SFK

STÖRFALL-KOMMISSION

beim
Bundesminister für
Umwelt, Naturschutz und Reaktorsicherheit

Leitfaden

Maßnahmen gegen Eingriffe Unbefugter

der ad hoc- Arbeitsgruppe
„Eingriffe Unbefugter“

SFK-GS-38

HINWEIS:

Die KAS hat vor dem Hintergrund der technologischen Entwicklungen und der geänderten Bedrohungslage auf ihrer 38. Sitzung am 23. und 24. November 2016 die dringende Notwendigkeit festgestellt, den SFK-GS-38 „Maßnahmen gegen Eingriffe Unbefugter“ konzeptionell und inhaltlich grundlegend zu überarbeiten. Vor diesem Hintergrund hat sie einen Arbeitskreis „Eingriffe Unbefugter“ mit folgendem Auftrag eingerichtet:

- Vorschläge für eine Neufassung des SFK-GS-38 im Sinne eines umfassenden Leitfadens zu Maßnahmen gegen Eingriffe Unbefugter auf Betriebsbereiche und andere relevante Industrieanlagen zu erarbeiten. Hierbei sind insbesondere veränderte und neuartige Risiken infolge der technologischen Entwicklung und der sich verändernden Bedrohungslage zu berücksichtigen.
- Leitsätze zum Schutz vor cyberphysischen Angriffen zu erarbeiten und konzeptionell in die Neufassung des SFK-GS-38 einzubinden.
- Erarbeitung von Vorschlägen, in welcher Form Drohnenangriffe in der Neufassung des SKF-GS-38 berücksichtigt werden können und ggf. Leitsätze zu formulieren.

Bis zur Neuveröffentlichung des überarbeiteten SFK-GS-38 kann der bisherige Leitfaden weiter verwendet werden. Bei der Anwendung ist jedoch zu beachten, dass der Leitfaden teilweise nicht mehr dem Stand der Technik entspricht. Insbesondere werden Cyberangriffe und Drohnenangriffe nicht behandelt.

Störfall- Kommission

Leitfaden

Maßnahmen gegen Eingriffe Unbefugter

verabschiedet auf der 41. Sitzung der SFK am 23. Oktober 2002

Die Störfall-Kommission (SFK) ist eine nach § 51a Bundes-Immissionsschutzgesetz beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit gebildete Kommission.

Ihre Geschäftsstelle ist bei der GFI Umwelt – Gesellschaft für Infrastruktur und Umwelt mbH eingerichtet.

Inhalt: Seite:

Anhänge

1. Auftrag

Das BMU hat aus Anlass der Terroranschläge vom 11. September 2001 in den USA die SFK um Prüfung der Frage gebeten, welche Konsequenzen aus der neuen Bedrohungssituation für den Bereich der Anlagensicherheit zu ziehen sind. Daraufhin hat die SFK in ihrer Sitzung am 25./26. September 2001 die Einrichtung einer ad hoc-Gruppe beschlossen. Die Ergebnisse ihrer Beratungen sind in diesem Leitfaden niedergelegt, den die SFK in ihrer Sitzung am 23.10.2002 verabschiedet hat.

Aus Sicht des BMU sollte sich die SFK insbesondere mit folgenden Themen befassen:

- Prüfung des VCI-Papiers über Sicherheitsvorkehrungen gegen Terroranschläge (s.u.) mit dem Ziel, die dort genannten Aspekte in geeigneter Weise zu konkretisieren.

- Vorschläge, inwieweit im Sicherheitsbericht sowie in der Alarm- und Gefahrenabwehrplanung der Verhinderung etwaiger Anschläge und der Begrenzung etwaiger Anschlagsfolgen Rechnung getragen werden sollte.

- Vorschläge, inwieweit in der vom BMU vorbereiteten Verwaltungsvorschrift zur StörfallV Eingriffe Unbefugter bei den Anforderungen an Sicherheitsvorkehrungen und Szenarienbeschreibungen berücksichtigt werden sollten.

- Vorschläge, wie ein Ausgleich zwischen dem berechtigten öffentlichen Interesse an Informationen über die Sicherheit von Industriebetrieben und möglicherweise daraus folgenden Sicherheitsrisiken erreicht werden kann.

Die ad hoc-Gruppe hat sich mit allen diesen Aspekten befasst. Dazu lag ihr das Grundsatzpapier des VCI vom 02.10.01 „Sicherheitsvorkehrungen der Unternehmen der chemischen Industrie gegen Terroranschläge“ vor, in dem die im Rahmen der Betreiberpflichten zum Schutz gegen Eingriffe Unbefugter aktuell zu berücksichtigenden Abwehrmaßnahmen gegenüber terroristischen Anschlägen beschrieben und den Mitgliedsfirmen zum Einsatz empfohlen wurden. Daneben lagen Stellungnahmen verschiedener Mitglieder der ad hoc- Gruppe, die „Site Security Guidelines for the U.S. Chemical Industry“ (2001), eine Broschüre der BP „Getting Security Right - The Basics for Security Management“ (Issue September 2000), sowie der im Auftrag des Umweltbundesamtes erstellte Forschungsbericht 104 09 210 „Technische und organisatorische Maßnahmen zur Sicherung der Störfallverordnung unterliegender Anlagen gegen Eingriffe Unbefugter“ (1988) vor.

Wesentliche Ergebnisse, auf die auch dieser Leitfaden aufbaut, wurden in einem Zwischenbericht vom Dezember 2001 zusammengefasst, der am 16. 1. 2002 von der SFK verabschiedet und am 12. 2. 2002 vom BMU veröffentlicht wurde.

2. Anwendungsbereich

In der vorliegenden Untersuchung sollen im Sinne der Aufgaben der Störfall- Kommission ausschließlich Anlagen und Betriebsbereiche nach StörfallV betrachtet werden. Anknüpfungspunkt ist die Pflicht der Betreiber, diese gemäß § 3 Abs. 2 Nr. 3 StörfallV gegen Eingriffe Unbefugter zu sichern. Dies hat so zu erfolgen, dass in den Anlagen vorhandene gefährliche Stoffe derart gegen durch Vorsatz ausgelöste Störungen gesichert sind, dass eine ernste Gefahr im Sinne der StörfallV vernünftigerweise ausgeschlossen werden kann.

Der Leitfaden richtet sich in erster Linie an Betriebsbereiche und Anlagen mit erweiterten Pflichten. Es können aber auch Betriebsbereiche und Anlagen nach §1 Abs. 3 und 4 der StörfallV mit Grundpflichten betroffen sein, wenn ein besonders schutzwürdiges Objekt nach Prüfung des Einzelfalls betroffen sein kann.

Entsprechend den bereits gültigen Vorgaben der StörfallV sind eine Reihe der im Folgenden vorgeschlagenen Untersuchungsschritte bzw. Maßnahmen ohnehin erforderlich. Dies wird im Text durch ***Kursivschrift*** verdeutlicht.

Der Leitfaden hebt ab auf eine Gefährdung von Menschen. Wenngleich Terroranschläge gegen die Umwelt („Ökoterrorismus“) durchaus auch eine gravierende Bedrohung darstellen können, werden im Sinne eines pragmatischen, schrittweisen Vorgehens reine Umweltauswirkungen in diesem Leitfadens nicht spezifisch behandelt. Es kann hierfür aber sinngemäß die gleiche Vorgehensweise angewendet werden.

Nicht Gegenstand der nachfolgenden Betrachtung sind außerbetriebliche Gefahrguttransporte. Grundsätzlich gilt aber, dass für Gefahrguttransporte ähnliche Sicherungsüberlegungen anzustellen sind, wie sie hier für die stationären Anlagen angestellt werden. Zu- und Abgangswege und insbesondere deren Sicherung müssen im Einzelfall auf Schnittstellen mit dem Transportwesen untersucht und behandelt werden. Für die Entwendung von Chemikalien bzw. deren vorsätzlichen Missbrauch sind ebenfalls gesonderte Überlegungen anzustellen.

Angriffe über die elektronische Vernetzung der Unternehmen („Cyberattacke“) werden für weniger gefährdend erachtet. Ein Zugang zu den Rechnern, welche die Anlagen direkt steuern (und nur diese sind für die Anlagensicherheit relevant), ist in der Regel von außen außerordentlich schwierig (keine oder keine ständige Verbindung mit von außen zugänglichen Datennetzen, andersartige Betriebssysteme, Prozessanlagen gehen in der Regel in Sicherheitsstellung bei Ausfall der Rechner). Sollten diese Voraussetzungen in Einzelfällen nicht gegeben sein, sollten die Betreiber entsprechende Maßnahmen zur Verhinderung von Eingriffen Unbefugter durchführen. Die ad hoc- Gruppe hat sich mit der Thematik jedoch nicht vertieft beschäftigen können.

Andere kriminelle Angriffe auf Unternehmen, wie z.B. Industriespionage, werden ebenfalls nicht betrachtet.

3. Definitionen (im Sinne dieses Leitfadens)

Besondere Schutzobjekte sind Einrichtungen, die zum regelmäßigen Aufenthalt von einer Vielzahl von Menschen vorgesehen sind (Schulen, Versammlungsstätten, Krankenhäuser, Bahnhöfe etc.). In diese Gruppe sind auch Wohngebiete mit dichter Bebauung und Verkehrswege mit hoher Verkehrsdichte einzuschließen. Es werden in diesem Zusammenhang nur solche Schutzobjekte betrachtet, bei denen direkt oder indirekt das Leben einer Vielzahl von Menschen bedroht oder deren Gesundheit schwerwiegend beeinträchtigt wird.

Sicherungsrelevante Anlagen sind Anlagen in einem Betriebsbereich nach §3 Abs. 5a BImSchG i. V. mit §1 Abs. 1 und 2 StörfallV und Anlagen nach § 1 Abs. 3 und 4 StörfallV, die bei Eingriffen Unbefugter eine ernste Gefahr im Sinne der Störfall- Verordnung für besondere Schutzobjekte hervorrufen können.

Ein **Unbefugter** im Sinne von § 3 Abs. 2 Nr. 3 der StörfallV ist hier jede Person, die vorsätzlich Handlungen mit dem Ziel vornimmt, unmittelbar oder mittelbar einen Schaden zu verursachen. Hierbei ist es unerheblich, ob es sich um einen Mitarbeiter des Betreibers, einen von ihm Beauftragten oder einen Dritten handelt.

Sicherung sind alle Aktivitäten zur Verhinderung von Gefahren, die durch Eingriffe Unbefugter ausgelöst werden können, sowie zur vorbeugenden Begrenzung von Auswirkungen möglicherweise von Unbefugten dennoch ausgelöster Störungen. Betreiber, Behörden oder sonstige Dritte können zur Sicherung beitragen. Sicherung entspricht dem Begriff „Security“ im englischen Sprachraum und ist zu unterscheiden von Sicherheit („Safety“).

Eine **Sicherungsanalyse** ist die Ermittlung und Bewertung von möglichen Eingriffen Unbefugter und der dadurch möglicherweise ausgelösten Gefahren unter Verwendung von systematischen Methoden. Ihre Erstellung setzt insbesondere Kenntnisse über mögliche Motivationen und Handlungsmöglichkeiten Unbefugter voraus. In der Sicherungsanalyse wird die Ermittlung und Beurteilung der spezifischen Gefährdungslage (**Gefährdungsanalyse**) mit den Ergebnissen der Ermittlung der Gefahrenstellen im Rahmen der im Sicherheitsbericht nach StörfallV ohnehin erforderlichen **Gefahrenanalyse** zusammengeführt. Die Sicherungsanalyse kann Voraussetzung für die Ableitung von **Sicherungszielen** und der erforderlichen **Sicherungsmaßnahmen** im Rahmen der Erstellung eines **Sicherungskonzeptes** sein. Ihre Dokumentation, regelmäßige Überprüfung und Fortschreibung sowohl bei wesentlichen Änderungen als auch bei besonderem Anlass wird angeraten.

4. Konzept zur Identifizierung und Sicherung von sicherungsrelevanten Anlagen (Sicherungskonzept)

Der Nachweis ausreichender Vorkehrungen insbesondere des Betreibers gegen Eingriffe Unbefugter sollte im Rahmen einer Sicherungsanalyse erfolgen. Ein geeignetes Verfahren wird hier in den Grundzügen dargestellt und in Anhang 1 beispielhaft beschrieben. Die Betreiber müssen hierfür insbesondere:

a) in Abstimmung mit den für die innere Sicherheit zuständigen Behörden Betriebsbereiche und Anlagen nach StörfallV systematisch daraufhin untersuchen, ob sie ein herausgehobenes Ziel darstellen können (Gefährdungsanalyse, s. Anhang 1, Kap. 3) und
b) im Benehmen mit den für die außerbetriebliche Gefahrenabwehr zuständigen Behörden untersuchen, ob Eingriffe Unbefugter in zerstörerischer Absicht zu einer ernsten Gefahr führen könnten (Gefahrenanalyse).

Es ist dem Betreiber freigestellt, andere Verfahren als das in Anhang 1 beschriebene zu wählen. Sie sollten jedoch das gleiche Schutzniveau gewährleisten.

Gefahrenanalyse und Gefährdungsanalyse sind gleichwertige Elemente der Sicherungsanalyse. Mit welchem dieser Schritte begonnen wird, sollte im Einzelfall entschieden werden. Die im folgenden Text gewählte Vorgehensweise, zunächst die Gefahrenanalyse durchzuführen, grenzt den Kreis der zu untersuchenden Anlagen (und damit den Geltungsbereich dieses Leitfadens) mit Hilfe in der Regel ohnehin vorhandener Informationen bereits im ersten Schritt ein. Die in Anhang 1 gewählte Vorgehensweise, erst die Gefährdung durch Eingriffe Unbefugter zu analysieren und danach erst die möglichen Konsequenzen, hat den Vorteil, auch Sicherungsprobleme zu erkennen, die unterhalb der Schwelle der ernsten Gefahr liegen.

4.1 Gefahrenanalyse

Besonders zu betrachten i.S. dieses Leitfadens sind Teile des Betriebsbereichs (z.B. Anlagen), bei denen durch einen Dennoch–Störfall im Bereich besonders schutzwürdiger Objekte das Leben von Menschen bedroht wird oder schwerwiegende Gesundheitsbeeinträchtigungen von Menschen zu befürchten sind.

Dabei sollten die Auswirkungen möglicher Eingriffe Unbefugter berücksichtigt werden durch:

- Beschreibung der „Dennoch–Störfälle“ (Freiwerden, Explosion oder Brand der größten zusammenhängenden Stoffmenge) gemäß § 3 Abs. 3 StörfallV i. V. mit dem Leitfaden SFK-GS 26. „Dominoeffekte“ müssen beachtet werden, insbesondere bei Industrieparks (Chemieparks). *Diese Informationen sind unter anderem Voraussetzung für die Information der Gefahrenabwehrbehörden gemäß § 10 Abs. 1 Nr. 2 StörfallV (s. unten) und sollten gemäß einer Empfehlung der Störfall-Kommission auch Bestandteil der Sicherheitsberichte sein.*
- Festlegung von besonderen Schutzobjekten im Sinne der o.g. Definition (s. auch Anhang 1, Kap. 4). Diese Objekte werden meist im Umfeld des Betriebsbereichs liegen. In "offenen“ Industrieparks können sie sich jedoch auch innerhalb des Industrieparkgeländes befinden. *Diese Informationen sind Bestandteil der Sicherheitsberichte.*
- Abschätzung der Auswirkungen von Dennoch–Störfällen auf die besonderen Schutzobjekte. *Diese Angaben sind ohnehin notwendig im Rahmen der den*

Gefahrenabwehrbehörden gemäß § 10 Abs. 1 Nr. 2 StörfallV zur Verfügung zu stellenden Informationen.

