Regelwerkversion	**2-0**	Vertraulichkeitsklassifikation	**intern**
gültig ab	**01.09.2015**	Eigner	**K-SQ**
		Betroffene Prozesse	**Safety**
		verfügbare Sprachen	**DE, FR, IT**
Betroffene Divisionen		**Infrastruktur, Personenverkehr, Cargo, Immobilien, Konzern**	
Spezifische Empfänger / Verteiler		**Fachführungseinheiten Sicherheit und Qualität der Divisionen**	
Ersatz für		**Regelwerkversion 1-0**	

Managementsystem SBB Konzern: Teil Safety

Methodik Riskmanagement Safety bei der SBB

1 Ziel

Beschreibung der bei der SBB verwendeten Methodik für das Riskmanagement Safety als Guideline für Fachspezialisten, die beauftragt sind Riskmanagement Safety bei der SBB durchzuführen.

2 Geltungsbereich

SBB, gemäss R Z 200.00: Riskmanager Safety.

3 Begriffe, Definitionen

Sicherheit

Sicherheit gegenüber einer Gefährdung besteht dann, wenn diese durch geeignete Massnahmen unter Kontrolle gehalten und auf ein akzeptierbares Mass beschränkt wird. Ein Zustand wird als sicher definiert, wenn das verbleibende Risiko akzeptierbar klein ist.

Gefahr (in Anlehnung an ONR 49000:2008)

Potenzielle Quelle eines Risikos, die zu einem plötzlich eintretenden Schadenereignis führen kann. Arten von Gefahren:

- Naturgefahren (Erdbeben, Hochwasser, geolog. Massenbewegungen, …)
- Technische Gefahren (Eisenbahnunfall, Brand, Freisetzung von Gefahrgut, …)
- Gesellschaftliche Gefahren (Berufsunfall, Freizeitunfall, …)

Gefährdung (in Anlehnung an ONR 49000:2008)

Gefahr, die sich negativ auf Personen (Mitarbeitende, Reisende, Dritte), Umwelt oder Sachwerte (Anlagen, Rollmaterial) auswirkt.

Risiko (in Anlehnung an ONR 49000:2008)

Ein Risiko besteht, wenn es durch das Eintreten einer Handlung, eines Ereignisses[1] oder einer Entwicklung[2] zu einer Zielabweichung kommen kann.

Risikohöhe (in Anlehnung an ONR 49000:2008)

Ausmass eines Risikos, geschätzt oder gemessen als bestimmte Kombination von Häufigkeit (H) und möglichem Ausmasses (A) eines Schadensereignisses an Personen, der Umwelt oder an Sachwerten.

[1] plötzlicher Eintritt einer bestimmten Kombination von Umständen
[2] allmähliche Veränderung von Umständen

Individuelles Risiko

Als individuelles Risiko ri bezeichnet die Häufigkeit, dass bei einem bestimmten Schadenereignis eine Einzelperson z.B. als Benützer des Bahnsystems zu Schaden kommt (Sicht des Individuums; Messgrösse: jährliche Todesfallwahrscheinlichkeit).

Kollektives Risiko

Als kollektives Risiko Rk wird jenes Risiko bezeichnet, das die Gesellschaft (oder Teile davon) betrifft, die eine entsprechende Tätigkeit ausübt und z.B. als Benützer des Bahnsystems einer Gefährdung ausgesetzt ist (Sicht des Kollektivs). Es ist gleich der Summe der individuellen Risiken in einem System und entspricht dem Produkt aus Häufigkeit und Schadenausmass:

$$R_k = H * A \qquad (I)$$

Bei der SBB wird in der Regel das kollektive Risiko Rk (z.B. Todesopfer pro Jahr) betrachtet, da davon ausgegangen wird, dass das individuelle Risiko ri aus dem Bahnbetrieb für Mitarbeiter, Reisende und Dritte ausreichend gering ist.

4 Massgebende Dokumente

- PB Z 200.9 MS SBB Konzern: Teil Safety, Prozessbeschreibung Riskmanagement Safety
- K 200.1, Anhang I MS SBB Konzern: Teil Safety, Vorgaben zum Riskmanagement Safety an Divisionen, Konzernbereiche
- G Z 018.1 Grundsätze des Verwaltungsrates der SBB zu Safety und Security
- G Z 018.2 Fachbereichsrichtlinie der SBB im Bereich Safety

5 Methodik Riskmanagement Safety bei der SBB

Das Grundkonzept des risikoorientierten Ansatzes basiert auf den ermittelten Risiken des Systems sowie auf einer expliziten Bewertung derselben. Es erlaubt, die Zusammenhänge bei der Beurteilung von Sicherheitsproblemen und dem Entscheid über Sicherheitsmassnahmen systematisch und transparent zu strukturieren. In einem ersten Schritt werden die Risiken des zu untersuchenden Systems ermittelt und analysiert *(Risikoidentifikation und -analyse)*. In einem zweiten Schritt werden die Risiken anhand von Kriterien bewertet *(Risikobewertung).* Auf dieser Grundlage erfolgt – soweit notwendig – die Planung von Massnahmen *(Risikobewältigung)*.

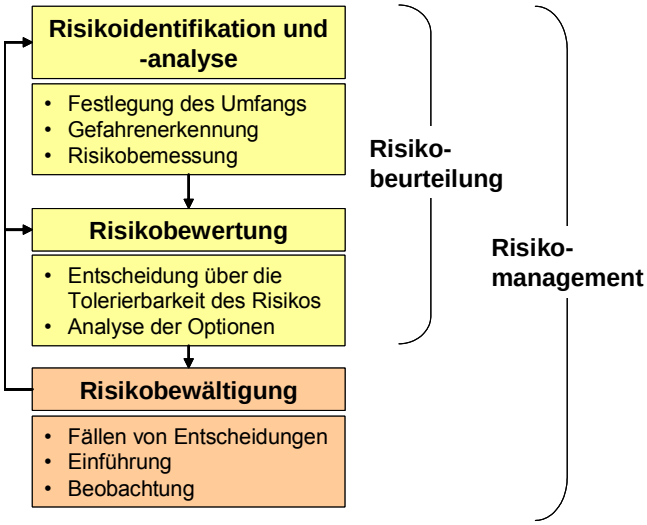


Abbildung 1: Prozess Riskmanagement Safety

5.1 Risikoidentifikation und -analyse

Im *ersten Schritt* des Riskmanagement - **der Risikoidentifikation** – werden die Risiken in einem definierten System erfasst und beschrieben ("Was kann passieren?"). Die Risiken werden in einer zweiten Phase – **der Risikoanalyse** - von definierten Risikogrössen bezüglich Häufigkeit und zu erwartendem Schadensausmass abgeschätzt.

Schadenindikatoren als Risikomessgrössen

Ereignisse im Eisenbahnumfeld können verschiedene Arten von Schäden nach sich ziehen. Übliche Schadenindikatoren als Messgrössen für das Risiko sind in untenstehender Tabelle dargestellt.

Personenschäden	Sachschäden	Umweltschäden
■ Todesopfer ■ Verletzte	■ Bahninfrastruktur, Rollmaterial ■ Betriebsstörungen, Betriebsunterbruch ■ Sachschäden Dritter	■ Verschmutztes Grundwasser ■ Verschmutztes Oberflächengewässer ■ Verschmutzter Boden

Tabelle 1: Schadenindikatoren

Bei Sicherheitsfragen im Eisenbahnbetrieb steht die Messgrösse Todesopfer im Vordergrund. Die anderen Schadenarten werden häufig nur indirekt mit einbezogen. Es gibt jedoch Risikoarten wo andere Indikatoren berücksichtigt werden. So werden bei Abschätzungen der Naturgefahren Betriebsunterbrüche berücksichtigt. Bei den Gefahren aus dem Transport gefährlicher Güter werden auch Umweltrisiken (Schädigung von Grundwasser und Oberflächengewässern) explizit betrachtet.

Sensitivitätsanalyse

Da einige der in einer Risikoanalyse erfolgten Abschätzungen nicht präziser Art sind, sollte i.d.R. eine Sensitivitätsanalyse vorgenommen werden, um die Auswirkungen von Unsicherheiten von Annahmen und der vorliegenden Daten zu testen. Zudem kann festgestellt werden, welche Parameter für die Ergebnisse sensitiv (risikobestimmend) sind. Hierzu werden die eingesetzten Parameter jeweils einzeln in einem vorgegebenen Bereich (zB in einem Bereich von ± 10 % ausgehend vom Basiswert) variiert und die Auswirkungen dieser Modifikation auf das Ergebnis geprüft.

Risikoarten und Detaillierungsgrad

Risikoanalysen können abhängig vom Risiko selbst, dem Zweck der Analyse und den zur Verfügung stehenden Daten und Ressourcen unterschiedlich detailliert erfolgen. Die Analyse kann je nach Ausgangslage und Fragestellung qualitativer, semiquantitativer oder quantitativer Art sein. Für die meisten Anwendungen bei den SBB wird ein qualitativer oder semiquantitativer Ansatz ausreichen. Häufig werden verschiedene Ansätze kombiniert (vgl. auch die Tools im Anhang).

5.2 Risikobewertung

Im *zweiten Schritt* – **der Risikobewertung** – erfolgt der Nachweis, dass die Sicherheit eines Systems oder Verfahrens ausreichend ist ("Was darf passieren?").

Für die Risikobewertung und damit das Befinden, welches Risiko akzeptabel ist, gibt es je nach Art des Risikos unterschiedliche Bewertungsansätze. So gibt es für die Bewertung der Störfallrisiken aus dem Transport gefährlicher Güter vom Bund festgelegte quantitative Grenzwerte (vgl. Tools Risikobewertung im Anhang).

In anderen Bereichen des Eisenbahnbetriebs hat die SBB selbst Überlegungen zu Schutzzielen und Grenzwerten für die Risiken angestellt. Die Festlegung dieser Schutzziele erlaubt es, Risiken anhand eines konzernweit gültigen Massstabs zu bewerten.

In der Safety hat sich die Risikomatrix Safety SBB durchgesetzt und wird verbindlich im Rahmen des generellen Riskassessments Safety SBB verwendet (vgl. Abbildung 2). Mit ihren Häufigkeits- und Ausmassklassen hat sie sich für die Darstellung von Safetyrisiken bewährt.

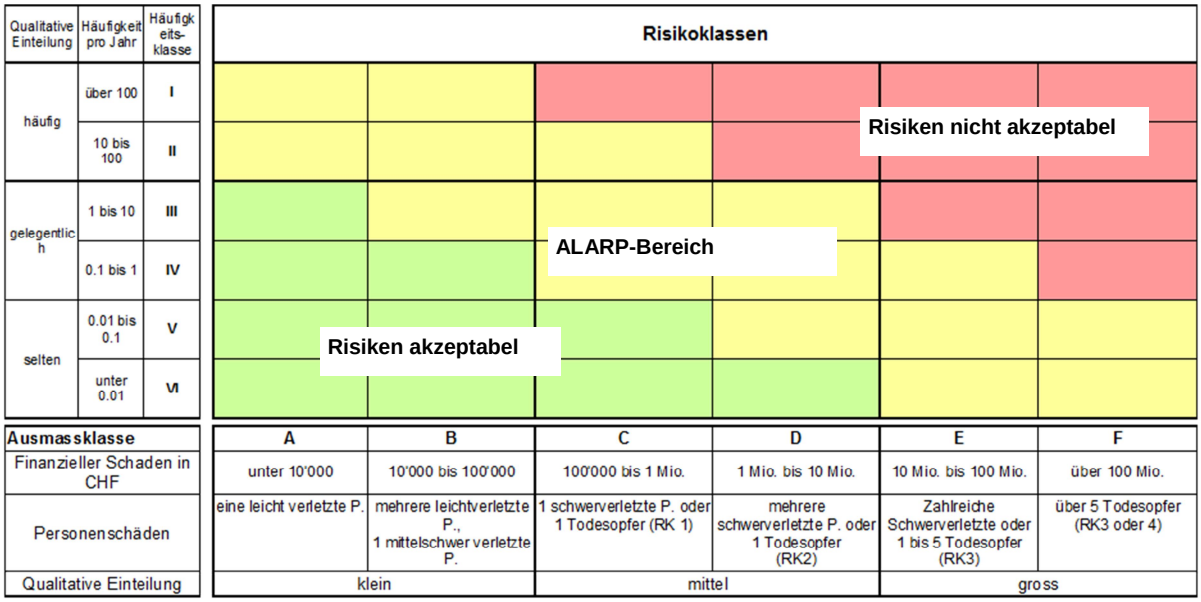


Abbildung 2: Risikomatrix Safety SBB

Die drei farbig markierten Bereiche, die sogenannten Risikoakzeptanzbereiche, machen eine Aussage zur Tragbarkeit von Risiken auf Stufe des Gesamtsystems SBB. Sie sind wie folgt zu verstehen:

Risiken akzeptabel	Es handelt sich um kleine Risiken, die im Allgemeinen akzeptiert sind und keine weitergehenden Massnahmen erfordern.
ALARP Bereich = Übergangsbereich	Liegen die Risiken in diesem sog. Übergangsbereich, ist die Tragbarkeit des verbleibenden Risikos abzuwägen. Mögliche Massnahmen werden unter Berücksichtigung der Kosten/Nutzen-Optimierung beurteilt (ALARP-Prinzip bzw. Grenzkostenprinzip, vgl. unten).
Risiken nicht akzeptabel	Liegt das Risiko im nicht tragbaren Bereich, sind zwingend Massnahmen zur Senkung des Risikos mindestens in den ALARP-Bereich vorzusehen.

