit der TLZ allein aus betrieblicher bzw. Ressourcensicht hohe Priorität.

Daraus lässt sich als **übergeordnetes Ziel** ableiten, dass für die Gewährleistung des Sicherheitsniveaus im Tunnel – auch im Fall von extremen Ereignissen / Extremsituationen – die **Funktionsfähigkeit der TLZ** aufrechterhalten werden soll. Dieses Ziel zum Schutz der Einrichtung lässt sich weiter konkretisieren, z.B.

- Vermeidung eines Totalausfalls der TLZ (ggf. Definition der maximal tolerierbaren Ausfallzeit)
- Aufrechterhaltung der Funktionalität besonders kritischer Systeme (z.B. Steuerung, Kommunikation)
- Reduzierung der Wiederanlaufzeiten

Je nach Ausrichtung des Risikomanagements und der Risikoanalyse – All-Gefahrenansatz oder die Betrachtung nur bestimmter Gefahren? Gesamtbetrachtung der Einrichtung oder Begrenzung des Analysebereichs auf einzelne Ressourcen und Systeme? – können spezielle Ziele, z.B. Schutz der Einrichtung vor Angriffen (physischer Schutz), Schutz des Personals oder Sicherheit der Informations- und Kommunikationstechnik Grundlage für das Risikomanagement sein.

Strukturanalyse: Bestandsaufnahme der Prozesse und Prozesselemente

Als Ausgangspunkt der Risikoanalyse ist eine Übersicht der Prozesse und der jeweiligen Ressourcen (Elemente), die die diese Prozesse unterstützen bzw. ermöglichen, zu erstellen.

Prozesse lassen sich unterteilen in *Führungsprozesse*, *Kernprozesse* sowie *Unterstützungsprozesse*. *Führungsprozesse* enthalten die leitenden Aufgaben einer Einrichtung. *Kernprozesse* beschreiben die eigentlichen operativen Aufgaben der Organisation, in einer TLZ sind es die Tunnelüberwachung, Beseitigung von Störungen (einschließlich Betreuung der Wartungs- und Instandsetzungsarbeiten im Tunnel) und im Ereignisfall die Einleitung von Hilfsmaßnahmen sowie

die Unterstützung der Einsatzkräfte. *Unterstützungsprozesse* sichern die Arbeitsfähigkeit der Einrichtung, indem sie alle erforderlichen Ressourcen (Personal, Technik, Informationen) für die Führungs- und Kernprozesse bereitstellen sowie durch Umsetzung administrativer Aufgaben. Die Prozesse lassen sich in Teilprozesse oder Prozessschritte weiter unterteilen.

Jedem Prozess können Elemente zugeordnet werden, die diesen Prozess unterstützen. Dabei handelt es sich prinzipiell immer um die gleichen Elemente wie Personal, Gebäude und Gelände, Allgemeine und einrichtungsspezifische Anlagen, Daten und Unterlagen sowie Betriebsmittel (z.B. Ersatzteile, Dieselvorrat für Notstromaggregat). Gegenstand der weiteren Risikobetrachtung sind nicht die Prozesse selbst, sondern die den Prozess tragenden jeweiligen Elemente, deren Bedeutung für die Aufrechterhaltung von Prozessen im Rahmen einer Kritikalitätsanalyse / Schutzbedarfsfeststellung festzulegen ist.

Im Zuge der Bestandsaufnahme der Prozesselemente ist es sinnvoll und angebracht, diese nach zusammenhängenden Einheiten und ähnlichen Objekten zu gruppieren, und somit auch die Zahl der in der Risikoanalyse zu berücksichtigenden Elemente und der technischen Komponenten zu reduzieren. Dies gilt vor allem für die IT-Anwendungen und IT-Systeme, die an eine oder auch mehrere Hardwarekomponenten gebunden sein können und folglich im weiteren Verlauf der Risikoidentifikation als ein Objekt zu betrachten sind. In einer Gruppe können z.B. mehrere Clients oder auch Server, welche die gleichen Aufgaben wahrnehmen, zusammengefasst sein.

II.1.2.3 Kritikalitätsanalyse / Feststellung des Schutzbedarfs

Eine Kritikalitätsbetrachtung der Prozesse und der dazugehörigen Prozesselemente im Vorfeld der eigentlichen Risikoanalyse hat das Ziel, die kritischen und unverzichtbaren Bereiche zu identifizieren, deren Funktionieren für die Einrichtung von existenzieller Bedeutung ist. Durch eine Priorisierung der kritischen Elemente kann der Untersuchungsaufwand der Risikoanalyse begrenzt werden, indem nur die als kritisch angesehenen Bereiche einer Risikoidentifikation unterzogen und die aus der Risikobewertung abgeleiteten vorbeugenden Maßnahmen zur Risikominderung darauf konzentriert werden.

Für die Bestimmung der Kritikalität der Prozesselemente wird die IT-Grundschutz-Vorgehensweise herangezogen. In der Terminologie des IT-Grundschutzes wird in Analogie an den Begriff „Kritikalität“ der Begriff „Schutzbedarf“ verwendet, der durch das Ausmaß der entstandenen Schäden definiert wird. Im Rahmen der Schutzbedarfsfeststellung wird ermittelt, welchen Schutzbedarf die Prozesselemente in Bezug auf die Grundwerte *Verfügbarkeit, Vertraulichkeit und Integrität* besitzen. Die Wertigkeit des Schutzbedarfs wird qualitativ beschrieben und den Schutzkategorien zugeordnet, beispielsweise „normal“, „hoch“ und „sehr hoch“. Die Bewertungskriterien für die Bestimmung des Schutzbedarfs sind einrichtungsspezifisch festzulegen.