Es wird angeraten, die bereits erstellten Dennoch-Störfall- Betrachtungen darauf zu überprüfen, dass die Gefahren berücksichtigt sind, die gemäß Gefährdungsanalyse durch Eingriffe Unbefugter ausgelöst werden können, selbst wenn sie als Störungen vernünftigerweise ausgeschlossen wurden (z.B. Zerstörung passiver Sicherheitseinrichtungen, s. auch Anhang 1, Kap. 5).

4.2 Gefährdungsanalyse

Falls in der Gefahrenanalyse unter 4.1 festgestellt wurde, dass für besondere Schutzobjekte eine ernste Gefahr im Sinne der StörfallV bestehen kann, ist zu untersuchen, inwieweit die Anlagen für terroristische Angriffe besonders „attraktiv“ erscheinen. Dazu ist eine systematische Analyse durchzuführen, in der insbesondere die folgenden Aspekte zu berücksichtigen sind. Die hierfür erforderlichen Informationen müssen die Betreiber z.T. bei den für die innere Sicherheit zuständigen Behörden einholen, deren Einbindung in diesem Schritt ohnehin zu empfehlen ist.

- Beurteilung der Gefährdungslage (allgemeine Sicherheitslage, Größe und Zusammensetzung der Belegschaft, Qualität der Sicherheitsorganisation, gesellschaftliche Position von Angehörigen der Unternehmensleitung, Art der Vertriebsverbindungen und Auslandsaktivitäten, bisher festgestellte Kriminalität, etc. (s. auch Anhang 1, Kap. 3),
- örtliche Lage des Betriebsbereichs und der Anlagen (Angreifbarkeit von außen und innen, Entfernung zum Werkszaun, Einsehbarkeit von außen, Straßenführung innen und außen, Industriepark - Situation etc. s. auch Anhang 1, Kap. 3.4),
- die Bedeutung der Verfügbarkeit der Anlagen für nachgelagerte Produktionsprozesse und Dienstleistungen,
- der Symbolcharakter des Unternehmens bzw. der Anlage (Eigentumsverhältnisse, Art der Produktion und der Lagerung von Stoffen, Produktpalette, wirtschaftlich-strategische Bedeutung des Unternehmens usw).

4.3 Sicherung von sicherungsrelevanten Anlagen

Anlagen, die sich in den Schritten 4.1 und 4.2 als sicherungsrelevant erweisen, sind von den Betreibern unter Einbeziehung der für die innere Sicherheit zuständigen Behörden in besonderem Maße gegen Eingriffe Unbefugter zu sichern. Hierfür sind Sicherungsziele festzulegen (s. Anhang 1, Kap. 6). Zur Erreichung dieser Sicherungsziele kommen insbesondere folgende Maßnahmen in Betracht:

- Die Grenzen von Betriebsbereichen – bei Industrieparks gegebenfalls die gemeinsame Grenze - (Werkszaun, Tore etc.) sind durch technische und organisatorische Maßnahmen so zu sichern, dass Unbefugte ohne Anwendung von Gewalt (z.B. Beschädigung der Werkseinfriedung, Angriff auf Kontrollpersonal) oder arglistige Täuschung (z.B. Fälschung von Werksausweisen) nicht eindringen können und ein gewaltsames Eindringen in angemessener Zeit erkannt wird (z.B. durch Alarmanlagen, Videoüberwachung, Streifengänge etc.).
- Betriebsfremde sollen identifizierbar sein, z.B. durch offenes Tragen von unterscheidbaren Werksausweisen. Besucher und Fremdfirmen sind angemessen zu überwachen.
- Die Anlagen selbst sind so zu sichern, dass ein Störfall ohne interne Kenntnisse und/oder technische Hilfsmittel durch Unbefugte nicht ausgelöst werden kann.

- Die Mitarbeiter sind im Hinblick auf die Sicherung des Betriebsbereichs zu sensibilisieren und einzubeziehen, z.B. durch Teamtraining, Seminare, Schulungen etc. (siehe hierzu auch Kapitel 7).

Industrieparks (insbesondere Chemieparks) stellen wegen der Vielzahl rechtlich selbständiger Betreiber besondere Anforderungen an die Sicherungsmaßnahmen. Die Angreifbarkeit gefährlicher Anlagen kann hier in der Regel nur durch eine einheitliche Überwachung minimiert werden (gemeinsamer Werkszaun und Werkschutz).

Die Auswahl der geeigneten Maßnahmen erfolgt zweckmäßigerweise gemäß der hier beschriebenen systematischen Sicherungsanalyse. Beispiele für Sicherungsmaßnahmen werden in **Anhang 1, Kap. 7** beschrieben, Beispiele für Präventivmaßnahmen gegen Angriffe in **Anhang 2.**

Die Mehrzahl dieser Maßnahmen wird bereits praktiziert oder kann vergleichsweise rasch eingeführt werden. Die Betreiber sollten die Wirksamkeit bestehender Maßnahmen, so weit noch nicht geschehen, überprüfen und gegebenenfalls erforderliche Maßnahmen ergreifen. Dabei kommt der qualitativen und quantitativen personellen und technischen Ausstattung des Personals mit Sicherungsaufgaben (z.B. Werkschutz) besondere Bedeutung zu. Die Behörden sollten ihrerseits im Rahmen der Überwachung gemäß §16 StörfallV die getroffenen Maßnahmen überprüfen.

Die Sicherheitsberichte sind entsprechend § 9 Abs. 5 Nr. 3 StörfallV um die Analysen der möglichen Auswirkungen und der Gefährdung sowie um die daraus abgeleiteten Maßnahmen und die Informationen für die Erstellung externer Alarm- und Gefahrenabwehrpläne zu ergänzen bzw. fortzuschreiben. Soweit bei Anlagen und Betriebsbereichen lediglich Grundpflichten vorliegen, wird empfohlen, dass die entsprechenden Informationen ebenfalls schriftlich dokumentiert werden.

Besonders wichtig ist neben den möglichen sicherheitstechnischen und organisatorischen Verbesserungen vor allem die gute und intensive Zusammenarbeit zwischen Betreibern und Sicherheits- und Gefahrenabwehrbehörden. Soweit zum Schutz vor Eingriffen Unbefugter externe Unterstützung z.B. durch die Polizei erforderlich ist, sollte der Betreiber unverzüglich den Kontakt zu den zuständigen Behörden aufnehmen.

4.4 Maßnahmen zur Begrenzung der Auswirkungen von Störfällen

Für den Fall eines Dennoch-Störfalls haben die Betreiber Maßnahmen zu ergreifen, um dessen Auswirkungen so gering wie möglich zu halten (§ 3 Abs. 3 StörfallV). Gängige und erprobte Maßnahmen zur Begrenzung der Auswirkungen von Dennoch-Störfällen sind z.B. im Anhang 6 des SFK-Berichts SFK-GS-04 aufgelistet.

Um die Folgen eines eventuellen Eingriffes Unbefugter auf sicherungsrelevante Anlagen beherrschen zu können, müssen diese Informationen über Dennoch-Störfälle den Gefahrenabwehrbehörden vorliegen. Diese wiederum müssen die Szenarien in entsprechende Alarm- und Gefahrenabwehrpläne umsetzen.

Die Rechtslage sieht hierzu vor, *dass Betreiber, die den erweiterten Pflichten unterliegen, diese Informationen den Gefahrenabwehrbehörden ohne Aufforderung zu übermitteln haben (§10 Abs. 1 StörfallV). Betreiber, die lediglich den Grundpflichten der StörfallV unterliegen, haben die notwendigen Informationen, um externe Alarm- und Gefahrenabwehrpläne zu erstellen, den Gefahrenabwehrbehörden auf Verlangen zu liefern (§6 Abs. 4 StörfallV). Die Behörden können ihnen im Einzelfall ggf. Pflichten nach den §§ 9 bis 12 der StörfallV*

auferlegen, z.B. die Erstellung eines Sicherheitsberichts mit Darlegungen zum Schutz gegen Eingriffe Unbefugter bzw. die Erstellung eines internen Alarm- und Gefahrenabwehrplans.

Hinsichtlich der auswirkungsbegrenzenden Maßnahmen werden folgende **Empfehlungen** ausgesprochen:

- Auch Betreiber von Betriebsbereichen und Anlagen, die nicht den erweiterten Pflichten der StörfallV unterliegen, sich aber als sicherungsrelevant erwiesen haben, sollen sich auch aus eigenem Interesse unverzüglich mit den Gefahrenabwehrbehörden in Verbindung setzen, um ihnen die nötigen Informationen zur Erstellung externer Alarm- und Gefahrenabwehrpläne zu übermitteln. Die Immissionsschutz- und Gefahrenabwehrbehörden sollen sich zwecks Identifizierung dieser möglichen relevanten Anlagen untereinander verständigen.

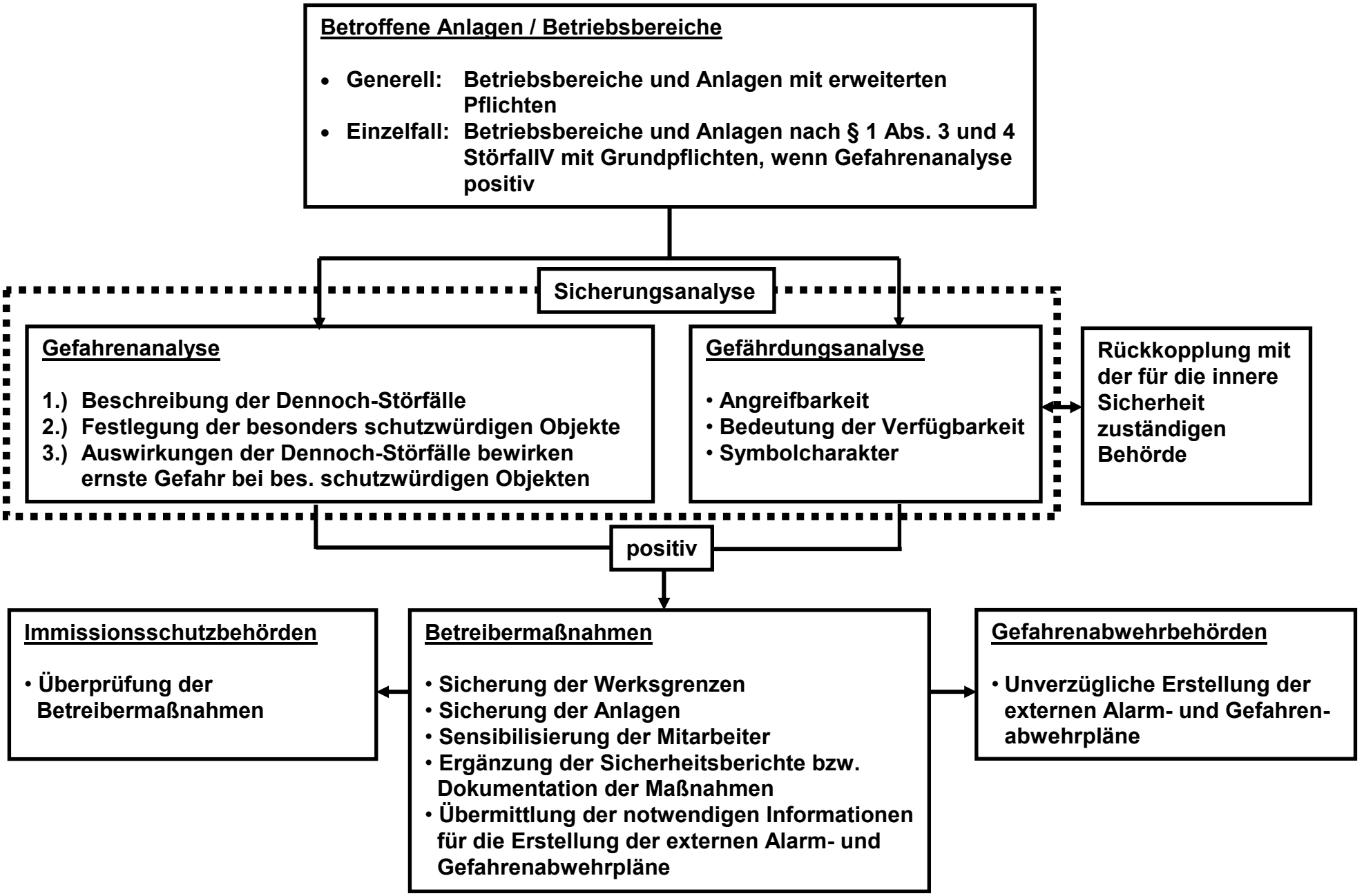
- Die zuständigen Gefahrenabwehrbehörden sollen auf der Grundlage der vorhandenen Informationen der Betreiber zum Schutze der Bevölkerung vor Eingriffen Unbefugter unverzüglich die notwendigen externen Alarm- und Gefahrenabwehrpläne erstellen.

- Zur Erstellung der notwendigen Unterlagen durch die Betreiber für die Gefahrenabwehrbehörden wird auf den Bericht SFK-GS-26 verwiesen.

4.5 Graphische Darstellung des Konzepts zur Identifizierung und Sicherung von sicherungsrelevanten Anlagen

Eine Übersicht über das vorgeschlagene Konzept gemäß Kapitel 4 ist dem nachfolgenden Bild zu entnehmen:

Sicherung von Betriebsbereichen/Anlagen gegen Eingriffe Unbefugter



5. “Good Security” Practice / Sicherungsmanagement

Zur Umsetzung der Sicherungsziele und -Maßnahmen wird ein Sicherungsmanagement empfohlen, das Teil des Sicherheitsmanagements sein kann. Zum Aufbau und zum Unterhalt eines Sicherungsmanagements werden Hinweise in **Anhang 3** geben.

Es wird empfohlen, die Maßnahmen im Hinblick auf die aktuelle Gefährdungslage zu staffeln („keine Gefährdung“ bis „Unbefugte in den Betriebsbereich eingedrungen“). Ferner sollte berücksichtigt werden, dass die Gefährdungslage sich durch interne und externe Entwicklungen u.U. sehr kurzfristig verändern kann und somit kontinuierlich beobachtet werden sollte.

6. Offenlegung von Sicherheitsunterlagen

Hinsichtlich der Bedenken bezüglich der Veröffentlichung von sensiblen Daten in Genehmigungsverfahren oder im Sicherheitsbericht ist zunächst festzuhalten, dass die bestehenden Rechtsgrundlagen bereits ausreichend sind, um ggf. erforderliche Einschränkungen zuzulassen. Bei Entscheidungen dieser Frage im Einzelfall bedarf es einer sorgfältigen Abwägung der betroffenen Rechtsgüter. Weiter ist zu beachten, dass die Information Betroffener über sie betreffende Risiken nicht nur ein Freiheitsrecht darstellt, sondern auch ein Element der Störfallvorsorge ist. Neben der Abwägung der Rechtsgüter bedarf es daher der Entwicklung von Kriterien, um den möglichen Verlust an Sicherheit gegen einen möglichen Gewinn an Sicherung abzuwägen.

In § 11 Abs. 3 der StörfallV ist dazu festgelegt, dass der Betreiber den Sicherheitsbericht zur Einsicht durch die Öffentlichkeit bereitzuhalten hat. Er kann jedoch von der zuständigen Behörde verlangen, dass bestimmte Teile des Sicherheitsberichtes, u. a. aus Gründen der öffentlichen Sicherheit, nicht offengelegt werden müssen. Dies bedarf der Zustimmung durch die zuständige Behörde. Es ist dann ein geänderter Sicherheitsbericht der Öffentlichkeit zugänglich zu machen. Dieser muss so ausführlich sein, dass insbesondere es Dritten möglich ist, zu beurteilen, ob und in welchem Umfang sie von den Auswirkungen eines Störfalls im Betriebsbereich betroffen werden können (analog § 10 Abs. 2 BImSchG).

