

Technische Sicherheit

ATHLETIC SAFETY FOOTWEAR

Durably waterproof

Highly breathable

Lightweight

GORE-TEX
PRODUCTS



gore-workwear.de



Brandschutz

Schäden bei
Pelletheizungen

Explosionsschutz

Spritzlackieren mit
VOC-freien UV-
Lacken

Arbeits- und Gesundheitsschutz

Brandschaden-
sanierung

Risikosteuerung in der Industrie

Basismerkmale eines effektiven Sicherheitsmanagementsystems

Waldemar Witt, Hannover



Das Sicherheitsmanagement von technologischen Prozessen sieht vorbeugende organisatorische Maßnahmen und Mittel des Notfallschutzes zur Verhinderung, Einschränkung und Beseitigung gefährlicher Folgen industrieller Unfälle vor. Die gesetzlichen Vorgaben sollen das erforderliche Maß industrieller Sicherheit in allen Phasen gewährleisten, d. h. bei der Planung, Konstruktion, Anlagenfertigung und -montage, beim Betrieb, Umbau, Abbruch sowie bei der Stilllegung und beim Recycling.

Ein Unfall ist das Endergebnis eines Fehlerakkumulationsprozesses. Dies schließt u. a. Anlagen- und Systemausfälle, das Versagen der Schutzeinrichtungen und Notfallsysteme, aber auch menschliche Fehler ein.

Natürlich sollten alle Schutzeinrichtungen und Maßnahmen so konzipiert und ausgewählt werden, dass sie durch kohärent und aufeinander abgestimmte Prozesse negative Folgen eines Unfalls sicher verhindern können. Dies erfordert vor allem eine hochwertige Gefährdungsbeurteilung sowie eine Risiko- und Zuverlässigkeitsanalyse unter Berücksichtigung der technologischen Kohärenz und Kompatibilität der Ereignisse, der Teilnahme von Menschen als Elemente des Systems, der charakteristischen Besonderheiten der Entstehung und der Unfallentwicklung der jeweiligen Technologie.

Bezogen auf Anlagen mit erhöhtem Gefährdungsrisiko sind physikalische Bedrohungen wie Explosionen, Feuer und Ausbreitungen von toxischen Substanzen in der Atmosphäre, im Boden und im Wasser zu beachten. Ebenso sind Strahlungsgefahren zu berücksichtigen.

Unfälle mit katastrophalen Folgen sind seltene Ereignisse. Daher führt eine

statistische Bearbeitung der Parameter zu einer deutlichen Ausweitung des Vertrauensintervalls und damit zu unzuverlässigen Schlussfolgerungen und Entscheidungen.

Eine bessere Modellierung von Prozessen unter Berücksichtigung wichtiger Faktoren ermöglicht ein realistischeres Bild möglicher Folgen. Die Auswahl präventiver Mittel und Schutzeinrichtungen soll die dynamischen Eigenschaften der Prozesse berücksichtigen und ihre Schutzwirkung zuverlässig garantieren. Darüber hinaus sollten auch die Auswirkungen ihres Einsatzes betrachtet werden sowie ihre Konformität mit gesetzlichen Vorgaben.

Bei der Bestimmung des Sicherheits- und Zuverlässigkeitsniveaus werden häufig Fehler gemacht. Das Sicherheitsniveau kennzeichnet die möglichen Folgen der Störung (personelle, Sach- und Umweltschäden) und die Fähigkeit, durch organisatorische Maßnahmen und Schutzeinrichtungen diese Folgen zu verhindern, zu isolieren oder zu beseitigen. Das Sicherheitsniveau wird auch durch die Wahrscheinlichkeit gekennzeichnet, dass diese Mittel ihre Funktion zum richtigen Zeitpunkt zuverlässig durchführen.

Die Charakteristik der Sicherheit und Zuverlässigkeit wird durch sog. technologische Risiken dargestellt.

Ist das Risiko als quantitatives Maß der Gefahr und Gefahrauswirkung zu betrachten, ist der Prozess der Analyse und Überwachung der Risiken eine notwendige und hinreichende Bedingung für die Bewertungen und die Entscheidungen im Bereich der technischen Anlagensicherheit.

Aktives Management des technologischen Risikos

Die modernen Technologien werden immer komplexer und umfassender. Dies führt wiederum zu einem exponentiell steigenden Bedürfnis nach sicherer Betriebsführung und technischer Zuverlässigkeit. In der Folge macht die verstärkte Automatisierung die Produktionsprozesse oftmals anfälliger.

Die hohe Integration und Komplexität des Systemmanagements, Notfallschutzes und der technischen Unterstützungssysteme haben auch ihren Anteil an der Ausfallwahrscheinlichkeit. Gleichzeitig erhöht sich auch die Wahrscheinlichkeit menschlicher Fehler bei Betrieb und Wartung. In vielen Fällen steigt entgegen den Erwartungen das technologische Risiko.