Die Schutzbedarfsfeststellung wird in einer bestimmten Reihenfolge vorgenommen; Zunächst wird der Schutzbedarf für Anwendungen (z.B. Software, Datenträger, schützenswerte Dokumente) bestimmt und anschließend der Schutzbedarf für IT-Systeme, Räume sowie die Kommunikationssysteme abgeleitet.

II.1.2.4 Gefahrenanalyse und Szenarienentwicklung

Im Rahmen der Gefahrenanalyse werden jene Gefahren identifiziert, die die Einrichtung in ihrer Funktionsfähigkeit beeinträchtigen oder gar zum Ausfall der gesamten Einrichtung führen können. Nach dem All-Gefahren-Ansatz werden sowohl Naturgefahren, Gefahren, die aus menschlichen oder technischen Versagen resultieren, als auch vorsätzliche Handlungen, wie z.B. Cyber-

kriminalität oder Terrorismus, betrachtet. Welche Gefahren am Standort bzw. für die Einrichtung relevant sein könnten, lässt sich u.a. mit Hilfe folgender Fragestellungen bestimmen:

- Wurde die Einrichtung in der Vergangenheit durch das Ereignis betroffen und könnte es sich wiederholen?
- Gibt es Ereignisbeispiele, die für die eigene Einrichtung herangezogen werden können?
- Welche natürlichen oder von Menschen gemachten Gefahren sind aufgrund der räumlichen Lage und Veränderungen der Rahmenbedingungen (z.B. klimatische Veränderungen, Entwicklungen in der IT-Technik, Entwicklung der sicherheitspolitischen Lage) möglich?

Die Basis für die Überprüfung des Sicherheitsniveaus der Einrichtung im Rahmen der IT-Grundschutzanalyse bilden die Gefährdungskataloge. Dennoch wird darauf hingewiesen, dass es zusätzliche relevante Gefährdungen im Bereich der Informationssicherheit für einzelne betrachtete Elemente geben kann, die im IT-Grundschutz nicht berücksichtigt sind. Es handelt sich dabei um Gefährdungen, die

- durch eine besondere Technologie, ein spezielles Produkt oder einen besonderen Anwendungsfall bedingt sind oder
- bei den üblichen Szenarien nur unter sehr speziellen Voraussetzungen zum Schaden führen können oder
- sehr gute Fachkenntnisse, Gelegenheiten und Mittel eines Angreifers voraussetzen [9].

Die im Rahmen der Gefahrenanalyse zu erstellende Gefahrenliste sollte generell nicht nur Ereignisse aufnehmen, die mit hoher Wahrscheinlichkeit eintreten können und bei denen die zu erwartenden Schäden relativ gering sind (z.B. kurzer Stromausfall durch Kabelbeschädigung bei Bauarbeiten). Vielmehr sind in der Gefahrenanalyse die Ereignisse zu betrachten, die zwar seltener auftreten, jedoch das Potenzial haben, aufgrund ihrer Intensität und / oder Dauer einen erheblichen Schaden bzw. auch einen längerfristigen Ausfall der Einrichtung herbeizuführen.

Nach der Zusammenstellung der für den Standort / die Einrichtung relevanten Gefahren sind realistisch anzunehmende Szenarien zu entwickeln, die die Gefährdung näher erläutern. Ein Szenario beschreibt ein Ereignis im Detail (Exposition, Intensität, Dauer, räumliche Ausdehnung, etc.) bzw. zeigt auf, welche Entwicklung ein bestimmtes Ereignis nehmen könnte und mit welchen Auswirkungen zu rechnen ist. Somit sind Szenarien auch ein Instrument, um sich auf Ereignisse in Form von entsprechenden Notfallplänen vorzubereiten. Um die Bandbreite möglicher Entwicklungen im Rahmen eines Szenarios aufzuzeigen, ist es sinnvoll, Eskalationsstufen zu bilden, d.h. das Szenario hinsichtlich der Intensität und den zu erwartenden Auswirkungen zu variieren (z.B. Stromausfall mehrere Stunden oder auch mehrere Tage).

Relevante Ereignisse, die zum Ausfall einer TLZ führen oder den Betriebsablauf erheblich beeinträchtigen können, sind z.B.:

- Stromausfall, z.B. durch extreme Wetterereignisse
- (Teil-) Ausfall des Standortes durch Naturereignisse oder Brand etc.
- Zusammenbruch der Informationstechnik oder der Kommunikationsinfrastruktur, z.B. durch Hackerangriffe
- Ausfall einer kritischer Anzahl der Mitarbeiter
- Räumung der TLZ, z.B. aufgrund einer Bombendrohung
- Terroristischer Anschlag

II.1.2.5 IT-Grundschutzanalyse

Nachdem die Informationen zur Kritikalität bzw. dem Schutzbedarf der betrachteten Prozesselemente vorliegen, gilt es zunächst zu prüfen, ob der realisierte Schutzniveau ausreichend ist, oder insbesondere für Objekte mit hohem oder sehr hohem Schutzbedarf zusätzliche Maßnahmen erforderlich sind. Die im IT-Grundschutz beschriebene Vorgehensweise gemäß BSI-Standard 100-2 geht dabei von einer pauschalisierten Gefährdungslage aus und bietet für die betrachteten Gefahren einen Maßnahmenkatalog für die Bereiche Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation sowie die Notfallvorsorge an.