Es wird empfohlen, nur bei solchen Betriebsbereichen/ Anlagen eine Beschränkung der Offenlegung von Informationen aus Gründen der öffentlichen Sicherheit zuzulassen, die auf Grund der Gefahrenanalyse (Kapitel 4.1) und der Gefährdungsanalyse (Kapitel 4.2) als sicherungsrelevant anzusehen sind. Erst dann ist eine Beschränkung der Offenlegung unter Änderung oder Auslassung der betroffenen sicherungsrelevanten spezifischen Informationen in Form einer geänderten Fassung („qualifizierte Inhaltsdarstellung“) zulässig, die jedoch eine aus sich heraus verständliche und zusammenhängende Darstellung bleiben muss (analog § 4 b Abs. 3 der 9.BImSchV).

Ein Beispiel für die Entscheidung, welche Informationen vertraulich zu behandeln sind und welche der Öffentlichkeit zugänglich gemacht werden sollten, ist in **Anhang 4** wiedergegeben.

7. Maßnahmen gegen Innentäter

Ein Risiko kann insbesondere auch von sogenannten Innentätern ausgehen. Hierunter werden Mitarbeiter des eigenen Unternehmens bzw. von Fremdfirmen verstanden, die sich befugt im Bereich sicherungsrelevanter Anlagen aufhalten und unbefugte Eingriffe vornehmen. Sie können über gute Kenntnis der entsprechenden Anlagen verfügen und dies in krimineller Absicht nutzen wollen.

Wenngleich dieser Täterkreis besonders problematisch ist, so sind neben den allgemeinen Maßnahmen der Sicherheitsbehörden auch den Betreibern präventive Maßnahmen möglich. Diese sind vor allem dem Bereich der Personalführung und -überwachung zuzuordnen (Erzeugung einer Identifikation mit dem Unternehmen, Motivation, sensibler Umgang mit belastenden Personalmaßnahmen, Schulung der Vorgesetzten etc.). Darüber hinaus sollte eine allgemeine Sensibilisierung aller Mitarbeiter gegenüber diesem Problemkreis geschaffen werden (vgl. auch Anhang 1, Kap. 3.9). Eine Beratung durch besonders qualifizierte Psychologen kann ggf. sinnvoll sein.

Bleibt nach Ausschöpfen aller dieser sowie der weiter oben abgehandelten Sicherungsmaßnahmen ein relevantes Risiko durch Innentäter bestehen, sollten die für die innere Sicherheit zuständigen Behörden zu Rate gezogen werden. Als „ultima ratio“ kann auch eine Sicherheitsüberprüfung von Mitarbeitern in hochsensiblen Bereichen nicht ausgeschlossen werden, soweit dies rechtlich, insbesondere auch datenschutzrechtlich, zulässig ist.

8. Zusammenfassung

Zusammenfassend werden folgende Feststellungen getroffen:

1. Grundsätzlich sind Anschläge auf einen Betriebsbereich von Außen- und von Innentätern möglich. Hinsichtlich der Abwehrmaßnahmen sind sowohl der Staat als Garant der inneren Sicherheit als auch die Betreiber in der Pflicht. Dies wird auf beiden Seiten erhöhte Aufwendungen erfordern.

2. Pflicht der Betreiber nach der StörfallV ist es bereits seit vielen Jahren, ihre Betriebsbereiche und Anlagen gegen Eingriffe Unbefugter zu sichern. Hierzu wird das Konzept gemäß Kapitel 4 empfohlen. Unter der neuen Bedrohungssituation ist ein Eindringen von Unbefugten in den jeweiligen Betriebsbereich zu erschweren und ggf. zu erkennen, wie etwa durch wirkungsvolle und überwachte Umzäunungen, Organisation von Torkontrollen und Streifengängen etc. Besonders gefährliche und hinsichtlich terroristischer Anschläge gefährdete Anlagen bzw. Anlagenteile sind gegen Eingriffe Unbefugter ggf. zusätzlich zu sichern.

3. Pflicht des Staates ist es, terroristische Angriffe von außen sowie das gewaltsame Eindringen in Betriebsbereiche mit vorbeugenden und abwehrenden Maßnahmen zu erschweren bzw. zu verhindern. Beispiele hierzu sind in Anhang 2 gegeben. Hierfür müssen auch in Zeiten knapper Budgets die entsprechenden Ressourcen zur Verfügung gestellt werden.

4. Die Maßnahmen sowohl des Staates als auch der Betreiber sollen sich an Art und Ausmaß des Risikos orientieren.

5. Da ein vollständiger Schutz nie gewährleistet werden kann, kommt den Maßnahmen der

außerbetrieblichen Gefahrenabwehr besondere Bedeutung zu. Die hierfür zuständigen Behörden müssen von den Betreibern die erforderlichen Informationen erhalten und unverzüglich die in ihrer Zuständigkeit liegenden Maßnahmen treffen.

6. Die für die Einschätzung der Gefährdungssituation durch die Betreiber und die Behörden erforderlichen Informationen sind zu einem erheblichen Teil auf Grund der Vorschriften zum Sicherheitsbericht (§ 9 StörfallV) sowie zu den Alarm- und Gefahrenabwehrplänen (§ 10 StörfallV sowie die Landesgesetze zum Brand- und Katastrophenschutz) vorhanden oder waren bis spätestens 3. 2. 2002 zu erheben.

7. Für die notwendigen Maßnahmen sind wesentliche Rechtsgrundlagen insbesondere in den §§ 3 bis 6, 9 und 10 StörfallV sowie den Landesgesetzen zum Brand- und Katastrophenschutz bereits gegeben. Eine Präzisierung dieser Vorgaben im Sinne dieses Leitfadens soll im Rahmen der vom BMU geplanten neuen StörfallVwV erfolgen.

8. Es wird empfohlen, nur bei solchen Betriebsbereichen/ Anlagen eine Beschränkung der Offenlegung von Informationen aus Gründen der öffentlichen Sicherheit zuzulassen, die auf Grund der Gefahrenanalyse (Kapitel 4.1) und der Gefährdungsanalyse (Kapitel 4.2) als sicherungsrelevant anzusehen sind. Erst dann ist eine Beschränkung der Offenlegung unter Änderung oder Auslassung der betroffenen sicherungsrelevanten spezifischen Informationen in Form einer geänderten Fassung („qualifizierte Inhaltsdarstellung“) zulässig, die jedoch eine aus sich heraus verständliche und zusammenhängende Darstellung bleiben muss (analog § 4 b Abs. 3 der 9.BImSchV).

9. Insgesamt wird festgestellt, dass eine Gefährdung von Betriebsbereichen/ Anlagen durch terroristische Angriffe sowohl hinsichtlich der Wahrscheinlichkeit als auch potentieller Folgen differenziert zu betrachten ist. Bisher schon gebräuchliche Sicherungsmaßnahmen bieten nach wie vor einen erheblichen Schutz. Sie sollten daher konsequent und unter Berücksichtigung der in diesem Leitfaden gemachten Empfehlungen angewendet werden, so weit dies nach dem 11. 9. 2001 erforderlich und noch nicht geschehen ist. Falls dies geschieht, kann eine Bedrohung durch terroristische Angriffe auf Betriebsbereiche/Anlagen weitgehend beherrscht werden.

Anhänge

Die Anhänge sollen beispielhaft die Aussagen des Leitfadens verdeutlichen. Sie stammen aus verschiedenen Quellen. Sie sollen in Zukunft fortgeschrieben werden. In Zweifelsfällen sollten die Aussagen des voranstehenden Textes herangezogen werden.

Anhang 1

Muster eines Sicherungskonzeptes[1]

Inhalt

[1] Dieses Beispiel für eine Sicherungsanalyse beruht auf dem F&E-Vorhaben 104 09 210 des Umweltbundesamtes „Technische und organisatorische Maßnahmen zur Sicherung der StörfallV unterliegenden Anlagen gegen Eingriffe Unbefugter“, Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V. (1988)

1 Vorbemerkungen

Es wird ein Verfahren vorgestellt, das die in Kapitel 4 dieses Leitfadens gestellten Anforderungen an eine Sicherungsanalyse beispielhaft erfüllt, und entsprechende Erläuterungen hierzu gegeben. Es ist dem Betreiber freigestellt, andere Verfahren zu wählen. Sie sollten jedoch das gleiche Schutzniveau gewährleisten.

2 Vorgehensweise bei einer Sicherungsanalyse

Die ausreichende Sicherung von Betriebsbereichen gegen Eingriffe Unbefugter ist in der Regel nur auf der Grundlage einer systematischen Analyse hinreichend zu ermitteln. Dabei wird schrittweise vorgegangen:

1. Ermittlung und Beurteilung der Gefährdungslage
2. Identifikation der spezifischen Gefährdungsstellen im Betriebsbereich
3. Bewertung der Gefahren im Verhältnis zu den gesetzten Schutzzielen
4. Auswahl der Sicherungsmaßnahmen, Erstellung des integrierten Sicherungskonzepts.

Eine Übersicht ist *Bild 1* zu entnehmen. Die Beurteilungen sind aufgrund neuer Erkenntnisse und regelmäßig zu überprüfen.

2.1 Ermittlung und Beurteilung der Gefährdungslage

Bei der Ermittelung der Gefährdungslage müssen für jeden Betriebsbereich eine Reihe unterschiedlicher Faktoren beachtet werden, wie z.B.:

- Art der Produktion,
- Lagerung von Gefahrstoffen,
- Örtliche Lage des Betriebsbereichs,
- Umgebung des Betriebsbereichs,
- Art und der Umfang der Bebauung,
- personelle Ausstattung,
- betriebsspezifische Besonderheiten

Der Bedrohungsgrad ist dabei abhängig von

- den eventuell infrage kommenden Verursachern mit ihrer möglichen Vorgehens- oder Verhaltensweise, im folgenden Gefährdungsart genannt sowie
- der Anzahl, Art und Beschaffenheit einzelner Stellen im Betriebsbereich, bei denen ein Störfall mit mehr oder weniger großem Aufwand herbeigeführt werden könnte, im Folgenden Gefährdungsstellen genannt.

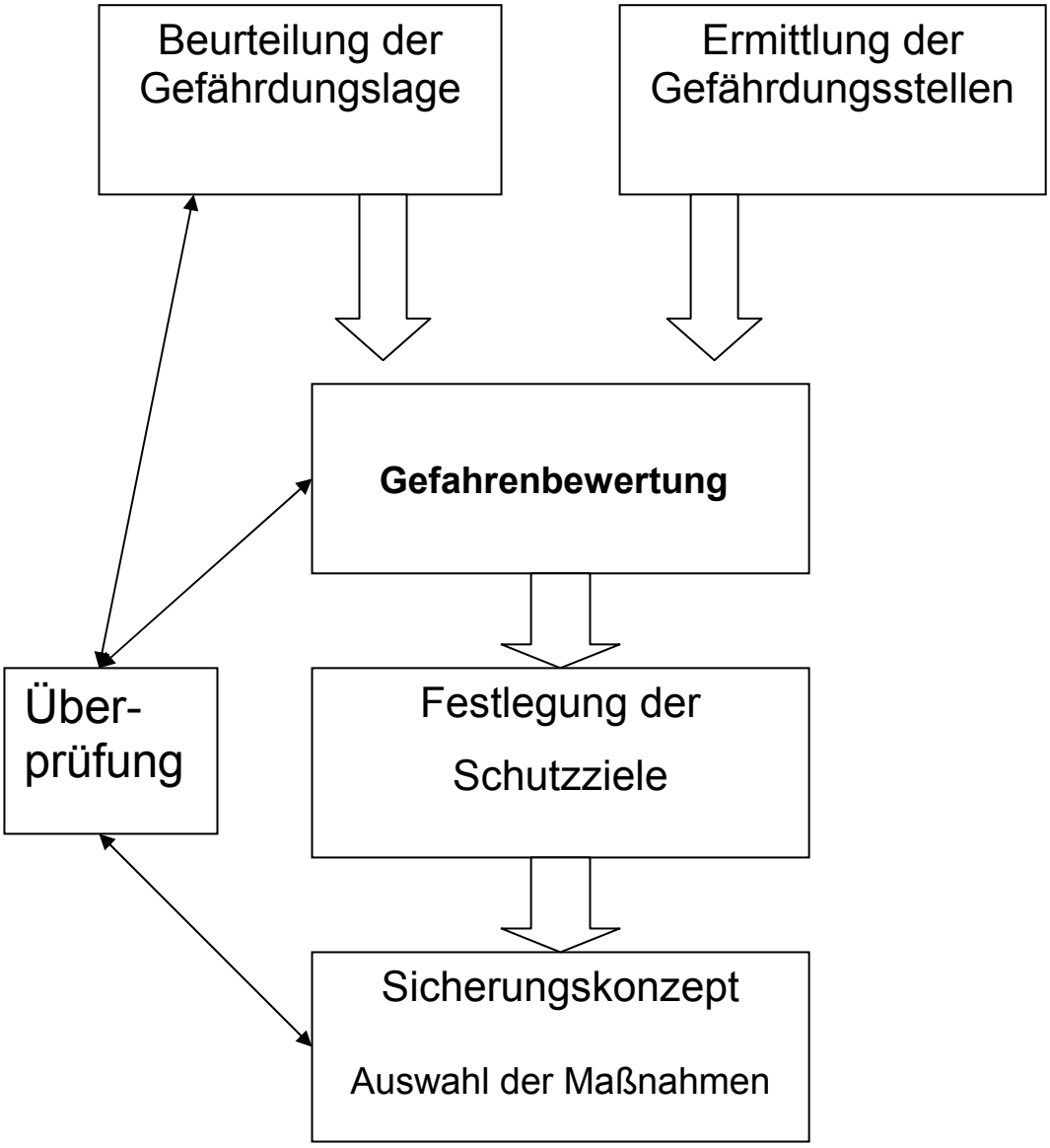


Bild 1: Vorgehensweise bei der Sicherungsanalyse

Die Frage nach eventuell zu erwartenden Tätern und ihrer Handlungsweise ist naturgemäß nicht mit Sicherheit zu beantworten. Auf der Grundlage von Erfahrungen bei der Betriebssicherung lässt sich jedoch eine Grobeinteilung mit Verursacher- bzw. Tätergruppen, ihren typischen Motiven und möglichen Verhaltensweisen in einer nach Gefährlichkeit abgestuften Tabelle *(Gefährdungsarten-Tabelle)* vornehmen.
Voraussetzung ist eine nähere Untersuchung der Gesamtsituation des Betriebsbereichs. Hinweise für das Durchführen dieser Untersuchung, sowie einen Vorschlag für das Aufstellen einer Gefährdungsarten-Tabelle enthält Anhang 1, *Kap. 3 "Gefährdungslage"*.

2.2 Identifikation der spezifischen Gefährdungsstellen im Betriebsbereich

Zuverlässiger zu ermitteln sind die Gefährdungsstellen innerhalb eines Betriebsbereichs. Ein Gefährdungsbild ergibt sich hier aus der Fragestellung, auf welche Weise an welcher Stelle ein Störfall ausgelöst werden könnte oder ein erhebliches Risiko dafür besteht.

Auch in diesem Falle kann mit Hilfe einer Tabelle das Gesamtbild übersichtlich dargestellt werden *(Gefährdungsstellen -Tabelle)*.

Besondere Hinweise auf Gefährdungsmöglichkeiten ergeben sich dabei aus dem Sicherheitsbericht nach § 9 StörfallV, der als wichtige Erkenntnisquelle für das Untersuchen der fahrlässigen oder vorsätzlichen Einwirkung im Rahmen der vorgeschlagenen Sicherungsanalyse angesehen werden muss. Die notwendigen Untersuchungen zum Ermitteln und Beurteilen der betrieblichen Gefahrenstellen werden im Anhang 1, *Kap. 4, "Gefährdungsstellen"*, erläutert.

