Handbuch zur Störfallanalyse von nuklearen Ver- und Entsorgungs-einrichtungen

Teil D

Exemplarische Anwendung der Störfallanalyse auf Einrichtungen der nuklearen Ver- und Entsorgung

GRS - 510

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Handbuch zur Störfallanalyse von nuklearen Ver- und Entsorgungs-einrichtungen

Teil D
Exemplarische Anwendung der Störfallanalyse auf Einrichtungen der nuklearen Ver- und Entsorgung

Robert Kilger
Alexander Kolbasseff

November 2025

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) unter dem Förderkennzeichen 4722E03240 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUKN übereinstimmen.

GRS - 510
ISBN 978-3-946607-95-3

Deskriptoren
Nukleare Sicherheit, nukleare Ver- und Entsorgung, Störfall

Kurzfassung

Das vorliegende Handbuch wurde vornehmlich mit dem Ziel erstellt, den in Behörden oder Forschungseinrichtungen tätigen und mit Störfallanalysen befassten Personen Informationen an die Hand zu geben, die bei der Planung, der Erstellung, dem Betrieb und dem Rückbau von Anlagen der nuklearen Ver- und Entsorgung eine zutreffende und rasche Beurteilung von Störfällen erlaubt. Es liegt jedoch nicht in der Absicht der Verfasser des Handbuchs, fertige Lösungen für komplexe Probleme der Störfallanalyse anzubieten. Derartige Fragen werden stets einer eingehenden Analyse und Berechnung durch Fachleute auf dem Gebiet der Störfallanalyse vorbehalten bleiben müssen.

Der sinnvolle Gebrauch der im Handbuch vorliegenden Informationen erfordert ein grundsätzliches Verständnis der Störfallproblematik und der Terminologie der nuklearen Sicherheit. In Teil A „Grundlagen der Störfallanalyse“ werden daher zunächst die wichtigsten Begriffe und Grundlagen eingeführt und erläutert, und der gesetzliche Rahmen gesteckt. In Teil B „Physikalisch-chemische Grundlagen der Störfallanalyse“ werden die bei einem Störfall beteiligten Prozesse erläutert. In Teil C „Auswertung der Betriebserfahrung von Vorkommnissen“ werden die bisherig aufgetretenen nationalen wie auch internationalen Vorkommnisse statistisch ausgewertet. In Teil D „Exemplarische Anwendung der Störfallanalyse auf Einrichtungen der nuklearen Ver- und Entsorgung“ werden die verschiedenen Aspekte der Störfallanalyse exemplarisch auf zwei generische Störfalle angewendet.

Abstract

This handbook was prepared primarily with the aim to provide information to experts of authorities or research facilities engaged in incident analysis. It will allow an adequate and rapid assessment of accidents in the planning, preparation, operation and dismantling of nuclear supply and waste disposal facilities. However, it is not the intention of the authors of the handbook to offer ready solutions to complex problems of incident analysis. Such questions must remain subject to an in-depth analysis and assessment to be carried out by dedicated experts of incident analysis.

The expedient use of the information given in this handbook requires a fundamental understanding of incident analysis and the terminology of nuclear safety. Therefore, in part A *fundamentals of incident analysis* the most important terms and fundamentals are introduced and explained, and the legal framework is set. Part B *Physical and chemical fundamentals of incident analysis* explain the physical and chemical processes involved in an incident. In Part C *Evaluation of the operational experience of events*, the national and international events happened so far, are statistically evaluated. In Part D *Exemplary application of incident analysis to nuclear supply and waste disposal facilities*, the various aspects of incident analysis are applied exemplary to two generic incident cases.

Inhaltsverzeichnis

1 Einleitung

In dieser Arbeit werden verschiedene Aspekte der Störfallanalyse exemplarisch auf zwei generische Störfälle angewendet. Dabei wird auf Informationen und die übliche Terminologie der nuklearen Sicherheit zurückgegriffen, die in den Teilen A und B des *Handbuchs zur Störfallanalyse von nuklearen Ver- und Entsorgungseinrichtungen* zusammengefasst und dokumentiert sind. In Teil A, *Grundlagen der Störfallanalyse,* sind die wichtigsten Begriffe und Grundlagen und der gesetzliche Rahmen erläutert /GRS 19a/. In Teil B, *Physikalisch-chemische Grundlagen der Störfallanalyse*, sind die Prozesse aufgelistet und erklärt, die bei einem Störfall beteiligt sein können /GRS 19b/.

Teil C, *Auswertung der Betriebserfahrung von Vorkommnissen*, beschreibt und bewertet statistisch Vorkommnisse in nationalen und internationalen Anlagen der nuklearen Versorgung bis Ende 2018 /GRS 19c/. Dieser Teil wurde in der vorliegenden Arbeit nicht behandelt.

In Kapitel 2 wird die Störfallanalyse auf den exemplarischen Störfall *Brand in einer Tablettenschleifmaschine* angewendet. In Kapitel 2.1 wird zunächst für die Brennelementfertigung ein charakteristisches Störfallszenario einschließlich der beteiligten technischen Komponenten überissen. In Kapitel 2.2 wird die ausgewählte Komponente *Schleifmaschine* im Detail beschrieben. Dabei wird in Anlehnung an reell existierende Bauteile ein generischer Anlagenteil konstruiert, der zur Generierung des Störfalls gezielt Schwachstellen aufweist, da der Fokus dieser Arbeit nicht auf das technische System an sich, sondern auf die prinzipielle Anwendung der Störfallanalysenmethoden ausgerichtet ist. Bei der gewählten Anordnung wurden vorsätzlich nicht alle Vorgaben des kerntechnischen Regelwerks eingehalten, diese wäre also aus kerntechnischer Sicht in Deutschland so nicht genehmigungsfähig. Der Fokus liegt auf der Anwendung der Methodik. Es existieren keine bekannten Parallelen zu vorhandenen Anlagen. In Kapitel 2.3 wird das fiktive Schadensszenario als Fließdiagramm entwickelt sowie der mechanische Schadensauslöser „Lagerschaden“ und seine Folgewirkungen bis hin zur Brandauslösung beschrieben. Es folgt eine detaillierte Schilderung des Ansprechens der Sicherheitseinrichtungen, sowie eine Beschreibung des Verhaltens des für dieses Ereignis relevanten Schleifstaubs. In Kapitel 2.4 erfolgt zunächst eine Einstufung des Ereignisses gemäß internationaler Bewertungsskala INES, sowie nach der deutschen Meldeverordnung. In der Folge werden auf das konstruierte Beispiel und dessen Verlauf verschieden Analysearten wie What-If, HAZOP, ETA, und FTA mit ihren jeweiligen Charakteristiken beispielhaft angewendet. Abschließend wird, basierend auf einer Abschätzung von

Fehlerwahrscheinlichkeiten der Komponenten per Handrechnung, für die einzelnen Fehlerzweige die Fehlereintrittswahrscheinlichkeit ermittelt. Kapitel 2.5 enthält eine Zusammenfassung des hypothetischen Störfallscenarios sowie den ermittelten Eintrittswahrscheinlichkeiten.

In Kapitel 3 erfolgt eine Analyse für den generischen Störfall *Freisetzung von UF_6 in der Brennelementfertigung im heißen, gasförmigen Zustand*. Dieser Heißzustand wird für die Behälterentladung mittels Ausdampfprozess benötigt und birgt das höchste chemotoxische Gefahrenpotential von UF_6. In Kapitel 3.1 wird zunächst der generische Handhabungsprozess des UF_6-Behälters in der Anlage beschrieben. Im Detail sind dies der Transport vom Behälterzwischenlager in die Betriebshalle, das Einfahren in den Ausdampf-Autoklav, die Ankoppelung des Behälters an das UF_6-System der Anlag, sowie der nachgelagerte Erhitzungsvorgang des Behälters. In Kapitel 3.2 erfolgt dann die Schilderung des Ablaufs des hypothetischen Störfalls mit einer Freisetzung von gasförmigem Uranhexafluorid. Durch inkonsistent angezeigte Temperaturmesswerte wird der übliche betriebliche Vorgang noch kurz vor dem Erreichen der notwendigen Entladetemperatur des Behälters abgebrochen. Der Behälter soll dann nach einer möglichst zeitnahen Abkühlung ausgefahren und eine Fehlerursachenklärung eingeleitet werden, um möglichst eine Unterbrechung des Produktionsvorgangs zu verhindern. Zur Unterstützung des Abkühlprozesses des heißen Behälters wird der Autoklav geöffnet und der Behälter hinsichtlich einer weiteren Verbesesrung der Naturkonvektion in seiner Position etwas nach vorne gezogen. Durch einen verkeilten Fremdkörper zwischen der Wand des Autoklavs und des Behälters kommt es beim Vorziehen des Behälters zu einem Leck an der Behälteroberseite, mit nachfolgendem Ausdampfen von UF_6. In Kapitel 3.3 werden exemplarisch die drei Analysemethoden Ereignisbaum, Fehlerbaum und HAZOP-Analyse mit ihren jeweiligen Charakteristika auf das postulierte Störfallereignis unter Zuhilfenahme von abgeschätzten Wahrscheinlichkeiten angewendet. Hinsichtlich einer besseren Übersichtlichkeit werden zuvor noch der fiktive Gesamtvorgang in einem Fließdiagramm dargestellt, sowie die zum Störfall führenden Teilschritte diskutiert.

2 Anwendung der generischen Störfallanalyse auf einen exemplarischen Störfall: Brand in einer Tablettenschleifmaschine

Prinzipiell besteht die Brennelementfertigung aus den folgenden Hauptprozessen:

- UF_6-Konversion nach dem nass- oder trockenchemischen Verfahren zu Urandioxid-Pulver (UO_2)
- Pulvervorbereitung
- Herstellung der Pellets
- Brennstabfertigung inklusive vorgelagertem Strukturteileeingang
- Brennelementmontage

Bedingt durch die bessere großtechnische Umsetzbarkeit hat das modernere UF_6 Trockenkonversionsverfahren das früher häufig angewandte nasschemische Verfahren weitgehend abgelöst. Unter Berücksichtigung von bisherigen, zu diesen Themen durchgeführten Arbeiten der GRS zur UF_6 Trockenkonversion (inklusive der Ausgasungsthematik) sowie der nachgeschalteten Pulvervorbereitung, z. B. /GEU 09/, fiel der Fokus bei dieser generischen Sicherheitsanalyse auf den Hauptprozess *Pelletherstellung* und insbesondere hier die Konfektionierung der Pellets auf ihr Sollmaß mittels eines materialabtragenden Schleifprozesses. Bei der Systemtechnik der Pelletherstellung wird unterstellt, dass für den Schleifprozess der Pellets eine an Kerntechnikbelange adaptierte aber dennoch konventionelle Maschinentechnik zum Einsatz kommt. Daher fiel die Wahl auf den Hauptprozess *Pelletherstellung* mit dem Fokus auf den Teilprozess *Pelletschleifen*.

2.1 Definition des Störfallszenarios

Die dem Schleifprozess vorgelagerten Arbeitsschritte wie z. B. eine Sinterpaletten-Auskippung, d. h. der Transport der Tabletten vom Sinterofen zum Schleifprozess, der dem Schleifprozess folgende Arbeitsschritt der Tablettentrocknung sowie dem darauffolgenden Arbeitsschritt der Tabletteninspektion, besitzen ein deutlich geringeres Fehlerpotential als die Bearbeitung der Tabletten selbst.

Bei den letzten beiden Hauptprozessen dieser generischen Produktionseinrichtung geht es primär um die Handhabung des den Brennstoff umschließenden Hüllrohrs bzw. im nächsten Schritt, um die Assemblierung der Hüllrohre zu Brennelementen. Basierend auf diesem Umstand werden diese beiden Hauptprozesse für die hier gewählte Zielsetzung als weniger signifikant eingestuft.

Da hier die Demonstration der Methodik der Störfallanalyse im Fokus liegt, wird bewusst ein mit Schwachstellen versehener Komponentenaufbau konstruiert. Dabei handelt es sich nicht um einen für kerntechnische Anlagen mit Moderationskontrolle möglichst realitätsnahen Aufbau, bei dem diese Schwachstellen typischerweise vermieden würden.

2.2 Beschreibung der fiktiven Schleifmaschine

Die hier fiktive Schleifmaschine orientiert sich an einem Aufbau, der bei typischer kostenoptimierter industrieller Massenware vorkommen kann. Hervorzuheben ist dabei, dass ein solches Modell in realen Kernbrennstoff-verarbeitenden Anlagen, bedingt durch die dort herrschenden strengen Auswahlkriterien für Komponenten, kaum zum Einsatz kommen würde. Ein konkreter Bezug zu konkreter Anlage besteht nicht bzw. wäre rein zufällig.

Der Aufbau der fiktiven Schleifmaschine besteht aus den Komponenten Tabletten-Zuförderung, Schleifeinheit, Antriebseinheit (die wiederum aus Motor, Getriebe inkl. Ölversorgung, Schleifschmiermittel und Kühlmittelversorgung besteht), der Pufferstation sowie der Tabletten-Abförderung und ist im Kapitel 2.2.2 im Detail charakterisiert. Der Aufbau sowie die Einzelkomponenten sind so gewählt, dass die Maschine in der Regel autark, d. h. ohne äußere Bedienungshandlungen arbeitet. Die partielle Einhausung der Maschine wurde bis auf die Rahmenstruktur mittels transparenten Polycarbonatscheiben realisiert, um auch von außen eine optische Funktionskontrolle und Funktionsüberwachung zu ermöglichen. Diese besitzen eine maximale Gebrauchstemperatur von kurzzeitig 140 °C und eine Schmelztemperatur von ca. 148 °C (Werkstoffnummer 2301, ISO 11357 /DIN 16a/).