Die Bearbeitung der IT-Grundschutzkataloge gliedert sich in folgende Schritte:

Schritt 1: *Abbildung des Informationsverbunds[2] durch die vorhandenen Bausteine*

Im ersten Schritt besteht die wesentliche Aufgabe darin, alle betrachteten Prozesselemente durch die in den IT-Grundschutzkatalogen aufgeführten Bausteine möglichst genau abzubilden. Falls bereits ein Grundschutz-Konzept existiert, kann in diesem Schritt auch geprüft werden, ob neue Bausteine (diese werden vom BSI kontinuierlich aktualisiert) relevant sein können.

Schritt 2: *Anpassung der Maßnahmen*

Im zweiten Schritt werden die empfohlenen Maßnahmen hinsichtlich ihrer Anwendbarkeit geprüft. Es kann der Fall sein, dass manche Maßnahmen unter den konkreten Rahmenbedingungen entbehrlich sind oder manche Gefährdungen bereits durch anderweitige Maßnahmen abgedeckt sind. Grundsätzlich sollten alle im Baustein empfohlenen Maßnahmen für den Grundschutz umgesetzt werden. Etwaige Änderungen sind zu dokumentieren.

Schritt 3: *Soll-Ist-Abgleich zwischen den vorhandenen und empfohlenen Maßnahmen*

In diesem Schritt wird der Umsetzungsstatus der empfohlenen Maßnahmen geprüft. Sinnvoll ist es, bereits beim Soll-Ist-Abgleich den Bedarf für ggf. zusätzliche Sicherheitsmaßnahmen herauszuarbeiten und zu dokumentieren.

II.1.2.6 Detaillierte Risikoanalyse

Bei der Durchführung einer detaillierten Risikoanalyse steht die Frage im Vordergrund, ob die schützenswerten Elemente durch die Standardsicherheitsmaßnahmen, so wie der IT-Grundschutz sie empfiehlt, in Anbetracht der (Extrem-) Szenarien und ggf. neuer Gefahren ausreichend geschützt sind oder nicht. Die potenziellen Risiken sollen unter Berücksichtigung der Eintrittswahrscheinlichkeiten, der Verwundbarkeiten sowie des Schadensausmaßes bewertet werden, um darauf aufbauend Maßnahmen gezielt einzusetzen. Das Vorgehen für eine detaillierte Risikoanalyse wird im Folgenden beschrieben.

Abschätzung der Eintrittswahrscheinlichkeit / Plausibilität

Die Eintrittswahrscheinlichkeit einer Gefahr kann quantitativ oder qualitativ bestimmt werden. Gleichwohl lassen sich statistisch exakt belegbare Eintrittswahrscheinlichkeiten nur für wenige Gefahren ermitteln. Sofern für die betrachtete Gefahr keine wissenschaftlichen / statistischen Erkenntnisse vorliegen, gilt es eine Abschätzung vorzunehmen, die sich auf begründeten Annahmen / Erfahrungswerten und Expertenmeinungen stützt. Eine Hilfestellung kann die Analyse

[2] *„Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen“ [3].*

der jeweiligen Rahmenbedingungen sein, z.B. Häufigkeit der Ereignisse aufgrund der Klimaänderung, Referenzereignisse oder die Betroffenheit der eigenen Einrichtung durch ein Szenario in der Vergangenheit.

Im Zusammenhang mit Terrorismus oder anderen kriminellen Handlungen sind Wahrscheinlichkeitsbetrachtungen mit Zuordnung von Häufigkeiten sehr schwierig, weil es für solche Ereignisse (mit Ausnahme der Regionen mit kriegerischen Auseinandersetzungen) nur wenige Erfahrungen gibt. So hat es z.B. in Deutschland noch keine erfolgreich durchgeführten, spektakulären terroristischen Anschläge auf Infrastruktureinrichtungen gegeben. Auch wenn derartige Ereignisse unvorhersehbar sind und sich somit einer Wahrscheinlichkeitsbetrachtung eigentlich entziehen, stellen sie eine latente Gefahr mit unabsehbaren Folgen dar. Um dennoch eine Risikoabschätzung vornehmen zu können, ist es daher sinnvoll, nicht die Eintrittswahrscheinlichkeit zu bestimmen, sondern sich auf Plausibilitätsüberlegungen zu stützen. Folgende Kriterien können u.a. hierfür herangezogen werden:

- Aktuelle sicherheitspolitische Lage[3]
- Bedeutung des betroffenen Ortes bzw. der Einrichtung (Motivation der Angreifer)
- Aufwand zur Durchführung des Anschlags:
  - Erforderliche Fähigkeiten und erforderliches Know-how
  - Verfügbarkeit und Handhabbarkeit des Anschlagsmaterials
  - Lage der Einrichtung und Zugänglichkeit

Im Bereich der Informationstechnik stellen Cyber-Angriffe eine ständige Gefahr dar, gegen die IT-Systeme entsprechend zu schützen sind. Der Begriff „Eintrittswahrscheinlichkeit“ bezogen auf derartige Cyber-Bedrohungen ist allerdings ein wenig irreführend, da solche Angriffe zum heutigen Alltag gehören.

