SSI BULLETIN

1/2013

Schweizerische Vereinigung unabhängiger Sicherheitsingenieure und -berater

Quantifizierte Risikoanalysen als Basis für die Planung komplexer Sicherheitssysteme

Wo keine gezielte Normgebung vorhanden ist und die anerkannten Regeln der Technik nicht genau zum Projektumfang passend sind, wird immer häufiger die Durchführung einer umfangreichen quantitativen Risikoanalyse verlangt, um den Nachweis zur Erfüllung des erforderlichen Sicherheitsniveaus zu erbringen. Somit lassen sich Massnahmen zur Verminderung des Risikos eines Störfalls klar identifizieren und in die Planung integrieren.

Von Nicola Norghauer
Pöyry Infra AG

Zu Beginn der Projektierung von sicherheits- und brandschutztechnischen Anlagen eines komplexen unterirdischen Bauwerks wird immer häufiger darüber debattiert, welche normativen Vorgaben für solche Anlagen vorhanden sind bzw. welche anerkannten Regeln der Technik umgesetzt werden sollen. In einem konkreten Fall waren die existierenden Normen nicht ausreichend für ein unterirdisches Stollen- und Kavernensystem zugeschnitten, weshalb vom Kunden die Durchführung einer umfangreichen quantitativen Risikoanalyse verlangt wurde. Diese anspruchsvolle Analyse wurde iterativ und in enger Zusammenarbeit mit dem Planerteam der brandschutztechnischen Anlagen sowie mit Unterstützung seitens des Kunden durchgeführt. Externe Experten wurden punktuell vom Kunden zusätzlich hinzugezogen, um wichtige Aspekte der Sicherheit im Rahmen von Workshops zu diskutieren.

Im Vordergrund standen die im Brandschutzkonzept konzeptionell formulierten Ziele zur Selbstrettung der Personen und zur Sicherstellung der Fremdrettung. Mit einer quantifizierten Risikoanalyse sollte das aktuelle Personenrisiko aufgrund von Brandereignissen bestimmt werden. Ebenfalls wurden Risikogrenzen (erforderliches Sicherheitsniveau) kompatibel mit den Zielen des Brandschutzkonzeptes definiert und – wo notwendig – Massnahmen vorgeschlagen, um die Risikogrenzen einzuhalten. Diese Massnahmen konnten sowohl technischer als auch organisatorischer Natur sein. Da sich die Verantwortung des Planerteams über die Projektierung hinaus bis zur Ausführung, Inbetriebnahme und Abnahme erstreckt, begleitete die Risikoanalyse den gesamten Projektablauf und stellte sicher, dass die identifizierten Massnahmen realisiert werden konnten.

Die Risikoanalyse wurde nicht nur für den Endzustand der Anlagen des Stollen- und Kavernensystems, sondern auch für die Zwischenphase (die Bauphase) erstellt. Sachschäden und Folgeschäden, beispielsweise aus Business Interruption, wurden in diesem Fall nicht berücksichtigt. Ebenfalls wurden Ereignisse mit Einbezug von toxischen Gasen, welche nicht aus Bränden resultierten, und mechanische Gefahren sowie mutwillige Beschädigungen, terroristische Angriffe, Naturgefahren usw., welche ebenfalls ein Personenrisiko darstellen, nicht berücksichtigt.

Vorgehen

Die Risikoanalyse wurde gemäss der Abbildung 1 in drei Hauptschritte unterteilt. Im Zuge der Grunddaten- und Systemdefinition wurden das zu betrachtende System definiert, systembedingte Annahmen getroffen sowie Beurteilungs- und Akzeptanzkriterien bestimmt.

Der Prozessschritt Risikoidentifikation (Gefahrenidentifikation) umfasst die Identifikation von Gefahren. Dieser Schritt stellt die wichtigste Aktivität im Zuge der Analyse dar, denn es können nur jene Gefahren untersucht werden, welche auch identifiziert wurden. Innerhalb der eigentlichen Risikoanalyse wird die Systemverfügbarkeit der Sicherheitseinrichtungen modelliert und berechnet. Die Ereignishäufigkeiten der identifizierten Gefahren wurden bestimmt und das ent-