2.2.1 Aufstellungsort

Im Gesamtkontext der Brennelementfertigung befindet sich der Aufstellungsort der Schleifmaschine prozessbedingt zwischen Tablettensortierer und Tablettentrocknung. Die Schleifmaschine ist dabei in einem separaten Raum innerhalb des gesamten Kontrollbereichs des Fabrikgebäudes aufgestellt. Dieser ist als eigenständiger, feuerbeständiger und abgeschlossener Bereich ausgeführt. Zusätzlich erfüllt er die dazu gehörigen Anforderungen eines Kontrollbereichs, wie gestaffeltes Unterdrucksystem, Brandschutzanforderungen etc. Neben einem üblichen Türzugang verfügt der Raum über je eine Materialschleuse aus den benachbarten Räumen der Tablettensortierung sowie der Tablettentrocknung. Diese sind nur für die Zeiten der Zuführung bzw. den Abtransport der Chargen-Pufferbehälter geöffnet. Der Betrieb der Schleifmaschine erfolgt automatisiert, d. h., dass in der Regel kein Bedienpersonal benötigt. wird bzw. anwesend ist. Die Mindestwechselluftzahl, d. h. der theoretische Gesamtaustausch der Raumluft pro Zeiteinheit, beträgt für diesen Raum ca. $1\,h^{-1}$.

Neben der allgemeinen Einbindung des Raumes in das gestaffelte Unterdrucksystem der Gesamtanlage mittels einer Abluft für den Raum an sich, wurde innerhalb der Einhausung der Schleifmaschine eine weitere, lokale Unterdruckstufe generiert. Deren Aufgabe ist die gerichtete, bereits weitgehende Eliminierung von möglichem Schleifstaub aus dem allgemeinen Abluftstrom, d. h. über eine primäre, rauminterne Filterstrecke.

2.2.2 Maschinenart und Aufbau

Bei der Schleifmaschine handelt es sich hier um einen allgemein industriell verfügbaren Maschinensatz höchster Automatisierung mit einer automatischen Zu- und Abförderung der zu schleifende Rohlinge. Während der Abarbeitung/Beschleifung der Brennstofftabletten aus dem Chargen-Pufferbehälter läuft der Prozess bedienerfrei. Zu diesem Maschinensatz zugehörig ist dessen Infrastruktur in Form einer Motor-Getriebekombination, Getriebeölversorgung, sowie einer mengenmäßig begrenzten Zu- und Abführung von Wasser als Schmier- und Kühlmittel für den Schleifprozess. Die Maschine verfügt über eine weitgehende Einhausung, die allerdings aufgrund diverser Öffnungen nicht vollumschließend und damit auch nicht hermetisch ausgeführt ist. Bedingt durch den automatisierten Zu- und Abförderungsprozess der Tabletten ist diese Einhausung nur partiell wirksam und dient vor allem dem Schutz gegen Gefahren aus der stationären Maschine. Hinsichtlich der Möglichkeit einer Sichtkontrolle des Prozesses wurden für die Einhausung durchsichtige und aufklappbare Polycarbonat-Scheiben verwendet. Speziell die

Bereiche der Material-Zu- sowie Abförderung besitzen keine dicht umschließende Einhausung.

Die Materialzuführungseinheit sorgt für eine geordnete Ausrichtung der Tabletten bei der Zuführung zur Schleifeinheit. Die Schleifeinheit besteht aus zwei Walzen, d. h. Regel- und Schleifscheibenwalze. Die von beiden Seiten gleichzeitig auf die Zylinderaußenfläche der Tabletten wirkende Regel- und Schleifscheibe bewirken zum einen eine Rotation sowie eine Vorschubbewegung der Tabletten, wobei die Schleifscheibe neben dem Vortrieb den Schleifprozess übernimmt. Der Antrieb der Regel- sowie der Schleifscheibe erfolgt über eine elektrische Motor-Getriebekombination. Der Schleifprozess wird unter lokaler Zugabe von Wasser aus einer Düse durchgeführt. Dabei fungiert das Wasser neben seiner Funktion als Schmier- und Kühlmittel auch als Schleifstaubbindemittel. Nach dem Schleifprozess wird die geschliffene Tablette automatisiert aus der Maschine in eine entsprechende Puffervorrichtung gefördert. Der Schleifmaschine nachgeschaltet ist eine primäre Filterstufe zur Zurückhaltung von luftgetragenem Schleifstaub. Abb. 2.1 zeigt den schematischen Aufbau der Schleifmaschine mit Kennzeichnung des Materialfluss.

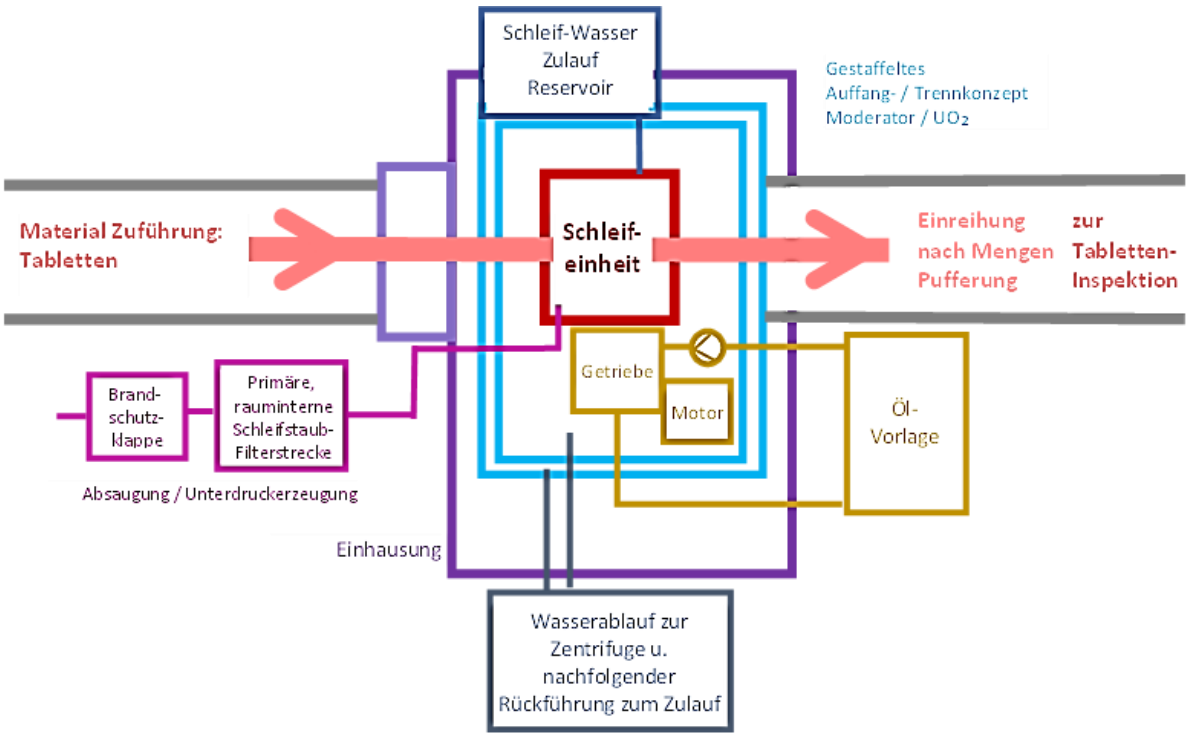

Abb. 2.1 Schematischer Aufbau der für das Störfallszenario postulierten Schleifmaschine

Das Schleifmodul

Die Schleifmaschine besteht aus einem typischen, allgemein industriell verfügbaren Maschinensatz mit der Anforderung einer effektiven Handhabung der automatisch zugeführten Rohlinge, möglichst unter Vermeidung von manuellen Arbeitsschritten.

Hierbei kommt das spitzenlose Rundschleifen zum Einsatz, das auf das Schleifen großer Serien gleicher Teile ausgerichtet ist. Bei dieser Schleifart ist das Werkstück nicht fest eingespannt, sondern liegt zwischen der Schleifscheibe, Regelscheibe und Stützleiste.

Im Einzelnen hat die Regelscheibe beim spitzenlosen Außenrundschleifen folgende Aufgaben zu erfüllen:

- Sie regelt die Umfangsgeschwindigkeit des zu schleifenden Werkstückes,
- zusammen mit der Werkstückauflage stützt sie das Werkstück gegen den Schleifdruck der Schleifscheibe ab,
- beim Durchgangsschleifen regelt sie durch ihre Schrägstellung die Durchlaufgeschwindigkeit des Werkstückes.

Den prinzipiellen Aufbau des Schleifmoduls einer Durchgangsschleifmaschine für eine Außenrundbearbeitung zeigt die folgende Abbildung.

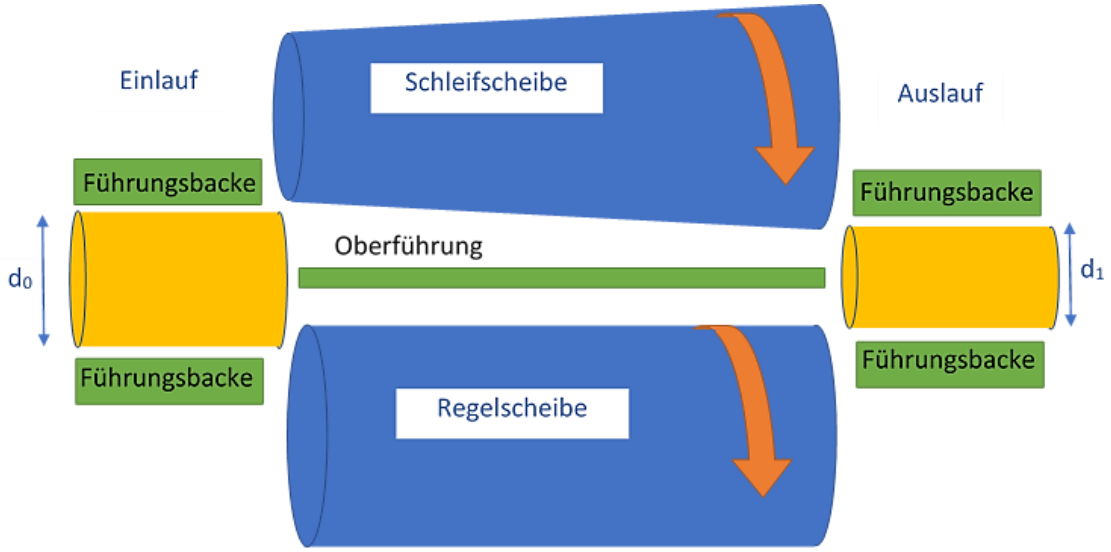

Abb. 2.2 Prinzipieller Aufbau des Schleifmoduls einer Durchgangsschleifmaschine für eine Außenrundbearbeitung

Die Werkstücke werden infolge der Neigung der Regelscheibe und ihrer Umfangsgeschwindigkeit in Achsrichtung durch den Schleifspalt transportiert und dabei bearbeitet. Die Führung der Werkstücke erfolgt dabei im Zu- bzw. Ablaufbereich mittels Führungsbacken, der Schleifprozess an sich beginnt mit dem Eintritt in den Schleifspalt.

Gemäß der Verteilung der Vektorkräfte teilt sich die Antriebskraft am Regelscheibenumfang auf in einen axialen, für die Vorschubbewegung relevanten Kraftvektor und einen vertikalen Kraftvektor für das Führen des Werkstückes. Mittels des Verhältnisses dieser beiden Vektoren lässt sich die Vorschubgeschwindigkeit des Werkstückes steuern.

Die Bearbeitung der Tabletten wird nach dem Nassschleifprinzip auf Wasserbasis durchgeführt. Das benötigte Wasser wird der Schleifscheibe so zugeführt, dass es den beim Schleifprozess anfallenden Schleifabrieb aufnimmt. Zusätzlich sorgt der Wasserfilm für eine Kühlung der geschliffenen Oberflächen. Zur Gewährleistung der Unterkritikalität unterliegt die eingesetzte Wassermenge einer strengen Mengenkontrolle bzw. Mengenbegrenzung.

Die Wasserversorgung erfolgt über einen geschlossenen, mengenbegrenzten und pumpengetriebenen Kreislauf. Bestandteil des Kreislaufes ist die Wasserzuführung und die Schleifscheibenbenetzung, der Auffangtrichter für das Wasser-Schleifabrieb-Gemisch, eine Sieb- sowie eine Rückhaltevorrichtung für größere Gegenstände und einer Rohr-Pumpen-Rohr-Kombination mittels der das Wasser zur Zentrifuge gefördert wird. Von dort aus wird das vom Schleifabrieb getrennte Wasser wieder dem volumenkontrollierten Wasser-Vorlagebehälter der Schleifmaschine zugeführt.

2.2.2.1 Das Antriebsmodul

Der Antrieb der Schleifmaschine erfolgt über einen Elektromotor mit nachfolgender Getriebeeinheit sowie einem externen Schmierölversorgungsbehälter, der außerhalb der Einhausung aufgestellt ist. Die Umwälzung und Kühlung des Schmieröls und somit auch der Getriebeeinheit erfolgt über eine Zu- sowie einer Abförderungs-Zirkulationsleitung, wobei die elektrisch betriebene Schmierölförderpumpe in der Zulaufleitung zum Getriebe positioniert ist. Der Öl-Rücklauf erfolgt schwerkraftgetrieben über den vorhandenen geodätischen Höhenunterschied. Der externe Schmierölbehälter hat vornehmlich zwei Aufgaben: Zum einen werden durch ein entsprechendes Mengenreservoir, die Intervallzeiten zwischen einzelnen Ölwechseln vergrößert. Zum anderen wird durch dessen gerippte Behälteroberfläche die Ölkühlung und somit auch eine Temperaturbegrenzung

des Getriebes gewährleistet. Diese Kühlung basiert auf dem vorhandenen Naturzug, d. h. der natürlichen thermischen Konvektion. Innerhalb des Ölversorgungsbehälters erfolgt nur eine grobe Überwachung auf den Zustand *Getriebeölniveau niedrig*.