Nicht vorhersehbare Prozesse bergen besondere Gefahren, die ohne eine gründliche Analyse nicht intuitiv definier- oder abschätzbar sind. Darüber hinaus führen Kostenreduzierungen im Bereich der Sicherheit oft zu Entscheidungen, die in Wirklichkeit die Risiken ansteigen lassen.

Das zeigt sich auch an folgenden Parametern:

1. Auf der Basis der Unfallstatistiken der letzten Jahre lässt sich feststellen, dass sich durch die zunehmende Komplexität der Prozesse die Zuverlässigkeit und Sicherheit nicht verbessert hat, was für die Unternehmen materiell und sozial bedrohlich werden kann. Der materielle Verlust aus einem einzigen mittelschweren Unfall in einer petrochemischen Anlage ist beispielsweise hundertmal höher als die gesamten Kosten für eine integrierte Risikobewertung, Zuverlässigkeitsüberwachung und optimale Entscheidungsfindung im Bereich der sicheren industriellen Prozessführungen.

2. Im Rahmen der aktuellen wirtschaftliche Lage ist es durchaus sinnvoll, technische und organisatorische Lösungen zu ergreifen, um ein akzeptables Maß an Risiko für die Produktion zu erreichen. Mögliche Verluste durch ein bestehendes Risiko sind das Ausmaß der negativen Auswirkungen unter Berücksichtigung der Wahrscheinlichkeit (Frequenz) ihres Auftretens. Die Kosten für die Vermeidung dieser Verluste basieren auf den Kosten der organisatorischen und technischen Mittel, die notwendig sind, um ein akzeptables Sicherheitsniveau der technologischen Prozessführung zu erreichen.

3. Der Geschäftsbetrieb sollte in Übereinstimmung mit den nationalen und internationalen Rechtsvorschriften durchgeführt werden. Allerdings ist auch die vollständige Einhaltung regulatorischer und normativer Anforderungen noch keine Garantie gegen Unfälle.

Die Methode der Steuerung des technologischen Risikos ist auf einen Ausgleich zwischen einer nicht hinnehmbaren (ggf. akzeptablen) Höhe der erwarteten Verluste und überflüssigen (ggf. unzureichenden) Kosten der Schutz- bzw. Notmaßnahmen für deren Verhinderung konzipiert. Es handelt sich um folgende Verfahren:

- Gefahren- und Performanceanalyse der Objekte mit einem Gefährdungspotenzial auf einer Methodenbasis entsprechend nationaler und internationaler Standards und Richtlinien. Analyse der

Betriebssicherheit, Zuverlässigkeit und Effektivität der Schutzeinrichtungen. Projektbezogen: Projektanalyse, Aufstellung des Sicherheitsberichts, Definition der Brandschutzmaßnahmen.

- Quantifizierung der Wahrscheinlichkeit (Frequenz) der Entstehung von verschiedenen und für die untersuchten Objekte charakteristischen Unfällen. Unter Berücksichtigung der kausalen Beziehungen und der Entwicklung eines Unfalls muss ein gewisses Maß an Objektivität erreicht werden. Dafür ist eine Anwendung von Methoden wie der Fehlerbaumanalyse oder der Ereignisbaumanalyse unvermeidbar. Nur in seltenen Fällen dürfen statistische Daten benutzt werden. Ranking-Methoden gelten in diesem Einsatz als subjektiv und unzuverlässig.

- Simulation der Bildung einer gefährlichen Umgebung, Entwicklung von Unfällen und deren negativer Auswirkungen. Dabei sollte die Zahl der Unfälle und ihre wirtschaftlichen Folgen ermittelt werden.

- Berechnung integrierter Risikoindikatoren, wie das territoriale Risiko, die erwartete Anzahl von Verletzten, das individuelle Risiko, die erwarteten Schäden und andere Faktoren, die die Basis für die Entscheidungen und Versicherungen sind. Erstellung von Risikoberichten.

- Industrielle Sachversicherung und betriebliche Haftpflichtversicherung. Es ist erstrebenswert, die Entscheidungen im Versicherungsbereich auf der Basis eines qualitativen Underwritingsprozesses einschließlich einer umfassenden integrierten Risikoanalyse zu treffen.

- Risikoüberwachung als Entscheidungsgrundlage während des Betriebs und des Umbaus der Anlage, Änderungen in der Geschäftsstrategie und der Versicherung. Entwicklung der unternehmensinternen Standards in Bezug auf das Management von technologischen Risiken.

- Unabhängige Untersuchung von Unfällen und Konflikten.