EDITORIAL

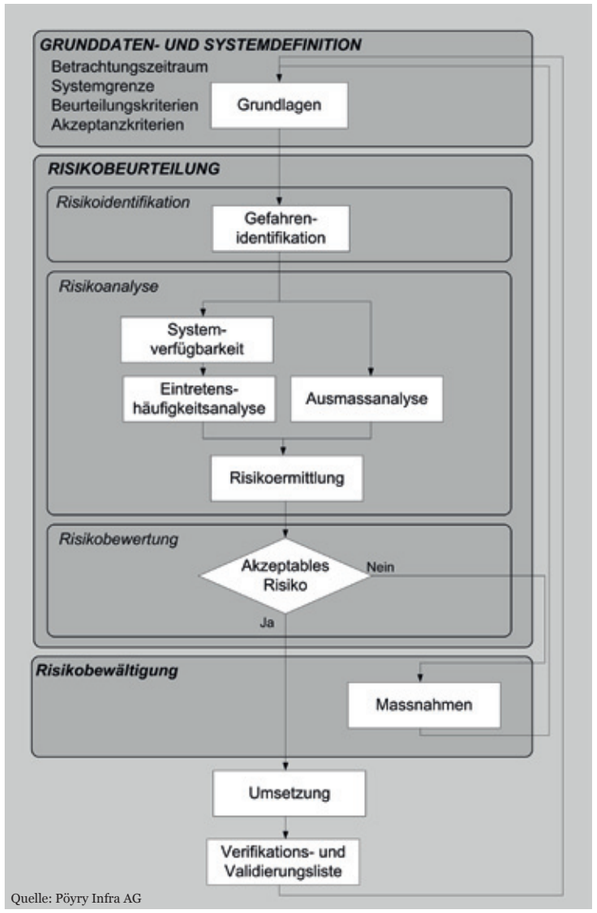
Modellvorstellung vs. Realität

Wer nach dem Begriff «Sicherheit» googelt, findet bei Wikipedia folgende Definition: «Sicherheit (von lat. sēcūritās, zurückgehend auf sēcūrus ‹sorglos›, aus sēd ‹ohne› und cūra ‹(Für-)Sorge›) bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.» Diese Definition stellt eine risikoaverse Sicht dar. Dem kann ein Zitat des Management-Gurus Peter Drucker zum Thema Sicherheit gegenübergestellt werden: «Es gibt Risiken, die einzugehen du dir nicht leisten kannst, und es gibt Risiken, die nicht einzugehen du dir nicht leisten kannst!» Risiken werden hier wertfreier dargestellt. Im Arabischen bedeutete Risiko einst sogar einfach, «das tägliche Brot» zu verdienen.

Drucker zeigt auf, dass es keine Entscheidungen ohne Risiken gibt. Entscheidungen haben immer eine Wirkung auf die Zukunft und diese lässt sich in einer komplexen Welt bei bestem Willen nicht genau voraussehen.

Wir können heute Risiken zwar quantifizieren, doch basieren diese Berechnungen immer auf akzeptierten Modellvorstellungen der Realität. Jede Berechnung ist aber nur so gut wie das hinterlegte Modell. So lassen sich «normale» Risiken relativ gut quantifizieren, aber je seltener ein Ereignis eintrifft, desto kritischer sind solche Berechnungen zu hinterfragen, weil die Modelle an ihre Grenzen stossen. Nassib Nicholas Taleb hat in seinem Buch «Der Schwarze Schwan» deutlich aufgezeigt, wie gefährlich unsere Modellvorstellungen insbesondere bei seltenen Ereignissen sein können. So haben rückblickend Ereignisse wie der Brand im Mont-Blanc-Tunnel 1999, die Krise im Bankensystem 2008 oder auch die Nuklearkatastrophe von Fukushima 2011 unsere (Modell-)Vorstellungen der Realität und damit auch das Risikobewusstsein massiv verändert. Bei allen Möglichkeiten, Risiken zu berechnen und darzustellen, sollten wir eine einfache Frage nie vergessen: «Wie stehe/n ich/wir da, wenn ein gewisses Szenario eintritt, sei es noch so unwahrscheinlich?»

Jon Mengiardi
Gruner AG, Geschäftsbereich Umwelt, Sicherheit



Quelle: Pöyry Infra AG

Die Risikoanalyse wurde in drei Hauptschritte unterteilt.

sprechende Ausmass wurde abgeschätzt. Auf Basis dieser Daten konnte das Risiko ermittelt werden. Das Risiko wurde in der Risikobewertung mit einem definierten Akzeptanzgrenzwert verglichen und es wurde bestimmt, ob risikomindernde Massnahmen zwingend nötig sind.
Im Prozessschritt Risikobewältigung wurden, falls erforderlich, verschiedene Massnahmen zur Risikominimierung definiert.