2.2.2.2 Eingehauster Bereich

Die Schleifmaschine inkl. der zugehörigen Antriebseinheit, d. h. der Elektromotor und die Getriebeeinheit, sind von einer umschließenden Einhausung umgeben, die jedoch nicht hermetisch abgeschlossen ist. Der Getriebeölversorgungsbehälter, der durch Rohrleitungsanschlüsse mit dem Getriebe verbunden ist, ist außerhalb der Einhausung aufgestellt, auch zur Reduzierung eines möglichen Öl-Moderationsrisikos. Der Ölvorsorgungsbehälter übernimmt zusätzlich die Kühlung des Getriebeöls.

2.2.3 Aufbau und Ausführung der Einhausung

Der Aufbau der Einhausung der Schleifmaschine ist als nicht permanente und partial offene Einhausung ausgeführt, d. h. zum einen können Türen bzw. Klappen geöffnet werden, zum anderen sind ständige Öffnungen zum Transfer der Tabletten vorhanden. Aufgabe der Einhausung ist es, einen nach innen gerichtetem Luftstrom basierend auf dem Abluft-Unterdruckkonzept zu erzeugen, um einen möglichen Schleifstaubaustritt aus der Einhausung zu minimieren.

Durch eine kontinuierliche Luftabsaugung im Bereich der Schleifeinheit wird gewährleistet, dass an den temporären bzw. ständigen Öffnungen ein in die Einhausung hinein gerichteter Luftstrom vorhanden ist. Dies soll der Vermeidung von sich ausbreitender Kontamination des Schleifabriebs oder von Tabletten-Bruchstäuben aus dem Schleifbereich heraus dienen. Der Luftabsaugstutzen, der den nach innen gerichtetem Luftstrom erzeugt, ist im Bereich oberhalb der Achse der Schleifscheiben und deutlich hinter dem Austritt des Schleifspaltes der Maschine angeordnet, um ein Ansaugen von Spritzwasser zu vermeiden. Zusätzlich verhindert eine vorgelagerte Gitterstruktur das Ansaugen von Kleinteilen und soll damit einem Funktionsausfall basierend auf einer Rohrverstopfung vorbeugen.

Die aus der Schleifmaschine stammende Abluft wird, bevor sie mit der üblichen Raumabluft zusammengeführt wird, über eine rauminterne Filterstrecke geführt, bevor sie über eine Brandschutzklappe den eigentlichen Raum verlässt und sich mit den sonstigen Luftabsaugströmen vereinigt.

Die verwendeten Materialien zur Einhausung der Schleifeinheit selbst bestehen vorwiegend aus Aluminium-Profilrahmen mit Edelstahlblechen, sowie aus schwer entflammbaren, selbstverlöschenden und transparenten Polycarbonat-Scheiben bzw. Wandteilen.

2.2.4 Zusätzliche Einbauten

Zusätzlich ist die Einhausung der Schleifmaschine mit einer CO_2-Flutungseinrichtung zur lokalen Brandbekämpfung innerhalb der Einhausung ausgestattet. Um eine gegenseitige Neutralisierung von Luftabsaugung und CO_2-Flutung auszuschließen, sind die CO_2-Flutung und die Schließung der Brandschutzklappen funktionell verbunden.

2.2.5 Ergänzende Modellannahmen

Neben einer primären, rauminternen und gegen Ansaugung von Schleifwasser geschützten Filterung der Abluft aus der Einhausung der Schleifmaschine erfolgt ansonsten keine vor-Ort-Filterung der Abluft aus dem Schleifraum. Dieser Abluftstrom ist ein Teil des im Gebäude bestehenden, gestaffelten Druckkonzepts und beinhaltet lediglich eine Filterung, sowie einen Schutz gegen äußere Einwirkungen (z. B. Regenwasser, Vögel, Insekten) im Bereich vor dem Fortluftkamin. Des Weiteren erfolgt eine strömungsgeschwindigkeitsbasierte Volumendurchsatz- und Aktivitätsüberwachung, sowie eine Überwachung der Filterbelegung mit redundanten Differenzdruckwächtern. Ebenfalls ist durch entsprechende Rückschlagklappen eine Strömungsumkehr der Fortluft ausgeschlossen.

2.3 Schadensszenario

Das hier definierte Schadensszenario ist fiktiver Natur. Eventuelle Ähnlichkeiten bzw. Überschneidungen zu realen Vorkommnissen sind rein zufällig.

2.3.1 Überblick über den Ablauf des Schadensszenarios bezogen auf den schematischen Aufbau der Schleifmaschine

Abb. 2.3 zeigt im Überblick den Ablauf des Schadensszenarios als Fließdiagramm, bezogen auf den Maschinensatz der Abb. 2.1 des Kapitels 2.2.2. Dort ist besonders der Ölvorlage-Behälter mit der Zu- und Ablaufleitung zu sehen, die durch die eigentliche Einhausung der Schleifmaschine hindurchgeführt werden.

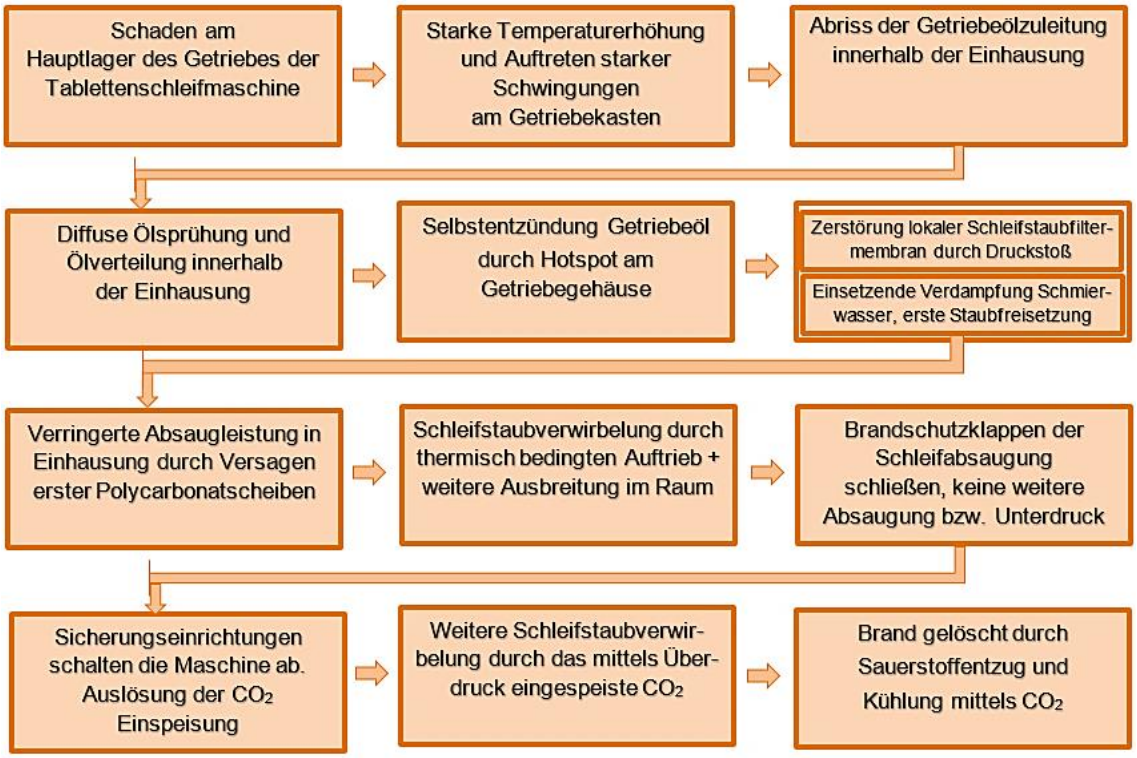

Abb. 2.3 Schematischer Ablauf des postulierten Schadenszenarios

Die einzelnen Punkte sind in den folgenden Kapiteln erklärt.

2.3.2 Schadensauslöser

Durch einen auftretenden Schaden am Hauptlager der Getriebeeinheit kommt es dort zu einem starken Anstieg der Lagertemperatur sowie durch die weitergehende Lagerschädigung zu starken, zunehmenden Schwingungsamplituden. Die Hitzeentwicklung des am inneren Teil des Getriebegehäuses fixierten Lagers bewirkt eine vergleichbar hohe Temperatur an der gleichen Position außen am Getriebegehäuse.

In der Folge des eskalierenden Lagerschadens kommt es durch die parallel dazu auftretenden massiven Schwingungsamplituden zu einem Abriss der externen Getriebeölleitung an einer innerhalb der Einhausung liegenden Position.

Durch eine scharfkantige Leitungsbruchfläche, den hohen Leitungsdruck und die nicht automatisch stoppende, sondern weiter fördernde Ölpumpe (nur grobe Überwachung auf den Zustand *Getriebeölniveau niedrig*) ergibt sich eine diffuse Öl-Sprühung, die sich an dem äußeren Hotspot der Oberfläche des Getriebegehäuses entzündet. Das aus der

Rohrbruchfläche unter Druck austretende Getriebeöl verteilt sich zusätzlich räumlich diffus, auch in den Bereich der Schleifscheibe.

Durch die temperaturbedingte Entzündung und die sich durch die breitflächige Verteilung des Öls ebenfalls breitflächig aufbauende Flammfront, setzt eine starke Wärme- und Rauchentwicklung innerhalb der Einhausung der Schleifmaschine ein.

Bei der Entzündung wird eine entsprechende Druckwelle auf die rauminterne primäre Filterstufe der einhausungsinternen Absaugung aufgebracht, die zu einer Teilzerstörung dieser Filtereinheit führt. Bis zum Schließen der Brandschutzklappe, der Absaugung an der Schleifmaschine, tritt daher eine erhöhte Partikelkonzentration des Schleifabriebs im vorhandenen Abluftstrom auf.

Bis zum Schließen der Raumluft-Brandschutzklappe erfolgt aufgrund des Ausfalls der lokalen Erstfilterung eine starke Erhöhung der Aktivität des den Raum verlassenden Abluftstromes durch den raumluftgetragenen Schleifabrieb.

2.3.3 Ansprechen der Sicherheitseinrichtungen

Die Maschine läuft ab dem Zeitpunkt der Öl-Selbstentzündung, t = 0 s, noch 90 Sekunden weiter, bevor die Sicherheitseinrichtung Getriebeöl-Füllstandsüberwachung die Maschine abschaltet, t = 90 s.

Kurz vor der Maschinenabschaltung schließen sich die lokalen Brandschutzklappen der primären Filterung der Einhausungsabluft sowie der Raumfortluft. Mit Schließung der Brandschutzklappen ist der Abluftstrom abgeriegelt und somit die dadurch erzeugte Druckstaffelung in der Maschinen-Einhausung sowie des Raumes aufgehoben, bevor die CO_2-Löschanlage der Schleifmaschinen-Einhausung auslöst und die Flammfront final erstickt.

Mit Schließung der Brandschutzklappen geht der Gebäudeteil in den Feueralarmmodus über, d. h., dass alle dafür vorgesehenen planerischen Handlungsstränge aktiviert werden. Nach Auslösung der Brandschutzklappen sowie der darauffolgenden Auslösung der CO_2-Löschanlage ist der Brand nach weiteren 15 Sekunden erstickt, t = 105 s. Somit hat das betrachtete Szenario eine Gesamtdauer von 105 Sekunden.

In den benachbarten Räumen gab es kein Ansprechen von Sicherheitseinrichtungen. Dafür war durch dieses transiente Ereignis nicht genügend Energie bzw. Effekteintrag vorhanden. Bei dem Übergang des Anlagenteils in den Feueralarmmodus liefen dagegen alle planerischen, d. h. vorgeschriebenen Handlungsabläufe stringent und ohne Abweichungen von den Soll-Vorgaben ab.

2.3.4 Der Schleifabrieb im Schadensszenario

Die Abschaltung der Schleifmaschine erfolgt nach 90 Sekunden ab dem Zeitpunkt der Öl-Selbstentzündung. Durch die einsetzende Wärmeentwicklung verdampft ein Großteil des Schleifschmiermittels. Der Dampf sowie die vorhandene thermische Luftausbreitung können von dem Absaug- /Unterdrucksystems nur zum Teil aufgenommen werden, der größere Teil entweicht durch die Öffnungen der Einhausung in die Atmosphäre des Raums. Es wird angenommen, dass von den in dieser Zeit noch insgesamt 75 g anfallenden Schleifabrieb 25 g in den einhausungsinternen Absaug-Unterdruckpfad gelangen und 50 g Schleifabrieb in Form von Staub in die Atmosphäre des Raumes freigesetzt werden.

Dabei wird im Verlauf des einsetzenden Brandes die auf den Schleifscheibenbereich gerichtete Unterdruckabsaugleistung zunächst schwächer. Im gegebenen Szenario kommt es zum lokalen Versagen der Polycarbonat-Fenster, da deren Schmelztemperatur von 148 °C überschritten wird, und somit eine breitere Ansaugung von Raumluft, bzw. eine daraus resultierende geringere lokale Absaugleistung im Bereich der Schleifscheibe stattfindet.

Durch die thermischen Verwirbelungen sowie dem zunehmenden thermischen Auftrieb bei nachlassender Integrität der Polycarbonat-Einhausung erfolgt eine vermehrte Verteilung des Schleifabriebs im Raum. Durch das automatische Schließen der Brandschutzklappen der primären Filterstrecke der Einhausung-Absaugung sowie der Brandschutzklappe der eigentlichen Raumabluft wird die Unterdruckerzeugung gestoppt. In der Folge kommen beide Absaugleistungen völlig zum Erliegen.

