KAPITEL 7

Einführung in die Gefährdungs-Analyse

Jan Sanders 2010

7.1 Einführung

Diese Einführung in die Gefährdungsanalyse (engl. Hazard Analysis) soll einen kurzen Überblick über 3 grundlegende, oft verwendete Methoden verschaffen.

- Das systematische Suchen nach Gefährdungen in Systemdesigns mit HazOp, der Hazard and Operability Study,
- die Kritikalitätsbewertung von bekannten Gefährdungen mit FMECA, der Failure Modes, Effects and Critcality Analysis und
- der Abschätzung des operationellen Risikos mit Hilfe der FTA, der Fault Tree Analysis.

In dieser kurzen Einführung werden vereinfachte Versionen der drei Methoden verwendet, die aber alle noch die grundlegenden Prinzipien beinhalten.

Zuerst verwenden wir HazOp um eine möglichst vollständige Liste von Gefährdungen zu erhalten. Die Liste der dadurch gefundenen Gefährdungen wird danach einer Bewertung der Kritikalität unterzogen. Dafür verwenden wir die FMECA. Mit den bis hierhin gewonnenen Erkenntnissen kann ein untersuchtes System verbessert werden, so dass Gefährdungen durch Redesign, Sicherheitsfunktionen, Mitigationsmassnahmen und Redundanz vermieden oder beschränkt werden können. Um das verbleibende Restrisiko beurteilen zu können verwenden wir die FTA, die uns Kenn-

zahlen für Fehlerhäufigkeit und den zu erwartenden Schaden liefert.

Alle drei Methoden zusammen ermöglichen es eine nachvollziehbare Aussage über die Gesamtsicherheit eines Systems zu treffen.

Das System das hier als Beispiel dient ist bewusst klein gehalten. Die Methoden liefern keine tiefgreifenden Erkenntnisse über die Sicherheit des Beispielsystems und der Analyst wird vielleicht das Gefühl haben, dass er die Erkenntnisse auch aus dem Stegreif hätte erreichen können. Das Ziel dieser Einführung ist es aber ersteinmal mit der Funktionsweise der Methoden und ihrem Aufbau aufeinander vertraut zu werden.

Die Methoden selbst werden hier nur in einer verkleinerten Version verwendet, so dass sie im Rahmen der Einfühung noch für einen Person handhabbar und verständlich bleiben.

Für eine tiefergehende Betrachtung empfehlen wir "Probabilistic Risk Assessment", von Kunamoto und Henley.

7.2 Das Beispielsystem

Als Beispielsystem verwenden wir eine hypothetische Produktionsanalge für ein chemisches Produkt. Das System wird auf einer hohen Abstraktionsebene beschrieben, so dass es übersichtlich bleibt. Zwei flüssige Ausgangsprodukte werden in einem chemischen Reaktor zu einem gasförmigen Endprodukt hergestellt, welches dann in einem Gastank gelagert wird.

(Siehe Bild 1)

Legende:

RES 1, RES 2: 2 Reservoirs in denen zwei verschiedene flüssige Ausgangsprodukte lagern.

RGV 1, RGV 2: 2 Regelventile, die der Durchflusssteuerung dienen. Die Ventile regeln den Fluss der Ausgangsprodukte in Richtung des Reaktorbehälters (RKT)

RSV 1, RSV 2: 2 Rückschlagventile, die verhindern sollen, dass ein Überdruck im Reaktorbehälter dazu führt, dass Flüssigkeit oder Gas aus dem Reaktorbehälter in die Reservoirs RES 1 und RES 2 zurückfliesst.

RKT: Der Reaktorbehälter. In diesem Behälter vermischen sich die beiden Ausgangs-

produkte miteinander. In einer exothermen Reaktion entsteht ein gasförmiges Endprodukt.

RSV 3: Ein Rückschlagventil, das verhindern soll, dass ein erhöhter Druck im Gasreservoir GRES zu einem Rückfluss des Endproduktes in den Reaktor RKT führt.

GRES: Das Gasreservoir in dem das gasförmige Endprodukt gelagert wird.

7.3 Die HazOp des Beispiel-Systems

Das Ziel einer HazOp ist es eine möglichst vollsteändige Liste möglicher Abweichungen vom gewünschten Verhalten eines Systems zu entwickeln. Der Nachweis, dass eine solche Liste vollständig ist ist leider nicht möglich. Aber es ist möglich mit einer strukturierten Herangehensweise diesem Ideal möglichst Nahe zu kommen.