Bestimmung der Risikoakzeptanzbereiche

Die Festlegung der Akzeptanzbereiche folgt dem Grundsatz[3], dass die Risiken des Gesamtsystems SBB tragbar sind („existing is tolerable“) und damit höchstens im Übergangsbereich liegen. Dies begründet sich in der seit Jahrzehnten erfolgten stetigen Entwicklung und Verbesserung der Sicherheit, welche die Erwartungen der Gesellschaft an die SBB widerspiegeln. Tatsächlich liegen die meisten Risiken aufgrund der Vorgabe „Sicherheitsniveau halten und wo sinnvoll verbessern“ im ALARP-Bereich. Der rote Bereich indiziert Handlungsbedarf bis eine Risikosenkung mindestens in den ALARP-Bereich eintritt. Der grüne Bereich enthält kleine Risiken, die im Allgemeinen mit verhältnismässigen Massnahmen nicht weiter reduziert werden können.

[3] Der Grundsatz „existing is tolerable“ ist dadurch begründet, dass die SBB ein grundsätzlich sicheres Eisenbahnsystem betreibt. Er ist durch die Festlegungen in den „Grundsätzen des Verwaltungsrats zu Safety und Security“, G Z 018.1 (und entsprechend der „Fachbereichsrichtlinie Safety“, G Z 018.2) abgestützt, insb.:

- In Ergänzung zu den gesetzlichen Bestimmungen ist in Bezug auf Safety das heutige Safetyniveau mit Sicherheitskennzahlen zu definieren und mindestens beizubehalten.
- Die kontinuierliche Verbesserung des Sicherheitsniveaus erfolgt unter Berücksichtigung des technischen Fortschritts, der Gefährdungspotenziale und der wirtschaftlichen Möglichkeiten.

Skalierung zur Unternehmensgrösse

Die Skalierung der Risikomatrix und die Einteilung in die Risikoakzeptanzbereiche gelten für das Gesamtsystem SBB (SBB Konzern) und bis auf die Ebene der Divisionen. Die Verwendung der gleichen Risikoakzeptanzbereiche ist aufgrund der geringen Grössenunterschiede zwischen Konzern und Divisionen und der Tatsache, dass einzelne Szenarien oft eine oder zwei Divisionen betreffen, vertretbar[4].

Die definierten Risikoakzeptanzbereiche können jedoch nicht für die Beurteilung von Risiken kleinerer Einheiten verwendet werden (einzelne Projekte, Objekte oder detailliert aufgeschlüsselte Szenarien).

ALARP

Die SBB verfolgt als Grundsatz für die Risikoakzeptanz das sog. ALARP-Prinzip. Es besagt, dass Risiken auf ein Mass reduziert werden sollen, welches den höchsten Grad an Sicherheit garantiert, der vernünftigerweise praktikabel ist (ALARP = As Low As Reasonably Practicable). Die Beurteilung der Risiken anhand der Verhältnismässigkeit zusätzlicher Massnahmen ist unabhängig von der Grösse des betrachteten Systems und der betrachteten Szenarien immer mit dem gleichen Kriteriensatz möglich (Universalität). Die Anwendung des ALARP-Prinzips garantiert einerseits, dass das Risiko mit verhältnismässigem Aufwand reduziert wird, andererseits bedeutet es auch, dass das verbleibende Risiko nach Umsetzung aller verhältnismässigen Massnahmen als tragbar eingestuft wird ("akzeptiertes Restrisiko").

Prinzip der Grenzkosten

Eine grosse Problematik bei der Risikobeurteilung besteht darin, dass Risiken messbar und vergleichbar gemacht werden müssen. Mit den Grenzkosten werden die mit den definierten Schadenindikatoren erfassten Schäden monetarisiert und vergleichbar gemacht (→ monetarisiertes Risiko). Die Grenzkosten drücken aus, wie viel Geld die Gesellschaft aufzuwenden bereit ist, um Schäden im Ereignisfall zu reduzieren (= Zahlungsbereitschaft der Gesellschaft oder willingness to pay). Die Festlegung der Grenzkosten stützt sich dabei auf zwei Elemente:

- Volks- und betriebswirtschaftliche Folgekosten (z.B. Abgeltungskosten, Arbeitsausfall, Heilungskosten).
- Zusätzliche Bereitschaft der Gesellschaft abhängig von der Gefahrenart solche Schäden zu minimieren. Hier spielt insbesondere eine Rolle, ob es sich um freiwillige oder unfreiwillige Gefahrensituationen handelt (→ Risikokategorien). Die Zahlungsbereitschaft nimmt mit dem Grad der Freiwilligkeit ab.

Die bei der SBB verwendeten ***Grenzkosten*** K_G sind abhängig von den verschiedenen Risikokategorien und werden von K-SQ festgelegt. Sie werden auf Anfrage an die Divisionen, Konzernbereiche weitergegeben.

[4] Diese Konvention stellt einen praxisorientierten Kompromiss dar und ist aus der Erfahrung im Riskmanagement Safety vertretbar.

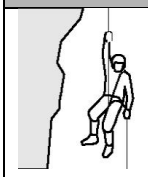
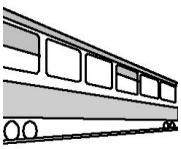
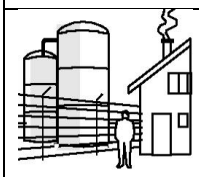
Risikokategorien		Grenzkosten [CHF / Todesopfer bzw. Verletzte]		
		Verletzte	Schwer Verletzte	Tote
	**Risikokategorie 1** Bewusst und freiwillig eingegangenes Risiko (z.B. Betreten der Gleise ausserhalb eines Bahnübergangs, Zugsurfer)			
	**Risikokategorie 2** Risiken, die den betroffenen Personen bekannt sind und durch das eigene Verhalten stark beeinflusst werden können. (z.B. Bahnübergänge, Arbeitssicherheit)			
	**Risikokategorie 3** Bekannte Risiken, die jedoch selbst kaum beeinflusst werden können (z.B. Reisender im Zug)			
	**Risikokategorie 4** Risiken die selbst kaum beeinflusst werden können (z.B. Schädigung Dritter aufgrund Unfall mit gefährlichen Gütern)			

Tabelle 1: Risikokategorien und Grenzkosten für Personenrisiken

Das sogenannte **monetarisierte Risiko R_m** berechnet sich wie folgt:

$$R_m = R_k * K_G \qquad \text{(II)}$$

Mit diesem Ansatz wird gewährleistet, dass knappe Geldmittel so eingesetzt werden, dass insgesamt eine grösstmögliche Risikoreduktion erzielt wird.

Risikoaversion gegen Ereignisse mit grossem Ausmass

Die Tatsache, dass ein Unfall mit grossem Ausmass – auch wenn das selten ist – in der Bevölkerung schlimmer empfunden wird als mehrere Unfälle mit kleinerem Ausmass, wird mit ***Risikoaversion*** bezeichnet. Berücksichtigt wird dieser Umstand bei der Berechnung der Risiken mit einem Faktor φ (Risikoaversionsfaktor), der eine Funktion des Ausmasses A ist. Dies führt zum **empfundenen Risiko R_e**:

$$R_e = R_k * \varphi = H * A * \varphi \qquad \text{(III)}$$

Folgende Ansätze für die Bestimmung von φ finden bei der SBB Anwendung:

$\varphi = 0.8 * A^{0.5}$ für Eisenbahnrisiken (IVa), bzw.

$\varphi = 0.8 * A$ für Gefahrgutrisiken (IVb)

Das monetarisierte Risiko mit Berücksichtigung der Risikoaversion ergibts sich demnach wie folgt:

$$R_m = R_e * K_G \qquad \text{(V)}$$

5.3 Risikobewältigung – integrale Massnahmenplanung

Im *dritten Schritt* – **der Risikobewältgung** – wird über die notwendigen und geeigneten Massnahmen entschieden, deren Umsetzung sichergestellt, sowie die Auswirkungen auf die Sicherheit beobachtet ("was ist zu tun?"). Wird das Risiko nicht im erwarteten Mass reduziert, werden Risikoidentifikation, -analyse und -bewertung erneut durchgeführt.

Grundsätzlich sind diejenigen Massnahmen zu ergreifen, bei denen Kosten und Massnahmenwirkung in einem sinnvollen Verhältnis zueinander stehen (Prinzip der Kostenwirksamkeit).

6 Überführung der Szenarien aus dem Riskassessment in die Risikomatrix CRM

Damit die Szenarien aus dem Riskassessment Safety (Matrix in Abbildung 2) in die Risikomatrix des Corporate Risk Managements (CRM) in Abbildung 6 übertragen werden können, sind folgende Schritte nötig:

6.1 Clusterung (Schritt 1)

Im Riskassessment Safety werden Einzelszenarien betrachtet und ausgewiesen. Diese werden zu übergeordneten Gruppen, sog. Ereignisarten zusammengefasst.

Qualitative Einteilung	Häufigkeit pro Jahr	Häufigkeitsklasse	Risikoklassen					
häufig	über 100	I	Arbeitsunfall Übrige	Arbeitsunfall Sturz; Entgleisung Rangier; Zusammenstoss R/R				
	10 bis 100	II	Bäume Äste	Anprall Rangier; Brand Rollmaterial Steinschlag Felssturz	Murgang Rutschung; Hochwasser Überschwemmungen			
gelegentlich	1 bis 10	III		Arbeitsunfall Strom; Anprall Zug/Gegenstand; Lawinen	Entgleisung RZ (S); Entgleisung GZ (S); Zusammenstoss Z/Z (S); Zusammenstoss Z/R (S); Zusammenstoss Z/R (V); Anprall Zug/Fz; Anprall Zug/Profilverletzung; Brand Gebäude	Personenunfall Ein/Aussteigen; Personenunfall Vorbeifahrt; Personenunfall Betreten Gleis; Personenunfall übrige; Unbewachte Bahnübergänge		
	0.1 bis 1	IV		Personenunfall Verlust Ladung	Entgleisung GZ (V); Zusammenstoss Z/Z (V)	Personenunfall im Zug; Personenunfall Stromschlag; Arbeitsunfall Rangier; Arbeitsunfall im Gleisbereich; Arbeitsunfall Überqueren Gleise; Entgleisung RZ (V); Zusammenstoss Z/R (T); Bewachte Bahnübergänge	Entgleisung RZ (T)	
selten	0.01 bis 0.1	V			FL-Unfall Reisende	Zugstillstand Personenunfall; Entgleisung GZ (T)	Zusammenstoss Z/Z (T); Gefahrgutbrand (S)	
	unter 0.01	VI			Panik Tunnel	Panik Personansammlung	Freisetzung Tropfen; Brand GZ Tunnel	Freisetzung tox Gas; Freisetzung Explosion; Gefahrgutbrand (>10 T); Brand RZ Tunnel; Brand unterird. Bahnhof; Erdbeben Stellwerk; Erdbeben Gebäude; Einsturz Brücke; Einsturz Gebäude

Ausmassklasse	A	B	C	D	E	F
Finanzieller Schaden in CHF	unter 10'000	10'000 bis 100'000	100'000 bis 1 Mio.	1 Mio. bis 10 Mio.	10 Mio. bis 100 Mio.	über 100 Mio.
Personenschäden	eine leicht verletzte Person	mehrere leichtverletzte P., 1 mittelschwer verletzte P.	1 schwerverletzte P.	mehrere schwerverletzte P. oder 1 Todesopfer	2 bis 10 Todesopfer oder zahlreiche Schwerverletzte	10 oder mehr Todesopfer
Qualitative Einteilung	klein		mittel		gross	

Abbildung 3: Einzelszenarien aus dem Riskassessment Safety (Beispiel aus 2013)

Beispiel: Im Bereich Arbeitssicherheit werden alle Einzelszenarien der Arbeitssicherheit zur gleichnamigen Ereignisart Arbeitssicherheit zusammengefasst / aggregiert.