2.3 Bewertung der Gefahren im Verhältnis zu den gesetzten Schutzzielen

Das Gegenüberstellen der Ergebnisse aus den Untersuchungen zur Gefährdungslage (Ermitteln von Gefährdungsarten) mit den einzelnen Gefährdungsstellen ergibt die individuelle Bedrohung für die Anlage. Es kann nunmehr abgeschätzt werden, an welchen Stellen mit welcher Einwirkung vernünftigerweise zu rechnen ist. Dieser Vorgang wird im Anhang 1, *Kap. 5, "Gefahrenbewertung"*, beschrieben.
Aus der so vorgenommenen Gefahrenbewertung lassen sich grundsätzliche Schutzziele (s. auch Festlegung in § 3 StörfallV) und die im Einzelnen erforderlichen Maßnahmen zum Verhindern des Störfalleintritts durch Einwirken von Personen ableiten *(Anhang 1, Kap. 6 " Sicherungsziele“)*.

2.4 Auswahl der Sicherungsmaßnahmen, Erstellung des integrierten Sicherungskonzepts

Die Sicherung eines Betriebsbereichs stellt immer ein Gesamtsystem dar, in dem die Komponenten organisatorischer, personeller sowie baulich/technischer Art gemeinsam wirken müssen. Zweckmäßig ist deshalb das Beschreiben der einzelnen *Sicherungsmaßnahmen* im Rahmen eines umfassenden *Sicherungskonzepts*, das die Zusammenhänge erkennen lässt. Der mögliche Aufbau eines derartigen Konzepts wird im Anhang 1, *Kap. 7, "Beschreibung der Sicherungsmaßnahmen/Sicherungskonzept"*, beispielhaft erläutert.

3 Gefährdungslage

3.1 Überblick

Die Gefährdungslage eines Betriebsbereichs hängt von einer Reihe unterschiedlicher Faktoren ab. Im vorliegenden Kapitel werden daher die für eine Lagebeurteilung wichtigen Einflussgrößen angesprochen. Zu den wesentlichsten Einflussgrößen gehören dabei die

- allgemeine Sicherheitslage,
- Zugehörigkeit des Betriebsbereichs zu anderen Unternehmen,
- örtliche Lage des Betriebsbereichs,
- Art der Produktion und der Lagerung von Stoffen,
- Bedeutung des Betriebsbereichs für nachgelagerte Produktionen und Dienstleistungen,
- Größe und Zusammensetzung der Belegschaft,
- Qualität der Sicherheitsorganisation,
- Gesellschaftliche Position von Angehörigen der Unternehmensleitung,
- Art der Vertriebsverbindungen und Auslandsaktivitäten,
- bisher festgestellte Kriminalität.

Welches Gewicht einzelne Faktoren für die Gefährdungslage annehmen, wird betriebsindividuell sehr verschieden sein. Die Diskussion der Einflussgrößen soll jedoch das Einordnen in bestimmte Gefährdungsarten ermöglichen, die Angaben über denkbare Verursacher, ihre Motive, Vorgehensweise, verwendete Hilfsmittel usw. enthalten. Insgesamt werden drei Gefährdungsarten aufgezeigt.

3.2 Allgemeine Sicherheitslage

Die allgemeine Sicherheitslage beschreibt Gefährdungen, wie sie für Betriebsbereiche generell gelten, gegebenenfalls mit regionalen Unterschieden. Verlässliche Gradmesser hinsichtlich der „klassischen“ Kriminalität sind die polizeiliche Kriminalstatistik sowie Veröffentlichungen der Versicherer. Die Sicherheitslage hinsichtlich politisch motivierter Straftaten wird bestimmt durch laufende Erkenntnisse der Behörden aufgrund ihrer kriminalpolizeilichen und verfassungsschutzmäßigen Tätigkeiten. Hiernach können auch regionale Aspekte stärker berücksichtigt werden.

3.3 Zugehörigkeit zu anderen Unternehmen

Gehört der zu untersuchende Betriebsbereich zu einem größeren Unternehmen (Unternehmensbereich, Tochter, Mehrheitsbeteiligung usw.), so muss die Gefährdungslage des Gesamtunternehmens zusätzlich berücksichtigt werden. Dies gilt hauptsächlich in Hinblick auf politisch motivierte Straftaten.
Erfahrungsgemäß wächst die Gefahr allgemein mit der Größe und (globalen) Bedeutung des Gesamtunternehmens.

3.4 Örtliche Lage des Betriebsbereichs

Der Bedrohungsgrad hängt in gewissem Umfang weiterhin von der örtlichen Lage des Betriebsbereichs ab. Zum Beispiel können sich beispielsweise alteingesessene Betriebsbereiche in ländlichen Gebieten meist auf die Betriebsverbundenheit und Loyalität

ihrer Mitarbeiter verlassen, ein Umstand, der zu einer stabilen Sicherheitslage beitragen kann.

Eine Rolle spielen auch benachbarte Betriebsbereiche oder anderweitige Einrichtungen, wenn von dort besondere Gefahren (Domino-Effekt) ausgehen (z.B. Brand/Explosion).

Weitere Faktoren betreffen die unmittelbare Umgebung des Betriebsgeländes. Hier stellt sich z.B. die Frage, ob ein unbemerktes Annähern an die Betriebsgrenze (z.B. aufgrund der Bepflanzung) möglich ist oder auch umgekehrt das Überklettern des Werkzaunes wegen der Anwohner mit hohem Entdeckungsrisiko verbunden ist. Zu beachten ist schließlich die durchschnittliche Anfahrtszeit der Polizei und deren Zufahrtsmöglichkeiten. Führt z.B. nur eine Zufahrtsstraße zum Betriebsbereich, besteht ein größeres Risiko der Blockierung aufgrund winterlicher Verhältnisse oder durch ein vorsätzliches Versperren.

Zusammengefasst sollten die folgenden Informationen vorhanden sein:

- Angaben zur allgemeinen Umgebung des Betriebsbereichs,
- Charakterisierung des Umfeldes, gegebenenfalls Hinweise auf besondere Gefahren aus dem Umfeld,
- Angaben zur unmittelbaren Peripherie bei allen Werkseiten,
- Angaben über die Zufahrten von der nächsten Ortschaft, gegebenenfalls Hinweise auf die Möglichkeit der Beeinträchtigung,
- durchschnittliche Anfahrtszeiten der externen Hilfskräfte, insbesondere der Polizei,
- Lageplan mit allen für die Objektsicherung wichtigen Details (Anforderungen an einen derartigen Lageplan sind im Anhang 1, *Kap. 7.1* beschrieben).

3.5 Sicherungsmanagement

Hinweise zum Aufbau und der Dokumentation eines Sicherungsmanagements enthält Anhang 3 dieses Leitfadens.

3.6 Sicherungsorganisation

Umfang und Ausbildungsstand der Sicherungsorganisation (Personal mit Sicherungsaufgaben), insbesondere des Werkschutzes, eines Betriebsbereichs spielt eine besondere Rolle bei der Abwehr von Gefahren, die sich aus vorsätzlichem Verhalten von Personen ergeben können.

Von großer Bedeutung ist dabei der Werkschutz, zu dessen Aufgabe insbesondere die Abwehr vorsätzlicher bzw. krimineller Handlungsweisen gehört.

Für die erforderlichen vorbeugenden Maßnahmen zum Vermeiden von Schäden durch Fehlbedienung oder Fahrlässigkeit sind die Betreiber, unterstützt durch ihre Störfallbeauftragten sowie ihre Fachkräfte für Arbeitssicherheit verantwortlich. Ihre Aufmerksamkeit sollte verstärkt auch auf die Prävention vorsätzlicher Fehlhandlungen sowie die Begrenzung von deren eventuellen Folgen gerichtet werden. Bei größeren Betriebsbereichen gibt es noch Werkfeuerwehren und Umweltschutzabteilungen, die insbesondere in die schadensbegrenzenden Maßnahmen eingebunden sind.
.
Außerordentlich wichtig ist die Zusammenarbeit aller Organisationen, die erfahrungsgemäß bei einer einheitlichen Führung im besonderem Maße gewährleistet ist.

3.7 Art der Produktion und Lagerung

In diesem Kapitel soll ein Überblick über Produktion und Lagerung gefährlicher Stoffe und der hieraus erwachsenden prinzipiellen Risiken gegeben werden (eine detaillierte Betrachtung erfolgt im Anhang 1, *Kap. 4 "Gefährdungsstellen"*).
Zu betrachten sind dabei auch benachbarte Betriebsteile, die nicht der StörfallV unterliegen. In diesem Fall können Risiken erwachsen, wenn z.B. hier gelegte Brände auf den "Störfallbereich" übergreifen könnten oder auch besondere Kriminalitätsanreize aufgrund der Produktion/Lagerung in der Nachbaranlage bestehen.

Von großer Bedeutung für die Gefährdungseinstufung ist schließlich die Frage, inwieweit das hergestellte und gelagerte Produkt oder auch das Herstellungsverfahren Gegenstand erheblicher politischer oder gesellschaftlicher Diskussionen ist.

3.8 Bedeutung des Betriebsbereichs für nachgelagerte Produktionen und Dienstleistungen

Bestimmte Anlagen können eine Schlüsselfunktion für nachgelagerte Produktionen oder Dienstleistungen haben. Hierzu gehören Anlagen, die in einem Wirtschaftsraum nur einmal vorhanden sind oder deren Kapazitäten voll ausgelastet sind und die nicht in kurzen Zeiträumen wiedererrichtet werden können. Der durch ihren Ausfall ausgelöste wirtschaftliche Schaden und die damit verbundenen politischen Konsequenzen können vor allem das Ziel politisch motivierter Täter sein.

3.9 Belegschaft

Bei der Belegschaft geht es zunächst um die eigentliche Größenordnung. Je mehr Mitarbeiter beschäftigt sind, um so schwieriger ist ein Beurteilen der Bedrohung aus diesem Kreis und um so mehr muss mit Personen gerechnet werden, die willens und in der Lage sind, dem Betrieb zu schaden (Innentäter).

In diesem Zusammenhang spielt das Betriebsklima eine große Rolle. Ein unbefriedigendes Betriebsklima führt zur Demotivation von Mitarbeitern, die sich auch in der "laxen" Handhabung von Sicherheitsvorschriften äußern kann. Aus einem schlechten Arbeitsklima - dieses kann auch auf Betriebsteile/Abteilungen beschränkt sein- entwickelt sich meist Interesselosigkeit, insbesondere auch in Bezug auf Sicherheitseinrichtungen und -vorschriften; die Hemmschwelle zu fahrlässigem oder vorsätzlichem Verhalten ist geringer.

Ausländische Mitarbeiter stellen grundsätzlich kein größeres Sicherheitsrisiko dar als deutsche Arbeitnehmer. Ein Risiko kann erwachsen, wenn aufgrund von Sprachbarrieren oder wegen der Mentalität Sicherheits- bzw. Sicherungsvorschriften missverstanden oder missachtet werden.

Betriebsfremde Personen stellen ebenfalls kein höheres Risiko dar als Mitarbeiter unter der Voraussetzung, dass sie mit den betrieblichen Gegebenheiten und Sicherheits-/Sicherungsmaßnahmen voll vertraut sind und eine feste Beziehung zum Betriebsbereich haben.

Schließlich ist die Arbeitszeit und Schichteinteilung zu beachten. Hier geht es vor allem um Zeiten, in denen nicht gearbeitet wird und nur wenige oder keine Mitarbeiter im Werk sind. In den dienstfreien Zeiten - z.B. am Wochenende- ist das Risiko des kriminellen Einwirkens durch Betriebsfremde am größten.

Zusammengefasst sollten die folgenden Informationen vorhanden sein:

- Gesamtanzahl der Belegschaft mit Aufschlüsselung männlich/weiblich und Altersstruktur,
- Anteil ausländischer Mitarbeiter aufgeteilt in Nationalitäten,
- Anzahl ständig anwesender Leasing-Kräfte oder Fremdfirmenmitarbeiter und Angaben über deren Bindung an den Betriebsbereich (insbesondere Dauer der entsprechenden Zusammenarbeit),
- durchschnittliche Anzahl von Besuchern,
- Arbeitszeiten und Schichteinteilung in den Anlagen, wegen derer der Betriebsbereich der StörfallV unterliegt,
- Ggf. Angaben über das Verhältnis der Belegschaft zur Unternehmensleitung, das sich z.B. in Fluktuationsraten und im Bild des Betriebsbereichs in der Öffentlichkeit ausdrücken kann,
- Erkenntnisse über Aktivitäten radikal-politischer Gruppierungen im Betriebsbereich und im Umfeld des Betriebsbereichs.

3.10 Unternehmensleitung

Hier steht die Frage im Vordergrund, inwieweit Mitglieder des Unternehmensvorstandes z.B. durch ihre Aktivitäten oder aufgrund ihrer Positionen in Verbänden oder Parteien im Mittelpunkt gesellschaftspolitischer Auseinandersetzungen stehen und von daher Aktionen gegen den Betriebsbereich nicht ausgeschlossen werden können.

3.11 Vertriebsverbindungen

In diesem Zusammenhang sollte festgestellt werden, ob durch bestimmte Vertriebsverbindungen höhere Risiken bestehen. Dies könnte z.B. der Fall sein bei Geschäftsverbindungen mit politisch instabilen Ländern. Da Betriebsbereiche mit Exportausrichtung in der Regel meist in alle Welt liefern, besteht ein erhöhtes Risiko vor allem bei besonders herausragenden Verbindungen zu derartigen Ländern.

3.12 Bisher festgestellte Kriminalität

Umfang, Schwere und Art der in einem Betriebsbereich bisher festgestellten Delikte können ebenfalls Hinweise auf den Gefährdungsgrad geben. Dabei kann ein Zeitraum von etwa 5 Jahren angesetzt werden. Insgesamt sollten die folgenden Informationen enthalten sein:

- pauschale Angaben über die festgestellten kleineren Delikte wie z.B. einfacher Diebstahl (hoch, mittel, niedrig),
- Anzahl der bisher verübten Einbrüche oder schweren Diebstahlsdelikte,
- Feststellung von organisierter Kriminalität im Betriebsbereich,
- Anzahl bisher verübter Sabotagehandlungen einschließlich unaufgeklärter Fälle, bei denen ein erheblicher Sabotageverdacht besteht,
- Anzahl der bisher verübten Bombendrohungen oder anderweitige Bedrohungshandlungen,
- Anzahl bisher verübter Brandstiftungen oder Sprengstoffanschläge einschließlich der Verdachtsfälle.

3.13 Gefährdungsarten

Als Ergebnis der Untersuchungen zur allgemeinen Gefährdungslage eines Unternehmens kann ein Zuordnen bestimmter Gefährdungsarten vorgenommen werden. Die einzelnen Stufen geben dabei einen Überblick über eventuell zu erwartende Täter, deren mögliche oder auch typische Vorgehensweise, ihre Ziele und Motive sowie über den Grad der kriminellen Energie. Mit ihrer Hilfe kann übersichtlich dargestellt werden, welche Risiken vernünftigerweise in Betracht zu ziehen sind.

Inwieweit die angenommenen Täter tatsächlich ernsthaften Schaden anrichten können und an welcher Stelle dies möglich und wahrscheinlich ist, muss Gegenstand weiterer Untersuchungen sein (*siehe Anhang 1, Kap. 4 "Gefährdungsstellen"*).

Die insgesamt drei aufgezeigten Gefährdungsarten enthalten eine Reihe von Annahmen, die eine Zuordnung zur ermittelten Gefährdungslage ermöglichen sollen. Zu diesen Annahmen gehören im Wesentlichen die:

- möglichen Begleitumstände der Tat,
- möglichen Motive und typische Handlungsweisen,
- wahrscheinlich verwendeten Hilfsmittel und
- zu erwartende kriminelle Energie.

Die zusammenpassenden Annahmen innerhalb einer Gefährdungsart beruhen auf kriminalistischer Erfahrung, müssen jedoch nicht in jedem Einzelfall unbedingt genau zutreffen.