Mittels der Einspeisung von CO_2 innerhalb der Maschine und der Einhausung wird ebenfalls Schleifabrieb aufgewirbelt und durch den eingebrachten Volumenstrom und den Überdruck aus der Einhausung heraus in die Raumatmosphäre transportiert. Mit der CO_2-bedingten Erstickung des Ölbrandes wird nach 15 s Einblaszeit auch die weitere CO_2 Gaszufuhr gestoppt.

Nachgängig werden im Rahmen einer ersten Augenscheinnahme durch Feuerwehr und Betriebspersonal erste Messungen hinsichtlich des noch vorhandenen CO_2 sowie der Raumluftkontamination vorgenommen, um die weitere Vorgehensweise festzulegen.

Am Abluftkamin ist noch vor der dortigen Kaminfilterstrecke ein begrenzter, jedoch weit unter dem Abgabegrenzwert von 0,3 mSv liegender Aktivitätsanstieg zu verzeichnen. Durch die Filterung wird dieser Wert nochmals um ein Vielfaches abgesenkt, sodass am Eingang zum Übergabepunkt zur Fortluft keine Auffälligkeit zu verzeichnen ist.

2.3.5 Zusammenfassung des Schadensszenarios

Im Rahmen des postulierten Ereignisses werden primär folgende Maschinenkomponenten mechanisch zerstört:

- Hauptlager Getriebe,
- Ölversorgungsleitung (abgerissen),
- primäre Schleifstaubfiltermembran,
- Polycarbonatscheiben (geschmolzen),
- Dichtungen sowie verschiedene Dichtungspakete.

Parallel dazu wird die elektrische Infrastruktur der Schleifmaschine erheblich beschädigt.

2.4 Analyseszenarien

Abgesehen von der bewertungstechnischen Einstufung ist die generelle Zielsetzung dieses Bandes, die in den Teilen A bis C des Handbuchs zur Störfallanalyse beschriebenen Vorgehensweisen und Strategien anzuwenden und ein Gesamtmodell zu erstellen, in dem die Ereignisse sowie die darauffolgenden relevanten Systemantworten als untereinander dargestellte Verknüpfungen ausgeführt sind. Im gesamten Kapitel wird der Begriff *kritisch* nicht im Sinne von Kritikalität, sondern im Sinne von *hat relevante, negative Auswirkung* verwendet.

Begonnen wird mit einer Einstufung des angenommenen Störfalls nach der internationalen Bewertungsskala INES, sowie nach der nationalen atomrechtlichen Sicherheitsbeauftragten und Meldeverordnung AtSMV, Atomgesetz § 7, Anlage 2 der melde-

pflichtigen Ereignisse der Kernbrennstoffversorgung und -entsorgung. Im Anschluss wird eine *What-If* Analyse (siehe Kapitel 2.4.2 /PRE 17/) sowie eine *Hazard and Operability* Analyse (HAZOP, Kapitel 2.4.4, /DIN 16b/) durchgeführt, gefolgt von einer Deterministischen Störfall- und Ereignisbaumanalyse (*Event Tree Analysis*, ETA, Kapitel 2.4.5). Abschließend folgt eine Fehlerbaum- und probabilistische Sicherheitsanalyse (*Fault Tree Analysis*, FTA und PSA, Kapitel 2.4.6, /GEU 09/, /NRC 99/).

Voreilend zeigt Tab. 2.1, basierend auf der DIN EN 60300-3-1, einige Merkmale von typischen Zuverlässigkeitsanalyseverfahren. Integral ist zu erwähnen, dass es keine für alle Fragestellungen universelle Zuverlässigkeitsanalyse gibt, sondern jede Methode ihren besonderen Fokus hat.

Tab. 2.1 Merkmale von typischen Zuverlässigkeitsanalyseverfahren

Basierend auf /DIN 05/

Verfahren	Fehlerbaum-analyse	Ereignisbaum-analyse	HAZOP-Untersu-chung	What-If-Untersuchung
Geeignet für komplexe Systeme	Ja	NE[1]	Ja	Ja
Geeignet für neuartige Systemauslegungen	Ja	NE	Ja	Ja
Quantitative Analyse	Ja	Ja	Nein	Nein
Geeignet für Kombinationen v. Fehlerzuständen	Ja	NE	Nein	Nein
Geeignet zur Behandlung v. Abfolgeabhängigkeiten	Nein	Ja	Nein	Nein
Geeignet für abhängige Ereignisse	Nein	Ja	Nein	Nein
Deduktiv oder induktiv	Ded.[2]	Ind.[3]	Ind.[3]	Ind.[3]
Geeignet für Zuverlässigkeitszuweisung	Ja	NE	Nein	Nein
Erforderl. Ausbildungsgrad des Anwenders	Mittel	Hoch	Niedrig	Niedrig
Akzeptanz u. Allgemeingültigkeit	Hoch	Mittel	Mittel	Mittel
Braucht Werkzeugunterstützung	Mittel	Mittel	Niedrig	Niedrig
Plausibilitätsprüfungen	Ja	Ja	Ja	Ja
Verfügbarkeit von Werkzeugen	Hoch	Mittel	Mittel	Mittel
IEC-Norm	IEC 61025	---	IEC 61882	---

[1] NE = Nicht empfohlen, kann für einfache System verwendet werden, als alleiniges Verfahren nicht empfohlen, ist gemeinsam mit anderen Verfahren zu benutzen.
[2] Ded. = Deduktiv, von oben nach unten.
[3] Ind.= Induktiv, von unten nach oben.

2.4.1 Ausgangspunkt, internationale sowie nationale Einstufung des konstruierten Ereignisses

Um eine erste Einschätzung des Gesamtereignisses zu erhalten, werden basierend auf dem Ereignisbericht in Kapitel 2.3 die einzelnen Zuordnungskriterien der internationalen INES-Kategorisierung am Ereignisverlauf gespiegelt sowie eine Einstufung nach nationaler Bewertung vorgenommen.

Internationale Einstufung

INES-Kriterium *Auswirkung auf Menschen und Umwelt*

Basierend auf der zeitlich und mengenmäßig begrenzten Menge an Schleifabrieb und der noch vorhandenen Funktionsfähigkeit der Filterstufe vor Übergabe der Abluft an den Fortluftkamin kommt es nach der Filterstufe zu keiner Erhöhung oder Überschreitung der gesetzlich festgelegten Abgabewerte sowie zu keiner Strahlenexposition einer Einzelperson der Bevölkerung jenseits der gesetzlich festgelegten Grenzwerte.

Durch den vollautomatisierten Ablauf des Bearbeitungsprozesses Pelletschleifen sowie der leittechnischen Beherrschung des Ereignisses kommt es ebenfalls zu keiner unmittelbaren Strahlenexposition von vor-Ort-Personal.

INES-Kriterium *Beeinträchtigung von Sicherheitsvorkehrungen*

Das Auftreten eines Brandes in einem Kontrollbereich an sich ist als ein Ereignis mit sicherheitstechnischer Bedeutung zu bewerten. Jedoch war am Ort des Geschehens die im Raum vorhandene Brandlast sowie die vorhandene Aktivitätsmenge sehr begrenzt und der Ablauf sowie auch die verbleibenden, gestaffelten Sicherheitsvorkehrungen zur vollständigen Beherrschung des Ereignisses ausreichend.

INES-Kriterium *Beeinträchtigung radiologischer Barrieren und Überwachungsmaßnahmen*

Die radiologischen Überwachungsmaßnahmen waren zu keinem Zeitpunkt gefährdet. Hinsichtlich der Beeinträchtigung radiologischer Barrieren ist zu der teilzerstörten Filtermembran der Abluftabsaugung in der Einhausung anzumerken, dass dieser Filter, basierend auf den Auslegungsdaten der Anlage, als nicht explosionsgeschützt ausgeführt ist. Ein Grund hierfür ist sicher der Umstand, dass keinerlei größere Mengen explosionsgefährdeter Gefahrenstoffe vorhanden sind.

Unter Würdigung der aufgezählten Randbedingungen ist das Ereignis als maximal INES-Stufe 1 einzustufen.

Nationale Einstufung

Die nationale Einstufung erfolgt gemäß der *Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung* der deutschen Bundesregierung (AtSMV) /BUN 18/, die insbesondere auf § 12 Abs. 1 Nr. 7 Atomgesetz /BUN 21/ basiert, folgende vier Kategorien S, E, N und V definiert:

- Kategorie S:

  Ereignisse, die der Aufsichtsbehörde unverzüglich gemeldet werden müssen, damit diese gegebenenfalls in kürzester Frist Prüfungen einleiten oder Maßnahmen veranlassen kann. Hierunter fallen auch die Ereignisse, die akute sicherheitstechnische Mängel aufzeigen.

- Kategorie E:

  Ereignisse, die der Aufsichtsbehörde binnen 24 Stunden gemeldet werden müssen, damit diese gegebenenfalls in kurzer Frist, Prüfungen einleiten oder Maßnahmen veranlassen kann. Hierunter fallen auch die Ereignisse, deren Ursache aus Sicherheitsgründen in kurzer Frist, geklärt und gegebenenfalls in angemessener Zeit behoben werden muss. In der Regel handelt es sich dabei um sicherheitstechnisch potentiell – aber nicht unmittelbar– signifikante Ereignisse.

- Kategorie N:

  Ereignisse, die der Aufsichtsbehörde innerhalb von 5 Werktagen gemeldet werden müssen, um eventuelle sicherheitstechnische Schwachstellen erkennen und beseitigen zu können, ohne dass kurzfristige Maßnahmen der Aufsichtsbehörde notwendig werden. Dies sind in der Regel Ereignisse von geringer sicherheitstechnischer Bedeutung, die jedoch über routinemäßige betriebliche Ereignisse bei vorschriftsmäßigem Anlagenzustand und -betrieb hinausgehen.

- Kategorie V:

  Ereignisse, die vor Inbetriebnahme der Anlage auftreten und über die die Aufsichtsbehörde im Hinblick auf den späteren Betrieb der Anlage informiert werden muss.

Einen Leitfaden für die vorzunehmenden Kategorisierungen geben die *Erläuterungen zu den Meldekriterien für meldepflichtige Ereignisse gemäß Anlage 2 der AtSMV /BUN 18/*.

Bedingt durch die im diskutierten Scenario vorliegenden Umstände ist zwischen Kategorie S und Kategorie E abzuwägen. Eine Einwirkung von innen oder außen unterliegt nicht alleine deshalb der Meldepflicht nach Kategorie E, weil unmittelbar nach Eintreten des EVI- oder EVA-Ereignisses vorsorglich oder nur zur Ermittlung von Ursachen und Anlagenzustand die Anlage oder Teilanlage abgeschaltet wird. Die Meldepflicht nach Kategorie E beginnt dann, wenn hinreichend genau erkennbar wird (z. B. aufgrund des festgestellten Schadensausmaßes, hier der Ölbrand der Schleifmaschine mit Zerstörung der Abluftmembran), dass der Betrieb der Anlage oder Teilanlage aus sicherheitstechnischen Gründen nicht fortgeführt werden kann.

Bedingt durch den begrenzten Charakter und dem korrekten Ablauf der Schutzeinrichtungen wurde hier für das Schadensscenario die Kategorie E gewählt.

Die weitere numerische Unterklassifizierung erfolgt ebenfalls auf Basis der oben genannten Anlage 2 *der AtSMV*. Die nachfolgende Aufzählung gibt Aufschluss über die weitere Unterteilung eines Ereignisses mit seinen ersten beiden Kennziffern.

1. Radiologie und Strahlenschutz
    1.1. Ableitung radioaktiver Stoffe
    1.2. Freisetzung radioaktiver Stoffe
    1.3. Kontamination
    1.4. Verschleppung radioaktiver Stoffe
2. Anlagentechnik und Betrieb
    2.1. Funktionsstörungen, Schäden und Ausfälle in sicherheitstechnisch wichtigen Systemen oder Anlagenteilen
    2.2. Schäden oder Leckagen an Rohrleitungen oder Behältern sicherheitstechnisch wichtiger Systeme
3. Einwirkung von außen und anlageninterne Ereignisse
    3.1. Einwirkungen von außen
    3.2. Anlageninterne Ereignisse

Gemäß dem Schadensablauf ist hier die Detaillierung 3.2 relevant.

Zur Festlegung der dritten Ordnungszahl wurde gemäß Anlage 2 der Unterpunkt 1, also E. 3.2.1 identifiziert. Dieser lautet nach Anlage 2 *der AtSMV*:

E 3.2.1 Anlageninterner Brand, anlageninterne Explosion, heftige chemische Reaktion, Überflutung, der Absturz einer schweren Last oder eine sonstige Entwicklung von innen, sofern der Betrieb der Anlage oder der Teilanlage aus sicherheitstechnischen Gründen nicht fortgeführt werden kann.

Damit wurde dieses generische Ereignis als E 3.2.1 eingestuft.

2.4.2 Kennwerte

Als Kennwert der Schleifmaschine wird im Nennbetrieb ein Schleifabrieb von ca. 50 g/min bei einem korrespondierenden Wasserdurchsatz von ca. 5 dm³/min angenommen. Im Rohrleitungs-Pumpsystem bis zur Zentrifuge kann sich ein Schleifabrieb-, bzw. Urandioxidinventar von bis zu 12 g ansammeln. Bedingt durch das geodätische Gefälle von der Schleifmaschine zur Zentrifuge ist keine Rückströmung in diesen Bereich zu erwarten und somit nur für mögliche, hier in diesem Rahmen nicht durchgeführte Kritikalitätsbetrachtungen von Relevanz. Integral wurde vorzugsweise auf eine schnelle Wasserwiederaufbereitung anstelle eines hohen Wasserinventars geachtet. Eine Wasserergänzung erfolgt aufgrund der geringen Verlustmengen im Schleifbetrieb in der Regel nur vor Start einer neuen Bearbeitungscharge.