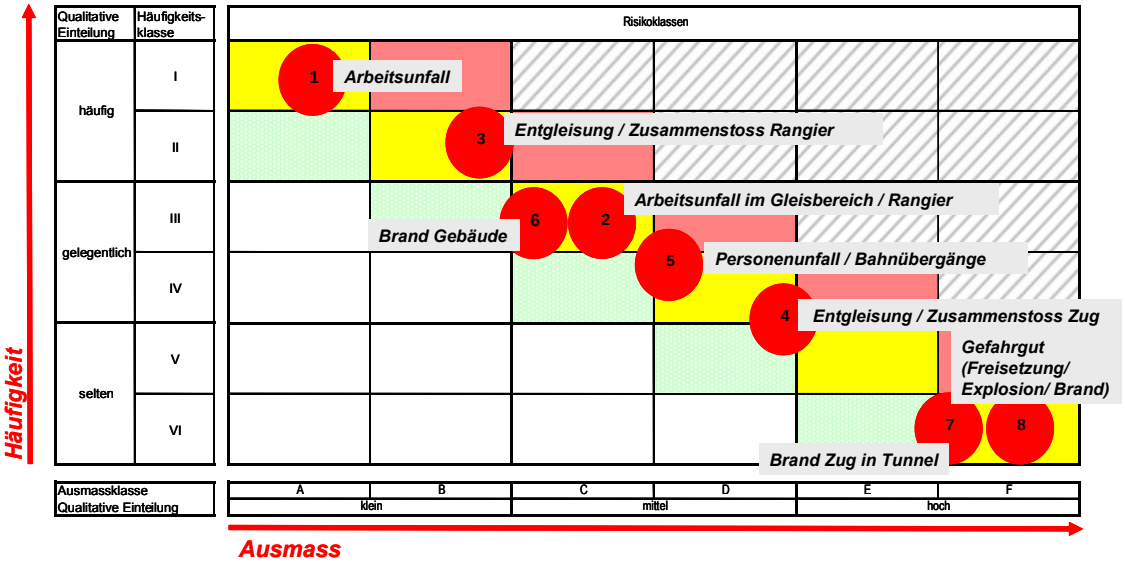


Abbildung 4: Clusterung zu Ereignisarten

6.2 Bestimmung und Monetarisierung der Ausgangsrisiken (Schritt 2)

Basierend auf den Szenarientabellen der Divisionen werden die Häufigkeiten der Einzelszenarien (Anzahl / Jahr) und deren Ausmasse folgenden sechs Klassen A – F zugeordnet.

Zur Quantifizierung der Ausgangsrisiken der einzelnen Szenarien sind die Ausmassklassen mit den **Klassenwerten** gemäss folgender Tabelle zu ergänzen:

Klasse	**finanzieller Schaden [CHF]**	**Klassenwert [CHF]**
A	unter 10'000	10'000
B	10'000 bis 100'000	100'000
C	100'000 bis 1 Mio.	1 Mio.
D	1 Mio. bis 10 Mio.	10 Mio.
E	10 Mio. bis 100 Mio.	100 Mio.
F	über 100 Mio.	300 Mio.

Die Ausgangsrisiken pro Einzelszenario werden als Produkt von Häufigkeit und Ausmass bestimmt. Die Risiken der Einzelszenarien innerhalb einer Ereignisart werden dabei zu einem Gesamtrisiko aggregiert, d.h. summiert.

Beispiel: Bestimmung der Ausgangsrisiken für die Ereignisart „Brand im Tunnel“:

			bekannt aus Riskassessment		Berechnung Ausgangsrisiko	
Ereignisart	Code	Szenario	Häufigkeit [1/J.]	Ausmassklasse	Klassenwert [CHF]	Ausgangsrisiko [CHF]
Brand	BR2	Reisezug im Tunnel	0.003	F	300'000'000	900'000
	BR3	Güterzug im Tunnel	0.004	E	100'000'000	400'000
					Summe	1'300'000

Das monetarisierte Risiko der Ereignisart „Brand im Tunnel“ beträgt somit 1.3 Mio. CHF pro Jahr (ohne Berücksichtigung einer zusätzlichen Risikoaversion).

6.3 Bestimmung der Eintretenswahrscheinlichkeit und des Ausmasses von Risiken für das CRM (Schritt 3)

Während das Riskassessment Safety auf der Anzahl gemessener oder zu erwartender Ereignisse basiert und somit die jährliche Häufigkeit von Szenarien ausweist, verwendet das CRM die Eintretenswahrscheinlichkeit eines Szenarios innerhalb des MUP (6 Jahre bei der SBB).

Die Einschätzung der Risiken für die CRM-Matrix beruht auf den Safetyszenarien mit schweren Ausmassen. Die Häufigkeit eines Risikos ergibt sich somit aus der Summe der Häufigkeiten der entsprechenden Szenarien.

Zur **Bestimmung des Ausmasses** einer Ereignisart wird wie folgt vorgegangen:

$$Ausmass = \frac{Ausgangsrisiko}{H}$$

Am **Beispiel aus 6.2** beträgt

die Häufigkeit H = 0.003 + 0.004 = **0.007 [1/J]**,

das Ausmass somit 1.3 Mio. / 0.007 = **185.7 Mio. [1/J]**

Umrechnung jährliche Häufigkeit in Eintretenswahrscheinlichkeit des MUP

Beim Übertrag in die CRM-Matrix muss die Häufigkeit aus dem Riskassessment Safety nun in die Eintretenswahrscheinlichkeit (EW) pro MUP-Periode umgerechnet werden. Ereignisse, die mehr als einmal zu erwarten sind, erreichen eine Wahrscheinlichkeit nahe 1. Das heisst, es ist nahezu sicher, dass sie eintreten werden. Ereignisse, die erfahrungsgemäss 1x, 10x oder gar 100x eintreten, unterscheiden sich kaum mehr in ihrer Wahrscheinlichkeit. Eine Umrechnung erübrigt sich, die EW entspricht der Wahrscheinlichkeitsklasse „sehr gross“.

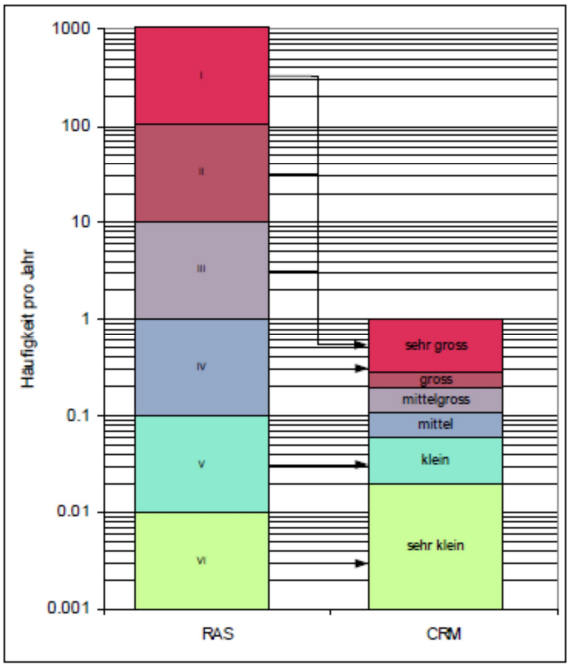


Abbildung 5: Übertragung der Häufigkeiten gem. Risikomatrix Riskassessment Safety (RAS) in die Wahrscheinlichkeitsklassen gem. CRM

Bei Szenarien, deren Häufigkeit kleiner als 1x pro Jahr ist, muss eine Umrechnung[5] erfolgen. Demnach entspricht eine Wahrscheinlichkeit >85% in der CRM-Matrix gemäss Wahrscheinlichkeitsrechnung einer Häufigkeit von > 0.27 pro Jahr in der Matrix des Riskassessment Safety.

Beispiel aus 6.2:

Häufigkeit der Szenarien total [1/J] = 0.007. Dies entspricht gemäss der Umrechnung einer *Eintretenswahrscheinlichkeit* in 6 Jahren von 1-(1-0.007)^6 = 0.041 = **4.1%**

Ausmass = **185.7 Mio. CHF**

6.4 Eintrag in die Risikomatrix CRM (Schritt 4)

Das ermittelte Ausmass wird nun der Ausmassklasse und die EW der Häufigkeitsklasse der Risikomatrix CRM zugeordnet. Positionierung des Beispiels (Ereignisart „Brand im Tunnel“):

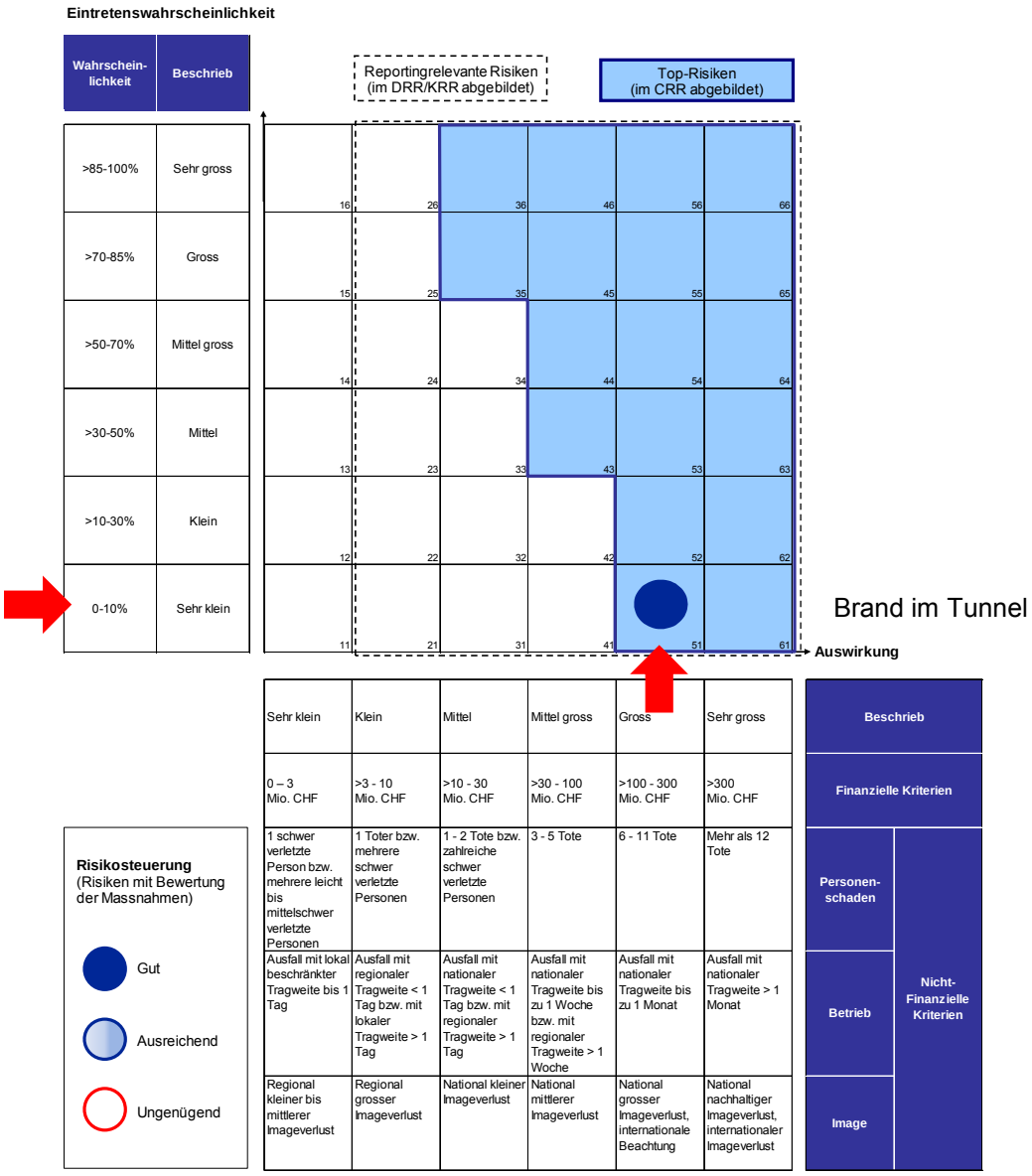


Abbildung 6: Eintrag Safetyrisiken in die Risikomatrix CRM

[5] Die Wahrscheinlichkeit, dass ein Ereignis innerhalb von 6 Jahren auftritt, errechnet sich anhand der Wahrscheinlichkeit pro Jahr (p) wie folgt: $p_6 = 1-(1-p)^6$. Konkretes Beispiel: Wahrscheinlichkeit im MUP bei jährlicher Wahrscheinlichkeit von 0.27: 1-(1-0.27)^6 = 0.85