Herausgeber:

SSI, Schweizerische Vereinigung unabhängiger Sicherheitsingenieure und -berater

Sekretariat
Güstrasse 46
8700 Küsnacht

Telefon 044 910 73 06
www.ssi-schweiz.ch
sicherheitsingenieure@bluewin.ch

Es wurde dabei unterschieden zwischen zwingend umzusetzenden Massnahmen, welche die Personensicherheit gewährleisten bzw. das geforderte Sicherheitsniveau erst durch deren Realisierung erreichen wird, und Massnahmen zur weiteren Erhöhung der Personensicherheit. Letztere wurden umgesetzt, sofern sie zumutbar und verhältnismässig sind. Die Anforderungen aus der Risikoanalyse wurden in die Verifikations- und Validierungsliste eingetragen und deren Umsetzung überwacht.

Grunddaten- und Systemdefinition

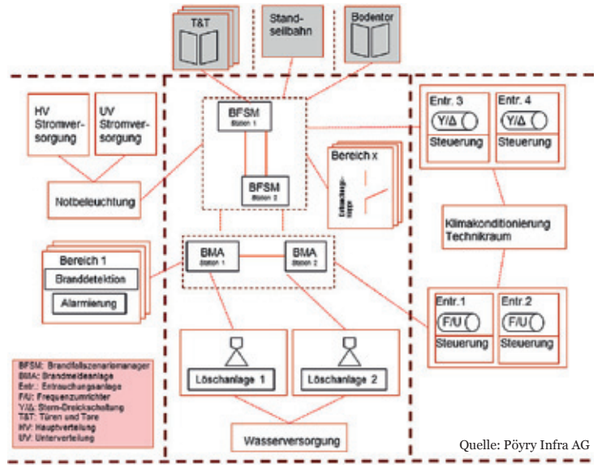
Für die erfolgreiche Durchführung einer quantitativen Risikoanalyse sind eine klare Bestimmung der Grunddaten, die Definition der örtlichen und zeitlichen Systemgrenzen und die Zustimmung der Annahmen sowohl mit dem Kunden als auch mit dem künftigen Betreiber dieser technischen Systeme von grosser Bedeutung. Im Rahmen von Expertenworkshops wurden folgende wichtigen Themen besprochen und somit saubere Grundlagen für die Risikoanalyse erstellt:

- Klare Definition der Nutzung der gesamten unterirdischen Anlagen während der Bauphase und im Endzustand, inkl. Unterhaltsarbeiten/Wartung
- Bestimmung der Betriebsabläufe und deren Besonderheiten (Anzahl Transporte mit Personen, Personenbelegung, Transport von Gütern/Gefahrgütern)
- Identifikation von relevanten/kritischen Störfällen (z.B. Brandereignisse)
- Bestimmung der Eintrittshäufigkeit der Brandereignisse
- Berücksichtigung der richtigen Nahtstellen mit anderen technischen Anlagen und mit den Bautätigkeiten

In der Risikoanalyse wurden zahlreiche Sicherheitssysteme berücksichtigt (siehe auch Abbildung 2):
Entrauchungsanlagen, Löschanlagen, Wasserversorgung, Brandmeldeanlagen, Notbeleuchtungen, Raumlufttechnische Anlagen und Notkühlung, Schaltgerätekombinationen, Elektroinstallationen, Energieversorgung, Kommunikationsnetz.
Es bestehen Nahtstellen zu den folgenden technischen Anlagen: übergeordnete Stromversorgung, Leitstelle, Türen und Tore, Bodentore, Transportsysteme inkl. Standseilbahn.