Abgesehen von den alltäglichen, flächendeckenden Cyber-Angriffen stellt sich die Frage, ob eine Tunnelleitzentrale ein ausgesuchtes Objekt für einen gezielten Cyber-Angriff sein kann. Ein Motiv könnte sein, durch Manipulation der Software oder der IT-Systeme in der TLZ die Betriebstechnik in Tunneln zu stören oder gar außer Funktion zu setzen, so dass der Betrieb der überwachten Tunnel eingestellt werden muss. Dies würde beträchtliche verkehrliche Auswirkungen nach sich ziehen. Die Plausibilität eines solchen Szenarios sollte geprüft werden, wobei auch bei Cyber-Angriffen folgende Faktoren heranzuziehen sind:

- Mögliche Motive der Angreifer, sicherheitspolitische Lage
- (Zeit-) Aufwand, um den Angriff vorzubereiten
- Mögliche Schwachstellen im System: Ist die Schwachstelle leicht zu identifizieren? Ist Spezialwissen erforderlich oder reichen verfügbare Werkzeuge hierfür aus?
- Erforderliche Fähigkeiten und Know-how: Sind tiefgehende Kenntnisse für den Angriff erforderlich oder reichen wenige technische Kenntnisse aus?
- Angriffsentdeckung: Wie schnell kann der Angriff entdeckt und somit der potenzielle Schaden vermieden bzw. minimiert werden (kurzfristig, mittel- oder langfristig?)

[3] Für die Einschätzung der Bedrohungen durch politisch motivierte Anschläge können Informationen des Bundeskriminalamtes oder der jeweiligen Landeskriminalämter herangezogen werden.

Abschätzung der Verwundbarkeit

In der Verwundbarkeitsanalyse wird ermittelt, wie anfällig die Prozesselemente gegenüber einem bestimmten Szenario sind. Die Auswirkungen einer Gefahr auf die Prozessabläufe sind umso stärker, je höher die Verwundbarkeit der Prozesselemente ist. Betrachtet werden sollen diejenigen Elemente, die für die Aufrechterhaltung der Abläufe von besonderer Bedeutung sind, folglich einen hohen oder einen sehr hohen Schutzbedarf haben. Mit diesem Verfahren soll die Vulnerabilität der wesentlichen Komponenten überprüft und keine Gesamtvulnerabilität für die Einrichtung ermittelt werden.

Die Verwundbarkeit der Prozesselemente wird durch folgende Faktoren bestimmt:

- *Exposition:* Ist das betrachtete Element der Gefahr ausgesetzt?
- *Funktionsanfälligkeit:* Würde das Element beim betrachteten Szenario weiter funktionieren?
- *Ersetzbarkeit:* Inwiefern kann die Funktion / Leistung des Elements ersetzt werden?

Die Faktoren *Funktionsanfälligkeit* und *Ersetzbarkeit* beinhalten eine Reihe weiterer Kriterien (Robustheit, Pufferkapazität, Abhängigkeiten von anderen Infrastrukturen, Wiederherstellungsaufwand, etc.). Welche dieser Kriterien zur Abschätzung der Verwundbarkeit herangezogen werden, sollte einrichtungsspezifisch festgelegt werden.

Ergebnis der Verwundbarkeitsabschätzung ist eine Verwundbarkeitstabelle der betrachteten Prozesselemente. Elemente mit hohem oder sehr hohem Schutzbedarf und beispielsweise hoher Verwundbarkeit gegenüber dem Szenario geben Aufschluss über die mögliche Schwere der Auswirkungen auf die Prozesse und folglich auf das zu erwartende Schadensausmaß.

Bewertung der Schadensauswirkungen

Prinzipiell reicht eine Verwundbarkeitsabschätzung aus, um risikomindernde Maßnahmen ergreifen zu können. Will man jedoch – als Entscheidungsgrundlage für eine Maßnahmenpriorisierung – einen Risikovergleich der betrachteten Szenarien vornehmen, so ist zunächst das durch das jeweilige Szenario entstandene Risiko für die Einrichtung zu bestimmen.

Um Aussagen über das Risiko zu treffen, bieten sich zwei Möglichkeiten an:

1. Aus der Zusammenschau der im Rahmen der Verwundbarkeitsabschätzung ermittelten verwundbaren Elemente wird eine Gesamtverwundbarkeit für die Einrichtung bestimmt. Diese sollte durch Experten und Mitarbeiter, die mit den Prozessen der Einrichtung vertraut sind und die Konsequenzen des Ausfalls abschätzen können, vorgenommen werden. Aus den Parametern Eintrittswahrscheinlichkeit und Gesamtverwundbarkeit ergibt sich das Risiko durch das jeweilige Szenario. Dieses Verfahren bietet sich an, wenn Daten zur Quantifizierung von Schadensparametern nicht zur Verfügung stehen bzw. aufwendig zu ermitteln sind.
2. Ein gängiges Verfahren zur Ermittlung des Risikos besteht darin, das Schadensausmaß quantitativ zu bestimmen, etwa durch die entstandenen direkten Kosten für Sachwerte, Reparatur / Wiederherstellungsaufwand und den erhöhten Personalaufwand, wenn beim Ausfall der TLZ die überwachten Tunnel vor Ort mit Personal besetzt werden müssen. Führt der Ausfall einer TLZ zu einer mittel- oder längerfristigen Sperrung eines Tunnels, so könnten auch die indirekten volkswirtschaftlichen Kosten durch Umwegfahrten und die damit verbundenen Mehrreisezeiten bei der Bestimmung des Schadensausmaßes einbezogen werden.