7 Anwendungen des Riskmanagement Safety bei der SBB AG im Überblick

Anwendungen	Ziel / Zweck	Schwerpunkte (zB Betriebs-sicherheit / Arbeitssicherheit)	Unternehmensebene / Ausrichtung (präventiv od. reaktiv))	Weiterführende Dokumente
Generelles Riskassessment				
Generelles Riskassessment Safety SBB	Erstellung Überblick über die Safetyrisiken bei der SBB	Safety generell	Strategisch, unternehmensweit präventiv	
Spezifisches Riskmanagement				
Spezifisches Riskmanagement	Riskmanagement quantitativer Schwerpunkte, sowie safetyrelevanter Änderungen	Safety generell	Operativ präventiv	K 250.0 Umgang mit sicherheitsrelevanten Änderungen
Ereignisanalyse EA	Beurteilung, ob das Risiko nach einem Ereignis akzeptierbar ist	Safety generell	Operativ (Prozess / Arbeitsplatz) Auslöser reaktiv; Zielrichtung präventiv	R K 203.1
Methode Suva zur Beurteilung von Risiken an Arbeitsplätzen und Arbeitsabläufen	Beurteilung von Risiken an Arbeitsplätzen und Arbeitsabläufen	Arbeitssicherheit	Operativ (Prozess / Arbeitsplatz) Auslöser extern; Zielrichtung präventiv	SUVA Bestellnr. 66099
Screening Personen- und Umweltrisiken	Beurteilung von Risiken aus dem Transport gefährlicher Güter	Safety Transport gefährlicher Güter TgG	Operativ (TgG) präventiv, periodisch	SR 814.012 Störfallverordnung StFV
Das Risikokonzept als Basis für die Beurteilung von technischen Risiken zum Schutz von Reisenden und Angestellten	Beurteilung von technischen Risiken zum Schutz von Reisenden und Angestellten insbesondere bereits bestehender Anlagen	Safety generell	Operativ (technische Risiken) präventiv	Sicherheit bei SBB, I-SA Das Risikokonzept
Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)	Beurteilung technischer Risiken neuer Anlagen oder ganze Systeme (z.B. neue Stellwerke, neue Software etc.) im Rahmen von Typenzulassungen, Sicherheitsbescheinigungen etc.	Safety generell	Operativ (technische Risiken) Auslöser extern, Zielrichtung präventiv	EN 50126

8 Tools des Riskmanagement Safety bei der SBB im Überblick

Bei den einzelnen Schritten des Riskmanagements sind bei der SBB die Tools gemäss folgender Darstellung anzuwenden. Es ist zentral, dass die Risiken nach einer einheitlichen Grundphilisophie beurteilt werden, weshalb sich die Anwendung der Tools beschränkt.

Welche der Tools eingesetzt werden, ist abhängig von der zu bearbeitenden Fragestellung. Innerhalb der einzelnen Schritte kann auch ein Mix sinnvoll sein.

Zusätzlich zur Anwendung kommende Tools sind mit K-SQ zu vereinbaren.

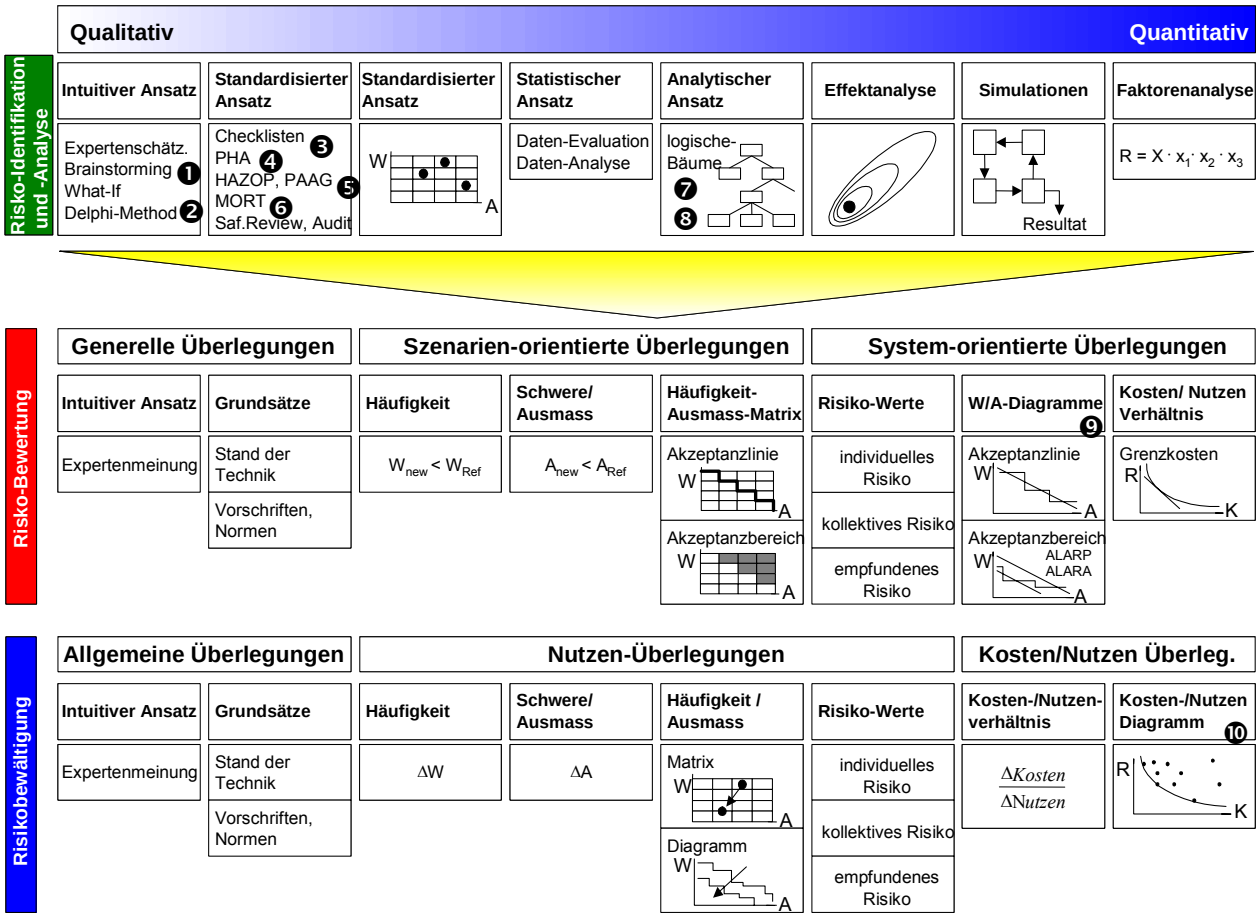


Abbildung 7: Riskmanagement Tools

Die gängigsten bei den SBB eingesetzten Tools (Ziffern 1 bis 10) werden im folgenden Anhang genauer erläutert.

K-SQ

K-SQ-RKD

sig. Hans Vogt
Leiter Sicherheit und Qualität

sig. Joëlle Vouillamoz
Leiterin Risiko- und Datenmanagement

Änderungsverzeichnis

Version	Gültig ab	Kapitel	Änderung
1-0	01.02.2014		Überführung vom SMS Konzern ins Regelwerk.
2-0	01.09.2015	5.2 6	Ergänzt um Bestimmug der Risikoakzeptanz-bereiche und Skalierung zur Unternehmens-grösse. Ergänzung des Kapitels „Überführung der Szenarien aus dem Riskassessment in die Risikomatrix CRM“.

Anhang: Tools Riskmanagement Safety

Einfache Anwendungen

Beim Startpunkt aller Risikoüberlegungen ist eine allgemeine Unterscheidung zwischen einfachen und komplexen Anwendungen angezeigt. Für einfache Anwendungen/Probleme mit geringer Komplexität und/oder kleinem Schadenpotenzial genügt in der Regel eine Grobrisikoanalyse (Analyse mittels Checklisten, Gewichtungstabellen etc.; entsprechende Hilfsmittel vgl. Anhang).

Eine Grobrisikoanalyse liefert überwiegend qualitative Aussagen zur Risikosituation. Nach deren Bewertung mittels geeigneten Massstabs sind den grössten Risiken mit entsprechenden Massnahmen zu begegnen oder Detailfragen gezielt anzugehen. In der Grobrisikoanalyse sind unter anderen folgende Fragen zu beantworten:

- Können Risiken zum Vornherein erkannt werden?
- Sind Eintretenswahrscheinlichkeit und Schadenpotenzial hoch?
- Können Fehler zu unabsehbaren Konsequenzen führen?

Praxis-Tipp

Eine Grobrisikoanalyse kann im Normalfall durch den Projektleiter selbst oder in Form einer Gruppenarbeit von entsprechenden Personen unter seiner Leitung erstellt werden. Eine Gruppenarbeit ist auf jeden Fall vorzuziehen. Der Projektleiter entscheidet aufgrund des Resultates der Grobrisikoanalyse oder aufgrund seiner Erfahrung in ähnlichen Anwendungen, ob eine Detailrisikoanalyse notwendig ist.

Komplexe Anwendungen

Für umfangreiche und entsprechend komplexe Anwendungen/Probleme ist eine Detailrisikoanalyse erforderlich. In einem solchen Fall ist zusätzlich zum projektspezifischen Wissen ein analytisches Know-how bezüglich Ablauf und Durchführung von Risikoanalysen unumgänglich.

Im Sinne einer umfassenden "Risikolandschaft" mit vergleichbaren Risiken und zur Gewährleistung eines integrierten Riskmanagements sind die Spezialisten vom Konzernbereich Sicherheit und Qualität Ansprechpartner und sollten durch die Projektleiter beigezogen werden.

Tools Risikoanalyse - Intuitiver Ansatz

❶ BRAINSTORMING

Risikoidentifikation und -analyse

Beschreibung

- Beim klassischen Brainstorming nehmen verschiedene Teilnehmer an einer gemeinsamen kurzen, von einem Moderator (kann auch der Projektverantwortliche sein) geleiteten Sitzung teil.
- Die Ideen werden spontan und unstrukturiert vorgetragen und in einer nächsten Phase (Auswertungsrunde) geprüft und verschiedenen Kategorien zugeordnet (z.B. K.O.-Risiken, belastende Risiken, nicht zu beachtende Risiken, zu prüfende Risiken).
- Die Diskussion der Ideen und deren Beurteilung können auch unter Zuzug von Fachleuten erfolgen, auch wenn diese beim eigentlichen Brainstorming nicht anwesend waren.
- Die Beiträge der Teilnehmer werden für alle sichtbar festgehalten.
- Die Mitwirkung verschiedener Teilnehmer (Experten, Laien, verschiedene Hierarchiestufen) verbreitert das Spektrum und ist erwünscht.
- Die Voten Ideen der einzelnen Teilnehmer werden für alle sichtbar festgehalten.
- Variante: What-if-Methode
  Konkrete Fragestellung "Was passiert wenn…?", Beantwortung im Team

Resultat

Das Ergebnis eines Brainstormings ist eine Zusammenstellung von möglichen Gefahren und/oder Massnahmen.

+ / -

+ Einfache, spontane Methode
+ Mit relativ geringem Aufwand kann ein erster guter und umfassender Überblick erhalten werden
+ Unkonventionelle Ansätze werden durch Kreativität der Methode gefördert
+ Ausnutzung von Synergieeffekten infolge der Gruppenbildung
- Ergebnis ist stark von den beteiligten Personen abhängig
- Garantie, dass alle wichtigen Aspekte eines Systems / Projekts erkannt und beschrieben werden, ist nicht gegeben

Anwendung

- Brauchbar als Einstieg in ein Thema/Projekt, um das Feld der Lösungsansätze abzustecken
- Für Problemarten einfacher Komplexität
- Geeignet zur Sammlung von Ideen
- Methode zur Identifikation und Analyse von Gefahren
- Generieren von Massnahmen

❷ DELPHI-METHODE

Risikoidentifikation und -analyse

Beschreibung

- Systematische, mehrstufige Befragung (anonym, schriftlich) von Experten mit Rückkopplung das dazu dient, eine Schätzmethode, zukünftige Ereignisse, Trends, technische Entwicklungen und dergleichen möglichst gut einschätzen zu können.
- Durch die Anonymität der Befragung wird in einer ersten Phase die Beratung zwischen den Experten bewusst unterdrückt, um die gegenseitige Beeinflussung zu vermeiden.
- Ziel der Befragung ist es, möglichst zuverlässige und weitgehend übereinstimmende Ansichten einer Expertengruppe zu einer Problemstellung zu erhalten.
- Die erste Befragung erfolgt mit einem vorbereiteten Fragebogen.
- Bei gravierenden Diskrepanzen erfolgen weiteren Befragungsrunden, in welchen die Ergebnisse der jeweils vorangehenden Runden eingehen.
- In weiteren Befragungsrunden wird eine gewisse Angleichung der Meinungen erfolgen. Durch diesen Vorgang können extreme oder nicht plausible Meinungen ausgemerzt werden.
- Von allen Schätzungen werden die Mittelwerte errechnet und als finale Schätzung präsentiert.