Methodik

Um das Personenrisiko von anwesenden Personen aufgrund von Bränden bestimmen zu können, wurde der Risikobeurteilung das ALARP-Prinzip (As Low As Reasonably Practicable) mit den entsprechenden Grenzwerten zugrunde gelegt. Diese Risikogrenzen beziehen sich auf das individuelle Todesfallrisiko. Beim individuellen Todesfallrisiko wird das Risiko eines einzelnen Individuums ermittelt, welches sich eine begrenzte Zeit in der Anlage aufhält. Als Personengruppen wurden Baustellenarbeiter, Betriebspersonal und Besucher berücksichtigt.
Liegt das individuelle Risiko im Bereich oberhalb des Grenzwertes, müssen zwingend Massnahmen definiert werden, um mindestens in den Übergangsbereich (ALARP-Bereich, Verhältnismässigkeitsbetrachtung) zu gelangen. In diesem Fall wurde vorausgesetzt, dass der ALARP-Grenzwert für Arbeiter (individuelles Todesfallrisiko aufgrund von Bränden) bei 1×10^{-4} Todesopfern pro Jahr liegen darf. Dies entspricht einem Todesopfer alle 10 000 Jahre.
Der Grenzwert der Todesfälle durch Brände für die Öffentlichkeit wird auf 5×10^{-5} Todesopfer pro Jahr festgelegt (ein Todesopfer alle 20 000 Jahre). Dieser Grenzwert wird in der Risikoanalyse für den Transport von Personen (z.B. Besucher) herangezogen.
Die Grenzkosten für das gerettete Leben wurden mit CHF 5 Mio. quantifiziert. Bei Einhaltung der Grenzwerte werden Zusatzmassnahmen hinsichtlich ihrer Kostenwirksamkeit beurteilt.



Quelle: Pöyry Infra AG

In der Risikoanalyse wurden zahlreiche Sicherheitssysteme berücksichtigt.

Verfügbarkeitsmodell und -berechnung

Das Personenrisiko ergibt sich aus der Eintrittshäufigkeit eines Brandereignisses und dem möglichen Personenschaden. Bei der Bestimmung des Personenschadens wird berücksichtigt, ob die vorhandenen sicherheitsrelevanten Anlagen verfügbar sind oder nicht. Eine grosse Herausforderung stellte die Erstellung des Modells für die Berechnungen dar. Alle sicherheitsrelevanten Anlagen und Komponenten wurden in einem Verfügbarkeitsmodell miteinander verknüpft. Anhand dieses Modells wurden die Verfügbarkeit der sicherheitsrelevanten Gesamtanlage sowie die möglichen Optimierungsmassnahmen für unterschiedliche Betriebszustände ermittelt.
Im Rahmen der Workshops wurden die entsprechenden Grundlagen und Modellierungsansätze für die Berechnung der Verfügbarkeit plausibilisiert und validiert. Für Aspekte, in denen statistisch quantifizierte Informationen nicht verfügbar waren, wurden entsprechend der Erfahrungen der Teilnehmer der Workshops Abschätzungen erarbeitet.
Die folgenden Annahmen wurden für die Verfügbarkeitsmodelle getroffen, welche die realen Bedingungen ausreichend gut repräsentieren:

- Die Ausfallrate der Komponenten ist über die Zeit konstant.
- Alle Systeme sind reparierbar (ein Austausch von Komponenten wird als Reparatur betrachtet).
- Es wird immer mit aktiver Redundanz gerechnet (aktive Redundanz = beide Systeme laufen parallel. Bei Ausfall eines Systems wird umgeschaltet; passive Redundanz = ein System ist im Stand-by-Betrieb. Beim Ausfall des laufenden Systems wird das andere hochgefahren).
- Abhängigkeiten (Common Cause Failures) von Komponenten wurden mit dem β-Faktor-Modell abgebildet. Mit dem β-Faktor wird angegeben, wie häufig ein gemeinsamer Ausfall von beiden Systemen stattfindet. Die Common Cause Failures sind bei allen Redundanzen berücksichtigt.
- Die Kennzahl «Mean Time To Repair» (MTTR-Wert) beinhaltet die Reparaturzeit (vor Ort), die Zeit, bis das Reparaturteam vor Ort ist, die Ersatzteilbeschaffung und ein halbes Testintervall bei nicht kontinuierlich arbeitenden Systemen.
- Ein nicht detektierter Ausfall der Sicherheitsanlage kann im Ereignisfall zu einem Personenschaden führen. Aus diesem Grund wurde beim MTTR-Wert bei nicht kontinuierlich arbeitenden Systemen das halbe Testintervall hinzugefügt (Einfluss auf die Verfügbarkeit der Anlage). Bemerkung: Die Zeit, bis ein Ausfall zwischen zwei Testintervallen erkannt wird, entspricht im Mittel dem halben Testintervall.
- Das Testintervall für nicht kontinuierlich arbeitende Systeme beträgt drei Monate.
- Wartung, Unterhalt und Instandhaltung aller sicherheitsrelevanten Anlagen werden entsprechend den Unternehmervorgaben umgesetzt.