In einer HazOp verwendet man eine High-Level Systembeschreibung, die die Verhältnisse der Untersysteme zueinander beschreibt. Das Ergebis einer HazOp ist Abhängig von der Qualität der Systembeschreibung. Bei einem System mit meherern System-Untersystem Ebenen (siehe Bernd) wird die HazOp rekursiv auf den Untersystemen weitergeführt, sobald eine Abstraktionsebene behandelt worden ist. Dies wird hier nicht gemacht. Es soll nur der Prozess der Abweichungsfindung vorgestellt werden.

Das strukturierende Element einer HazOp bilden die sogenannten Leitwörter (engl. Guidewords). Dabei handelt es sich um abstrakte Begriffe, die eine Abweichung eines Systems von seinem gewünschten Verhalten suggerieren sollen. In vieln Branchen gibt es ganze Kataloge mit Listen von Leitwörtern. Im Rahmen dieser Einführung soll aber die folgende Liste genügen:

Leitwörter:

- zu viel
- zu wenig
- nichts
- etwas anderes
- etwas zusätzliches

7.3.1 Ein erstes Beispiel

Betrachten wir das Regelventil 1 (RGV 1) unseres Beispielsystems. Die Aufgabe des Ventils ist es zu jedem Zeitpunkt nur eine so grosse Menge des Ausgangsproduktes durch die Leitung zu lassen wir gewünscht, bzw. gebraucht wird. Wir verwenden jedes der Leitwörter als Hilfe um eine Abweichung des gewünschten Verhaltens von RGV 1 festzustellen.

zu viel: RGV 1 lässt eine zu grosse Menge des Ausgangsproduktes durch.

zu viel (als Spezialfall): RGV 1 lässt eine Menge des Ausgangsproduktes durch obwohl es geschlossen sein sollte.

zu wenig: RGV 1 lässt eine zu kleine Menge des Ausgangsproduktes durch.

nichts: RVG 1 ist geschlossen, obwohl eine Menge des Ausgangsproduktes fliessen soll (Speziallfall von zu wenig).

etwas Anderes: eine andere Substanz als das Ausgangsprodukt fliesst durch RGV 1

etwas Zusätzliches: das Ausgangsprodukt wird durch eine Fremdsubstanz kontaminiert

Mit einer längeren Liste von Leitworten liessen sich selbstverständlich noch weitere Abweichungen feststellen. Eine weitere Eigenschaft längerer Listen ist, dass die Leitwörter nicht immer eine sinnvolle Interpretation zulassen. Die Interpretation der Leitwörter in Zusammenhang mit dem betrachteten System soll sich auf Abweichungen beschränken, die vom betrachteten System ausgehen. Das mag in unserem Beispiel für die letzten beiden Abweichungen eher unwahrscheinlich wirken, da der Inhalt des Reservoirs RES 1 den Inhalt des Produktstroms bestimmt. In einer tiefergehenden Analyse könnten wir das Regelventil in weiterm Detaill analysieren und feststellen, dass Schmierstoffe, die das Ventil zum Arbeiten benötige in den Strom durchsickern. Dass RGV 1 allerdings ein komplett anderes Ausgangsprodukt wird fliessen lassen können ist aber unwahrscheinlich. Diese Abweichung würde bei eingehenderer Untersuchung als unbegründet eingestuft und nicht weiter behandelt.

Auf alle Komponenten, ausser die Leitungen, angewendet könnte eine fertige HazOp wie folgt aussehen: (Hier: Eine tabellarische komplette HazOp des Systems)

7.4 Failure Mode, Effects and Criticality Analysis (FMECA)

Das Ziel der FMECA ist die Analyse des Schweregrades einer bekannten Abweichung. Abweichungen haben wir bis jetzt mit Hilfe der HazOp festgestellt.

Nun müssen die Abweichungen nach der Schwere ihrer Auswirkungen klassifiziert werden. Dafür ist es notwendig für jede Abweichung festzustellen welche weiteren Effekte die Abweichung nach sich ziehen kann. Im Rahmen dieser kurzen Einführung sollten Effekte erster und zweiter Ordnung betrachtet werden. HazOp und FMECA ergänzen sich gut und auch organisatorisch können wir einfach unsere in der HazOp erstellte Tabelle um weiter Spalten erweitern um die Ergebnisse der FMECA festzuhalten.