Es ist offensichtlich, dass das integrierte Risikomanagement auf einer Informationstechnologie basiert. Dies erfordert entsprechende Software-Werkzeuge für ihre Realisierung. Die Komplexität solcher Software-Lösungen ist enorm hoch. Ein solches System bietet durch die Zusammenführung von Naturwissenschaft, Technik, Ingenieurwesen, Informatik und gesetzlichen Vorgaben eine neue Möglichkeit, das Sicherheitsniveau von Industrieanlagen auf ein hohes Niveau zu bringen.

Informationstechnologie für die Sicherheitsanalyse und die Risiko-steuerung

Das Management technogener Risiken beinhaltet zunächst eine Klassifizierung technogener Objekte und eine Zuordnung zu Gefährdungsgruppen. Dafür kommen üblicherweise Methoden oder Verfahren zum Einsatz, wie z. B. HAZID (hazard identification) oder die Rang-Identifikation oder Klassifizierung nach Inhaltsmenge der gefährlichen Stoffe. Danach folgt die Untersuchung und gründliche Analyse des Objekts und seiner Umgebung.

Bei der Untersuchung werden charakteristische Gefährdungen und Performances von Einrichtungen (Hazard and Operability – HAZOP) unter kritischen Ausfallsituationen und Störungen einschließlich menschlicher Fehlhandlungen betrachtet. Der Analyse der Ursache-Wirkungs-Beziehungen der gefährlichen Prozesse kommt hierbei eine besondere Bedeutung zu.

Erste Voraussetzung für einen Unfall ist eine Änderung der Prozessparameter außerhalb der Grenzen des zugelassenen Bereichs, aber noch ohne Kontrollverlust über den gesamten Betriebsprozess. In diesem Stadium sichern eine einwandfreie technische Funktionalität der automatischen Schutzeinrichtungen und korrekte Handlungen des technischen Betriebspersonals den Erfolg.

Fehler und Ausfälle in diesem Stadium und den Vorstufen (Design, Installation, Ermittlung der Restressourcen etc.) können zur zweiten Stufe der Unfallentwicklung führen – unzulässige Parameteränderungen mit vollständigem Kontrollverlust. In diesem Stadium können richtige Handlungen des Fachpersonals und effektive Notfalleinrichtungen schwerwiegende Folgen vermeiden.

Mit einer Beschädigung und Zerstörung der Betriebseinrichtungen oder der Technologieelemente beginnt das dritte Stadium. In diesem Stadium ist mit möglichen Erscheinungsformen gefährlicher physikalischer Prozesse (Explosionen, Feuer, toxische, biologische oder radiologische Kontamination etc.), Verletzungen von Menschen, Sach- und Umweltschäden zu rechnen. Die Unfälle können katastrophale Auswirkungen haben und schwerwiegende langfristige negative Folgen verursachen.

Die Identifikation möglicher Folgen von Stör- und Unfällen ist eines der wichtigsten Ziele des Risikomanagements. Hierzu werden Modelle eingesetzt.

Die Qualität der Modellierung, ihre Grenzen und die Bewertung der Unfallfolgen sollten innerhalb eines akzeptablen Vertrauensintervalls liegen. Hier wird ein konservativer Ansatz (schlimmste Folge) bevorzugt.

Ein sehr wichtiger Aspekt bei der Modellierung ist die Transparenz und das Verständnis (Grundlage) der Definitions- und Anwendungsbereiche der Modelle.

Die nächste Stufe des Risikomanagements ist die Auswahl aller möglichen Notsituationen, die den stabilen Betrieb erheblich beeinträchtigen oder offensichtlich inakzeptablen Verlust und Beschädigungen auslösen können. In diesem Stadium ist es sinnvoll, die Entscheidungen zusammen mit dem Management des Unternehmens sowie den betreffenden Behörden zu treffen. Nur wenn diese eingebunden sind, kann das akzeptable Risiko definiert werden.

Der nächste Schritt ist die Bestimmung der Ereigniswahrscheinlichkeiten (Frequenzen) von Notsituationen für eine Bewertungsperiode. Dies erfordert den Einsatz von Fachleuten.

Das Resultat ist eine Quantifizierung von Unfallwahrscheinlichkeiten auf der Basis eines formalen Modells.

Meist werden für die Auswertung der operationellen Risiken die Fehlerbaum-Methode (FTA) und für die Beurteilung der Wirksamkeit und Zuverlässigkeit von Schutzmaßnahmen die Ereignisbaum-Methode (ETA) verwendet.

In einigen Fällen sind Rangliste-Methoden zulässig oder eine quantitative Ermittlung der Wahrscheinlichkeit auf der Basis der statistischen Datenverarbeitung. Wie schon erwähnt führen Statistiken für schwere Unfälle (die eindeutig seltenen Ereignisse sind) meist zu einem sehr großen Vertrauensintervall.