Grundsätzlich werden zwei «Betriebsarten» von technischen Systemen unterschieden:

- Systeme, welche dauernd in Betrieb sind, werden als kontinuierlich arbeitende Systeme bezeichnet, wie z.B. die Brandmeldeanlage.
- Nicht kontinuierlich arbeitende Systeme, welche nur im Bedarfsfall eingeschaltet werden, wie z.B. die Entrauchungsanlage.

Für die Berechnung der Verfügbarkeit der Sicherheitsanlagen werden je nach Betriebsart folgende Informationen benötigt:

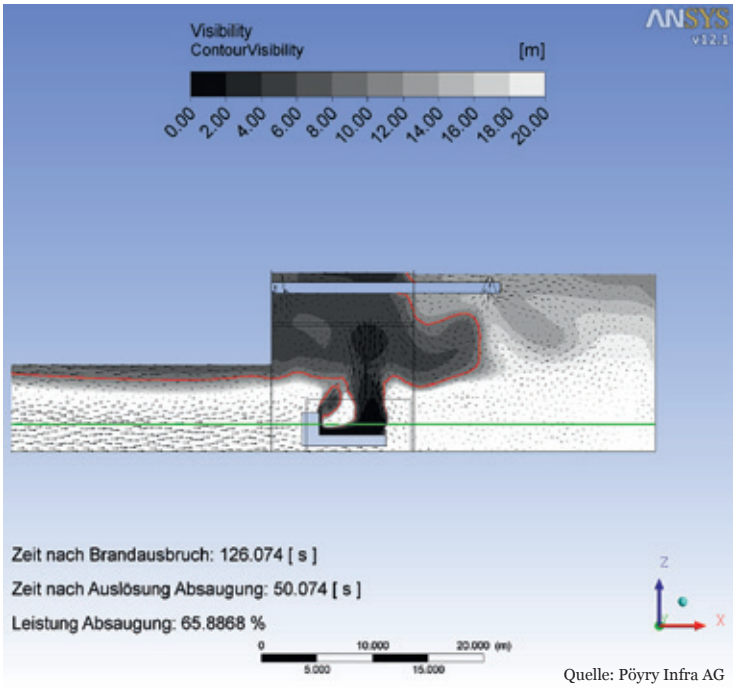
Bei kontinuierlich arbeitenden Systemen:
– Zuverlässigkeit im Dauerbetrieb: Durchschnittliche Betriebszeit, bis eine Störung auftritt (MTBF = Mean Time Between Failures).
– Reparaturzeit: Durchschnittliche Dauer der Reparatur (MTTR) inkl. Anreisezeit, Reparaturzeit, Ersatzteilbeschaffung, Fehlerentdeckungszeit

Bei nicht kontinuierlich arbeitenden Systemen, welche nur im Bedarfsfall eingeschaltet werden, wie z.B. die Entrauchungsanlage:
– Zuverlässigkeit «on demand»: Anzahl Fälle pro Einsatz, in denen ein Ausfall zu erwarten ist.

Die Verfügbarkeitsanalyse hat zum Ziel, zu ermitteln, wie häufig eine technische Anlage prinzipiell verfügbar ist. Verfügbar bedeutet, dass die Anlage operativ einsatzfähig ist. Nicht verfügbar ist die Anlage beispielsweise dann, wenn eine Komponente, z.B. ein Ventilator oder eine Pumpe, infolge eines Defektes ausgetauscht oder repariert werden muss. In der Zeit, bis die Reparatur erfolgt ist, ist das System entsprechend nicht operativ verfügbar.
Für einzelne technische Komponenten können in der Regel die Hersteller diese mittlere Zeit bis zum Versagen der Komponenten angeben. Dies ist die sogenannte Mean Time Between Failures (MTBF). Die MTBF entspricht einer konstanten Ausfallrate pro Zeiteinheit. Die MTBF gilt für Komponenten, die sich im gewarteten Zustand befinden und keine Alterungserscheinungen aufweisen und sich in der Anfangsphase des Einsatzes bewährt haben bzw. Initialdefekte bereits erkannt und beseitigt worden sind.
Um die Berechnung möglichst realitätsnah durchzuführen, wird bei allen Anlagen, welche nicht kontinuierlich betrieben werden, der MTTR-Wert mit der Fehlerentdeckungszeit (halbes Testintervall) erhöht. Somit wird auch ein Ausfall zwischen zwei Testbetrieben (dieser Ausfall wird erst beim nächsten Test erkannt) berücksichtigt.
In den berechneten Verfügbarkeiten wurden die geplanten Wartungen und Unterhaltsarbeiten nicht berücksichtigt. Es wird davon ausgegangen, dass bei Wartungsarbeiten an den Sicherheitsanlagen ein entsprechend eingeschränkter Betrieb hinsichtlich der Transporte usw. vorgeschrieben wird und somit die Personensicherheit gewährleistet ist.