Resultat

Das Ergebnis einer Delphi-Befragung sind angeglichene Meinungen verschiedener Experten zu Eintretenswahrscheinlichkeiten und möglicher Schadenshöhen.

+ / -

+ Durch wiederholte Konfrontation mit der eigenen Prognose und den Prognosen anderer sowie die Begründung derselben bei starken Abweichungen erfolgt eine besonders intensive Auseinandersetzung mit der Problemstellung.
+ Möglichkeit zum Einbezug von verschiedenen Experten in die Befragung (unabhängig von Zeit und Ort)
+ Kein Gruppenzwang oder Prestigedenken zu befürchten.
+ Durch den Einbezug der Experten in einen Konsensfindungsprozess wird das Ergebnis mitgetragen.
- Durchführung ist personal- und zeitintensiv und somit auch kostenintensiv.
- Starke Abhängigkeit der Methode von der Eignung des Befragers (Delphisten).
- Ungeeignet, wenn Resultate schnell vorliegen müssen.

Anwendung

- Einsatzgebiet heute vorwiegend bei techn. Entwicklungen
- Geeignet bei ungenügender Datenlage und wenn die Expertenschätzung alleine zu wenig präzis ist.

Tools Risikoanalyse - Standardisierter Ansatz

❸ CHECKLISTENVERFAHREN

Risikoidentifikation und -analyse

Beschreibung

- Das Checklistenverfahren ist eine einfache, rein qualitative Methode und eignet sich sehr gut für eine erste Einsichtnahme in ein Projekt / System. Verwendung als vorbereitende Analysemethode oder in Kombination mit anderen Methoden.
- In einer Checkliste (Frageliste) werden eine Vielzahl von Merkmalen und Ausprägungen zu einem abgegrenzten Themengebiet gesammelt und strukturiert dargestellt.
- Checklisten beinhalten über lange Jahre gesammelte Erfahrungen in den jeweiligen Bereichen und werden laufend fortgeschrieben.

Resultat

Listen mit „kritischen“ Systemkomponenten, -zuständen, Abläufen, die in einer späteren Projektphase gefährlich werden können. Checklisten bilden die Basis für weitergehende Analysen.

+ / -

+ Einfache Methode, einfacher Aufbau und breite Anwendungsmöglichkeiten.
+ Mit geringem Aufwand kann ein erster guter und umfassender Überblick erhalten werden, der eine Vielzahl an möglichen Sicherheitsproblemen aufzeigt.
- Bei komplexen Problemen aufgrund der Übersichtlichkeit weniger geeignet. Ausgereifte Checklisten fehlen oft.
- Garantie, dass alle wichtigen Aspekte eines Systems / Projekts erkannt und beschrieben werden, ist nicht gegeben.
- Probleme aus der Kombination prozessspezifischer Gegebenheiten können nur ungenügend erfasst werden.
- Qualität der Analyse hängt stark von der Vollständigkeit der Checklisten sowie vom Wissen der am Checklistenverfahren beteiligten Personen ab.
- Checklisten können sehr schnell umfangreich werden (Übersichtlichkeit nicht gewährleistet).

Anwendung

- Methode zur Analyse technischer Systeme / Prozesse
- Methode zur Identifikation und Analyse von Gefahren
- Anwendung, wenn Ergebnisse einer Risikoidentifikation anderen Projektmitgliedern dienen sollen
- Geeignet für routinemässige, sich wiederholende Überprüfungen

❹ PHA Preliminary Hazard Analysis

Risikoidentifikation und -analyse

Beschreibung

- PHA = Vorläufige/einleitende Gefahrenanalyse
- PHA ist eine Erweiterung des Checklistenverfahrens indem sowohl ereignisverursachende Komponenten als auch entsprechende Massnahmen berücksichtigt werden.
- Das Ziel der PHA ist, sicherheitskritische Bereiche zu erkennen und erste Bewertungen von Gefahren zu liefern, sowie dazu benötigte adäquate Gefahrenkontrollen und Massnahmen zu definieren.
- Sie besteht typischerweise aus einem Brainstorming, in dem der vorläufige Entwurf auf der Basis der Erfahrung der an dem Brainstorming beteiligten Personen diskutiert wird.
- Eine vorgegebene Tabelle sorgt für einen formalisierten und strukturierten Aufbau der Analyse.

Resultat

Ergebnis sind strukturierte Tabellen, in denen die Gefahren eines Prozesses und die dagegen vorgesehenen Massnahmen qualitativ beschrieben sind.

+ / -

+ Einfache Methode, einfacher Aufbau und breite Anwendungsmöglichkeiten.
+ Mit geringem Aufwand kann ein erster guter und umfassender Überblick erhalten werden, der eine Vielzahl an möglichen Sicherheitsproblemen aufzeigt.
- Bei komplexen Problemen aufgrund der Übersichtlichkeit weniger geeignet. Ausgereifte Checklisten fehlen oft.
- Garantie, dass alle wichtigen Aspekte eines Systems / Projekts erkannt und beschrieben werden, ist nicht gegeben.
- Probleme aus der Kombination prozessspezifischer Gegebenheiten können nur ungenügend erfasst werden.
- Qualität der Analyse hängt stark von der Vollständigkeit der Checklisten sowie vom Wissen der am Checklistenverfahren beteiligten Personen ab.
- Checklisten können sehr schnell umfangreich werden (Übersichtlichkeit nicht gewährleistet).

Anwendung

- Methode zur Analyse technischer Systeme / Prozesse
- Methode zur Gefahren-/Ursachen und Ereignisidentifikation insb. in der Konzeptphase
- Identifikation und Beschreibung von Massnahmen

Teilsystem: *Wagen (Wa)* **Betriebsart:** *normal*
Subsystem: *Reisewagen (rw)*

Gefahr (Gefahrenquelle, Energie)	Index A	Anlass für Gefährdung	Gefährdung durch Interaktion mit	Index U	Ursache für Ereignis (auslösende Faktoren)	Ereignis	Auswirkungen Primärereignis	Primär-ereignis-szenarien
Brennbare Materialien	rw-1	Personentransport	Zündquellen im Reisewagen	rw-1	Technisches Versagen (z.B. el. Anlagen, Festbremsung, Heissläufer)	Brand in Reisewagen	• Hitze • Rauch • Verletzung • Tod	B-2
				rw-2	Menschliches Verhalten (fahrlässige Handhabung mit brennbaren Materialien, Vandalismus oder Sabotage, etc.)			
Fahrender Reisezug			Fahrbahn	rw-1	Technisches Versagen im Bereich Drehgestell (Heissläufer, Radscheiben- und Achsbruch, etc.)	Entgleisung eines Reisezuges Zusammenstoss Reisezüge Zusammenstoss RZ/GÜZ	• Mechanische Auswirkungen • Verletzung / Tod von Personen	E-1 Z-1 Z-2
				rw-2	Menschliches Verhalten (Vandalismus, Sabotage, Fehlverhalten Unterhalt)			
Wagentüre an fahrendem Reisezug			Passagieren	rw-1	Technisches Versagen Türverriegelung, keine Türverriegelung	Sturz aus dem fahrenden Zug	• Verletzung • Tod	P-1
				rw-2	Menschliches Verhalten (Betätigung der Notentriegelung, Irrtum Türverriegelung)			
Reise- und Güterverkehrssystem	rw-2	Menschliches Verhalten	Passagieren		U-rw-1, U-rw-2	Partieller Betriebszusammenbruch	Psychische und physische Belastung Personen (z.B. Verlassen des stehenden Zuges)	Bz-1

Abbildung 8: Strukturierte PHA-Tabelle; Auszug aus Sicherheitskonzept Gotthard-Basistunnel

Tunnel: **Ausgestaltung für die Rettung**	**Wirkung***	**Rohbaurelevanz****	**Index**
Ersteller/Status:	A↓	x	Bau_A20.01

Ausmassmindernde Massnahme:

Bereiche: Bauten	Bereiche: Bahntechnik	Bereiche: Rollmaterial	Bereiche: Betrieb	Teilsystem / Subsystem	Beeinflusste Ereignisse / Auswirkungen
x				Tunnel	Anzahl geretteter Personen bei allen Ereignissen

Beschreibung / Literatur:

- **Seitenwege**
  In beiden Einspurtunneln ist auf der Seite der Querschläge ein begehbares, hindernisfreies Bankett (Höhe über SOK: min. 35 cm) von min. 1.0 m Breite angeordnet, das als Fluchtweg für die Selbstrettung dient. Die Fluchtwege sind an der Tunnelwand mit Handläufen ausgerüstet.
- **Tunnelbeleuchtung**
  Die Tunnelbeleuchtung ist sektoriell unterteilt und kann von der Betriebsleitzentrale (FstZ), lokal im Tunnel über Handtaster und an den Verteilerstandorten und den Tunnelportalen über Schlüsselschalter eingeschaltet werden.
- **Beschilderung**
  Ca. alle 100 m ist ein Hinweisschild angebracht, welches den nächsten Weg zu den Querschlägen, zum Portal bzw. zu den Nothaltestellen weist.

Generelle Wirkung:

Die vorgesehenen Massnahmen ermöglichen eine wirkungsvolle Selbst- und Fremdrettung (genügende Platzverhältnisse und Ausleuchtung, hohe Fluchtgeschwindigkeiten, Rettung und Evakuation in Nachbarröhre).

Zusätzliche Angaben:

Tunnelröhre: Ausgestaltung für Selbst- und Fremdrettung (A1.2)

Abbildung 9: Massnahmenblatt; Auszug aus Sicherheitskonzept Gotthard-Basistunnel

❺ HAZOP / PAAG

Risikoidentifikation und -analyse

Beschreibung

- Die HAZOP (Hazard and Operability) ist ein qualitatives Verfahren; auch PAAG-Verfahren (**P**rognose, **A**uffinden der Ursache, **A**bschätzen der Auswirkungen, **G**egenmassnahmen) genannt.
- Der Schwerpunkt liegt in der mit Hilfe von Leitwörtern systematisierten Nutzung von Wissen und Erfahrung eines Expertenteams über eine Anlage um mögliche Gefahren und Betriebsstörungen zu erkennen.
- Die HAZOP wird von einem Team durchgeführt, das alle am Prozess beteiligten Fachleute zusammenfasst.
- Anlagen werden in Teilsysteme unterteilt. Die "Sollfunktion" eines Anlageteils wird mit Hilfe von Leitwörtern (kein, mehr, weniger, anders,…) hinterfragt.

Resultat

Das Ergebnis einer HAZOP-Analyse ist eine Liste der möglichen Gefahren und Betriebsstörungen sowie Vorschläge zu Gegenmassnahmen. Die Auslegung einer Anlage kann so verbessert werden.

+ / -

+ Systematische Vorgehensweise für die Gefahrenanalyse
+ HAZOP vereinigt Fachleute der Planung und des Bauprozesses. Dies fördert das Systemverständnis und deckt Schnittstellenprobleme auf.
- Externe Anlageneinflüsse werden meist nicht betrachtet.
- Einfache Fragestellung (Leitwörter) kann dazu führen, dass gefährliche oder komplexe Ereignisketten unerkannt bleiben.
- Gefahren, welche sich aus gleichzeitigem Versagen mehrerer Komponenten ergeben, werden nicht systematisch aufgedeckt.
- Arbeits- und zeitaufwändig, da ein Anlagenteil nach dem anderen untersucht wird. Umfangreiche Unterlagen (Handbücher, Schemata, Betriebsvorschriften...) sind notwendig.

Anwendung

- Identifikation und Analyse von Gefahren und Schwachstellen.
- Generieren von Massnahmen aufgrund der Gefahrenanalyse.
- Ausrichtung auf Erhöhung der Zuverlässigkeit, weniger auf Ermittlung der Risiken eines Systems
- Idealer Zeitpunkt liegt vor dem definitiven Abschluss der Entwurfsphase einer Anlage. Die Anlagenbeschreibung ist bereits vollständig und es besteht die Möglichkeit Änderungen in Konstruktion und Auslegung der Anlage.