Sicherlich können konkrete Daten Verantwortliche und Entscheidungsträger eher überzeugen. Ob der Aufwand, der mit der Datenbeschaffung verbunden ist, gerechtfertigt ist und ob eine auf

Basis von Verwundbarkeitsabschätzung vorgenommene Schadensermittlung nicht ebenso zum Ziel führen kann, ist abzuwägen.

Risikobewertung / Risikovergleich

Im letzten Schritt der Risikoanalyse werden auf Basis einer Klasseneinteilung die Werte für die abgeschätzten Eintrittswahrscheinlichkeiten, die Verwundbarkeit oder die Schadensausmaße für die betrachteten Szenarien in eine Risikomatrix übertragen. Diese Darstellung ermöglicht einen einfachen Vergleich der von den Szenarien ausgehenden Risiken. Insbesondere bei qualitativen und semiquantitativen Analysen ist der Vergleich der Risiken in Relation zueinander sinnvoll, da die qualitativ ermittelten Ergebnisse keine absolute Aussagekraft besitzen. Mit Hilfe der Risikomatrix können somit diejenigen Szenarien erkannt werden, die das größte Risiko für die Einrichtung darstellen. Auf welchen Prozesselementen das jeweilige Risiko beruht, kann der Vulnerabilitätsanalyse entnommen werden. Die in der Vulnerabilitätsanalyse vorgenommene Dokumentation der Schwachstellen bietet Ansatzpunkte für Maßnahmen zur Reduzierung der Anfälligkeit. Die Maßnahmen sollten vorrangig bei den Prozesselementen ansetzen, welche aufgrund ihrer hohen Kritikalität bzw. ihrer hohen Schutzbedarfe in dem betrachteten Szenario einem besonders hohen Risiko ausgesetzt sind. Letztlich ist es aber die Aufgabe der Leitung des Betreibers, Handlungsziele und Prioritäten in der Maßnahmenumsetzung festzulegen.

II.1.2.7 Vorbeugende Maßnahmen und Strategien

Wurde aus der Risikobewertung ein Handlungsbedarf abgeleitet, so sind vorbeugende Maßnahmen zu erarbeiten, die zur Risikoreduzierung beitragen sollen. Dies können technische, organisatorische oder personelle Maßnahmen sein. Bei der Auswahl der Maßnahmen soll dem Kosten-Nutzen-Aspekt Rechnung getragen werden, indem die potenziellen Investitionen sowie die durch das Ereignis entstandenen direkten und indirekten Kosten gegenübergestellt werden. Neben Kosten-Nutzen-Aspekten sollten auch die rechtlichen Rahmenbedingungen sowie soziale Überlegungen in die Entscheidung über Schutzmaßnahmen einfließen.

Grundsätzlich gibt es mehrere Strategien für den Umgang mit den erkannten Risiken:

- Risikovermeidung

  Risiken können vermieden werden, indem man beispielsweise bei der Standortwahl für Gebäude oder Anlagen gefährdete Bereiche ausschließt. Ebenso können hochrisikobehaftete Prozesse eingestellt und durch andere Prozesse ersetzt oder riskante Technik außer Betrieb genommen werden.

- Risikominimierung

  Die meisten vorbeugenden Maßnahmen zielen darauf ab, die Verwundbarkeit der Prozesselemente gegenüber der Gefahr und somit das Schadensausmaß zu reduzieren sowie kritische Prozesse durch Schaffung redundanter Systeme aufrechtzuerhalten.

- Risikotransfer

  Risikotransfer bedeutet die Übertragung des Risikos auf eine andere Institution. So können finanzielle Schäden durch den Abschluss einer Versicherung gesenkt werden, da diese ganz oder teilweise ersetzt werden. Auch das Outsourcing von Aufgabenbereichen an vertrauenswürdige Dienstleister, die wirtschaftlich oder technisch besser in der Lage sind, die entsprechenden Risiken zu tragen, ist eine Form des Risikotransfers.

- Risikoakzeptanz

  Da nicht alle Risiken durch vorbeugende Maßnahmen gemindert oder ausgeschaltet werden können, weil z.B. die Abdeckung dieser Risiken wirtschaftlich nicht mehr vertretbar wäre, werden die verbleibenden Restrisiken akzeptiert. Risikoakzeptanz bedeutet aber, dass im Fall von (extremen) Ereignissen organisatorische Vorkehrungen für die Bewältigung einer solchen Lage getroffen werden müssen.

Welche der genannten Strategien zur Risikobehandlung zum Tragen kommt, hängt von der Bewertung der jeweiligen Risiken ab und ist eine Entscheidung, die auf der Leitungsebene getroffen und verantwortet werden sollte. Ziel muss es sein, durch wirtschaftlich angemessene Maßnahmen die vorhandenen Risiken auf ein vertretbares Maß zu senken.