3D-Simulationen

Dreidimensionale CFD-Simulationen wurden im Rahmen der Risikoanalyse bei ausgewählten Brandszenarien zur Bestimmung des Ausmasses durchgeführt. Diese Simulationen wurden auch unter Berücksichtigung eines Ausfalls der Entrauchungsventilatoren wiederholt, um die Wirkung der Entrauchungsanlage genau zu überprüfen. Abbildung 3 zeigt einen Lastwagenbrand in einer Kaverne mit funktionstüchtiger Entrauchung. Die rote Grenzlinie entspricht einer Sichtweite von 10 m, und die grüne Linie stellt die Höhe von 2,5 m dar. Unterhalb dieser Linie ist eine minimale Sichtweite von 10 m für die Selbstrettung sicherzustellen.



Dreidimensionale CFD-Simulationen wurden bei ausgewählten Brandszenarien zur Bestimmung des Ausmasses durchgeführt.

Quelle: Pöyry Infra AG

Ergebnisse

Die durchgeführte Risikoanalyse hat aufgezeigt, dass das durch Brände verursachte individuelle Todesfallrisiko für die Bau- und Betriebsphase knapp über den Grenzwerten liegt. Die Auswertung des Personenrisikos für die unterschiedlichen Bereiche zeigt, dass Massnahmen zur Erreichung des erforderlichen Sicherheitsniveaus in wenigen Bereichen vorzusehen sind.
Es wurden verschiedene organisatorische, betriebliche sowie technische Massnahmen analysiert und in verschiedenen Kombinationen hinsichtlich ihres Einflusses auf das individuelle Todesfallrisiko untersucht. Das Ergebnis der Auswahlempfehlung sieht wie folgt aus:
– Die für den Endzustand vorgesehene automatisierte Löschanlage der Hauptkaverne wird bereits in der Bauphase umgesetzt. Diese Massnahme reduziert das individuelle Todesfallrisiko in dieser Kaverne. In der Bauphase kann somit das individuelle Todesfallrisiko fast um den Faktor 10 reduziert werden.
– Es liegen keine gesicherten Daten für die Verfügbarkeit des Brandfall-Szenariomanagers (BFSM) ohne SIL-Anforderungen vor (SIL = Safety Integrity Level). Aufgrund der Komplexität des Systems und der zentralen Stellung des BFSM für die Personensicherheit ist der BFSM mit SIL-Anforderungen zu realisieren, sodass die hohe Verfügbarkeit sichergestellt wird.
– Die Beleuchtung des Fluchtwegs wird bei einem langen Stollen verstärkt. Zusätzlich sind in diesem Bereich eine passende optische Signalisierung der Fluchtrichtung inkl. Distanzangabe sowie eine akustische Alarmierung zu realisieren.
– Ein Transformator mit entsprechender Vorkehrung für den Betrieb bei sehr hohen Temperaturen (keine Selbstabschaltung) und eine Lagerhaltung der Transformatoren sind zu realisieren.

Um das individuelle Todesfallrisiko infolge von Fehltransporten (durch brennbare Materialien) zu reduzieren, können folgende Massnahmen umgesetzt werden:
1. Bei Materialtransporten mit der Standseilbahn dürfen auf der Gegenbahn keine Personentransporte (auch kein Fahrer) stattfinden.
2. Jede Materiallieferung wird durch einen Sachverständigen vorgängig auf die zulässige Brandlast untersucht und freigegeben. Dieses erfordert die ständige Präsenz eines Fachkundigen.

Nach Umsetzung dieser Massnahmen ist gewährleistet, dass die definierten Grenzwerte – bezogen auf das individuelle Risiko – unterschritten werden.

Über den Autor:

Nicola Norghauer ist Abteilungsleiter Safety & Security der Firma Pöyry Infra AG (ehem. Electrowatt Engineering AG). Seit 13 Jahren tätig in der Projektierung von sicherheitstechnischen Anlagen, besonders bei grossen Projekten im Untertagebau.