Das im Getriebe befindliche Ölinventar wird kontinuierlich überwacht und wird mit 2 dm³ angenommen. Der Behälter der Ölvorlage, welcher u. a. auch zur Kühlung dient, verfügt über ein Reservoir von 4 dm³, die über eine Zu- und Ablaufleitung kontinuierlich durch die Getriebeeinheit umgewälzt werden. Die fördernde Getriebeöl-Umwälzpumpe sitzt dabei in der Zuführungsleitung zum Getriebe. Die Leistungsaufnahme der Pumpe liegt bei 300 Watt. Dies ist primär der diffusen Öleinspritzung über Düsenstrukturen ins Getriebe und somit einem benötigten hohen Vordruck in der Ölzuleitung geschuldet.

2.4.3 What-If Analyse

Die *What-If* Analysetechnik (WIFT) bzw. Analysemethode (zu Deutsch „Was-Wenn-Analysemethode“) gehört zu der Klasse der Brainstorming-basierten Vorgehensweisen und ist eine Methode zur Analyse von potenziellen Risiken durch die Anwendung von zielorientierten Fragen zu Störungen, Auswirkungen und Gegenmaßnahmen bei einem System, wie zum Beispiel: *Was passiert, wenn die Maschine bzw. die betrachtete Funktionseinheit nicht dem Sollzustand entspricht?* /PRE 17/. Mit dieser Fragetechnik werden die Maschinen, Systeme, Subsysteme bzw. Funktionen nacheinander durchleuchtet, um letztendlich einerseits den vordefinierten Systemumfang abzudecken, andererseits die als Arbeitsergebnis angestrebte qualitative Risikomatrix erstellen zu können. Im Gegensatz zu anderen Analyseansätzen gibt es bei der What-If Vorgehensweise keine fest vorgegebene Struktur. Sie ist somit offen für jegliche Brainstorming-Variante bzw. auch Abwandlungen. Die What-If Analyse ist nicht zur Aufdeckung von Mehrfachfehlern geeignet.

Der Ablauf der Analyse entspricht der Abfolge im Prozess mit insgesamt drei Fragen, beginnend mit Frage 1: *Welche Störung, bzw. Abweichung vom Soll-Zustand, kann auftreten?* Auf Basis der Antwort auf diese Frage wird im Folgenden als Frage 2 nach *möglichen Auswirkungen zu den zugehörigen Abweichungen* gefragt. Je nach Aufgabenbeschreibung und Zielsetzung bzw. Analysetiefe kann hier auch eine qualitative Risikoeinschätzung vorgenommen werden. Mit der dritten Frage: *Welche Gegenmaßnahmen sind dazu möglich?* soll eine Abhilfestrategie aufgezeigt werden. Die Fragen können sich dabei nicht nur auf den (evtl. automatisierten bzw. teilautomatisierten) Prozess an sich, sondern auch auf mögliche Fehlbedienungen (manuelle Eingriffe) oder sonstige, mögliche Interaktionen beziehen.

Ein möglicher Aufbau einer Ergebnistabelle einer What-If Analyse ist eine Tabelle, die die folgenden typischen Inhaltspunkte enthält:

- Benennung des Prozessschrittes der sequenziellen, stringenten Abarbeitung der Prozessabfolge des Systems;
- What-If Frage nach möglichen Abweichungen bei dem zugehörigen Prozessschritt;
- Auswirkungsbeschreibung bei der betroffenen Abweichung und je nach Vorgabe eine qualitative, verbale, Risikoeinschätzung;

- vorgeschriebene/mögliche Maßnahme beim Eintreten der Auswirkung, wobei hier nach Möglichkeit auch zwischen verschiedenen Arten wie betriebliche oder sicherheitstechnische Maßnahmen etc. unterschieden werden kann/sollte;
- anzuratende/mögliche Maßnahmen, um die ungewollte Auswirkung zu unterbinden/zu begrenzen. Je nach Aufgabe und Situation sollte nach der Möglichkeit der Bereitstellung von vorgefertigten What-If Fragen als Analyseunterstützung, hinsichtlich einer voll umfänglichen Hinterfragung des Prozessschrittes, gesucht werden.

Bei einer erweiterten Umsetzung von klaren Strukturierungen der What-If Technik, z. B. angefangen von einer systematischen Systembetrachtung bis hin zur zu erstellenden, dann auch systematisch aufgebauten Risikomatrix, wird auch von einer *Strukturierten What-If Analysetechnik* (SWIFT) gesprochen. Sowohl bei der What-If als auch bei der SWIFT-Analyse ist die Qualität des Ergebnisses maßgeblich von dem Wissen und Handeln der daran beteiligten Personen abhängig, sodass hier der Einsatz von Personen mit praktischen Erfahrungen sowie fundiertem Hintergrundwissen eine essenzielle Grundvoraussetzung dafür ist, einerseits die zu erfragenden Auswirkungen und Risiken, und andererseits mögliche Abhilfemaßnahmen qualifiziert benennen zu können.

Diese Analysen werden vor allem als ein erster orientierender Einstieg vor der Durchführung formalisierter Risikobeurteilungsmethoden gesehen, um bereits hier mögliche relevante Schwerpunkte zu identifizieren. Ein Vorteil dieser beiden Methoden WIFT und SWIFT ist, dass bereits in der Entwicklungsphase oder bei neuen Funktionen relativ schnell erste Ergebnisse gefunden werden können. Der Nachteil liegt darin, dass die Betrachtung tendenziell oberflächlich und sehr selten voll umfänglich ist. Die SWIFT-Methode ist ursprünglich als eine vereinfachte Methode zur HAZOP (Hazard and Operability Study, siehe Kapitel 2.4.4) Systemanalyse entwickelt worden. SWIFT bietet einen breiteren Anwendungsbereich, hat jedoch im Vergleich zu HAZOP einen geringeren Detaillierungsgrad.

Neben der Auswahl der zu betrachtenden Einheit sowie der vorgegebenen Zielsetzung, der beteiligten Personen und des zeitlichen Rahmens sind aus operativer Sicht die sogenannten Kategorien zu bestimmen. Eine Kategorie entspricht dabei im allgemeinen Fall einem prozessbezogenen oder einem komponentenbezogenen Schlagwort, welches ein Problem bzw. dazu mögliche Fehlerursachen beschreibt und eine eigene Spalte in der zu erstellenden Risikomatrix bekommt. Um am Ende der Betrachtung diese

Risikomatrix strukturiert erstellen zu können, sollten daher bereits zu Beginn des Brainstorming-Prozesses die Kategorien aufgestellt werden. Insgesamt besteht die Risikomatrix aus den Spalten *Kategorie*, *Auswirkung*, *Maßnahmen* und *Empfehlungen*. Wichtig ist dabei die konstante Beibehaltung der zuvor ausgewählten Frage, wie z. B.: *Was wäre, wenn.* Der Detaillierungsgrad der Kategorie bestimmt dabei die Anzahl der möglichen weiteren Whalt-If Einträge und umgekehrt.

Von der SWIFT-Analyse gibt es wiederum verschiedene Varianten, wie z. B. die Analyse nach Haferkamp-Jäger, bei der potenzielle generelle Gefahren ähnlich der SWIFT-Kategorien bereits vordefiniert sind /PRE 17/. Die Hauptunterscheidung erfolgt dabei nach generell betrieblichen und generell außerbetrieblichen Gefahrenquellen. Bei den betrieblichen Gefahrenquellen ist wiederum zwischen anlagenbezogenen Gefahrenquellen (z. B. Rohrleitungsbruch als eine Gefahr, die aus der Anlage selbst heraus entsteht) sowie den ereignisbezogenen Gefahrenquellen (z. B. Explosion eines Betriebsstoffes als Ereignis, das wiederum auf die Anlage einwirkt) zu unterscheiden. Bei den generellen außerbetrieblichen Gefahrenquellen sind Punkte wie: Beschädigung der Anlage hinsichtlich ihres Aufbaus, eine Einwirkung von Wärmeenergie durch feste Teile etc. gelistet und entsprechend den Vorgaben sequenziell abzuarbeiten.

Im Folgenden werden die ersten drei Teilfunktionseinheiten des Gesamtprozesses *Pelletschleifen*, nämlich *Auskippen Pellets* aus dem zufördernden Transportbehälnis, auch basierend auf seiner Form, Transportschiffchen genannt, *Einreihen Pellets* und *Zufördern Pellets* zur Schleifmaschine betrachtet, siehe Abb. 2.4.

Abb. 2.4 Die ersten drei Funktionseinheiten des betrachteten, generischen Gesamtprozesses *Pelletschleifen*

Für diese Teilfunktionseinheiten ist in den Tab. 2.2 bis Tab. 2.4 beispielhaft und in knapper Form die Anwendung der SWIFT-Methode (als strukturierte What-If Abfrage) dargestellt. Als eine der vielen dabei geltenden Randbedingungen sei ebenfalls beispielhaft das chargenmäßige Abarbeiten der Pellets genannt. Das bedeutet, dass erst nach

Abschluss der Bearbeitung der Pellets aus dem aktuellen Transportschiffchen die Anforderung der nächsten Charge erfolgen kann und somit Überfüllungsszenarien der Anlage ausgeschlossen werden. Damit ist eine Überfüllung eines stehenden Teilprozesses durch die weitere Anlieferung von Pellets via Transportschiffchen (*double batching*) ausgeschlossen. Die Spalte *Maßnahmen* ist dabei nur dann ausgefüllt, wenn bei der Auswirkung implizit ein gewisses Risiko gesehen wird. Der Ausdruck Maßnahme ist dabei sehr allgemein gehalten. Theoretisch können dies technische und / oder organisatorische Maßnahmen sein. Wenn es sonst keine weiteren Vorgaben gibt, ist jedoch den technischen Maßnahmen im Allgemeinen der Vorzug vor organisatorischen Maßnahmen zu geben. Besonders in diesem Fall, da mit dem Einsatz von Handlungsanweisungen gearbeitet wird.

Tab. 2.2 What-If Abfragen zu der generischen Funktionseinheit *Auskippen Pellets*

Kategorie	What-If	Auswirkung	Maßnahme	Empfehlung
Fehlfunktion	Ausfall Motor	keine Aktorik [1], Prozess bleibt unkritisch stehen	--	--
	nicht korrekte Positionierung Transportschiffchen	Prozess steht, unkritisch da Entriegelungsmechanismus das Auskippen nicht frei gibt	--	--
Abweichung des Prozesses vom Normalbetrieb	Verklemmung Motor / Mechanik der Aktorik	Prozess steht, unkritisch, auftreten Überhitzung, Zwangskräfte	Auslegung Komponenten	Motor kurzschlussfest, Mechanik für max. auftretende Kräfte auslegen
	Unvollständige Entladung Transportschiffchen, Gewicht	Keine kritische Prozessauswirkung	--	--
Ausfall Betriebsmittel	Stromausfall	keine Aktorik, Prozess bleibt unkritisch stehen	--	--
Brandschutz	Aufbringen Zündenergie	Überhitzung Motor	Auslegung Komponenten	Motor kurzschlussfest auslegen
	Menge Brandlast	Minimal, da kaum Brandlast	--	--

1 Aktorik umfasst die Erzeugung von Bewegung oder Verformung

Tab. 2.3 What-If Abfragen zu der Funktionseinheit *Einreihen Pellets*

Kategorie	What-If	Auswirkung	Maßnahme	Empfehlung
Fehlfunktion	Ausfall Motor	keine Aktorik, Prozess bleibt unkritisch stehen	--	--
Abweichung des Prozesses vom Normalbetrieb	Verklemmung Motor / Mechanik der Aktorik	Prozess steht unkritisch, auftreten Überhitzung, Zwangskräfte	Auslegung Komponenten	Motor kurzschlussfest, Mechanik für max. auftretende Kräfte auslegen
Ausfall Betriebsmittel	Stromausfall	keine Aktorik, Prozess bleibt unkritisch stehen	--	--
Brandschutz	Aufbringen Zündenergie	Überhitzung Motor	Auslegung Komponenten	Motor kurzschlussfest
	Menge Brandlast	Minimal, da kaum Brandlast	--	--

Tab. 2.4 What-If Abfragen zu der Funktionseinheit *Zufördern Pellets*

Kategorie	What-If	Auswirkung	Maßnahme	Empfehlung
Fehlfunktion	Ausfall Motor	keine Aktorik, Prozess bleibt unkritisch stehen	--	--
Abweichung des Prozesses vom Normalbetrieb	Verklemmung Motor / Mechanik der Aktorik	Prozess steht unkritisch, auftreten Überhitzung, Zwangskräfte	Auslegung Komponenten	Motor kurzschlussfest, Mechanik für max. auftretende Kräfte auslegen
Ausfall Betriebsmittel	Stromausfall	keine Aktorik, Prozess bleibt unkritisch stehen	--	--
Brandschutz	Aufbringen Zündenergie	Überhitzung Motor	Auslegung Komponenten	Motor kurzschlussfest
	Minimal, da kaum Brandlast	Minimal, da kaum Brandlast	--	--

Wie zuvor in der Beschreibung von What-If ausgeführt, stellt die What-If Analyse letztendlich eine Untermenge einer HAZOP-Analyse dar. Da die Schleifstation im folgenden Kapitel mit all ihren Funktionsblöcken inklusive der infrastrukturellen Hilfssysteme in Form einer HAZOP-Analyse betrachtet wird, wird zur Vermeidung von Wiederholungen hier auf die weitere Betrachtung nach der What-If Anlayse der weiteren Komponenten bzw. Funktionsblöcke des Gesamtsystems *Pelletschleifen* verzichtet.