Für risikomindernde Maßnahmen ergeben sich prinzipiell folgende Handlungsoptionen:

- Physischer Schutz von Gebäuden, Räumlichkeiten und sonstigen Anlagen (bauliche und sicherheitstechnische Maßnahmen)
- Spezielle Sicherheitsmaßnahmen zum Schutz der IT-Infrastruktur
- Schaffung von Redundanzen / Ersatzverfahren
  - Dopplung wichtiger IT-Systemkomponenten wie beispielsweise Server, Netzwerk, Kommunikationsverbindungen nach außen etc.)
  - Daten- oder Informationsredundanz durch Speicherung der Daten auf externen Speichermedien sowie Vorhalten der wichtigen Informationen auch in Papierform
  - Alternative Kommunikationswege
  - Redundanz TLZ, etwa durch Besetzung der Betriebsgebäude am Tunnel vor Ort oder durch Übernahme der Steuerung durch eine andere TLZ, wie dies z.B. in NRW der Fall ist
- Standortplanung für die Technik
  - Verteilung der redundanten Systeme in mehreren Räumen
  - Auslagerung der Technik für Rückfallebenen (z.B. Einrichtungen einer USV bzw. Notstromversorgung) in andere Gebäude oder Gebäudeteile
- Notfallpläne
  - Einsatzpläne mit Festlegung der Meldewege, Zuständigkeiten und Verantwortlichkeiten für den Ereignisfall
  - Wiederanlaufpläne, um (IT)-Systeme und (IT)-Anwendungen möglichst schnell wieder in Betrieb nehmen zu können
  - Pläne zur Inbetriebnahme der Rückfallebenen (Besetzung der Betriebsgebäude am Tunnel vor Ort, Umschaltung der Steuerung auf eine andere TLZ)
  - Evakuierungspläne (z.B. im Fall einer Bombendrohung)
  - Pläne zur Aufrechterhaltung des Betriebs bei erheblichem Personalausfall

  Damit die festgelegten Notfallverfahren im Ereignisfall auch funktionieren, sind Schulungen der Mitarbeiter sowie entsprechende Übungen durchzuführen.

- Maßnahmen zur Sicherung der organisatorischen Abläufe im Zusammenhang mit IT, z.B.
  - Regelungen zu Datensicherung, Datenschutz, Datenverarbeitung, Rechtezuweisungen etc.
  - Schulung und Sensibilisierung der Mitarbeiter zur Informationssicherheit
  - Verhaltensanweisungen bei Sicherheitsvorfällen
- Kommunikationskonzept nach außen für den Fall, dass die TLZ ausfällt und sich in Folge dessen Störungen bzw. Verkehrsbehinderungen aufgrund eines eingeschränkten Tunnelbetriebs der überwachten Tunnel ergeben

Für die Auswahl der Maßnahmen insbesondere zur IT-Sicherheit können verschiedene Normen und IT-Grundschutz-Kataloge herangezogen werden:

- Die Norm DIN EN 50518 [10][11][12] definiert bauliche, technische und betriebliche Sicherheitsanforderungen zum Schutz der Alarmempfangsstellen.
- Die internationale Norm ISO 27002 [6] enthält insgesamt 135 generisch beschriebene technische und organisatorische Maßnahmen für die Gewährleistung der Informationssicherheit.
- Die IT-Grundschutz-Kataloge enthalten eine Vielzahl von Maßnahmen zu den Aspekten „Organisation“, „Personal“, „Notfallvorsorge“ (Übergreifende Aspekte), „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“. Auch diese Maßnahmen sind generisch beschrieben und bieten zunächst einen Basisschutz. Bei höheren Anforderungen in Bezug auf den Schutzbedarf müssen ggf. zusätzliche wirksamere Maßnahmen zur Erreichung der definierten Schutzziele ergriffen werden.
- Einen Überblick über die wichtigsten Sicherheitsmaßnahmen bietet der Leitfaden Informationssicherheit des BSI [13]. Im Fokus steht dabei die Darstellung der organisatorischen Maßnahmen, auf technische Details wird bewusst verzichtet.

Die Auswahl der Maßnahmen soll insbesondere unter Berücksichtigung der Kosten-Nutzen-Aspekte erfolgen. Gleichwohl müssen die Maßnahmen auch praxistauglich und den konkreten Gegebenheiten vor Ort angepasst sein. Auch die in den Regelwerken zur Informationssicherheit empfohlenen Maßnahmen sind generisch beschrieben, so dass diese bei der Planung an das konkrete Anwendungsumfeld angepasst werden müssen.

Für die Umsetzung der Maßnahmen sollte ein Umsetzungsplan erstellt werden, der Folgendes beinhaltet:

- Priorisierung der Maßnahmen

  Eine Priorisierung kann anhand des Kriteriums Schutzbedarf im Zusammenhang mit der Eintrittswahrscheinlichkeit und den Auswirkungen des Szenarios erfolgen. Darüber hinaus bietet es sich an, zunächst Maßnahmen umzusetzen, die sich im Rahmen des Soll-Ist-Abgleichs des IT-Grundschutzes als unzureichend oder als fehlend erwiesen haben. Es kann aber auch durchaus sinnvoll sein, ein Sofortprogramm mit Maßnahmen aufzustellen, die – unabhängig von der Dringlichkeit bzw. dem Schutzbedarf der jeweiligen Infrastrukturelemente – mit geringem finanziellen oder personellen Aufwand umgesetzt werden können.
- Festlegung der Verantwortlichkeiten für die Umsetzung der einzelnen Maßnahmen

  Während für die risikoanalytische Betrachtung eine Projektgruppe eingerichtet wird, die sich aus internen und externen Experten sehr unterschiedlicher Bereiche mit speziell definierten Verantwortlichkeiten für die Umsetzung der Risikoanalyse zusammensetzt, stehen im Zuge

der Umsetzung der sich aus der Risikoanalyse ergebenden Maßnahmen die jeweils fachlich zuständigen Mitarbeiterinnen und Mitarbeiter in der Verantwortung.

- Bereitstellung von Ressourcen

  Bei der Breitstellung der für die Umsetzung der Maßnahmen notwendigen Ressourcen sind nicht nur die Sachmittel zu berücksichtigen, sondern auch ggf. zusätzliche personelle Ressourcen einzustellen.