Im Gegensatz dazu wird die Verwendung statistischer Daten, technischer Parameter laut Hersteller sowie Ausfall-

daten einzelner Elemente (z. B. Armaturen, Messgeräte, Aktuatoren etc.) bei der Untersuchung ihres Verhaltens im Fehlerbaum nicht nur einen wesentlich zuverlässigeren Ansatz zur Bestimmung des Risikos ermöglichen, sondern auch helfen, durch spezielle Analyse-Methoden „Engpässe und Lücken“ in der Sicherheitstechnik und der Bedienung zu erkennen.

In der Endphase der Risikobeurteilung werden die entsprechenden Notsituationen ausgewertet und Risikoindikatoren bestimmt. Dazu gehören territoriale, persönliche und soziale Risiken, erwartete menschliche Verletzungen sowie erwartete Sachschäden. Auf der Basis dieser iterativen Methoden werden die Entscheidungen nur für solche Situationen, Elemente und Objekte getroffen, für die sich das Risiko als nicht akzeptabel herausgestellt hat.

Die Anwendung dieser Technologie bei der Bestimmung von „Maximalst möglichen Verlusten“ (PML), der Berichterstattung eines Sachverständigen oder bei einem qualitativen Underwriting-Prozess ermöglicht die Übertragung des Versicherungsprozesses von einer Finanztransaktion zu einer industriellen Sicherheitstechnologie.

Die Schwierigkeit bei der Umsetzung dieser Technologie sind fehlende (vollständige oder teilweise) effektive Informationssysteme. Darüber hinaus gibt es auch einen Mangel an hoch qualifizierten Spezialisten. Für eine vollständige und detaillierte Risikoanalyse eines Unternehmens muss eine Vielzahl von Informationen über die Objekte gesammelt und verarbeitet werden, was in Bezug auf den Aufwand und die Vertraulichkeit kein einfaches Unterfangen ist.

Fazit

Es gibt nur wenige Softwarelösungen, die sich meist nur am Rande mit dem Thema Risikoabschätzung beschäftigen

und dabei den Bereich Risikosteuerung gänzlich vermissen lassen.

Die enorme Komplexität, fehlendes Know-how und organisatorische Hindernisse bei der Erstellung solcher Informationstechnologien haben über Jahrzehnte die Entwickler ferngehalten.

Nach mehrjähriger Entwicklung hat nun die Fa. Savarex im Rahmen eines EU-Projekts das Informationstechnologie- und Programmsystem „Savarex Studio“ entwickelt.

Der multilinguale und autarke Systemaufbau stellt die Zusammenhänge von Prozessen, Ereignissen, Szenarien und Auswertungen dar und ermöglicht u. a. eine nachvollziehbare, vollständige und schnelle Sicherheits- und Risikobeurteilung.

Neben Lösungen zur Kostenoptimierung bei Wartungs- und Reparaturarbeiten dient das Programm auch bei der wissenschaftlich-technischen Gefahrenexpertise. So können u. a. Sicherheitsberichte und Notfallpläne für industrielle Einrichtungen mit erhöhtem Gefährdungspotenzial erstellt oder Risiken innerhalb eines Betriebs über den gesamten Lebenszyklus abgeschätzt werden.

Somit wird beim Einsatz dieser Informationstechnologie ein geschlossenes Loop-System mit einer informativen Feedback-Technologie realisiert und das Ziel – das höchste Sicherheits- und Zuverlässigkeitsniveau von Industrieanlagen zu erreichen – ermöglicht.

TS 318



Autor

Dipl.-Phys. Ing.-Inform.
Waldemar Witt,
Geschäftsführer,
Savarex GmbH,
Hannover.

Produkte

Komplettlösung für Detektion und Alarmierung

Der neue Integral CUBUS MTD 533X-SPCT von Hekatron verfügt über alle bewährten Eigenschaften des Mehrfachsensoren-Brandmelders MTD 533X – plus integrierter Ton- und Sprachausgabe. Damit unterstützt er im Brandfall

effektiv die Selbstrettung der Menschen aus dem Gefahrenbereich und ist somit prädestiniert für den Einsatz in Hotels, Schulen, Bürogebäuden, öffentlichen Gebäuden, Versammlungsstätten und anderen Objekten, in denen viele, oft ortsunkundige Personen zusammenkommen. Eine Sprachalarmierung mit klaren Aus-

sagen und Verhaltensanweisungen ermöglicht es gefährdeten Personen, im Brandfall schneller und zielgerichteter auf die Gefahr zu reagieren. Als kombinierter Rauch- und Wärmemelder erkennt der MTD 533X-SPCT frühzeitig Schwelbrände und offene Brände. Die integrierte CUBUS-Nivellierung mit ihrer