Insoweit darf kein zu enges Auslegen beim Zuordnen zu einer Anlage erfolgen. Zweckmäßig ist eine Wahrscheinlichkeitsabschätzung für das Vorhandensein einer Gefährdungsart nach den folgenden Schritten:

1: in jedem Fall anzunehmen
2: wahrscheinlich
3: kaum wahrscheinlich
4: kann ausgeschlossen werden

Beim Ergebnis "Schritt 1 oder 2" wird das Vorhandensein der betreffenden Gefährdungsart als gegeben angenommen. In fast allen Fällen werden mehrere Gefährdungsarten infrage kommen.

Die einzelnen Gefährdungsarten sind nachfolgend dargestellt. Fahrlässige Handlungen werden in diesem Sicherungskonzept nicht berücksichtigt. Nähere Informationen zu den Tatmitteln sind Anhang 1, Kap. 4.3 zu entnehmen.

Gefährdungsart 1

a)	Begleitumstände	:	<u>Bedingter Vorsatz</u> Der Verursacher (Straftäter) will einen aus seiner Sicht begrenzten Schaden verursachen. Eine weit höhere Gefahrensituation (Störfall) nimmt er billigend in Kauf oder ist ihm nicht bewusst.
b)	Motive	:	Rache, Frustration, Unzulänglichkeiten "nachweisen“, gesellschaftspolitische Effekte erzielen
c)	Vorbereitungshandlungen	:	Ausspähen, Beschaffen von Werkzeugen und anderen Tatmitteln.
d)	Tatmittel	:	Einfache und schwere Werkzeuge ggf. einfache Brandsätze
e)	Kriminelle Energie	:	Motivabhängig, durchschnittlich.
f)	Personenkreis	:	Straftäter aus dem Innen- und Außenbereich, die für sich selbst oder im Auftrag handeln. Entlassene, ehemalige Mitarbeiter, Mitarbeiter, Fremdfirmenangehörige und Besucher
g)	Anmerkungen / Beispiele	:	- Außerbetriebsetzen von Sicherheitseinrichtungen, - Eingriffe in Produktionsabläufe, - Nicht Weitermelden kritischer Anlagenzustände, - Brandstiftung, Vandalismus nach erfolglosem Einbruch, - Brandstiftung aus anderen Motiven.

Gefährdungsart 2

a)	Begleitumstände	:	<u>Direkter Vorsatz</u> Der Verursacher (Straftäter) will den Eintritt eines größeren Schadensfalles und die damit ausgelöste Gefährdungslage bis hin zum Störfall, ggf. auch als Ablenkungsmanöver.
b)	Motive	:	politische Radikalität, Racheakt, Erzielen von Vermögens-/Wettbewerbsvorteilen
c)	Vorbereitungshandlungen	:	Erkunden sicherheitsrelevanter Anlagenteile und Schwachstellen. Ausnützen von Lücken bei der Überwachung. Bei Notwendigkeit Beschaffen aufwendiger Hilfsmittel. Außerbetriebsetzen von Sicherheitseinrichtungen.
d)	Tatmittel	:	Einfache und Spezialwerkzeuge, Brandsätze, einfache Sprengmittel (Selbstbau).

e)	Kriminelle Energie	:	Überdurchschnittlich
f)	Personenkreis	:	Einzeltäter, Tätergruppen, auch im Rahmen der „organisierten Kriminalität", radikale politische Gruppen.
g)	Anmerkungen / Beispiele	:	- Brandstiftung/Sprengstoffanschlag, - Zerstören von wichtigen Betriebseinrichtungen, - Eingriffe in Steuerungsanlagen, - Fehlprogrammierung von Steuerprozessoren.

Gefährdungsart 3

a)	Begleitumstände	:	Massive terroristische Anschläge Gemeingefährliche, brutale Vorgehensweise, oft ohne Rücksicht auf (das eigene) Menschenleben. Bewaffnetes Vorgehen.
b)	Motive	:	"Fanal setzen", Anarchismus, Herbeiführen gesellschaftlicher Veränderungen mit Gewalt, "Bestrafen" von Unternehmen, glaubensbezogene Motive.
c)	Vorbereitungshandlungen	:	Logistische Vorbereitungen, Ausspähung, Außerbetriebsetzen von Sicherheitsanlagen.
d)	Tatmittel	:	Einfaches und schweres Werkzeug, Waffen, Brandsätze, Sprengstoff.
e)	Kriminelle Energie	:	Außergewöhnlich hoch.
f)	Personenkreis	:	Extremistische und terroristische Einzeltäter und Gruppen.
g)	Anmerkungen / Beispiele	:	- Bewaffneter Überfall, - Aufsprengen von Behältern, - Beschuss von Einrichtungen, - in Brand setzen größerer Anlagen, - Angriffe auf Werkschutzpersonal, - gezielte Sprengstoffanschläge auf besonders empfindliche Bereiche.

4 Gefährdungsstellen

Die im vorigen Abschnitt dargestellten Gefährdungsarten sind stets in Verbindung mit spezifischen Gefährdungsstellen zu betrachten. Es ist differenziert zu betrachten, an welchen Stellen oder in welchen Bereichen das Schadensereignis (Störfall) ausgelöst werden kann. So ergibt sich beispielsweise ein erheblicher Unterschied, wenn an einer Stelle durch einfaches Betätigen eines Handrades das Ereignis eintreten könnte oder aber der gleiche Schaden an anderer Stelle nur unter Sprengstoffeinsatz zu verursachen wäre.

4.1 Einteilen in Bereiche

Die nach Diskussion der Gefährdungslage aufgestellten Gefährdungsarten mit ihren Hinweisen auf die im Prinzip denkbare Bedrohung betreffen zunächst das gesamte Unternehmen. Jeder Betriebsbereich setzt sich jedoch aus Bereichen, Einheiten oder Anlageteilen zusammen, die sich nach Gefahrenpotential, Bauart, Nutzung, technischer Auslegung und vor allem in ihrer Empfindlichkeit gegen Störeinflüsse unterscheiden. Auch innerhalb von Anlageteilen sind in der Regel Stellen besonderer Empfindlichkeit vorhanden (Beispiel: Behälter, Sicherheitsventile, Notkühlaggregate usw.). Diese sind ggf. anhand einer getrennten Untersuchung systematisch zu ermitteln.

Wie bei dem Sicherheitsbericht nach § 9 StörfallV sind auch im Falle der Objektsicherung sowohl die eigentlichen Gefährdungspotentiale (Stoffart und -menge) als auch die Einrichtungen zum Versorgen und Steuern der Anlagen sowie die Stofftransportsysteme usw. zu betrachten.

In der Regel ist es deshalb sinnvoll, den Betriebsbereich in eine Anzahl von Teilbereichen unterschiedlicher Art und Gefährdung aufzuteilen.

Das Untersuchen restlos aller potentiellen Schwachpunkte kombiniert mit den vielfältigen, denkbaren Einwirkungsmöglichkeiten ergibt in der Regel eine nicht beherrschbare Zahl von Varianten. Es ist von daher eine mehr pauschale Zusammenfassung von Anlagebereichen oder -teilen geboten.

So kann es z.B. sinnvoll sein, einen zusammenhängenden Komplex als Ganzes zu betrachten, also ohne näheres Untersuchen, welche einzelnen Komponenten und Teile empfindlich sind und welche genaue Auswirkung ein eventueller Angriff auf die eine oder andere Komponente der Anlage zur Folge hat.

Der betreffende Anlagen-Komplex wird als sicherungsrelevant eingestuft und insgesamt so gesichert, dass alle Einzelkomponenten mit erfasst sind. Wird beispielsweise der Zugang zu einer Ventilgalerie für Unbefugte verhindert, ist es unerheblich, auf welche Weise und an welchen Ventilen manipuliert werden könnte.

Bei Versorgungssystemen, die im gesamten Betriebsbereich eingesetzt sind, sollten möglichst Teilbereiche mit Bezug auf störfallbedrohte Objekte gebildet und die Untersuchung nicht unnötig auf umfangreiche Gesamtnetze ausgeweitet werden. Sinnvolle Zusammenfassungen von Gefährdungsbereichen können z.B. sein:

- Behälter, Lagerstellen,
- Abfüllstationen,
- Steuerzentralen, Schaltwarten, EDV-Anlagen,
- Rohrkanäle,
- Kabeltrassen,

- Pumpenhäuser,
- Ventilgalerien,
- Produktionshallen, -abschnitte,
- Kühlaggregate,
- Notaggregate aller Art,
- Hochspannungsleitungen und Einspeisestellen,
- Elektroversorgungseinrichtungen,
- Energieversorgungsanlagen aller Art, usw.

4.2 Hinzuziehen des Sicherheitsberichts

Bei der Diskussion von Möglichkeiten der Schadensentstehung sind die Aussagen des Sicherheitsberichts heranzuziehen. Die hier aufzufahrenden Faktoren wie die Verfahrensbeschreibung, Ereignisabläufe, die Angaben über Lagermengen und vor allem das Darstellen einzelner Gefahrenquellen sind für das Sicherungskonzept von grundlegender Bedeutung.

Beim Betrachten des vorsätzlichen Einwirkens von Personen ergibt sich jedoch eine erweiterte Fragestellung, weil die absichtliche Handlungsweise zusätzliche Möglichkeiten der Schadensentstehung zulässt. So kann unter Sicherheitsaspekten das doppelte Auslegen einer Notversorgung als ausreichend betrachtet werden, nicht jedoch beim Unterstellen krimineller Handlungen, wenn z.B. durch Eingriff in die Steuerung beide Notaggregate auf einfache Weise auszuschalten sind. Häufig wird in den Sicherheitsberichten auch das Zusammentreffen unterschiedlicher Störeinflüsse (z.B. Stoffverunreinigung mit der Folge thermischer Reaktionen und Ausfall der Kühlanlage) als unwahrscheinlich ausgeschlossen. Im Rahmen der Sicherungsanalyse ist zu prüfen, inwieweit beide Störeinflüsse gezielt herbeigeführt werden können.

4.3 Gefährdungsstellen-Tabelle

Listet man eine Reihe denkbarer Einwirkungsmöglichkeiten auf und stellt diese den ermittelten Gefährdungsstellen gegenüber, so entsteht eine Tabelle, die in übersichtlicher Weise Auskunft darüber gibt, an welchen Stellen oder Bereichen des Betriebsbereichs mit welchen Mitteln und Methoden im Prinzip eine ernsthafte Störung hervorgerufen werden könnte. Das folgende *Bild 2* zeigt ein Beispiel hierzu. In der Praxis können die verschiedenen Einwirkungsmöglichkeiten, z.B. „Eingriff mit einfachem oder schwerem Werkzeug“, etc. auch zusammengefasst dargestellt werden.

Nr.	Einwirkungs-möglichkeit	Gefährdungsstelle 1 „Tanklager“	Gefährdungsstelle 2 „Halle Verfahrenstechnik“	Gefährdungsstelle 3 „Rohrbrücke“	Gefährdungsstelle 4 „Steuerzentrale“
01	vorsätzliches Fehlbedienen	Ja	Ja (Während der Produktion durch Mitarbeiter)	nein	nein
02	Manipulieren	Nein	Nein	nein	ja
03	Fahrzeug-verkehr	Ja	Nein	nein	nein
04	Eingriffe mit einfachem Werkzeug	Nein	Ja	nein	nein
05	Eingriffe mit schwerem Werkzeug	Ja	Ja	ja	nein
06	Brandstiftung mit einfachen Mitteln	ja (Im Ex-Bereich)	ja (Im Ex-Bereich)	nein	nein
07	Brandstiftung mit brandfördern-den Mitteln	Ja	Ja	nein	nein
08	Einsatz von Sprengstoff	ja	ja	ja	nein
09	Beschuss	ja	nein	ja	nein
10	Ereignisse außerhalb der eigentlichen Anlage	Ja (Brand in Gebäude 'X')	nein	nein	nein
11	Entwenden gefährlicher Stoffe	Nein	nein	nein	nein

Bild 2: Beispiel einer Gefährdungsstellen-Tabelle

Als prinzipiell denkbare **Einwirkungsmöglichkeiten/Tatmittel** werden angenommen:

Vorsätzliches Fehlbedienen (01)

Hierunter sollen alle vorsätzlichen Handlungen verstanden werden, bei denen durch einfache Handgriffe und ohne den Einsatz von Tatmitteln ein Störfall ausgelöst werden könnte.

Zu derartigen Handlungen könnten z.B. zählen das

- Schalten/Abschalten von Einrichtungen,
- Auf-/Zudrehen von Rohrleitungsverschlüssen (Schiebern),
- Drehen von Handrädern, Betätigen von Hebeln im Prozessverlauf usw.

Das vorsätzliche Fehlbedienen kann dabei durch Mitarbeiter oder Betriebsfremde vorkommen.

Manipulieren (02)
Unter Manipulieren wird das vorsätzliche Verändern oder Verstellen von Systemteilen zum Zwecke des Herbeiführens eines kritischen Anlagenzustandes verstanden. Beispiele hierfür könnten sein das

- Fehlprogrammieren von Steuerungen,
- Dejustieren von Messeinrichtungen,
- Unterdrücken von Prozess-, Stör- oder Alarmmeldungen,
- Vorbereitendes Verhindern des Startens von Notaggregaten
- Ausschalten von Schutzsystemen usw.

Als Täter kommen nur "Insider" mit genauen Anlagenkenntnissen in Frage.

Fahrzeugunfall (03)
Durch Fahrzeugunfälle im Straßen- oder Schienenverkehr des Betriebsbereichs könnten gefährliche Stoffe freigesetzt oder wichtige Anlagenteile beschädigt bzw. zerstört werden. Beispiele sind:

- Fassleckage durch Gabelstaplerunfall,
- Entgleisen von Kesselwagen,
- Zerstören von Anlagen durch LKW-Aufprall usw.

Als Täter kommen Mitarbeiter und Firmenfremde infrage.

Eingriffe mit einfachen Tatmitteln (04)
Hier ist an ein vorsätzliches, meist spontanes Eingreifen in wichtige Anlagenteile mit den in jedem Betrieb vorhandenen Hilfsmitteln und Werkzeugen gedacht (Hammer, Meißel, Zangen, Handbeil, Lötlampe, Schloss- Zylinder- Abzugsvorrichtung). Beispiele könnten sein das

- Durchtrennen von Leitungen,
- Zerschlagen von Glasteilen der Anlage (z.B. Füllstandsmesseinrichtungen),
- Festklemmen beweglicher Teile einer Anlage,
- Zumischen nicht erlaubter Stoffe in den Prozess usw.

Infrage kommen dabei in erster Linie Mitarbeiter.

Eingriffe mit schweren Tatmitteln (05)
Bei dieser Einwirkungsmöglichkeit wird das vorbereitete gewaltsame Zerstören von Anlageteilen unterstellt.
Als Angriffswerkzeuge können Brechstange, Elektrische Bohrmaschine, Schneidbrenner, Bolzenschneider, Vorschlaghammer, Entsperrwerkzeug für Zylinderschlösser, Pulverschneidbrenner, Diamantkronbohrgerät, Sauerstofflanze in Frage kommen.
Beispiele hierfür sind das

- Aufbrechen von Türen und anschließendes Zerstören von Einrichtungen,
- Zerschlagen von Mess- und Steuereinrichtungen,
- Aufschlagen von Behältern und Rohrleitungen mit der Folge größerer Leckagen usw.

Anstelle des gezielten Anschlages kann auch Vandalismus treten, so z.B. als blinde Zerstörungswut nach einem erfolglosen Einbruch.

Brandstiftung mit einfachen Mitteln (06)

Unter einfachen Mitteln wird das Zünden mit Streichhölzern, Feuerzeugen oder durch Zigarettenkippen verstanden. Die Einwirkungsmöglichkeit besteht daher nur beim Vorhandensein ausreichender Mengen brennbaren und ausreichend leicht entzündbaren Materials.
Beispiele könnten sein das

- Anzünden von brennbaren Flüssigkeiten aus dem verfahrenstechnischen Ablauf,
- In Brand Setzen von Lagerstellen mit der Folge des Freisetzens gefährlicher Stoffe,
- In Brand Setzen von peripheren Räumen oder Einrichtungen mit Auswirkungen auf wichtige Anlagenteile.