- Planung der einzelnen Maßnahmen

  Es empfiehlt sich, für die Umsetzung der einzelnen Maßnahmen Pläne zu erstellen, die den Ablauf inhaltlich und zeitlich strukturieren, etwa in Form eines Balkenplans, um auf diese Weise Einzelmaßnahmen besser aufeinander abstimmen, Überschneidungen zu erkennen und mögliche Doppelarbeit zu vermeiden.

Das auf Basis der Risikoanalyse entwickelte und umgesetzte Sicherheitskonzept bedarf einer fortwährenden Evaluierung und Aktualisierung. Dies ist beispielsweise der Fall, wenn

- im Zuge einer Umorganisation neue Prozesse bzw. Betriebsabläufe eingeführt werden, die hinsichtlich der Kritikalität neu bewertet werden müssen
- neue IT-Systeme eingesetzt werden und sich ggf. neue Sicherheitslücken ergeben
- sich die Gefährdungslage aufgrund neuer Gefahren oder Bedrohungen geändert hat und die Risikoanalyse entsprechend ergänzt werden muss
- sich Mängel bei den vorhandenen Sicherheitsmaßnahmen während einer Übung, Störung bzw. während eines Ereignisses gezeigt haben

Es sollte regelmäßig geprüft werden, ob die vorgesehenen Maßnahmen sowohl im Bereich technischer Sicherheitsmaßnahmen als auch organisatorischer Regelungen eingehalten werden. Darüber hinaus sind die Effizienz und die Praxistauglichkeit der eingesetzten Sicherheitsmaßnahmen, insbesondere der organisatorischen Regelungen, zu überprüfen. Gleichzeitig gilt es, den Stand der Technik und anderer Regularien (Normen, Vorschriften) zu verfolgen und in die Sicherheitskonzeption zu implementieren. Der BSI-Leitfaden IS-Revision bietet Hilfestellungen für die Durchführung solcher Überprüfungen [14].

Literatur

[1] Richtlinien für die Ausstattung und den Betrieb von Straßentunneln - RABT, FGSV-Nr. 339, Forschungsgesellschaft für Straßenwesen. Köln, 2006

[2] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS). Bonn 2008

[3] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. Bonn 2008

[4] Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen. Berlin 2005

[5] ISO/IEC 27001 Information technology – Security techniques – Information security management systems requirements specification, 2005

[6] ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management, 2005

[7] Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. Berlin, 2011

[8] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Methode für die Risikoanalyse im Bevölkerungsschutz (= Reihe Wissenschaftsforum, Band 8). Bonn 2010

[9] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3 Risikoanalyse auf Basis von IT-Grundschutz. Bonn 2008

[10] DIN EN 50518-1 (VDE 0830-5-6-1):2010-12, Alarmempfangsstelle – Teil 1: Örtliche und bauliche Anforderungen

[11] DIN EN 50518-2 (VDE 0830-5-6-2):2011-04, Alarmempfangsstelle – Teil 2: Technische Anforderungen

[12] DIN EN 50518-3 (VDE 0830-5-6-3):2011-09, Alarmempfangsstelle – Teil 3: Abläufe und Anforderungen an den Betrieb

[13] Bundesamt für Sicherheit in der Informationstechnik: Leitfaden Informationssicherheit. 2012 https://www.bsi.bund.de/DE/Publikationen/publikationen_node.html (01.08.2014)

[14] Bundesamt für Sicherheit in der Informationstechnik: Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. Bonn 2010 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?__blob=publicationFile (07.08.2014)

II.2 Die Notwendigkeit und Angemessenheit der geleisteten Arbeit

Mit den im Projekt erzielten Ergebnissen wird ein Beitrag zur Erhöhung des Sicherheitsniveaus in Straßentunneln geleistet. Während die Empfehlungen zum Ereignismanagement insbesondere die Einsatzkräfte bei der Vorbereitung auf Schadenslagen und bei der Lagebewältigung unterstützen sollen, stellt die Methode Risikoanalyse speziell für Tunnelleitzentralen einen weiteren anwendungsbezogenen Baustein im Kontext des - präventiven - Risikomanagements für Kritische Infrastrukturen dar.

Die geleisteten Arbeiten entsprachen den im Arbeitsplan formulierten Zielen und Aufgaben und waren zum Erreichen der Ergebnisse erforderlich und angemessen. Zusätzliche Ressourcen waren für die Durchführung des Vorhabens nicht erforderlich.

II.3 Wichtigste Positionen des zahlenmäßigen Nachweises

Die wichtigsten Positionen des zahlenmäßigen Nachweises beinhalten Ausgaben für Personal, Sachmittel und Dienstreisen, wobei der größte Anteil der Ausgaben auf Personalkosten entfiel. Das Teilvorhaben wurde von einer Mitarbeiterin mit einer Vollzeitstelle bearbeitet. Die Sachmittel wurden für die Literaturbeschaffung, Durchführung des Expertenworkshops sowie den Nachdruck und die Neuauflage der Broschüre „Ereignismanagement für Straßentunnel – Empfehlungen für Betriebs- und Einsatzdienste“ verwendet.