2.4.4 Hazard and Operability Analyse

Im folgenden Kapitel wird zunächst die Vorgehensweise bei einer *Hazard and Operability Study* (HAZOP-Systemanalyse) kurz beschrieben und anschließend am Beispiel der *Schleifstation Pellets*, exemplarisch aufgezeigt.

2.4.4.1 Beschreibung der HAZOP-Systemanalyse

Bei der HAZOP-Systemanalyse handelt es sich um eine Technik der Risiko- und Funktions-Problemidentifizierung mit der Zielsetzung, die Auswirkungen von Abweichungen vom Entwurfsziel aufzuzeigen. Hierzu sollen Risiken bzw. Funktionsprobleme, die von Einzel- oder Untersystemen durch eine nicht ordnungsgemäße Funktion ausgehen können, durch ein systematisches Hinterfragen aufgedeckt werden. Somit ist auch die Namensgebung auf die beiden Kernbegriffe *Hazard für Risiko und Operability* für die umgesetzte bzw. auszuführende Funktion zu verstehen. Eine Weiterentwicklung ist, dass HAZOP-Analysen heute auch auf diskontinuierliche Prozesse angewendet werden. Mittlerweile ist das HAZOP-Verfahren in der Norm IEC-61882, 2016 /DIN 16b/ beschrieben und definiert. In Deutschland hat sich diese Methode auch unter der Bezeichnung PAAG (Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen) etabliert. Im Vergleich zu anderen Analysen, z. B. der What-If Analyse, bietet die HAZOP-Vorgehensweise einen weitaus höheren Detaillierungsgrad.

Als Weiterentwicklung von HAZOP ist zu beobachten, dass zunehmend eine grobe Quantifizierung mit einfachen Klassifizierungsworten von Risikostufen, z. B. nach erwarteter Häufigkeit und Schwere des Ereignisses, angewendet werden.

Der Ablauf der HAZOP-Analyse an sich, erfolgt nach IEC 61882 in den vier vorgegebenen Aufgabenblöcken /DIN 16b/:

- Festlegungen,
- Vorbereitungen,
- Untersuchungen,
- Dokumentation und Folgeaktivitäten.

Im Aufgabenblock *Festlegungen* erfolgen die grundlegenden Vorbereitungen. Das Thema *Untersuchung* besteht aus der Unterteilung des Systems in Subsysteme, Auswahl von Subsystemen bzw. Funktionsblöcken, Bestimmung deren Zweck und Ziel, Identifizierung von Abweichungen mit Leitwörtern, Bestimmung deren Ursachen und Folgen, sowie Festlegung von Maßnahmen und Aktionen. Im letzten Arbeitsblock *Dokumentation und Folgeaktivitäten* werden die Ergebnisse aufgezeichnet, Aktionen nachverfolgt, Nachuntersuchungen durchgeführt, sowie der Abschlussbericht erstellt.

Das zentrale Moment dieser Methode ist das Hinterfragen von Eigenschaften bzw. die Untersuchung von Parameterabweichungen vom Sollwert bzw. von Abweichungen vom Entwurfsziel des Systems, auf die bereits weiter oben erwähnten Leitworte. Diese sollen für möglichst alle Abweichungen stehen. Bei Bedarf können spezielle, zusätzlich über die Norm hinausgehende Leitworte eigenständig definiert werden. Voraussetzung dafür ist, dass die Eigenschaft des Leitwortes eindeutig festgelegt und dokumentiert wird, wie beispielhaft in nachfolgender Tab. 2.5 gezeigt wird. Der Detaillierungsgrad der Unterteilung des Systems in Subsysteme oder Funktionsblöcke ist dabei abhängig von der gewünschten Betrachtungstiefe. Diese ist in der Regel selbst wiederum eine Funktion des erwarteten Risikos.

Tab. 2.5 Auswahl von in der Norm IEC 61882 gelisteten Leitworten nach /DIN 16b/

Leitworte (IEC61882)	Erklärung
nein, nicht	Sollverhalten tritt nicht ein
mehr	qualitativer Zuwachs der Größe, zu viel
weniger	qualitative Abnahme der Größe, zu wenig
sowohl als auch	zusätzliche Ereignisse zum Soll-Verhalten
teilweise	Soll-Verhalten nur unvollständig erreicht
Umkehrung	gegenteiliges Verhalten zur Soll-Funktion
anders als	etwas anderes als das Soll-Verhalten
früher/später	Soll-Verhalten tritt zu früherem/späterem Zeitpunkt ein
zuvor/danach	Soll-Verhalten in anderer Reihenfolge oder zum Ablauf
schneller/langsamer	nicht erwartete Änderung der Ablauf-/Ausführungsgeschwindigkeit

Die Untersuchung, basierend auf möglichst detaillierten Systeminformationen, ist dabei ein kreativer Prozess von den für die betrachteten Systeme/Subsysteme/Funktionsblöcke ausgewiesenen Spezialisten, die unter der Führung eines Moderators stehen. Die Qualität der Ergebnisse hängt dabei im wesentlichen Maße von der Qualität der Systembeschreibung, der Mitwirkenden und deren Kreativität, inklusiver der Qualität der Dokumentation ab. Die dabei erarbeiteten Maßnahmen zur Risikobehandlung, die in der Regel auf einer qualitativen Risikoeinschätzung durch die Beteiligten fußen, sind nicht das originäre Ziel einer HAZOP-Betrachtung, sollten aber, da diese auf entsprechendes Expertenwissen basieren, als wichtige Empfehlungen betrachtet werden.

Allgemein können HAZOP-Studien jeweils zu den unterschiedlichsten Systemlebens- bzw. Systemzyklusphasen wie Konzept-, Entwicklungs-, Umsetzungs- Nutzungs-, Optimierungs- und Stilllegungsphase mit ihren jeweiligen Besonderheiten durchgeführt werden. Bei der Untersuchungsreihenfolge kann auch typischerweise nach der Reihenfolge *Eigenschaften/Parameter zuerst* oder *Leitwort zuerst* gewählt werden. Der Grad der Unterteilung der Gesamtanlage in bearbeitbare Systeme wie Subsysteme oder Funktionseinheiten etc., richtet sich in der Regel nach ihrer Komplexität, den zu erwartenden Gefahren- bzw. Risikopotentialen, aber auch nach der Kompetenz und den Erfahrungen der Mitglieder der HAZOP-Gruppe.

Typische HAZOP-Studienergebnisse sind die Tabellen der ermittelten Risiken und Betriebsprobleme. Diese beinhalten auch die verwendeten Leitworte und Eigenschaften bzw. Parameter für die Art der Aufdeckung, möglich getätigte Vermerke in den Entwurfs-

bzw. Systemunterlagen, die möglichen Abhilfemaßnahmen mit ihren Empfehlungen wie z. B. für konkrete risikoärmere Techniken bzw. Arten zur systemtechnischen oder betriebstechnischen Risikoabwehr. Werden zur Risikominimierung typische elektronische Monitoring-Systeme eingesetzt, ist wiederum deren Qualität in Abhängigkeit des betrachteten Risikos bzw. der Risikostufe zu berücksichtigen. Es sei erwähnt, dass Risikominimierungsmaßnahmen nicht nur technischer, sondern auch administrativer Art sein können, wobei speziell passive technische Maßnahmen zu bevorzugen sind. Wichtig ist zudem, die durchgeführten Teamsitzungen der HAZOP-Gruppe mit ihren Ergebnissen und möglichen Anmerkungen, inklusive der beteiligten Personen, adäquat aufzuzeichnen und zu archivieren.

2.4.4.2 HAZOP Methode an dem generischen Beispiel des Schleifens von Pellets

Gemäß den vorherigen Kapiteln wurde das System *Pelletschleifen* für die beispielhafte Anwendung von verschiedenen Risikoanalysen ausgewählt. Die Zielsetzung ist die Aufdeckung besonders risikobehafteter Prozessschritte bzw. Szenarien durch Betrachtung möglicher Abweichungen vom Sollzustand bei deren Bearbeitung.

Das *Pelletschleifen* befindet sich in einem eigenen Raum, der zwischen der Pelletsortierung und der Pellettrocknung liegt. Eine wichtige Randbedingung ist, dass bei der nicht kontinuierlichen Zuführung von Pellets zu den Schleifscheiben der Maschine kein risikobehafteter Zustand eintreten kann. Zur Sicherstellung einer kontinuierlichen, sequenziellen Bearbeitung handelt es sich dann mehr um eine Frage der Wirtschaftlichkeit als um eine Risikobetrachtung. Da zu der Risikoanalyse nicht nur das im Raum installierte Schleifsystem, sondern auch die damit interagierenden Rauminfrastruktursysteme wie die Kontrolle der Raumabluft durch eine Brandschutzklappe und die vorhandene Raumabluft-Vorfilterung gehören, sind diese in die Betrachtung mit einzubeziehen. Abb. 2.5 oben zeigt die bereits in Funktionseinheiten untergliederte Schleifstation als vereinfachte Systemdarstellung mit den ihr spezifischen Prozessparametern bzw. Systemgrößen. In Abb. 2.5 sind die Subsysteme bzw. Funktionseinheiten der Rauminfrastruktur dargestellt, ebenfalls als vereinfachte Systemdarstellung.

Hinsichtlich einer festzulegenden Grobklassifizierung der Risikostufe einer Auswirkung wurden vier Stufen festgelegt: gering, mäßig, bedeutend und extrem. Der Begriff Risikostufe ist dabei nach DIN EN 61882 als die Größe eines Risikos oder Kombinationen von

Risiken ausgedrückt in Begriffen zu verstehen und als Verbindung der beiden Größen Folgen und deren Auftretenswahrscheinlichkeit /DIN 16b/ zu sehen. Für das mögliche häufigkeitsmäßige Eintreten wurden ebenfalls vier Stufen festgelegt: sehr selten, selten, mäßig und oft. Die Bezeichnung der Art der Auswirkung wurde aus dem vorherrschenden Umstand festgelegt, wie z. B. mechanisch, elektrisch, Fluid, Kontamination, Moderation, exotherm, Entsorgung, Rauch, Brandlast etc. In der Spalte *Maßnahme, die das Risiko minimiert*, ist das Wort Risiko nach dieser Definition als *ein Effekt der Unsicherheit, bezogen auf das Ziel* zu verstehen.

Die betrachtete generische Schleifstation wurde in sieben Funktionseinheiten mit der jeweiligen Sollfunktion als Name unterteilt. Die Hauptkomponente Schleifstation wurde mit römisch eins (I) bezeichnet, die einzelnen darin enthaltenen Funktionseinheiten mit arabischen Ziffern von 1 bis 7 (I-1/7 – I-7/7) nummeriert. Die beiden besonderen infrastrukturellen Funktionseinheiten wurden als weitere Hauptkomponente mit römisch zwei (II) nummeriert. Die darin enthaltene Raumabluft-Vorfilterung wurde mit II-1/2 und die Brandschutzklappe im Schleifraum mit II-2/2 und ebenfalls nach ihrer Funktion/Sollfunktion benannt.

In Abb. 2.5 sind die Funktionseinheiten ihrer Reihe entsprechend aufgeführt. Unterhalb des Sollfunktionsnamens folgen die relevanten Prozessparameter eines jeden Funktionsblocks, auf die dann die Leitworte angewendet werden. Es sei nochmals darauf hingewiesen, dass das Wort Parameter hier stellenweise als sehr weitgefasst zu verstehen ist. Zum Beispiel ist hier unter *Aktorik* die der Sollfunktion entsprechende korrekte Bewegung der Maschinenteile sowie des zu bewegenden Materials zu verstehen.

Als besondere weitere Beispiele seien die Parameter *Schleifwasser Zufluss* d. h. der für eine der Sollfunktion entsprechend korrekte Zufluss von Schleifwasser sowie der Parameter *Schleifscheibe* erwähnt, der für einen intakten, der Sollfunktion entsprechenden Zustand der Schleifscheibe steht. Die Verarbeitung der Pelletchargen erfolgt diskontinuierlich, d. h. erst nach der Abarbeitung und Abführung des gesamten Materials der aktuellen Charge kann die Anlieferung einer neuen Charge per Transportschiffchen erfolgen. Somit ist eine Überfüllung eines stehenden Teilprozesses durch die weitere Anlieferung von Pellets via Transportschiffchen ausgeschlossen.