Brandstiftung mit brandfördernden Mitteln (07)

Hier geht es um Brandanschläge, die mit Hilfe von schnell und intensiv abbrennenden Stoffen ausgeführt werden. Beispiele für Anschläge können sein das

- Ausgießen und Anzünden von brennbaren Flüssigkeiten (z.B. Benzin),
- Werfen von sogenannten "Molotow-Cocktails" (z.B. auch durch Fenster),
- Anbringen professioneller Brandsätze mit Zeit- oder Fernzündeinrichtungen.

Die Anschläge setzen eine hohe kriminelle Energie voraus.

Einsatz von Sprengstoffen (08)

Hier könnten Selbstlaborate, gewerbliche oder militärische Sprengstoffe eingesetzt werden. Mögliche Angriffsbeispiele sind z.B. das

- Anordnen einer "Feuerlöscher-Bombe" als Selbstlaborat innerhalb empfindlicher Anlagenteile oder wahrscheinlicher an der Gebäudeperipherie,
- Aufsprengen von Behältern und Rohrleitungen,
- Wegsprengen von tragenden Bauteilen mit der Folge des Umstürzens von Behältern,
- Zerstören von Anlageteilen usw.

In der Regel liegt bei dieser Angriffsart Fremdeinwirkung mit radikal-politischen Hintergrund vor.

Beschuss (09)

Im einfachsten Fall ist mit dem Beschuss durch Luftdruckgewehre oder Schleudern (Stahlkugel) zu rechnen bis hin zum Einsatz schwerer Waffen terroristischer Täter. Einwirkungsmöglichkeiten könnten sein

- Verursachen von Leckagen in freistellenden Behältern oder in Rohrleitungen,
- Ausschalten von Mess- und Überwachungseinrichtungen aus der Entfernung,
- Ausschalten von Versorgungseinrichtungen aus der Entfernung.

Ein Beschuss ist vor allen Dingen von außerhalb der äußeren Umfriedung eines Betriebsbereichs bzw. Industrieparks möglich, wobei in Zaunnähe installierte Anlagenteile stärker gefährdet sind.

Ereignisse außerhalb der eigentlichen Anlage (10)

Die Gesamtanlage oder sicherungsrelevante Teile der Anlage können auch durch vorsätzlich herbeigeführte Störfälle in benachbarten Betriebsbereichen oder Verkehrsanlagen in Mitleidenschaft gezogen werden. Einwirkungsmöglichkeiten können z.B. sein:

- im Brandfall das Übergreifen eines Feuers von benachbarten Einrichtungen,
- der Flug von Trümmern nach einer Explosion in benachbarten Einrichtungen,
- der Ausfall von Versorgungseinrichtungen durch Katastrophenereignisse außerhalb der Anlage usw.

Das Einwirken setzt besondere Gefährdungspotentiale bei den umgebenden Einrichtungen voraus (Domino – Effekt gemäß § 15 StörfallV).

Die Einwirkungsmöglichkeiten 01 bis 10 unterstellen Ereignisse, die mehr oder weniger alle Betriebsbereiche betreffen können. Darüber hinaus sind insbesondere vom Produktionsverfahren abhängige betriebsspezifische Gefahren denkbar. In diesem Fall ergeben sich u.U. zusätzliche Einwirkungsmöglichkeiten für Unbefugte.

Für jedes Feld der aufgestellten Tabelle muss die Frage diskutiert werden, inwieweit ein Störfall an dieser Stelle durch dieses Einwirken zustande kommen kann. In der Regel muss ein Abschätzen der Störfallgefahr vorgenommen werden, z.B. nach den Annahmen:

1. Störfall nicht möglich,
2. Störfall unwahrscheinlich,
3. Störfall kann nur zusammen mit anderen Einwirkungen eintreten.
4. Störfall ist möglich,
5. Störfall ist unvermeidlich,

Bei den Annahmen 1 und 2 wird das betreffende Feld mit "Nein", bei 4 und 5 mit "Ja" gekennzeichnet. Können nur zwei oder mehrere unterschiedliche Einwirkungsmöglichkeiten in Kombination zum Störfall führen (Annahme 3) sind entsprechende Hinweise einzutragen. Beispiele für Kombinationen sind:

- Leckage und Brandstiftung
- Ausfall Kühlung und Notkühlung usw.

Dabei muss ein allzu kompliziertes Einwirken von Unbefugten mit gleichzeitiger Aktion oder aufwendigen Tatvorbereitungen an mehreren Stellen meist nicht unterstellt werden.

5 Gefahrenbewertung

Eine Gefahrenbewertung unter Berücksichtigen der aufgestellten Gefährdungsarten ergibt für die einzelnen Einwirkungsmöglichkeiten eine Aussage, ob mit der angenommenen Möglichkeit auch vernünftigerweise gerechnet werden muss.

Sind nicht alle Gefährdungsarten gleichermaßen anzusetzen, was bei der überwiegenden Zahl der Anlagen zu unterstellen sein dürfte, kann die Gefährdungsstellen-Tabelle entsprechend reduziert werden. Wird z.B. ein massiver Terrorismus (Gefährdungsart 3) vollständig ausgeschlossen, entfallen in der Regel die Einwirkungsmöglichkeiten mit Sprengstoff (08) oder Beschuss (09) und es ergibt sich ein Bild der eigentlichen Gefährdung. *(s. Bild 3)*

Nr.	Einwirkungsmöglichkeit	Gefährdungsstelle 1 „Tanklager“	Gefährdungsstelle 2 „Halle Verfahrenstechnik“	Gefährdungsstelle 4 „Steuerzentrale“
01	vorsätzliches Fehlbedienen	ja	ja	_____
02	Manipulieren	_____	_____	ja
04	Eingriffe mit einfachen Tatmitteln	_____	_____	_____
06	Brandstiftung mit einfachen Mitteln	ja (Im Ex-Bereich)	ja	_____
07	Brandstiftung mit brandfördernden Mitteln	ja	_____	_____
10	Ereignisse außerhalb der eigentlichen Anlage	ja (Brand in Gebäude „X“)	_____	_____

Bild 3: Reduzierte Gefährdungsstellen-Tabelle

Weitere Reduzierungen ergeben sich, wenn Einwirkungsmöglichkeiten zu unterschiedlichen Zeiten betrachtet werden. So entfallen nach Arbeitsende beispielsweise die Einwirkungsmöglichkeiten "vorsätzliche Fehlbedienung" und "Fahrzeugverkehr". Während der Arbeitszeit z.B. ist das Risiko von Eingriffen mit schweren Tatmitteln deutlich geringer als außerhalb der Arbeitszeit.

6 Sicherungsziele

Sicherungsmaßnahmen können nur dann sinnvoll geplant werden, wenn klare Zielvorgaben über das bestehen, was sie bewirken sollen.

Aus der im Rahmen der Gefahrenbewertung aufgestellten Tabelle *(vergleiche Anhang 1, Kap. 5)* ergibt sich, an welcher Stelle mit welchen Mitteln ein Störfall ausgelöst werden könnte. Im Umkehrschluss können daraus geeignete Schutzziele abgeleitet werden, eben das Verhindern der Störfallauslösung an den infrage kommenden Stellen.

Ableitend von den Sicherungszielen ist es zweckmäßig, die grundsätzliche Richtung für das Auslegen der Sicherungsmaßnahmen vorzugeben, damit nicht in den Detailauslegungen eine zu große Fülle alternativer und oft überhaupt nicht infrage kommender Lösungen diskutiert werden muss. Hierbei wird es in der Regel nicht notwendig sein, für jeden ermittelten Schwachpunkt eine besondere Sicherungsmaßnahme festzulegen, vielmehr können meist mehrere Gefährdungspunkte gleichzeitig erfasst werden.
Befinden sich beispielsweise in einem Gebäude mehrere Räume mit wichtigen Komponenten, die als Gefährdungsstelle ausgewiesen sind, kann die Sicherungsmaßnahme lauten: "Das Betreten des Gebäudes XY durch betriebsfremde Personen ist zu verhindern".

Bei diesem Beispiel ist bereits ersichtlich, dass die Sicherungsmaßnahmen sehr sorgfältig und fachgerecht zu überlegen sind, damit ihre Durchführbarkeit gewährleistet ist und die zu treffenden Maßnahmen mit vernünftigem Mitteleinsatz zu verwirklichen sind.
Stellt sich bei dem gewählten Beispiel im Zuge der näheren Untersuchung heraus, dass der Zutritt für Fremde in das Gebäude aus Gründen unabdingbarer Betriebsabläufe nicht zu verhindern ist (z.B. fremde Wartungsfirma), könnte die Sicherungsmaßnahme wie folgt modifiziert werden: "Das Betreten der Räume A, B und C in Gebäude XY durch fremde Personen ist zu verhindern" oder, wenn auch das nicht durchzusetzen ist: "Das Betreten ist nur in Begleitung von Mitarbeitern der zuständigen Abteilung erlaubt".
Weitere typische Sicherungsvorgaben können z.B. sein:

- Der Zugriff auf die Steuerungseinrichtungen einschließlich der Software darf nur von besonders autorisiertem Personal vorgenommen werden können.
- Sicherungsrelevante Schalteinrichtungen sind durch die Gefahrenmeldeanlage zu überwachen. Beim Fehlbetätigen erfolgt Alarm in der Schaltwarte.
- Der Gefahrenbereich ist vom übrigen Betriebsgebäude durch baulich/mechanische Maßnahmen abzutrennen.
- Das Eindringen in das Lagergebäude nach Dienstende ist durch mechanische Barrieren zu erschweren und durch elektronische Überwachungsmaßnahmen zu melden usw.

7 Beschreibung der Sicherungsmaßnahmen/ Sicherungskonzept

Wie bereits erläutert, ist für die Wirksamkeit der Objektsicherung des funktionale Zusammenspiel aller Sicherungsmaßnahmen personeller, organisatorischer, baulicher oder technischer Art Voraussetzung. Um die Zusammenhänge transparent zu machen, sollte das Beschreiben der einzelnen Maßnahmen im Rahmen einer Gesamtkonzeption vorgenommen werden. Hierzu wird das Anwenden einer in der Praxis erprobten **Gliederung** empfohlen, die in den Hauptpunkten wie folgt aufgebaut sein könnte:

1 Standort und Lage
2 Äußere Umschließung
3 Zugangs-/Zufahrtskontrolle zum Betriebsgelände
4 Sicherung gefährdeter Bereiche
5 Organisatorische Maßnahmen
6 Sicherungsorganisation
7 Melde-, Überwachungs- und Kommunikationssysteme

Die umfassende Darlegung der Sicherungsmaßnahmen enthält zwangsläufig auch besonders geheimhaltungsbedürftige Informationen, siehe hierzu Anhang 1, Kap. 8.

7.1 Standort und Lage

Standort und Lage sind im Rahmen des Sicherheitsberichts bereits beschrieben. An dieser Stelle sind zusätzliche Angaben sinnvoll, wenn aufgrund des Standortes und der Lage bereits Sicherungsmaßnahmen vorgegeben sind. Dies ist z.B. der Fall bei Anlagen, die innerhalb eines größeren Betriebsareals liegen, das seinerseits bereits gesichert ist.

Zum übersichtlichen Darstellen der örtlichen Zusammenhänge ist ein Lageplan erforderlich. Viele der im folgenden geforderten Angaben können im Lageplan dargestellt werden. Dieser sollte im Einzelnen enthalten:

- Verlauf der juristischen Grenze des Betriebsbereichs,
- Verlauf der äußeren Umschließung mit Angaben über Art und Beschaffenheit,
- Lage der Tore und Zufahrtsstellen einschließlich der Pforten,
- Angaben über das Vorfeld des Betriebsbereichs (Gelände, Bebauung),
- Verkehrswege zum Betriebsbereich,
- Verkehrswege innerhalb des Betriebsbereichs,
- Parkplätze innerhalb und außerhalb des Betriebsbereichs, örtliches Anordnen der Beleuchtungseinrichtungen,
- Gebäude und Einrichtungen auf dem Betriebgelände mit Angaben der Funktionen,
- Gefährdungsbereiche und -stellen des Betriebsbereichs mit Kennzeichnen der Zugänge, gesonderte Umschließungen, usw. sowie
- Verlauf von sicherungsrelevanten Kabel- und Rohrleitungen.

7.2 Äußere Umschließung

Die äußere Umschließung eines Betriebsbereichs bzw. Industrieparks soll Unbefugte vom Betriebsgelände fernhalten und den Personen- sowie Fahrzeugverkehr über kontrollierte Zugangs- bzw. Zufahrtsstellen leiten. Voraussetzung dafür ist neben der allgemeinen Qualität der Umschließungsanlage ein völlig lückenloser Verlauf.
Im Einzelnen sollte die Beschreibung der äußeren Umschließung enthalten:

- Darstellen des Verlaufes der Umschließung, am besten anhand eines Lageplanes mit Angaben über die Beschaffenheit des vorgelagerten Geländes.
- Angaben über die Art und Konstruktion der Umschließungsanlage wie z.B. Metallgitterzaun, Mauerwerk u.a. -gegebenenfalls mit Kennzeichnen unterschiedlicher Ausführungen im Lageplan.
- Angaben über die Qualität der Umschließungsanlage mit
  - mechanischem Aufbau,
  - Höhe,
  - Überkletterschutz,
  - Unterkriech-/Untergrabschutz.
- Angaben über Zugänge und Zufahrten mit:
  - Art der Konstruktion (Fluchttür, Verkehrstor, Drehkreuz),
  - Verschluss,
  - Fernsteuerung,
  - elektronisches Überwachen,
  - Überwachen mit Videokamera.
- Angaben über die Beleuchtung der äußeren Umschließung.

7.3 Zugangs- und Zufahrtskontrolle zum Betriebsgelände

7.3.1 Kontrollmaßnahmen

Zur sicheren Funktion einer äußeren Umschließung gehört die Zugangs- und Zufahrtskontrolle zum Betriebsbereich bzw. Industrieparks. Hier ist zu beschreiben das Abwickeln des

- Personenverkehrs beim Zu- und Abgang mit Zugangsstellen und Wegen (Lageplan), Kontrollverfahren für Mitarbeiter, Kontrollverfahren für Besucher, Kontrollverfahren für Fremdfirmenmitarbeiter, gegebenenfalls Materialkontrollen (z.B. stichprobenweise) und

- Kraftfahrzeugverkehrs bei Zu- und Abfahrt mit Zufahrtsstellen (Lageplan), Kontrollverfahren für Personen und Warenverkehr bei Eigen- und Fremdfahrzeugen.

7.3.2 Pforten

Pforten sind wichtige Sicherungseinrichtungen mit der Hauptaufgabe "Zugangs- und Zufahrtskontrolle zum Betriebsgelände".

Außer bei größeren Betriebsbereichen/Industrieparks mit eigener Alarmzentrale sind in den Wachgebäuden am Tor meist zentrale technische Sicherheitsanlagen installiert. Diese betreffen z.B. die Funktionen:

- Entgegennehmen von Sicherheitsmeldungen aller Art (Feuer, Wasser,
- Störung, Einbruch);
- Alarmieren eigener oder fremder hilfeleistender Stellen im Notfall über

- Telefon, Lautsprecher, Personenrufanlage, Funkmeldeempfänger usw.;
- Fernüberwachen und Fernsteuern von Zugangsstellen z.B. über
- Videosysteme;
- Einschalten der Beleuchtung;
- Informieren der Belegschaft z.B. über Lautsprecheranlage;
- Kommunikation mit eigenen Sicherheitskräften z.B. über Sprechfunk
- Abfrage der Telefon-Nebenstellenanlage nach Dienstende usw.