II.4 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse im Sinne des fortgeschriebenen Verwertungsplans

Mit der Fortschreibung der Broschüre „Ereignismanagement für Straßentunnel – Empfehlungen für Betriebs- und Einsatzdienste“ wurden zusätzliche Aspekte der Vorbereitung auf Ereignisse sowie der Ereignisbewältigung im Kontext eines umfassenden Ereignismanagements aufgegriffen und entsprechende Empfehlungen formuliert. Die Veröffentlichung der Broschüre im April 2013 stieß insgesamt auf ein positives Echo, die erste Auflage war nach kurzer Zeit vergriffen und musste nachgedruckt werden. Seitdem wurden bereits 2.000 Exemplare verteilt. Der Nutzen der Empfehlungen liegt insbesondere darin, den beteiligten Einsatzdiensten (Feuerwehr, Polizei, Rettungsdienst) umfassende Informationen zu organisatorischen und betrieblichen Aspekten zu bieten, die auch zu Schulungszwecken genutzt werden können. Darüber hinaus dienen die Empfehlungen dazu, den für die Alarm- und Gefahrenabwehrplanung für Tunnelbauwerke Verantwortlichen, Anregungen für die Planung zu bieten und sie in Bezug auf „Katastrophen“-Szenarien stärker zu sensibilisieren.

Der Ausfall der Informations- und Kommunikationstechnik wurde in der Broschüre „Ereignismanagement für Straßentunnel“ als ein mögliches Szenario vorgestellt, mit der Empfehlung, ein IT-Sicherheitskonzept für den Tunnelbetrieb / die Tunnelleitzentrale zu erstellen. Im Nachfolgeprojekt SKRIBT^{PLus} wurde ein pragmatischer Weg zur Durchführung einer Risikoanalyse für Tunnelleitzentralen aufgezeigt. Mit der Veröffentlichung eines methodischen Leitfadens sollen die Tunnelbetreiber angeregt werden, ein betriebliches Risikomanagement zu etablieren, um Betriebsabläufe in einer Tunnelleitzentrale ausfallsicherer zu gestalten, Schäden an Menschen und Umwelt zu vermeiden sowie rechtliche oder vertragliche Anforderungen zu erfüllen.

Ein weiterer Projektnutzen für den Zuwendungsempfänger ergab sich darüber hinaus darin, dass das Verfahren einer Risikoanalyse für Betreiber Kritischer Infrastrukturen, auf den Spezialfall Tunnelleitzentralen angewendet, verifiziert werden konnte. Gleichzeitig wird mit dem gewählten Schwerpunkt auf IT-Sicherheit für eine spezifische Gefahrensituation sensibilisiert, ohne andere

Aspekte außer Acht zu lassen und auf diesem Weg den ganzheitlichen Ansatz beim Schutz Kritischer Infrastrukturen zu unterstreichen. Damit konnte das Projekt einen Beitrag zur Unterstützung der Länder und Betreiber Kritischer Infrastrukturen beim Schutz ihrer Einrichtungen und damit zur Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen leisten.

II.5 Bekannt gewordene Entwicklungen in der Projektlaufzeit (Fortschritte anderer Stellen auf dem Gebiet des Vorhabens)

Die International Fire Acadamy in der Schweiz hat im Jahr 2014 das Fachbuch „Brandeinsätze in Strassentunneln. Taktik – Technik – Hintergrund“ herausgegeben, auf das in Broschüre „Ereignismanagement“ verwiesen wird.

Darüber hinaus sind während der Projektlaufzeit keine Ergebnisse bekannt geworden, die sich explizit mit den in diesem Vorhaben bearbeiteten Fragestellungen befassten.

Auch die vom Bundesamt für Sicherheit in der Informationstechnik beauftragte „KRITIS-Sektorstudie „Transport und Verkehr“[4] , die einen umfassenden Überblick über die Sektoren und die darin erbrachten kritischen Dienstleistungen gibt, den sektorspezifischen Stand der Cyber-Sicherheit sowie Probleme und Trends zusammenfasst, erbrachte keine für das Projekt relevanten Ergebnisse.

II.6 Erfolgte und geplante Veröffentlichungen der Ergebnisse

Veröffentlichungen:

- Neuauflage (inhaltlich erweiterte Fassung) der Broschüre „Ereignismanagement für Straßentunnel – Empfehlungen für Betriebs- und Einsatzdienste“ in der vom BBK herausgegebenen Publikationsreihe „Praxis im Bevölkerungsschutz“, Band 9 (veröffentlicht im Mai 2015)
- Leitfaden zur Durchführung einer Risikoanalyse für Tunnelleitzentralen in der vom BBK herausgegebenen Publikationsreihe „Praxis im Bevölkerungsschutz“ (geplante Veröffentlichung Juli / August 2015)

Veröffentlichung von Informationen im Rahmen von Vorträgen, Workshops und Tagungen / Kongressen:

- Posterpräsentation des Projektes SKRIBT^{PLus} am Tag der offenen Tür des BBK / Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) am 14.09.2013
- Vorstellung des Projektes vor einer israelischen Delegation am 11.04.2013 in Bonn
- Vorstellung des Projekts im Rahmen eines internationalen geopolitischen Lehrgangs „Verkehrsinfrastruktur aus geopolitischer Sicht“ im Zentrum für Geoinformationswesen der Bundeswehr am 18.09.2014 in Fürstenfeldbruck
- Vortrag zu den Themen „Ereignismanagement für Straßentunnel“ und „Risikoanalyse für Tunnelleitzentralen“ auf der INTERSCHUTZ am 12.06.2015 in Hannover

[4] KRITIS-Sektorstudie Transport und Verkehr. Öffentliche Version – Revisionsstand 5. Februar 2015, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Transport_Verkehr.pdf?__blob=publicationFile