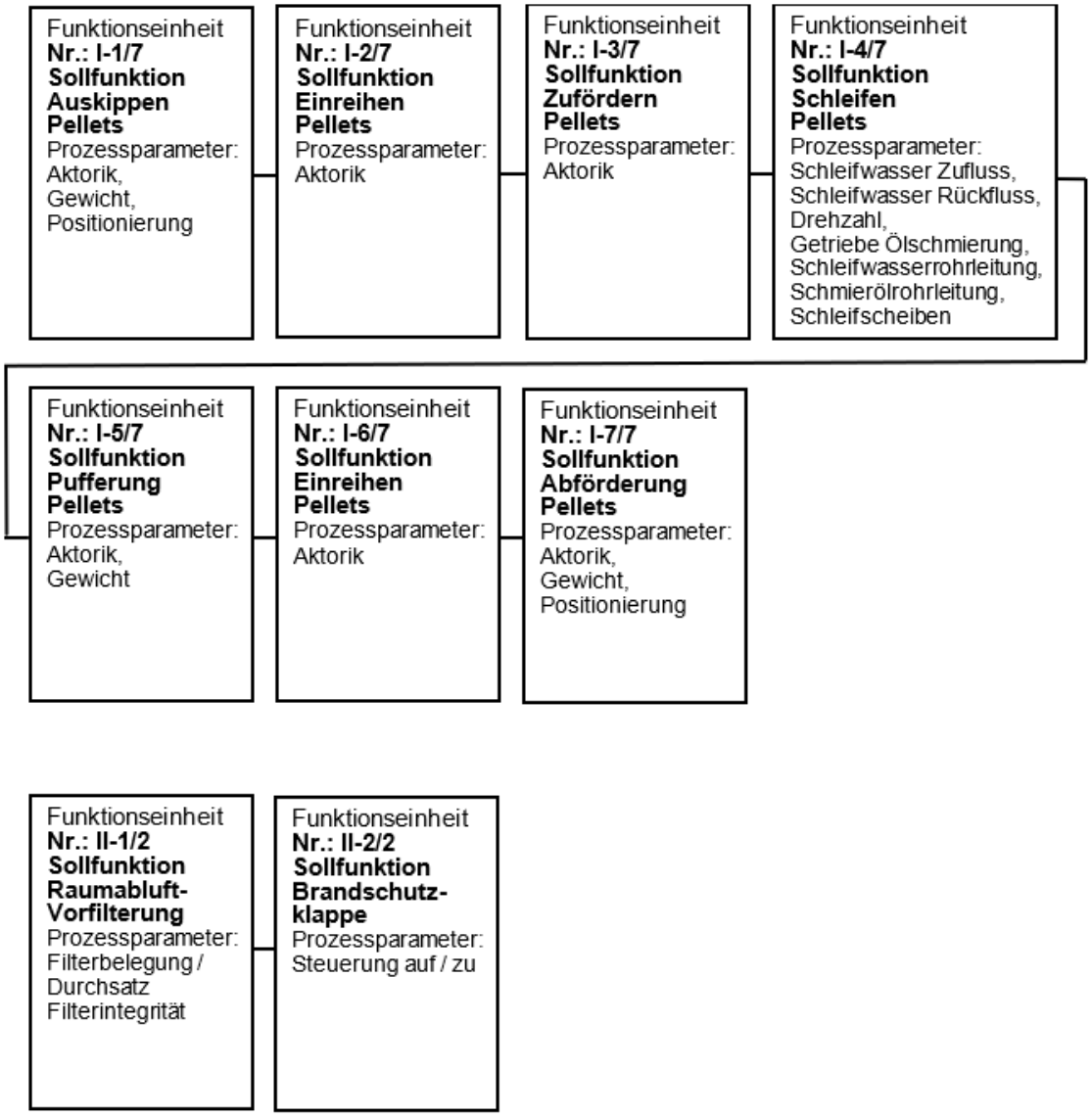

Abb. 2.5 Vereinfachte Systemdarstellung der Schleifstation und der zugehörigen infrastrukturellen Systeme und Funktionseinheiten

Im nächsten Schritt erfolgt die Prüfung von Leitworten auf die Parameter. Im aktuellen generischen Beispiel zum *Schleifen der Pellets* wurden Leitworte, die keine oder keine zusätzlichen Erkenntnisse bringen, zur Erhöhung der Übersichtlichkeit nicht in der Tabelle aufgeführt.

Bei der Wahl der Vorgehensweise ist auch prinzipiell zwischen den beiden Möglichkeiten der Auflistung aller, auch nicht besetzter Leitworte und der Variante zu unterscheiden, bei der nur Leitworte aufgelistet werden die einen Beitrag leisten. Werden alle Leitworte aufgeführt, kann dies als Nachweis dienen, dass alle gelisteten Fälle betrachtet wurden. Allerdings verschlechtern Matrixelemente, die keine neue Information bringen, die

Übersichtlichkeit und unter Umständen wird durch eine reduzierte Übersichtlichkeit die Akzeptanz bzw. schlimmstenfalls die Qualität des HAZOP-Ergebnisses reduziert.

Die Tab. 2.6 bis Tab. 2.14 zeigen spezifisch für die einzelnen Funktionseinheiten die Leitwort-Abfragen zu den gelisteten Sollparametern sowie im Weiteren auch die Maßnahmen, deren Umsetzung das Risiko minimieren.

Dies wird textlich zunächst exemplarisch an der Funktionseinheit I-1/7 *Auskippen der Pellets aus dem Transportschiffchen* mit der Sollfunktion *Vorstufe Zuführung Material zum Schleifprozess* beschrieben. Zur Erhöhung der Übersichtlichkeit bzw. des Auffindens erhält jede mögliche Ursache auf eine Leitwortabfrage innerhalb der betrachteten Funktionseinheit eine zugewiesene Nummer. Zu diesem Funktionsblock wurden als relevante Sollfunktionen die Parameter *Aktorik* für einen korrekten Antrieb der Mechanik bzw. einer korrekten Bewegung der Pellets, der Parameter *Gewicht* für die Prüfung der Pellets auf ihr Soll-Gewicht, sowie der Parameter *Positionierung* festgelegt. Für den Parameter Aktorik wurde das Leitwort *kein* festgelegt, d. h. es tritt keine der Sollfunktion entsprechende Aktorik ein. Als mögliche Ursachen dafür ergab das Brainstorming die zwei Fälle *keine lokale Stromversorgung, Nr. 1/3-1* sowie eine *möglich mechanische Verklemmung, Nr. 1/3-2*. Für die Ursache *keine lokale Stromversorgung* erfolgte die Auswirkung *keine Materialzuförderung*, für die Ursache *mechanische Verklemmung* die Auswirkung *elektrische Kurzschlussgefahr* und *keine Materialzuförderung*. Beides wurde mit der Risikostufe *gering* und bei der Häufigkeit die Ursache für *keine lokale Stromversorgung* als *sehr selten*, bei der mechanischen Verklemmung als *selten* eingestuft. Entsprechend folgt die Dokumentation der Art für den ersten Fall als *elektrisch*, für den zweiten Fall als *mechanisch / elektrisch*.

Als nächstes erfolgt ein qualifizierter Vorschlag für eine *Maßnahme, die das Risiko minimiert*. Da bei einem lokalen Stromausfall der Zuförderungsprozess einfach stehenbleibt, und sich keine kritische Situation entwickeln kann, wird *keine Maßnahme* empfohlen. Die finale Risikostufe und Häufigkeit bleiben bei den vorherigen Werten von jeweils *gering* bzw. *selten*. Für den zweiten Pfad der mechanischen Verklemmung ergeht als Risiko minimierende Maßnahme der Abhilfevorschlag die *Elektrik kurzschlussfest und die Mechanik ausreichend stabil* bei Einwirkung der maximalen Motorantriebsleitung auszulegen. Die Verifikation der Maßnahme erfolgt dabei durch z. B. Typenvorgaben für kurzschlussfeste Motoren bzw. entsprechend dimensionierten mechanischer Komponenten, wie z. B. Antriebswellen, Kugellager etc. Der Schweregrad bleibt in diesem Fall ohne

wesentliche Änderung im Design bzw. der fundamentalen Technik bei *gering*, die Häufigkeit konnte durch diese Verbesserungen von *selten* auf *sehr selten* reduziert werden.

Als zweiter Parameter wurde die *Positionierung* des Schiffchens mit dem Leitwort *anders als* aufgeführt. Hier ist zu beachten, dass bei einer falschen Positionierung des Transportschiffchens, die ein Nichterreichen der mechanischen Entriegelungsposition zur Folge hat, der Auskippprozess nicht gestartet werden kann. Die Auswirkung davon wäre, dass das System anhält und *keine Materialzuförderung* stattfindet. Die Risikostufe wurde mit der untersten Stufe als *gering* und die Häufigkeit mit der zweitniedrigsten Stufe als *selten* gelistet. Dementsprechend sind keine weiteren Maßnahmen zur Risikominimierung notwendig.

Als dritter Parameter wurde die Größe *Gewicht*, und als abzuprüfendes Leitwort *anders als* vom Sollwert festgelegt, d. h. eine mögliche nach oben oder unten abweichende Größe der Gesamtbeladung des Transportschiffchen. Als mögliche Ursache kann hier in dem gewählten generischen Prozess lediglich eine *unvollständige Entladung* des Transportschiffchens vorliegen. Dies hat jedoch auf den hier betrachteten Prozessablauf keine Relevanz. Die Risikostufe wurde als *gering* eingestuft und die Häufigkeit des Auftretens konservativerweise als *selten*. Die Beschreibung der Art ist dem Charakter entsprechend als *mechanisch* einzustufen. Da es keinen Grund für das Ergreifen von *Maßnahmen, zur Minimierung des Risikos* gibt, verändern sich die beiden letzten Spalten *Schweregrad* und *Häufigkeit* nicht.

Die Funktionseinheiten I-2/7 *Einreihen Pellets* und I-3/7 *Zufördern Pellets* ähneln der gerade beschriebenen Funktionseinheit I-1/7 und sollen daher nicht weiter ausgeführt werden. Die Parameter *Abprüfungen*, *Ursachen*, *Auswirkung* etc. sind in Tab. 2.7 und Tab. 2.8 aufgeführt.

Zu der Funktionseinheit I-4/7 *Schleifen Pellets*, wurden für die Abweichungen auf Soll-Parameter die sieben Größen *Schleifwasser Zufluss*, *Schleifwasser Rückfluss*, *Schleifwasser Förderrohrleitung*, *Drehzahl*, *Getriebe Ölschmierung*, *Ölförderrohrleitung* und *Schleifscheibe* gelistet, wobei hier die Größe *Schleifwasser Zufluss* auf zwei Leitworte abzuprüfen ist. Bei *Schleifwasser Zufluss* wird auf das Leitwort *weniger* fokussiert, was bei den Ursachen *keine pumpenspezifische Stromversorgung, Nr. 1/8*-1, *Ausfall Pumpe, Nr. 1/8-2*, *Verstopfung Rohrleitungssystem, Nr. 1/8-3* und *kein Wasservorrat, Nr. 1/8-4* jeweils in der Auswirkung einer *erhöhten Kontaminationsgefahr durch mangelnde Schleifstaubbindung* der Pellets mündet. Alle diese vier Szenarien wurden mit der Risikostufe *mäßig* und in der Häufigkeit als *selten* bewertet, abgesehen von der *Verstopfung Rohrleitungssystem*, die mit *mäßig* bewertet wurde. Als *Art* wurde in allen vier Fällen *Kontamination* angegeben. Für alle vier Szenarien wurde eine *Maßnahme, die das Risiko minimiert* vorgeschlagen. Dadurch konnten durch die individuellen Maßnahmen die erwartete Häufigkeit durchgängig auf *sehr selten* reduziert werden. Bei dem zweiten Leitwort *mehr* hinsichtlich des *Schleifwasser Zufluss, Nr. 2/8-1* ist auf die Ursache *ungeregelter Zufluss* mit einer *möglichen Moderationserhöhung* als Auswirkung, einer Risikostufe *bedeutend* und einer Häufigkeit, als *selten* in der Art *Moderation* fokussiert. Als Maßnahme, die das Risiko minimiert, wurde eine *Mengenbegrenzung ohne automatische Nachfüllung, d. h. nur manuelle Nachfüllung* vorgeschlagen und technisch sowie administrativ durch eine Betriebsanweisung festgeschrieben, wodurch sich die erwartete Häufigkeit auf die niedrigste Stufe auf sehr selten reduziert.

Beim *Schleifwasser Rückfluss* wurde auf das Leitwort *weniger* hinsichtlich eines mangelnden Abflusses bzw. in der Konsequenz auf eine lokale Mengenkumulierung anderenorts durch eine *Verstopfung des Rohrleitungssystems* mit der Auswirkung *mögliche Moderationserhöhung, Nr. 3/8-1*, bei einer Risikostufe *bedeutend* und der Häufigkeit *selten*, der Art *Moderation* fokussiert. Als Maßnahme, die das Risiko verringert, wurde eine *konstruktive Optimierung der Rohrausführung und Monitoring* vorgeschlagen und durch eine *Optimierung der Rohrdimension sowie seiner Innenbeschichtung inkl. Monitoring* umgesetzt, wodurch sich die erwartete Häufigkeit auf *sehr selten* reduziert.

Bei der Betrachtung des Systemparameters *Schleifwasserförderrohrleitung* wurde das Leitwort *nicht* zugeordnet, das dann in der Konsequenz als mögliche Ursache *Leckage* und den beiden möglichen Auswirkungen *erhöhte Kontamination durch mangelnde Schleifstaubbindung, Nr. 4/8-1*, Risikostufe *mäßig*, Häufigkeit *selten*, Art *Kontamination* bzw. je nach Ort der Leckage in eine *mögliche Moderationserhöhung, Nr. 4/8-2*, Risikostufe *bedeutend*, Häufigkeit *selten, Art Moderation* mündet. Beim ersten Fall (Nr. 4/8-1) wurde als Maßnahme, die das Risiko verringert, eine *Förderüberwachung* umgesetzt durch ein *Monitoring* mit der Risikostufe *mäßig* und der Häufigkeit *sehr selten*. Bei dem zweiten Fall (Nr. 4/8-2) wurde als Maßnahme, die das Risiko minimiert, eine *Überwachung auf eine Mindestmenge sowie einen Fußboden mit Gefälle für einen eindeutig definierten Ablauf* festgelegt, sodass die Häufigkeitsstufe auf den geringsten Wert, d. h. *sehr selten*, eingestuft werden konnte.

Als nächster Parameter wurde *Drehzahl* mit dem Leitwort *nein* und den beiden möglichen Ursachen *keine Stromversorgung Antrieb, Nr. 5/8-1* und *Ausfall Motor, Nr. 5/8-2* betrachtet. Die Auswirkung ist jeweils *Schleifprozess steht unkritisch*, mit der Risikostufe *gering*. Bei der Ursache *keine Stromversorgung* wurde die Häufigkeit auf *sehr selten*, bei der Ursache *Ausfall Motor* auf *selten* gesetzt. Die Art ist jeweils *elektrisch*. Da die Auswirkung *Schleifprozess steht* als unkritisch zu sehen ist und auch hier keine weitere Zuförderung erfolgen kann, wurden keine Maßnahmen zur Risikominimierung gelistet.