Den Pforten kommt deshalb über die Aufgabe der Zufahrts- und Zugangskontrolle hinaus meist erhebliche Sicherungsbedeutung zu. In diesem Zusammenhang stellt sich deshalb die Frage nach der Sicherung der Pforte selbst. Ist z.B. die Hauptpforte einzige Stelle für das Entgegennehmen von Alarm- und Störmeldungen (häufig auch erst nach der normalen Dienstzeit des Betriebsbereichs), so darf das Weitergeben der Meldungen an hilfeleistende Stellen nicht durch Zugriff auf die Fernmeldeinrichtungen oder Bedrohung des Werkschutzes in der Pforte unterbunden werden können. Dies ist insbesondere durch geeignete technische Schutzmassnahmen sicherzustellen. Auch ist das ständige Besetzen der Pforte von zentraler Bedeutung.

Im Sicherungskonzept sind in diesem Falle insbesondere die Hauptpforten ausführlich zu behandeln. Im Einzelnen sollte angegeben werden:

- Lage der Pforten auf dem Betriebsgelände (Lageplan);
- baulich/mechanische Ausführung;
- Lenkung des Kraftverkehrs mit Verkehrsleitung an der Pforte, Lage der Schranken und Tore, Sitz/Position des kontrollierenden Werkschutzmitarbeiters, Lage der Besucherparkplätze;
- Lenkung des Personenstromes mit Verkehrswegen, Abfertigungsstellen (für Mitarbeiter und Besucher);
- Beleuchtung des Pfortenbereiches;
- Beschreibung der baulichen Auslegungen, insbesondere Barrierenwirkung von Fenstern und Türen;
- Grundriss mit Raumaufteilung und Angaben der Funktionen;
- personelle Besetzung der Pforte (Anzahl, Schichtzeiten);
- Auflisten der Melde-, Überwachungs-, Steuer- und Kommunikationssysteme und Bedieneinrichtungen in der Pforte.

7.3.3 Betriebsgelände

Angaben über das Betriebsgelände dienen im Wesentlichen der Übersicht insbesondere über die Lage der gefährdeten und zu sichernden Objekte. In den Angaben sollten enthalten sein:

- Verkehrswege,
- Betriebsgebäude mit Nutzung/Funktion,
- gegebenenfalls Kennzeichnung einzelner wichtiger Bereiche,
- Verlauf von sicherungsbedeutsamen Rohr- und Kabelwegen, unterirdische Kanälen usw.,
- besondere Gefahrenstellen.

Wesentliche Details der Angaben zum Betriebsgelände können im Lageplan dargestellt werden.

7.4 Sicherung gefährdeter Bereiche

Das Sichern der einzelnen Gefährdungsbereiche stellt meist die wichtigste Abwehrmaßnahme dar, da mit den „äußeren" Maßnahmen, die den gesamten Betriebsbereich betreffen, selten ein völlig ausreichender Schutz zu erreichen ist. So wird z.B. ein Risiko vorsätzlichen Handelns durch Mitarbeiter von den "äußeren" Maßnahmen nicht berührt.
Auch kann die Zugangskontrolle zum Betriebsbereich (etwa bei Schichtbeginn) kaum in tatsächlich lückenloser Weise durchgeführt werden. Im Gegensatz hierzu bestehen durchaus Möglichkeiten, an einzelnen Stellen des Betriebsbereichs eine wesentlich wirksamere Kontrolle durchzuführen.
In den meisten Fällen haben deshalb die Maßnahmen zum Sichern des Gesamtgeländes die Funktion eines Grundschutzes; sie bilden eine erste Schwelle zur Abwehr unbefugter Personen.
Der individuelle Schutz aller vorhandenen Gefährdungsstellen muss als wirksamste Abwehr zusätzlich erbracht werden. Die „klassischen“ Maßnahmen zur Anlagensicherheit spielen hierbei eine wesentliche Rolle. Dies gilt insbesondere für die redundante Auslegung besonders kritischer Sicherheitseinrichtungen, wobei es angezeigt sein kann, sie aus Sicherungsgründen räumlich zu trennen.

Maßnahmen zur Abwehr von insbesondere terroristischen Angriffen sind in Anhang 2 beschrieben.

Im Sicherungsbericht sollten die Sicherungsmaßnahmen für jede einzelne Gefährdungsstelle dargestellt werden, wobei ein Zusammenfassen in Bereiche, Gebäude, Abschnitte oder Funktionseinheiten nach der in Anhang 1, *Kap. 4 "Gefährdungsstellen"* vorgenommenen Aufteilung sinnvoll ist. Es versteht sich von selbst, daß gerade diese Ausführungen besonders geheimhaltungsbedürftig sind.

Für die einzelnen Gefährdungsstellen sollte angegeben werden:

- Lage auf dem Betriebsgelände (Lageplan), Lage innerhalb von Gebäuden oder Bereichen (Grundrissplan);
- Zugänge, Zufahrten, Fluchtwege;
- baulich/mechanische Ausführung bei Bereichsabtrennungen (Mauern, Zäune),
- bauliche Ausführung von Gebäuden und den sicherungsbedeutsamen Räumen (Material, Bewehrung, Wandstärken);
- mechanische Sicherung von Türen, Fenstern und Durchbrüchen;
- elektronische Überwachungsmaßnahmen bei Türen, Fenstern, Räumen usw.;
- Abwickeln der Zugangskontrolle zu den betreffenden Stellen während und nach der Dienstzeit für Mitarbeiter und Betriebsfremde;
- Sicherung einzelner Bedienungselemente gegen Fehlbedienen oder Sabotage z.B. durch mechanischen Verschluss oder elektronisches Überwachen;
- Anbringen von Hinweis- und Warnschildern;
- besondere Sicherungsmaßnahmen;
- Dienst- und Schichtzeiten der zuständigen Abteilung, gegebenenfalls Unterscheiden von Sicherungsmaßnahmen;
- Bestreifen der Objekte durch den Werkschutz (Streifenwege, Streifenzeiten).

7.5 Organisatorische Maßnahmen

Organisatorische Maßnahmen bilden einen wichtigen Rahmen, in den unterschiedliche Einzelmaßnahmen eingepasst werden müssen, damit eine sichere Funktion der Gesamtsicherung gewährleistet ist. In diesem Zusammenhang sollte behandelt werden das

- betriebliche Ausweiswesen mit Ausweisausgabe/-rückgabe, Ausweiskodierung (Art und Abwicklung), Ausweisaufbewahrung (Sicherung vor Zugriff), Zuständigkeiten;
- Einstellungs- und Überwachungsverfahren für Mitarbeiter mit Sicherungsaufgaben, Zugangserlaubnis zu gefährdeten Stellen, Arbeitsplätzen innerhalb gefährdeter Bereiche,
- Ausbilden, Unterweisen und Trainieren von Personen z.B. zum Vermeiden von Fehlbedienungen;
- Regeln der Aufsicht und regelmäßige Kontrolle bei Arbeiten in sicherungsrelevanten Bereichen;
- Schlüsselwesen im Einzelnen mit Schließsystem (Art, Umfang, Alter), Schlüsselausgabe, -rückgabe, -registrierung, Schlüssel- und Zylinderaufbewahrung;
- Reinigen sicherungsrelevanter Bereiche mit Eigen- oder Fremdkräften, Reinigungszeiten, Aufsicht bei der Reinigung, Personalkontrolle (bei Fremdpersonal);
- Auflisten von Dienstanweisungen für alle im Zusammenhang mit der Sicherung stehenden Maßnahmen;
- Alarmpläne für Brand/Explosion, Leckagen, Abwassergefährdung, anlagenspezifische Ereignisse usw.

Eine umfassende Darstellung des Sicherungsmanagements enthält Anhang 3.

7.6 Sicherungsorganisation

In diesem Kapitel soll ein Überblick über die zur Sicherheit des Betriebsbereichs erforderliche personelle Organisation gegeben werden. Hierzu gehören Werkschutz, Brandschutz, Arbeits- und Umweltschutz sowie die für das Instandhalten der Anlagen verantwortlichen Abteilungen. Die Gesamtorganisation sollte in einem Organigramm dargestellt werden, aus dem die Unterstellungsverhältnisse ersichtlich sind.

Von zentraler Bedeutung für die Anlagensicherung ist der Werkschutz, über den nähere Angaben erforderlich sind, wie z.B.:

- Unterstellungsverhältnisse (Organigramm), Gesamtstärke,
- Schichteinteilung und -stärke,
- Einsatz von Eigen- und/oder Fremdkräften,
- Aufsicht/Stichproben (bei Fremdpersonal),
- Aufgaben und Einsatz,
- Ausbildung und Ausrüstung
- Training sowie
- Dienstanweisungen, Alarmpläne.

7.7 Melde-, Überwachungs- und Kommunikationssysteme

Für die einzelnen mit Sicherheitsfunktionen eingesetzten Anlagen sind zu beschreiben:

- Aufgabe und Einsatz im Betriebsbereich,
- örtliche Anordnung im Betriebsbereich,
- Standort und Sicherung der zentralen Einrichtungen,
- Anordnung und Sicherung der Bedienstation,
- Verlauf und Sicherung der Kabelwege.

Bei größeren Anlagen ist ein Übersichtsschaltbild vorteilhaft.

8 Dokumentation

Die Analyse und die daraus abgeleiteten Maßnahmen sollten dokumentiert werden. Diese Dokumentation ist jedoch in besonderem Maße geheimhaltungsbedürftig und sollte auch innerhalb des Unternehmens nur einem beschränkten Kreis von Mitarbeitern zugänglich sein. Aus Unterlagen, die allen Mitarbeitern und der Öffentlichkeit zur Verfügung stehen, sollte jedoch schlüssig hervorgehen, dass der Betreiber die notwendigen Maßnahmen zur Sicherung des Betriebsbereichs und der Anlagen gegen Eingriffe Unbefugter getroffen hat. Prinzipielle Aussagen hierzu enthält Kapitel 6 des Leitfadens und Anhang 4.

Präventive Maßnahmen zur Abwehr von Angriffen

1. Allgemeines

Bei den betrachteten Abwehrmaßnahmen ist zunächst an Angriffe von Externen zu denken, also Angriffe, die von außerhalb des Werkzaunes ausgeführt werden. Betrachtet werden müssen aber auch Angriffe, die durch Täter aus dem Inneren der Anlagen heraus durchgeführt werden (Innentäter). Dieses können sowohl Mitarbeiter des eigenen Unternehmens sein als auch Externe, die sich Zugang ins Unternehmen verschafft haben.

Vom Betreiber geforderte Maßnahmen unterliegen dem Verhältnismäßigkeitsgrundsatz. Dies gilt insbesondere für eingreifende Maßnahmen wie etwa die Veränderung der Lage der gefährlichen Anlage mit dem Ziel, dass diese von außerhalb des Betriebsgeländes nicht oder nur erschwert anzugreifen ist. Ist diese Möglichkeit nicht gegeben bzw. nicht verhältnismäßig, so muß der Betreiber die Behörden unterrichten.

Wenn Maßnahmen von Seiten der Sicherheitsbehörden erforderlich sind, so sollte sich der Betreiber direkt mit diesen in Verbindung setzen.

2. Flugzeugattentate

Gegen Attentate durch anfliegende Flugzeuge sind präventive Abwehrmaßnahmen im Einflussbereich des Unternehmens nicht möglich. Hier sind staatliche Maßnahmen gefordert, die es schwierig oder unmöglich machen, mit Flugzeugen gezielt gegen eine Industrieanlage zu fliegen. Denkbar sind Einschränkungen der Überflugrechte, gezielte Beobachtungen des in Frage kommenden Luftraums und Maßnahmen im Rahmen der Flugzeugnutzung bzw. Benutzung selbst.

3. Raketen und Panzerfäuste

Davon ausgehend, dass Angriffe mit fernwirkenden Waffen wie Raketen und Panzerfäusten ausschließlich von außen vorgetragen werden, sind auch hier vorwiegend Maßnahmen der öffentlichen Sicherheit gefordert. Gedacht werden kann hier z. B. an eine Bewachung bzw. großräumige Umstreifung des Geländes von gefährdeten Anlagen durch öffentliche oder öffentlich beliehene Sicherheitskräfte. Besonderes Augenmerk muss topografischen Anhöhen in der Nähe von Anlagen gelten.

4. Bomben in Fahrzeugen

Sollten sich Anlagen in der Nähe der Werksgrenze befinden, so dass ein Angriff mit einer außerhalb der Begrenzung angeordneten Autobombe (oder auch Schiffsbombe) erfolgreich zu sein verspricht, dann muss aus dem Inneren heraus das vor dem Werkszaun liegende Gelände (Gewässer) mit überwacht werden. Alternativ kommen auch Begehungen außerhalb des Werkszauns in Betracht. Ebenso kann durch Festlegen von Fahrstrecken und Parkplätzen/Parkverboten vor gefährdeten Bereichen eine höhere Sicherheit geschaffen werden.

Geht man von Außentätern aus, die eine Autobombe ins Innere eines Werkes bringen wollen, so ist dem durch entsprechende Zaunkontrollen bzw. Zugangskontrollen an den Toren zu begegnen. Die Zaunkontrollen müssen sich auf die ständige Überprüfung der Dichtigkeit beziehen. Dies kann durch regelmäßige Begehungen oder auch durch Videokameras erfolgen. Bei der Zugangskontrolle wird die Identifikation der Zugehenden genau zu überprüfen sein. Weiterer wichtiger Prüfpunkt ist die Berechtigung des Zutritt Begehrenden, ob überhaupt ein nachweisbares Interesse bzw. Recht am Zugang besteht. Fremde sollten sich grundsätzlich nicht allein im Werksgelände bewegen dürfen.

Bomben könnten auch von Innentätern, also eigenen Mitarbeitern ins Werk gebracht werden. Ebenso ist es möglich, dass an Fahrzeugen von Mitarbeitern, ohne deren Wissen Bomben von Außentätern angebracht werden. Um dies auszuschließen, sind einfahrende Fahrzeuge, auch von eigenen Mitarbeitern, stets oder zumindest in dichten Stichproben zu überprüfen.

Die präzisen Ausführungen zu Zugangskontrollen und Fahrzeugkontrollen (auch für interne Mitarbeiter) müssen durch das Sicherungsmanagementsystem garantiert werden.

5. Kleinere Spreng- oder Brandsätze (USBV-Unkonventionelle Spreng- und /oder Brandvorrichtung)

Auch bei kleineren Spreng- oder Brandsätzen, die in Taschen, Umschlägen oder Päckchen transportiert werden können, müssen sowohl Außen-, als auch Innentäter betrachtet werden.

Wie bei der Abwehr von Autobomben ist im wesentlichen auf die Zugangskontrolle abzuheben. Es muss vermieden werden, dass Unberechtigte ins Werk hineingelangen. Selbst bei Berechtigten, denen ein Zutritt gewährt wird, sind zumindest stichprobeartig die Taschеninhalte zu überprüfen.

Die präzisen Durchführungen der Zugangskontrollen und Fahrzeugkontrollen (auch für interne Mitarbeiter) müssen durch das Sicherungsmanagementsystem garantiert werden.

Diese Überlegungen sind gegen Außen- und Innentäter gleichermaßen wirksam.

6. Gefahrgut-LKW

Der Angriff mit einem Gefahrgut-LKW (mit oder ohne zusätzliche Zündvorrichtung) ist in der Regel ein Angriff von Außen. Eine Abwehrmöglichkeit besteht durch staatliche Maßnahmen, also Überwachung der Umgebung des Werkgeländes. Zur Unterstützung der Polizei sollten werkseitig auch mögliche Durchbruchspunkte durch den Zaun des Werks ermittelt werden.

Eine präventive Maßnahme seitens der Anlagenbetreiber besteht darin, dass die Fahrer, die Gefahrgut in die Werke transportieren oder aus den Werken abholen, außerordentlich exakt identifiziert werden müssen. Damit kann weitgehend verhindert werden, dass Unberechtigte einen Gefahrguttransport führen.

Des Weiteren könnten Maßnahmen von Seiten des Betreibers ergriffen werden, die gerade und von außen auf die Anlagen zulaufende Straßenzüge im Inneren des Werkgeländes unterbrechen (Wälle oder Gräben, etc.).