Normen

IEC 61882 Hazard and operability studies (**HAZOP** studies) - Application guide

❻ FMEA Risikoanalyse

Beschreibung

- Failure Method And Effects Analysis = Fehlermöglichkeits- und Einflussanalyse
- Dient der qualitativen Bewertung von Systemen hinsichtlich des Ausfalls von Teilsystemen oder einzelner Komponenten. Das Auffinden von Schwachstellen steht im Vordergrund. Versagen von Komponenten mit grosser Auswirkung auf das Gesamtsystem sollen ausfindig gemacht werden.
- Zerlegung eines Gesamtsystems in einzelne Subsysteme / Komponenten. Systematische Betrachtung der Ausfallarten jedes Subsystems und deren Auswirkungen auf das Gesamtsystem.
- Beurteilung der Ausfallwahrscheinlichkeit und der Auswirkungen eines Komponenten- oder Subsystemausfalls erfolgt semiquantitativ.
- Ausfallwahrscheinlichkeit und Auswirkung bei einem Komponentenausfall werden in einer Matrix

Resultat

Das Ergebnis einer FMEA sind Formulare, auf denen mögliche Gefahren bzw. Schwachstellen der Komponente oder des Teilsystems, mögliche Ursachen, vorhandene Massnahmen und Ausfallwirkungen auf das System festgehalten sind. Für diese einzelnen Gefahrenszenarien werden die Eintretenshäufigkeit und das Ausmass abgeschätzt und in einem Häufigkeits-Ausmass-Diagramm (Matrix) festgehalten.

+ / -

+ FMEA ist leicht verständlich, standardisiert, nicht mathematisch und leicht anwendbar.
+ Die FMEA ist in allen Bereichen der Technik anwendbar
- Die FMEA geht von Ausfällen einzelner Komponenten und Subsysteme und nicht von den Ausfallkombinationen aus. Solche Ausfallkombinationen bzw. Verkettungen werden oft ungenügend erfasst.
- Grosser zeitlicher Aufwand.

Anwendung

- Identifikation von Gefahren und Schwachstellen
- Grundlage zur Abschätzung von Häufigkeit und Ausmass

Normen

SN EN 60812 Analysetechniken fü rdie Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und auswirkungsanalyse (FMEA)

Tools Risikoanalyse - Analytischer Ansatz

❼ FTA Fehlerbaumanalyse | **Risikoidentifikation und -analyse**

Beschreibung

- Fault Tree Analysis = Fehlerbaumanalyse ist ein deduktives Verfahren, um die Wahrscheinlichkeit eines Ausfalls zu bestimmen
- Die FTA ist ein Hilfsmittel zur Ermittlung logischer Verknüpfungen von Komponenten- oder Teilsystemzuständen eines Systems, die zu einem unerwünschten Ereignis führen können (Top Event).
- Systematische Identifizierung aller Ausfallkombinationen, die zu einem vorgesehenen Top-Event führen können.
- Die Quantifizierung der Beziehungen führt zur Ermittlung der Eintretenswahrscheinlichkeit eines Top-Events.
- Vorgehensweise mittels Top-Down - Ansatz mit Top-Event als Systemzustand:
  - Festlegen Top Event (z.B. aus Checklistenverfahren)
  - Identifikation aller Ereigniskombinationen die zum Top Event führen
  - Ermittlung und Zuweisung von Kenngrössen zu jedem Basisereignis
  - Berechnung der Gesamteintrittswahrscheinlichkeit des Top Events

Resultat

Das Ergebnis einer Fehlerbaumanalyse sind quantitative Angaben zur Häufigkeit von Ereignissen. Die Darstellung anhand eines logischen Baumes zeigt die Verknüpfung und Abhängigkeiten in einem System.

+ / -

+ Methode liefert quantitative Aussagen.
+ Durch die Erarbeitung des log. Fehlerbaums wird das Verständnis für Zusammenhänge in einem System gefördert.
- Komplizierte und stark verzweigte Fehlerbäume bei komplizierten Systemen.
- Bei fehlendem statistischen Material ist oftmals Expertenwissen notwendig.
- Beizug von Experten (Ingenieurbüro) mit entsprechenden Softwaretools meist unumgänglich.
- Grosser zeitlicher Aufwand.

Anwendung

- Anwendung bei der Planung neuer (Systementscheid Zimmerberg-Basistunnel) wie auch bei der Analyse bestehender Systeme (Risikoermittlung gemäss Störfallverordnung für Propangastankanlagen zur Weichenheizung) sowie zur Untersuchung im Versagensfall.
- Analyse aller technischer Systeme
- Analyse der Ursachen unerwünschter Ereignisse
- Bestimmung von Häufigkeiten unerwünschter Ereignisse
- Zeigt Ansatzpunkte für Massnahmen

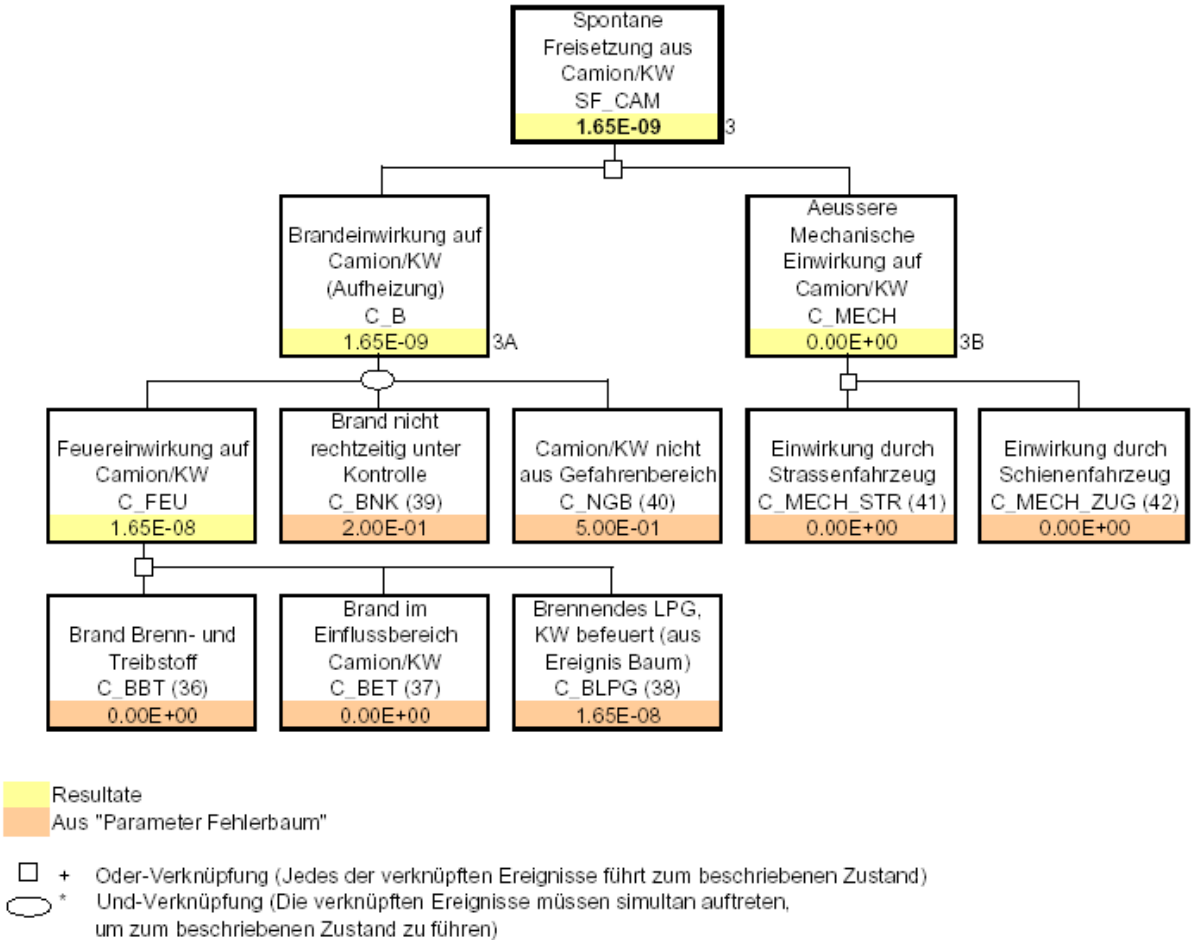


Abbildung 10: Fehlerbaum; Auszug aus Risikoermittlung für eine Propangastankanlage

Normen

DIN 25424-1 Fehlerbaumanalyse; Methode und Bildzeichen

DIN 25424-2 Fehlerbaumanalyse; Handrechenverfahren zur Auswertung eines Fehlerbaumes

❽ ETA Ereignisbaumanalyse

Risikoidentifikation und -analyse

Beschreibung

- Event Tree Analysis = Ereignisbaumanalyse ist ein induktives Verfahren, welches mögliche Folgen eines auftretenden Fehlers bestimmen soll.
- In der ETA werden (Folge-)Ereignisse ermittelt, die sich aus einem vorgegeben Ausgangsereignis entwickeln können (induktive Analyse).
- Erfassen der Ereignisabläufe in einem grösseren System, die nach einem auslösenden Ereignis durch die Reaktion nachfolgender Subsysteme entstehen können.
- Die Folgen werden bis zu einem Endzustand des Systems verfolgt.
- Jedes Ereignis in dieser Kette hat die Folgen der vorausgehenden Ereignisse zu tragen.
- Vorgehen:
  - Festlegen des auslösenden Ereignisses
  - Identifizierung der Folgenverkettung und Darstellung in einem Baum mit logischen Verknüpfungen
  - Zuweisung von Eintretenswahrscheinlichkeit für das auslösende Ereignis (z.B. aufgrund FTA) und der bedingten Wahrscheinlichkeiten für die Funktion bzw. nicht Funktion der Subsysteme
  - Berechnung der Eintretenswahrscheinlichkeit des Endzustandes

Resultat

Das Ergebnis einer Fehlerbaumanalyse sind quantitative Angaben zur Häufigkeit von Ereignissen.

Die Darstellung anhand eines logischen Baumes zeigt die Verknüpfung und Abhängigkeiten in einem System.

+ / -

+ Scharfe, quantitative Aussagen
+ Zeigt und strukturiert die möglichen Folgen eines Ereignisses systematisch
- Komplizierte und stark verzweigte Fehlerbäume bei komplizierten Systemen.
- Bei fehlendem statistischen Material ist oftmals Expertenwissen notwendig.
- Beizug von Experten (Ingenieurbüro) mit entsprechenden Softwaretools meist unumgänglich.

Anwendung

- Beschreibung und Quantifizierung von Ereignisabläufen aller Art
- Bevorzugter Einsatz bei Untersuchungen von Störungen und Störfällen in techn. Systemen
- Analyse der Abläufe (Folgen) von Ereignissen
- Bestimmung der Häufigkeit von Ereignissen
- Zeigt Ansatzpunkte für Massnahmen in einem System

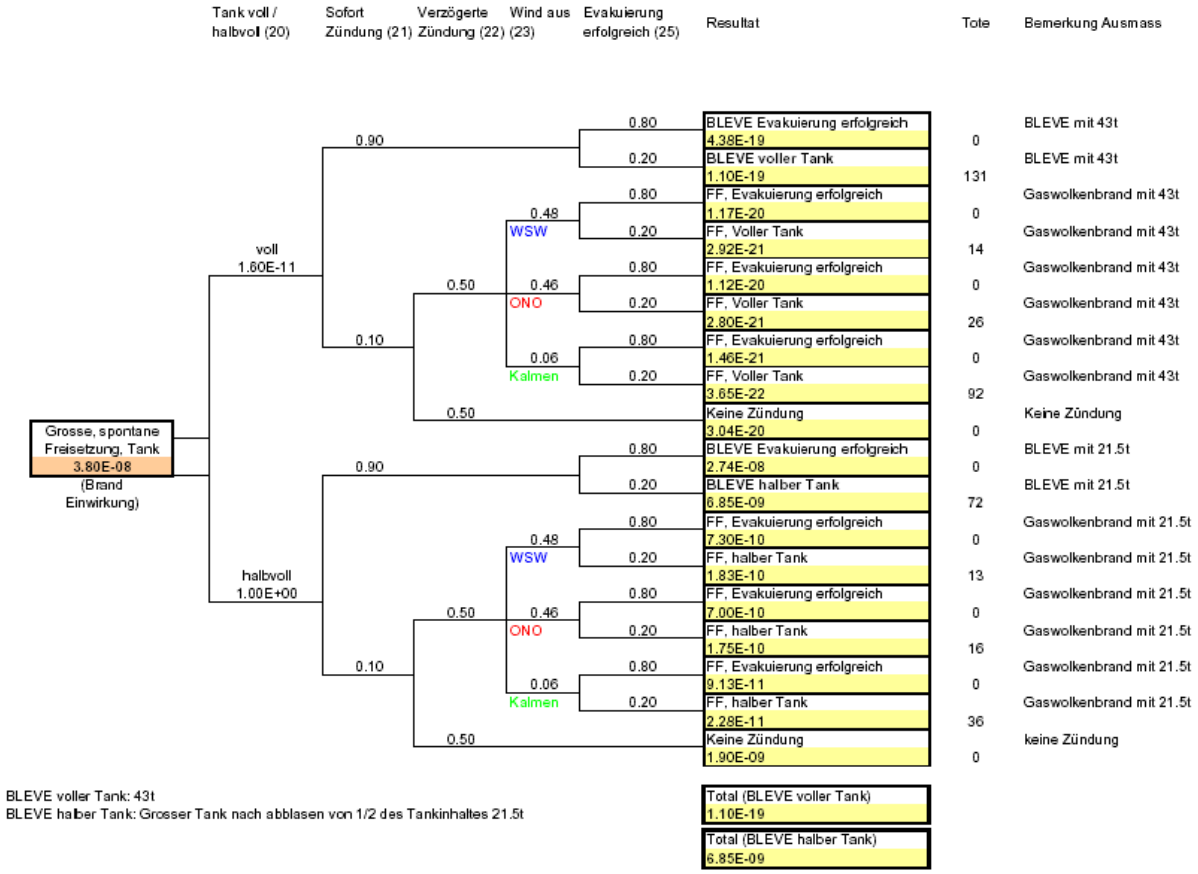


Abbildung 11: Ereignisbaum; Auszug aus Risikoermittlung für eine Propangastankanlage

Normen

DIN 25419 Ereignisablaufanayse; Verfahren, graphische Symbole und Auswertung

Tools Risikobewertung – W/A-Diagramm ⑨

Nach der Risikoanalyse (Abschätzung der Eintretenswahrscheinlichkeit und des Ausmasses) mittels obiger Methode(n) erfolgt die Risikodarstellung und –bewertung.