Wir fügen in die Tabelle die Spalten

- Auswirkungen erster Ordnung: eine kurze textuelle Beschreibung aller Effekte die eine bekannte Abweichung nach sich ziehen kann.
- Auswirkungen zweiter Ordnung: ebenfalls eine kurze textuelle Beschreibung, aber mit dem Hinweis auf eine Auswirkung erster Ordnung, die dieser Auswirkung vorangeht.
- Geschätzte Häufigkeit: für den Fall, dass Zahlen über die Häufigkeit einer Abweichung bekannt sind können diese hier verwendet werden; wir wollen hier davon ausgehen, dass dies nicht der Fall ist und versuchen die Häufigkeit in die Kategorien häufig, Täglich, Wöchentlich, Monatlich, Jährlich, 10-Jährlich, selten einzuordnen.
- Erwarteter Schaden: wie bei der Häufigkeit können bereites Zahlen zur Schadenshöhe bekannt sein. Falls dies nicht der Fall ist versuchen wir die Schadenshöhe wie folgt zu klassifizieren
  - Sachschaden: Unterbrechung der Produktion, Reparatur einer Komponente notwendig, Reparatur des Gesamtsystems notwendig, Verlust einer Komponente, Verlust des Gesamtsystems, Beeinträchtigung der Umwelt
  - Personenschaden: leicht verletzte Person, schwer verletzte Person, Gefahr für Leib und Leben, sicherer Verlust von Menschenleben
- Kritikalität: die Kritikalität wird festgelegt durch die Kombination von geschätzter Häufigkeit und Schadenshöhe.

Dies ist eine einfache und übersichtliche FMECA, die das grundlegende Prinzip demonstrieren soll. In einer grösseren FMECA Anwendung wird nicht nur der Detaillgrad steigern, auch wird viel Vorwissen in die Analyse einfliessen.

So werden sich z.B. in bestimmten Branchen bereits viele Erfahrungswerte für erwartete Häufigkeiten oder erwartete Schadenshöhen ergeben.

(FMECA Tabelle hier)

7.5 Fault Tree Analysis (FTA) / Fehlerbaumanalyse

Die Ergebnisse der FMECA liefern einen guten Überblick über die Unfallszenarien, die am wichtigsten zu verhindern oder zu mitigieren sind.

Mit Hilfe der FTA können die Unfallszenarien näher untersucht werden und ihre Eintrittswahrscheinlichkeit besser bestimmt werden.

Ein Fault Tree (FT) ist eine graphische Darstellung an der leicht abgelesen werden kann, welche Kombinationen von abweichendem Verhalten zu einem Unfall führen.

Ein FT enthält dabei 2 Arten von Knoten: Fehlerfaktorenknoten, die abweichendes Verhalten beschreiben und Konjunktionsknoten, die die Fehlerfaktorknoten ver-und-en oder ver-oder-n.

Es existieren noch einige andere Knotentypen, aber für dieses Beispiel sind die UND und ODER Knoten ausreichend. Sind die Eintrittswahrscheinlichkeiten für die Fehlerfaktoren bekannt, dann lässt sich die Gesamtwahrscheinlichkeit für einen Unfall daraus berechnen.

(Beispiel Fault Tree)

7.6 Vergleichende Analysen

Nachdem für ein gegebenes Design die HazOp, FMECA und eine erste FTA gemacht wurden beginnt die schrittweise Verbesserung des Designs.

Um die kritischsten Fehler (Ergebnis aus FMECA) zu verhindern oder zu mitigieren und dadurch das Betriebsrisiko der Gesamtanalage zu verbessern, werden änderungen vorgenommen. Um verschiedene Änderungen in ihrer Auswirkung auf das Design vergleichen zu können wird der Dreischritt von HazOp, FMECA und FTA wiederholt.

Am Vergleich der Ergebnisse lassen sich die Vor- und Nachteile der verschiedenen Änderungen ablesen. Wird ein Design durch eine Änderung sicherer gemacht so lässt sich durch eine vergleichende Vorher-Nachher Analyse der Sicherheitsfortschritt nachvollziehbar dokumentieren.

(Beispiel in Auszügen einer vergleichenden Hazop / FMECA / FTA)