7. Manipulationen

Um eine Anlage durch Manipulationen an den Steuerungs- und Regelinstrumenten zu stören, muss der Täter zunächst ins Werk eindringen. Als Abwehrmaßnahme greift hier die intensive Zugangs- und Zaunkontrolle. In besonders gefährdeten Bereichen könnte es ggf. nützlich sein, auch im Inneren des Werks eine Bestreifung durch Sicherheitsleute durchführen zu lassen.

Additiv sollten Maßnahmen ergriffen werden, um besonders sicherheitsrelevante Anlageteile zusätzlich zu sichern, da der Einsatz von dann benötigten technischen Hilfsmitteln (bei nicht elektrisch gesteuerten Anlagenteilen) bei Eingriffen Unbefugter erforderlich ist und ein Erkennen des Täters vereinfacht. Des Weiteren könnten hochsensible Anlagenteile zusätzlich durch klassische Überwachungsmaßnahmen (Kamera, Zugang mit Anmeldung) geschützt werden. Soweit Sicherheitseinrichtungen redundant ausgelegt sind, sollte aus Sicherungsgründen eine räumliche Trennung erwogen werden.

Erfolgt die Manipulation durch einen Innentäter, sind kaum Abwehrmöglichkeiten gegeben. Der Innentäter ist aus Sicht der Systeme kein Unbefugter (die rechtliche Frage, ob ein derartiger Eingriff überhaupt ein Eingriff Unbefugter ist, soll hier außen vor gelassen werden). Es helfen gegen diesen Täter keine genaueren Identifikations- oder Zugangskontrollen, denn in jedem Falle werden die Systeme diesen Täter nicht fernhalten können, da sie ihn als zum Zutritt Berechtigten erkennen. Dieser Täter hat auch die notwendigen Detailkenntnisse, um durch gezielte Manipulationen eine schwere Störung auszulösen. Vor derartigen Angriffen können die Unternehmen eine funktionierende Unternehmenskultur, ein gutes Betriebsklima und funktionierende Teams bewahren.

Bleibt nach Ausschöpfen aller anderen Sicherungsmaßnahmen ein relevantes Risiko durch Innentäter bestehen, sollten die für die innere Sicherheit zuständigen Behörden zu Rate gezogen werden. Als „ultima ratio“ kann auch eine Sicherheitsüberprüfung von Mitarbeitern in hochsensiblen Bereichen nicht ausgeschlossen werden.

Sicherungsmanagement

Das nachfolgend beschriebene Sicherungs-Management-System (SeMS) erweitert das Sicherheits-Management-System (SMS) nach Anhang III der StörfallV hinsichtlich der Sicherung von Betriebsbereichen gegen die Eingriffe Unbefugter. Die einzelnen Maßnahmen sind in geeigneter Weise in die vorgegebene Systematik des Anhangs III einzubauen, so dass **ein einheitliches** Managementsystem im Sinne des Anhangs III erhalten bleibt. Im Sicherheitsbericht ist das Vorgehen entsprechend darzulegen. Die Behörde bezieht im Rahmen ihrer Überwachung nach § 16 StörfallV die Überprüfung der SeMS-Bausteine ein.

Sicherungsmanagement
Managementsysteme haben sich in der Vergangenheit als Instrument zur systematischen Handhabung und Überprüfung von Unternehmensabläufen bewährt. Insbesondere im Zusammenhang mit Unternehmenssicherheit ist eine ständige systematische Steigerung von Effizienz und Transparenz der Prozesse von größter Bedeutung. Die Vorgehensweise und die zusätzlichen Elemente eines Managementsystems zur Sicherung des Unternehmens sollen im Folgenden kurz skizziert werden. Unternehmen sollten solche Systeme verbindlich einführen, um die notwendigen Sicherungen gegen den Eingriff Unbefugter jederzeit belegen zu können.

<u>Unternehmenspolitik</u>
In einer Selbstverpflichtungserklärung (Sicherungspolitik) macht das Unternehmen sein Verhältnis zu Sicherheit und Sicherung deutlich. Das Unternehmen verpflichtet sich, zusammen mit seinen Angestellten und seinen von ihm beauftragten Auftragnehmern dafür sorgen zu wollen, dass ständig eine sichere Arbeitsumgebung gewährleistet wird, in der die Investitionsgüter und die Betriebe gegen das Risiko von Verletzungen, Verlusten und Zerstörung durch kriminelle, feindliche oder heimtückische Angriffe geschützt und deren etwaigen Folgen für die Nachbarschaft begrenzt werden. Weiter erklärt das Unternehmen seine Verpflichtung, die angesprochenen Sicherheitsmaßnahmen auf dem aktuellen Stand der Technik zu halten und das SeMS regelmäßig zu überprüfen. Es wird versprochen, dass sämtliche Maßnahmen nicht gegen ethische Grundregeln verstoßen und nicht gegen die Interessen der Allgemeinheit gerichtet sein dürfen.

<u>Dokumentation</u>
Um ein Managementsystem prüfbar und überwachbar zu machen, ist es notwendig, einen Soll/Ist- Vergleich vornehmen zu können. Für ein Sicherungs-Managementsystem stellt dies eine Herausforderung dar, da zum einen eine Soll–Beschreibung vorhanden sein sollte, andererseits diese aber nicht dazu führen darf, dass durch die Art der Beschreibung das eigentliche Ziel - nämlich den Eingriff Unbefugter zu verhindern - durch eine zu detaillierte Darstellung aller organisatorischen und technischen Sicherungseinrichtungen in Frage gestellt wird.

Details der konkreten organisatorischen und technischen Maßnahmen sollten daher gegen den Zugriff aller Personen, die dieses Wissen nicht unmittelbar benötigen, geschützt werden und nicht öffentlich zugänglich aufbewahrt werden. Bei einer Überprüfung des Sicherungs–Managementsystems durch die einschlägigen Behörden sind die entsprechenden Unterlagen zu sichten und das Ergebnis der Prüfung ist zu dokumentieren.

Darüber hinaus sollten Unterlagen vorhanden sein, die es allen Mitarbeitern und auch Dritten (Nachbarn, Fremdfirmen etc.) deutlich machen, dass der Betreiber die notwendigen

Maßnahmen zur Sicherung des Betriebsbereichs und der Anlagen gegen Eingriffe Unbefugter getroffen hat und aufrecht erhält. Dies könnte z.B. dadurch geschehen, dass eingesetzte Ressourcen und Maßnahmen generell beschrieben werden.

Grundsätzliche Aussagen zur Offenlegung von Sicherheits- bzw. Sicherungsunterlagen enthält Kap. 6 des Leitfadens.

Organisation und Verantwortlichkeit
Die Verantwortung für die Sicherung eines Betriebes wird dem Management des Geschäftszweiges übertragen. Zu dieser Verantwortung gehört, dass die Manager Vorgehensweisen entwickeln müssen, die sicherstellen, dass die Sicherungsrisiken identifiziert (siehe Kapitel 4.1 und 4.2) werden und in Übereinstimmung mit der Firmenpolitik entschärft werden (siehe Kapitel 4.3). Die Manager sorgen für einen effektiven Prozess, der ausgehend von den Sicherungserwartungen die Umsetzung sicherstellt. Demzufolge sind die Sicherungserwartungen integriert in Planungs- und Entscheidungsprozesse des Geschäftszweiges. Für Sicherungsvorfälle wird ein Prozess eingeführt, der dafür sorgt, dass das Topmanagement unverzüglich unterrichtet wird.

Kommunikation und Schulung
Über Sicherungsvorfälle und Erfahrungen mit Sicherungstechnik wird mit anderen ein Informationsaustausch betrieben, um sicherzustellen, dass der jeweils aktuelle Stand der Sicherungstechnik bei den eigenen Maßnahmen eingehalten wird. Durch ständige Schulung ist dafür zu sorgen, dass nur fachkompetentes Personal beschäftigt wird und dass das Personal sich der aktuellen Sicherungsrisiken voll bewusst ist. Dies wird durch ständige Unterweisung zur Schulung des Bewusstseins für Sicherungsrisiken und ein spezielles Trainingsprogramm für das Personal mit Sicherungsaufgaben geleistet.

Festlegung der Sicherungsprozesse
Alle Unternehmensprozesse, in denen die Sicherung eine Rolle spielt, müssen festgelegt, dokumentiert und geplant sein. Hierbei sind insbesondere folgende Prozesse zu berücksichtigen:

- Kontraktorenüberwachung
  Alle Kontraktoren, die mit dem Unternehmen geschäftlich verbunden sind, müssen sich vollständig an die Sicherungsregeln und -prozeduren des Unternehmens anschließen und sich auch einer den Regeln entsprechenden Überwachung (Audit) unterwerfen .

- Risikobewertung
  Der Geschäftszweig muss jährlich Bewertungen des Sicherungsrisikos durchführen. Diese Bewertungen sind häufiger durchzuführen, wenn die Risikolage dies erfordert (Verfahren siehe Anhang 1, Kap. 3 –bis 5).

- Planung und Errichtung von Anlagen
  Bei der Planung und Errichtung von Anlagen ist die Beachtung der Sicherungsanforderungen (siehe Anhang 1, Kap. 6) ein wesentliches Element. Die Beachtung der Sicherungsziele muss entsprechend dokumentiert werden.

- Veränderungsmanagement
  Die Sicherungsauswirkungen von zeitweiligen oder andauernden Veränderungen müssen genau geprüft, gemanagt, dokumentiert und gegebenenfalls in ihren Auswirkungen auch beachtet werden. Um auf Veränderungen der Sicherungslage ohne Verzug reagieren zu können, sind Maßnahmenkataloge für die unterschiedlichen Niveaus von Gefährdungslagen vorzuhalten.

- Produktverantwortung

Sicherungsrisiken, die mit den Produkten des Unternehmens einhergehen, müssen geprüft und untersucht werden, um sicheren Umgang, Transport und Auslieferung zu gewährleisten und die Sicherheit der Kunden herzustellen.

- Notfallmanagement
  Ausrüstung, Installation und Personal für die Bewältigung von Sicherungsnotfällen ist zu identifizieren und jederzeit verfügbar zu halten. Für die Bewältigung von Notfällen ist eine Krisenabwehrorganisation bereitzuhalten, die ein ständig verfügbares Krisenreaktionsteam beinhaltet. Der „Kern“ des Teams sollte vorab festgelegt werden. Die Zusammensetzung des gesamten Krisenreaktionsteams kann jedoch je nach Situation unterschiedlich sein. So können einem Krisenreaktionsteam z.B. die Geschäftsführung, Vertreter der Rechtsabteilung, Vertreter der Revision, Vertreter der Sicherheitsabteilung, Vertreter der Arbeitsmedizin, Vertreter des Betriebsrates, ... angehören.

- Zusammenarbeit mit Behörden.
  Offener Dialog und offene Beratung mit Behörden und Interessenvertretungen stellen sicher, dass die möglicherweise von den Anlagen verursachten Sicherungsprobleme identifiziert und die Risiken minimiert werden können. Die Besorgnisse der Außenstehenden sind unbedingt ernst zu nehmen. Falls die regulative Möglichkeit gegeben ist, sollen Behörden in die Überwachung der Maßnahmen einbezogen werden.

Betrieb und Wartung der Sicherungseinrichtungen

Sicherungseinrichtungen müssen so betrieben und gewartet werden, dass sie sich stets auf dem aktuellen Stand der Technik befinden, immer einsatzbereit sind und ständig instandgehalten werden. Eine Sicherungsbetriebsanforderung ist zu entwickeln und das Sicherungsequipment sorgfältig so auszusuchen, dass diese Anforderungen erfüllt werden. Ein Qualitätssicherheitsprogramm existiert, um zu garantieren, dass die Ausrüstung stets einsatzbereit bleibt. Die Möglichkeit, die vorhandene Ausrüstung durch effektivere und eventuell kostengünstigere Systeme zu ersetzen, wird in angemessenen Zeiträumen immer wieder untersucht.

Überwachungsmaßnahmen

In Übereinstimmung mit der Unternehmenspolitik wird in regelmäßig wiederkehrenden Untersuchungen des Sicherungsmanagements der Status untersucht und festgehalten. Es werden jährliche und anlassbezogene Selbstüberprüfungen durch Experten durchgeführt. In diesen Überprüfungen wird gegen die in der Sicherungspolitik des Unternehmens festgelegten spezifischen Erwartungen an die Sicherungsmaßnahmen geprüft. Elemente solcher Sicherungsüberprüfungen können sein:

- Existenz der Sicherungsanalyse, eines Sicherungsplanes und eines Auditplanes
- Regelung der Verantwortlichkeiten für Sicherung
- Zustand der Sicherung der Einfriedung (Zugang, Zustand der Einzäunung, Beleuchtung, Videoüberwachung, Begehungen)
- Einrichtung der Sicherungsleitzentrale
- Qualifikation des Wachpersonals
- Identifikation von Punkten besonderer Gefährdung
- Sicherungsüberprüfung des eigenen Personals
- Unterrichtungen, Unterweisungen, Training
- Weitere Sicherungsprozesse wie Schlüsselverwaltung, Alarmierung bei Eindringversuchen, Verhalten bei Bombenalarm, Postüberprüfung usw.

Korrektur- und Vorbeugungsmaßnahmen

Sicherungsvorfälle werden festgehalten, berichtet und untersucht. Dies gilt insbesondere für schwere Vorfälle und Vorfälle mit dem Potential für einen schweren Vorfall. Die Untersuchung konzentriert sich auf die Ursachen, insbesondere auf die verdeckten,

hintergründigen Ursachen des Vorfalls. Die Vorfalluntersuchungen werden dokumentiert und die notwendigen präventiven Maßnahmen festgehalten. Die Umsetzung von zusätzlichen präventiven Maßnahmen ist ebenfalls zu dokumentieren.

Anhang 4

Beispiel für Kriterien der „qualifizierten Inhaltsdarstellung“

Anlage zur Herstellung von Toluylendiisocyanat (TDI) unter Verwendung von Phosgen

Vertrauliche Informationen können sein:

- Organisatorische, technische und bauliche Maßnahmen zur Sicherung der Anlage
- Hold-Up von Phosgen in einzelnen Anlagenteilen
- Exakte Lage von einzelnen Anlagenteilen
- Werkstoffe und Wandstärken einzelner Anlagenteile z.B. des Containments

Zu den nicht vertraulichen Informationen, die der Öffentlichkeit zugänglich zu machen sind, müssen i.d.R. gehören:

- Ziele der Sicherungsmaßnahmen (z.B.: Ein Eindringen Unbefugter auf das Werksgelände ohne technische Hilfsmittel ist aufgrund der baulichen und technischen Sicherungsmaßnahmen nicht möglich. Eine Annäherung Unbefugter an die Anlage wird vom Werksschutz durch geeignete Sicherungsmaßnahmen erkannt. Ein Zutritt zu der Anlage ist nur nach besonderer Identifikation der Person und Kontrolle aller mitgeführten Gegenstände möglich.)
- der Öffentlichkeit zugänglich zu machen sind alle sonstigen nach StörfallV geforderten Angaben, mit Ausnahme der oben genannten, insbesondere
- Hold-up der gesamten Anlage
- zumindest ungefähre Lage der Anlage auf dem Werksgelände
- Mögliche Auswirkungen im Störfall
- Mögliche Auswirkungen im Dennoch-Störfall
- Warnung und Information der Bevölkerung bei Störungen
- Erforderliches Verhalten der Bevölkerung bei Störungen

GFI Umwelt - Gesellschaft für Infrastruktur und Umwelt mbH

Geschäftsstelle
Störfall-Kommission und
Technischer Ausschuss für Anlagensicherheit

Königswinterer Str. 827
D-53227 Bonn

Telefon 49-(0)228-90 87 34-0
Telefax 49-(0)228-90 87 34-9
E-Mail sfk-taa@gfi-umwelt.de