Darstellung der Risiken

Eine gängige Form der Risikodarstellung ist die Darstellung der kumulativen Häufigkeitsverteilung mittels Summenkurve in einem doppelt-logarithmischen W/A-Diagramm (Wahrscheinlichkeits-Ausmass-Diagramm). Durch Summation der Häufigkeiten über alle Szenarien, deren Schadensausmass grösser oder gleich einem vorgegebenen Wert ist, kann die kumulative Häufigkeit für jedes Schadenausmass ermittelt werden.

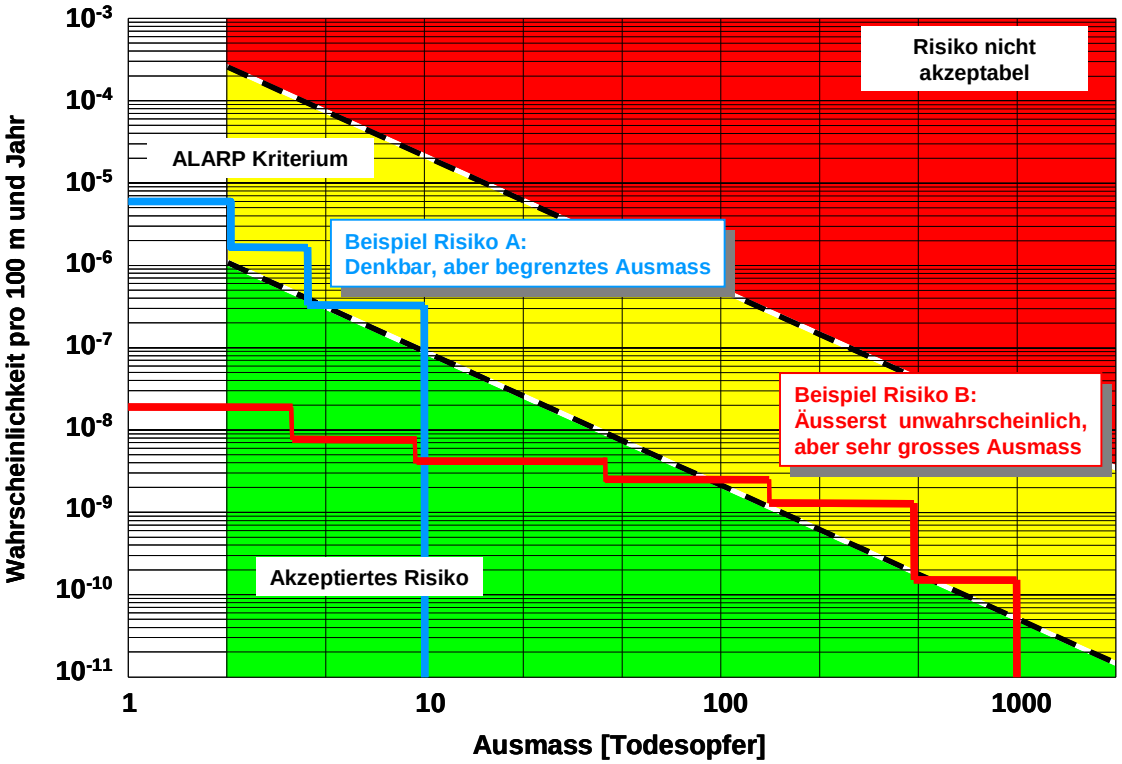


Abbildung 12: Exemplarische Risikosummenkurven im W/A-Diagramm

Für Risiko A sind Szenarien risikobestimmend, die häufiger vorkommen, deren Ausmass jedoch begrenzt ist (zB Entgleisung eines Zuges). Bei Risiko B werden Risiken dargestellt, welche unwahrscheinlich sind, bei Eintreten jedoch mit grossen Schäden (Todesopfer) zu rechnen ist (zB Brand eines Zuges im Tunnel).

Im obigen Beispiel liegen bezüglich Risikobewertung beide Risiken zwar im gleichen Beurteilungsbereich (hier Übergangs- oder ALARP-Bereich), da jedoch völlig andere Risikoszenarien hinterlegt sind, sind auch entsprechend andere Massnahmen zu treffen.

Risikobewertung am Bsp. Personenrisiken aufgrund des Transports gefährlicher Güter

Für die Risikobewertung der Transporte von Gefahrgütern auf der Bahn bestehen in der Schweiz einheitliche, quantitative Beurteilungskriterien. Diese erlauben eine Beurteilung der Tragbarkeit der Risiken für die Bevölkerung (und die Umwelt) infolge von Störfällen beim Transport gefährlicher Güter. Für die Beurteilung der Personenrisiken gelten folgende Grundsätze:

- Für die Beurteilung der Tragbarkeit des Risikos wird das W-A-Diagramm in drei Bereiche unterteilt: Bei der Definition der Grenzen zwischen den drei Bereichen wird eine Risikoaversion gegenüber Katastrophenereignissen berücksichtigt. So muss die Eintretenshäufigkeit eines Ereignisses mit einem

zehnfach höheren Schadenausmass nicht nur um einen Faktor 10, sondern sogar um einen Faktor 100 tiefer liegen.

- Einen nicht akzeptablen Bereich, einen Übergangsbereich und einen akzeptablen Bereich (vgl. Abbildung 13).
- Liegen Teile der Summenkurve im nicht akzeptablen Bereich, so ist das Risiko nicht tragbar und die Vollzugsbehörde ordnet die erforderlichen zusätzlichen Massnahmen an (nötigenfalls auch Verkehrsbeschränkungen oder –verbote).
- Liegen die Risiken im akzeptablen Bereich, sind sie ausreichend gering, das Verfahren kann abgeschlossen werden
- Risiken im Übergangsbereich verlangen eine Interessenabwägung zwischen dem Schutzanspruch der Bevölkerung/Umwelt und dem Eisenbahnbetrieb. Massnahmen müssen wirtschaftlich tragbar sein.

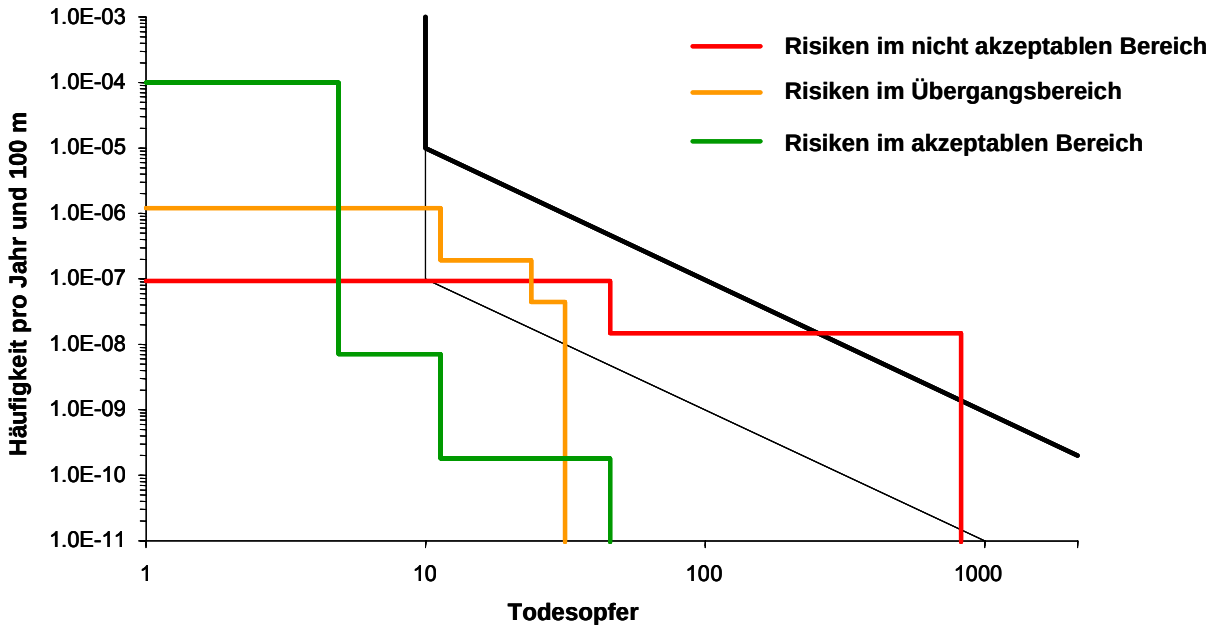


Abbildung 13: Exemplarische Risikosummenkurven im W/A-Diagramm

Tools Risikobewältigung - Kosten/Nutzen-Analyse ⑩

Wichtigste Entscheidungsgrundlage bei der risikobasierten, integralen Massnahmenplanung ist der Zusammenhang zwischen kollektivem Risiko und den Kosten für die Sicherheit bzw. Risikominderung. Dabei geht es darum, alle möglichen Massnahmen/-kombinationen zu erkennen und bezüglich ihrer Risikoreduktion und ihren Kosten zu beurteilen. Kernstück stellt die Kosten/Nutzen-Analyse mit folgenden Teilschritte dar:

- Risikoanalyse und Ermittlung des monetarisierten Risikos (← vgl. Tools Risikoanalyse oben)
- Massnahmenkatalog erstellen, Gliederung/Beschreibung der untersuchten Massnahmen inkl. einer quantitativen Abschätzung der Wirkung der einzelnen Massnahmen (→ siehe unten)
- Abschätzung der Massnahmenkosten (→ siehe unten)
- Beurteilung der Massnahmen bezüglich Kosten und Nutzen (→ siehe unten)

Abschätzung der Risikoreduktion

Um die Wirksamkeit einer Massnahme quantifizieren zu können, sind die verbleibenden Risiken nach Realisierung der Massnahme wenn immer möglich mit dem bei der Risikoanalyse angewandten Verfahren zu ermitteln. Die erzielbare Risikoreduktion ergibt sich aus der Differenz der Risiken vor und nach der Massnahme.

Ermittlung der Massnahmenkosten (Investitions-, Unterhalts- und Betriebskosten)

Bei der Umsetzung von Massnahmen werden folgende Kostenarten verursacht:

- Infrastruktur-, Planungs- und Realisierungskosten
- Betriebs- und Unterhaltskosten
- Kapitalkosten (Lebensdauer der Anlagen, Diskontsatz)

Während die Investitionskosten in der Regel zu einem bestimmten Zeitpunkt anfallen, sind Betriebs- und Unterhaltskosten laufend aufzubringen. Um diese Kostenarten miteinander und mit der monetarisierten Risikoreduktion (Nutzen) vergleichbar zu machen, müssen die Kosten in Jahreskosten umgerechnet werden.

Betriebs- und Unterhaltskosten:

Für Unterhaltskosten werden entweder bekannte absolute Erfahrungswerte eingesetzt, oder aber über Prozentanteile der Investition abgeschätzt.

Praxis-Tipp

Typische Werte für jährliche Unterhaltskosten sind:

für bauliche Massnahmen	1 %

Investitionskosten, Annuität

- Über die Bestimmung der sog. Annuitäten werden die Investitionskosten unter Berücksichtigung der Kapitalkosten in Jahreskosten umgerechnet und damit direkt mit dem monetarisierten Risiko vergleichbar.

Die Formel für die Berechnung der Annuitäten lautet:

$$A = K * (1 + p)^n * p / [(1 + p)^n – 1], \text{ mit}$$

A = Annuität

K = Investitionskosten

p = technischer Zinssatz (z.B. p = 0.05 resp. 5 %)

n = erwartete Lebensdauer der Massnahme

Praxis-Tipp

Für die Umrechnung der Investitionskosten in Jahreskosten sind folgende Überlegungen zu treffen:

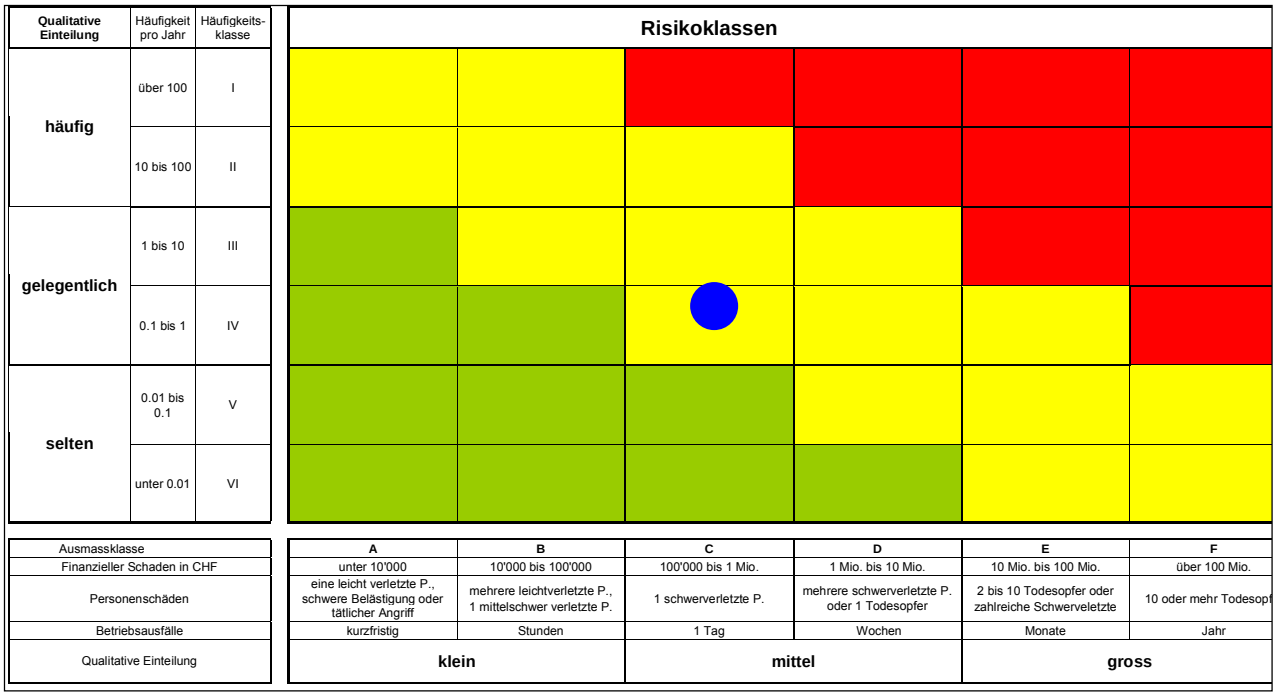
- Wie hoch ist die erwartete Lebensdauer der Massnahme?
- Zu welchem Zinssatz könnte das investierte Geld angelegt werden, wenn ich auf die Massnahmen verzichten würde? Ein typischer technischer Zinssatz für eine langfristige Kapitalanlage ist 5 %.

Für oft auftretende Fälle sind in der folgenden Tabelle die Faktoren F für verschiedene Kombinationen von n und p = 5 % zusammengestellt: Damit kann die Annuität sehr einfach wie folgt berechnet werden: A = K * F

Lebensdauer n [Jahre]	Faktor F bei einem Zinssatz p von 5 %
5	0.2310
10	0.1295
20	0.0802
50	0.0548
100	0.0504

Beispiel:

Risikoanalyse ergibt, dass das monetarisierte Jahresrisiko bei CHF 250'000 liegt. Aufgrund der Beurteilung anhand der Risikomatrix liegt das Risiko im Bereich der mittleren Risiken.



Zur Risikoreduktion wurden verschiedene Massnahmen (bauliche, bahntechnische und EDV-Massnahmen) evaluiert. Deren Investitions- und Unterhaltskosten wurden durch die entsprechenden Fachdienste abgeschätzt.

Massnahme	Investitionskosten [CHF]	Lebenserwartung [Jahre]	Annuität [CHF], bei p=5 %	Unterhaltskosten pro Jahr [CHF]	Gesamte Jahreskosten [CHF] ΔK
M1 Software	250'000	5	57'744	12'500	70'000
M2 Bahntechnik	400'000	20	32'097	20'00	52'000
M3 Bau	250'000	50	13'694	2'500	16'000
M4 Elektronik	600'000	10	78'000	2'000	80'000
M5 Bau	2'750'000	50	150'000	65'000	205'000

Tabelle 2: Ermittlung Jahreskosten der Massnahmen

Die vermeintlich günstigste Massnahme M1 ist gemessen an den Jahreskosten deutlich (Faktor >4) teurer als z.B M3. Dies sagt aber nicht aus, dass M3 auch bezüglich Kosten-Wirksamkeit die optimale Massnahme ist. Der Nutzen (monetarisierte Risikoreduktion) ist zu berücksichtigen.

Massnahme	Gesamte Jahreskosten [CHF] ΔK	Risiko R_0 [CHF]	Risikoreduktion relativ	Risikoreduktion Nutzen ΔN [CHF]	Kosten-/Nutzen Verhältnis ΔK/ΔN
M1	70'000	250'000	10 %	25'000	2.80
M2	52'000	250'000	75 %	187'500	0.28
M3	16'000	250'000	25 %	62'500	0.26
M4	80'000	250'000	55 %	137'500	0.58
M5	205'000	250'000	90 %	225'000	0.91

Tabelle 3: Ermittlung Kosten-/Nutzenverhältnis der Massnahmen

Massnahmen mit einem ΔK/ΔN-Verhältnis < 1 gelten als günstig. Massnahmen mit Werten zwischen 1 und 2 haben eine ausgeglichene Kostenwirskamkeit. Werte darüber werden als ungünstig beurteilt. Im Beispiel haben vier Massnahmen ein günstiges Kosten-Nutzen-Verhältnis, eine Massnahme (M1) ein ungünstiges.

Um diese Frage nach der Bestvariante zu beantworten, werden die Werte für die Kosten und den Nutzen in ein Diagramm eingetragen. Auf der x-Achse sind die Massnahmenkosten, auf der y-Achse das monetarisierte Ausgangsrisiko R_0 = Rm sowie für die einzelnen Massnahmen die Risikoreduktion (Nutzen) eingetragen.

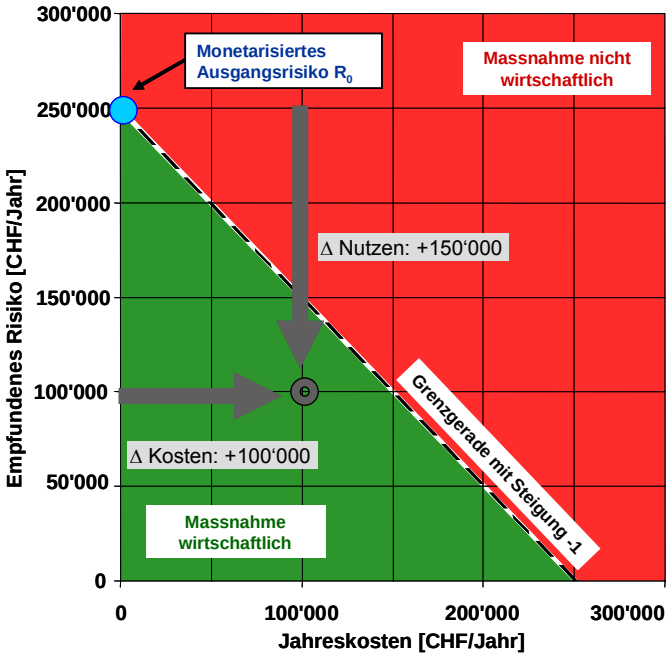


Abbildung 14: Kosten-Nutzen-Diagramm; Prinzip

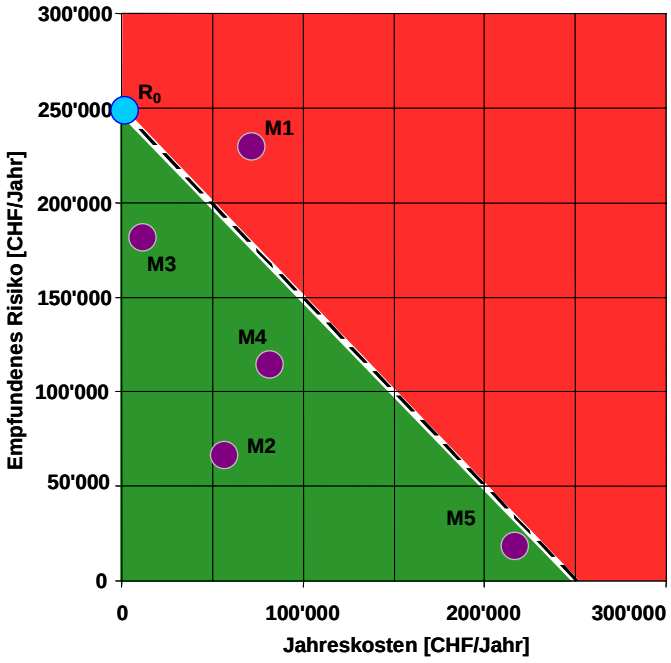


Abbildung 15: Massnahmenbeispiel

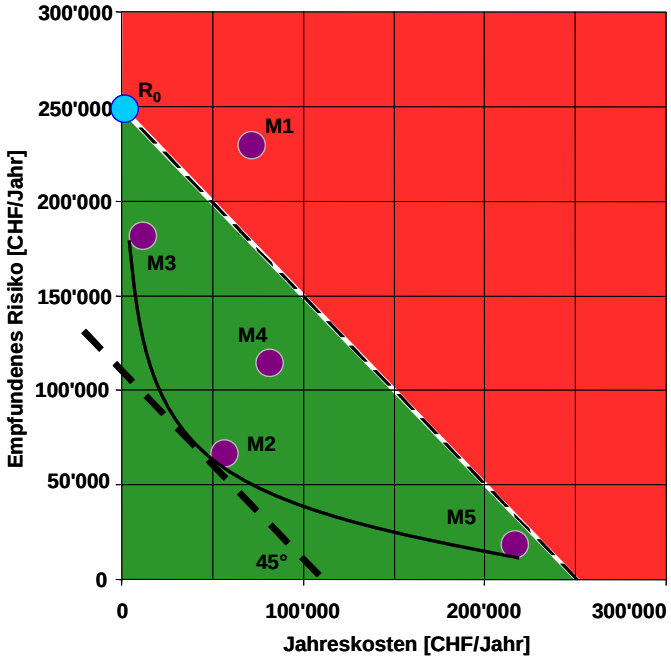


Abbildung 16: Kosten-Nutzen-Optimierung: Bestvariante M2

Massnahmen mit günstigstem Kosten/Nutzen-Verhältnis liegen auf der unteren Umhüllenden der eingetragenen Punkte. Die optimale Massnahme liegt dort, wo die Grenzkostentangente (45°) die Umhüllende berührt.

Das Beispiel zeigt, dass nicht grösstmögliche Sicherheit (M5) oder geringste Massnahmenkosten (M3) angestrebt wird, sondern grösstmöglich Effizienz im Mitteleinsatz. Es wird also das ALARA/ALARP-Prinzip (As Low As Reasonably Achievable / Practicable) verfolgt.

Weitere Kriterien

Bei der Bewertung der Kosten-Wirksamkeit ist zu berücksichtigen, dass die quantitative Beurteilung i.d.R eine beträchtliche Unschärfe (seitens Risiko und seitens Kosten) enthält und das Kriterium dem entsprechend nicht messerscharf angewendet werden sollte. Dies umso mehr, als für den Massnahmen-entscheid auch noch weitergehende Kriterien zur Anwendung kommen:

- Frage der Tragbarkeit des Restrisikos (insb. dort wo keine quantitativen Ziele vorgegeben sind)
- Interaktion mit anderen Massnahmen oder zukünftigen Entwicklungen (Wie sieht die Situation in 20 Jahren aus?)
- Ausgewogene Sicherheit nicht nur des Einzelobjekts sondern z.B. auf einem Streckenabschnitt (Liniengedanke). So kann es z.B. sinnvoll sein, einen kürzeren risikoärmeren Tunnel mit Sicherheitsmassnahmen auszurüsten, wenn die benachbarten Tunnel auf derselben Zufahrtsstrecke die Kriterien erfüllen und mit diesen Sicherheitsmassnahmen ausgestattet werden.
- Sensitivitätsbetrachtungen (z.B. Was passiert wenn doppelt soviel Gefahrgut auf Streckenabschnitt xy transportiert wird?)