Für den Parameter *Getriebe, Ölschmierung* erfolgt eine Prüfung auf das Leitwort *nicht* mit den möglichen Ursachen *Ausfall Ölförderpumpe, Nr. 6/8-1* und mit der Auswirkung *Erhöhter Verschleiß und Temperaturanstieg*, sowie als zweite Ursache *mangelnde Schmierölmenge, Nr. 6/8-2* mit der gleichen, zuvor genannten Auswirkung. Beide Auswirkungen wurden mit der Risikostufe *mäßig* und der erwarteten Häufigkeit *selten* in die Art *mechanisch/Temperatur* eingestuft. Als Maßnahme die das Risiko minimiert wurde für den Fall Nr. 6/8-1 eine *Funktionsüberwachung* und für den Fall Nr. 6/8-2 eine *Mengenüberwachung* umgesetzt, beide Male durch ein entsprechendes *Monitoring*. Somit konnte für beide Fälle die erwartete Häufigkeit auf *sehr selten* reduziert werden.

Bei der Ölförderrohrleitung ergibt die Abfrage auf das Leitwort *nicht* als mögliche Ursache eine *Leckage* und die drei möglichen Auswirkungen *ölhaltiges Abwasser, Nr. 7/8-1*, *mögliche Moderationserhöhung, Nr. 7/8-2* und *Leckageöl als mögliche Brandlast, Nr. 7/8-3*. Die Risikostufen wurden für die drei Auswirkungen als *gering*, *bedeutend* und *mäßig* bei jeweils einer angenommenen Häufigkeit von *selten* abgeschätzt. Die drei Arten wurden entsprechend ihrem Charakter als *Entsorgung*, *Moderatio*n und *Brandlast*

gelistet. Als Maßnahmen, die das Risiko minimieren, wurde für den Fall *ölhaltiges Abwasser, Nr. 7/8-1* ein *Ölabscheider* mit nachfolgender Typenvorgabe, für den Fall *mögliche Moderationserhöhung, Nr. 7/8-2* eine *Überwachung auf eine vorhandene Mindestmenge im Behälter und Boden mit Gefälle für eindeutigen Ablauf* mit nachfolgender Umsetzung, sowie für den Fall *Leckageöl als mögliche Brandlast, Nr. 7/8*-3 eine *Überwachung auf Mindestmenge im Behälter* mit anschließender Umsetzung gesetzt. Bei allen drei Auswirkungen konnte damit die Häufigkeit um eine Stufe auf *sehr selten* reduziert werden.

Bei dem letzten Parameter *Schleifscheibe* ergibt sich mit dem Leitwort *nicht* auf deren Sollfunktion als mögliche Ursache *größerer Materialausbruch* die Auswirkung *Projektil verlässt Maschinenbereich, Nr. 8/8-1*, mit der Risikoeinstufung *mäßig*, der Häufigkeit *selten* und der Art *Projektil*. Als Maßnahme, die das Risiko minimiert, wurde eine *Einhausung* mit entsprechenden Umsetzvorgaben festgelegt, wodurch die Häufigkeit für auftretende Schäden auf *sehr selten* reduziert wurde.

Die weiteren Funktionseinheiten Pufferung Pellets (I-5/7), Einreihen der Pellets (I-6/7) und Abförderung der Pellets (I-7/7) wurden in analoger Weise betrachtet und stellen im Wesentlichen nur Wiederholungen des vorherigen dar. Die Ergebnisse sind in Tab. 2.10 bis Tab. 2.12 zu finden.

Von größerem Interesse für die vorliegende generische Untersuchung sind die beiden infrastrukturellen Funktionseinheiten *Raumluft-Vorfilterung (II-1/2)*, die eine Vorfilterung von in der Raumluft möglicherweise vorhandenen Pellet-Schleifstaub übernehmen soll, sowie die *Brandschutzklappe (II-2/2)*, die für die Steuerung des Raumluftaustauschs relevant ist.

Bedingt durch eine mögliche Belastung der Raumluft mit Pellet-Schleifabrieb soll zur Reduzierung der Gesamtabluftbelastung bereits im Schleifraum eine Luft-Vorfilterung mit der Funktionseinheit II-1/2 erfolgen. Der Filter ist dabei durch die zwei Parameter *Filterbelegung sowie Filterintegrität* zu klassieren. Der Parameter *Filterbelegung* wird durch das Leitwort *mehr* auf eine zu hohe Filterbelegung abgeprüft. Als mögliche Ursache wird eine *ausgesprochen hohe Raumluftbelastung, bzw. ein fehlender zyklischer Filtertausch*, mit der Auswirkung einer *Verringerung der Wechselrate der Raumluft, bzw. mögliche höhere Raumluftkontamination, Nr. 1/2-1*, mit Risikostufe *bedeutend* und Häufigkeit *selten* gelistet. Als Maßnahme, die das Risiko minimiert, wurde ein *zyklischer Tausch* bei einer neuen Pellet-Chargenbearbeitung als Betriebsfreigabebedingung

festgelegt. Zur Sicherstellung dafür wurde auch eine Aufnahme der Vorgabe in das Betriebshandbuch der Anlage festgelegt. Somit wurde die verbleibende Häufigkeit auf *sehr selten* gestuft.

Bei dem Parameter *Filterintegrität* wird auf das Leitwort *weniger* geprüft. Als mögliche Ursachen kommt eine *mechanische Zerstörung der Filtermembrane, Nr. 2/2-1* oder eine *druckstoßmäßige Zerstörung der Filtermembrane, Nr. 2/2-2* in Frage. Die Auswirkung ist in beiden Fällen *erhöhte kontaminierte Abluf*t mit dem Schweregrad *bedeutend* und der Häufigkeit *selten*, identisch. Als Art wurde *mechanisch* bzw. als weitere Detaillierung *druckstoßtechnisch* gelistet. Als Maßnahme, die das Risiko minimiert, wurde im Fall Nr. 2/2-1 die Anbringung eines *Schutzgitters* gemäß einer Typenvorgabe bestimmt. Im Fall *druckstoßtechnischen Zerstörung der Filtermembran, Nr. 2/2-2* wurde lediglich allgemein eine *stabile Ausführung* als ausreichende risikoreduzierende Maßnahme erachtet, da im Raum sowohl druckführende Komponenten mit deren Möglichkeit der Druckabgabe in den Raum als auch explosionsgefährdete Materialien als potenziell auslösende Druckstoßquellen fehlen. In letztem Fall wären die Produktrichtlinien für das Inverkehrbringen von Geräten und Produkten in explosionsgefährdeten Bereichen (ATEX-Produktrichtlinie) /GAB 20/ zu betrachten. Der Häufigkeitsgrad wurde damit auf *sehr selten* gesenkt.

Tab. 2.6 HAZOP-Matrizen für die Funktionseinheit I-1/7: Auskippen Pellets aus Transportschiffchen, Sollfunktion: Vorstufe Zuführung Material zum Schleifprozess

Nr.:	Leitwort	Abweichung auf Parameter	Mögliche Ursache	Auswirkung	Risikostufe	Häufigkeit	Art	Maßnahme die das Risiko minimiert	Verifikation der Maßnahme	Resultierende Risikostufe	Resultierende Häufigkeit
1/3-1	kein	Aktorik	keine lokale Stromversorgung	keine Materialzuförderung	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1/3-2			mechanische Verklemmung	elektrische Kurzschlussgefahr, Überhitzung	gering	selten	mechanisch / elektrisch	Aktorik elektr. kurzschlussfest und mechanisch stabil auslegen	umgesetzt durch Typenvorgabe	gering	sehr selten
2/3-1	anders als	Positionierung	mechanische Entriegelungsposition nicht erreicht	keine Materialzuförderung	gering	selten	mechanisch	keine	---	gering	selten
3/3-1	anders als	Gewicht	Unvollständige Entladung	keine kritische Prozessrelevanz	gering	selten	mechanisch	keine	---	gering	selten

Tab. 2.7 HAZOP-Matrizen für die Funktionseinheit I-2/7: Einreihen Pellets, Sollfunktion: Vorstufe Zuführung Material zum Schleifprozess

Nr.:	Leit-wort	Abweichung auf Parame-ter	Mögliche Ursache	Auswirkung	Risiko-stufe	Häu-figkeit	Art	Maßnahme die das Risiko minimiert	Verifikation der Maß-nahme	Resultie-rende Risi-kostufe	Resultie-rende Häufigkeit
1/1-1	kein	Aktorik	keine lokale Stromversor-gung	keine Materialzuförde-rung	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1/1-2			mechanische Verklemmung	elektrische Kurzschluss-gefahr, keine Material-zuförderung	gering	selten	mechanisch / elektrisch	Aktorik kurzschluss-fest auslegen	umgesetzt durch Typen-vorgabe	gering	sehr selten

Tab. 2.8 HAZOP-Matrizen für die Funktionseinheit I-3/7: Zufördern Pellets, Sollfunktion: Zuführung Material zum Schleifprozess

Nr.:	Leit-wort	Abweichung auf Parame-ter	Mögliche Ursache	Auswirkung	Risiko-stufe	Häu-figkeit	Art	Maßnahme die das Risiko minimiert	Verifikation der Maß-nahme	Resultie-rende Risi-kostufe	Resultie-rende Häufikeit
1/1-1	keine	Aktorik	Keine lokale Stromversor-gung	keine Materialzuförde-rung	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1/1-2			mechanische Verklemmung	Elektrische Kurzschluss-gefahr, keine Material-zuförderung	gering	selten	mechanisch / elektrisch	Aktorik kurzschluss-fest auslegen	umgesetzt durch Typvor-gabe	gering	sehr selten

Tab. 2.9 HAZOP-Matrizen für die Funktionseinheit I-4/7: Schleifen Pellets, Sollfunktion: Schleifprozess

Nr.:	Leitwort	Abweichung auf Parameter	Mögliche Ursache	Auswirkung	Risikostufe	Häufigkeit	Art	Maßnahme die das Risiko minimiert	Verifikation der Maßnahme	Resultierende Risikostufe	Resultierende Häufikeit
1/8-1	weniger	Schleifwasser Zufluss	keine pumpenspezifische Stromversorgung	erhöhte Kontaminationsgefahr durch mangelnde Schleifstaubbindung	mäßig	selten	Kontamination	Kopplung an Stromversorgung Schleifantrieb	umgesetzt durch Verteilervorgabe	mäßig	sehr selten
1/8-2			Ausfall Pumpe	erhöhte Kontaminationsgefahr durch mangelnde Schleifstaubbindung	mäßig	selten	Kontamination	Förderüberwachung	umgesetzt durch Monitoring	mäßig	sehr selten
1/8-3			Verstopfung Rohrleitungssystem	erhöhte Kontaminationsgefahr durch mangelnde Schleifstaubbindung	mäßig	mäßig	Kontamination	Rohrdimensionierung für ausreichende Strömungs-geschwindigkeit	umgesetzt durch Dimensions- und Innenbeschichtungsvorgabe	mäßig	sehr selten
1/8-4			kein Wasservorrat	erhöhte Kontaminationsgefahr durch mangelnde Schleifstaubbindung	mäßig	selten	Kontamination	Überwachung auf Sollmenge	umgesetzt durch Monitoring	mäßig	sehr selten
2/8-1	mehr	Schleifwasser Zufluss	ungeregelter Zufluss	mögliche Moderationserhöhung	bedeutend	selten	Moderation	Mengenbegrenzung ohne autom. Nachspeisung d. h. nur manuell	umgesetzt durch Betriebsanweisung	bedeutend	sehr selten
3/8-1	weniger	Schleifwasser Rückfluss	Verstopfung Rohrleitungssystem	mögliche Moderationserhöhung	bedeutend	selten	Moderation	Konstruktive Optimierung Rohrausführung, Überwachung auf Sollmenge	umgesetzt durch Dimensions- und Innenbeschichtungsvorgabe Monitoring	bedeutend	sehr selten

Nr.:	Leitwort	Abweichung auf Parameter	Mögliche Ursache	Auswirkung	Risikostufe	Häufigkeit	Art	Maßnahme die das Risiko minimiert	Verifikation der Maßnahme	Resultierende Risikostufe	Resultierende Häufikeit
4/8-1	nicht	Schleifwasserförderrohrleitung	Leckage	erhöhte Kontaminationsgefahr durch mangelnde Schleifstaubbindung,	mäßig	selten	Kontamination	Förderüberwachung	umgesetzt durch Monitoring	mäßig	sehr selten
4/8-2				mögliche Moderationserhöhung	bedeutend	selten	Moderation	Überwachung auf Mindestmenge, Boden mit Gefälle für eindeutigen Ablauf	umgesetzt durch Monitoring, Neigung Boden	bedeutend	sehr selten
5/8-1	nein	Drehzahl	keine Stromversorgung Antrieb	Schleifprozess steht unkritisch	gering	sehr selten	Elektrisch	keine	---	gering	sehr selten
5/8-2			Ausfall Motor	Schleifprozess steht unkritisch	gering	selten	Elektrisch	keine	---	gering	selten
6/8-1	nein	Getriebe, Ölschmierung	Ausfall Ölförderpumpe	erhöhter Verschleiß & Temperaturanstiege	mäßig	selten	mechanisch/Temperatur	Funktionsüberwachung	umgesetzt durch Monitoring	Mäßig	sehr selten
6/8-2			mangelnde Schmierölmenge	erhöhter Verschleiß & möglicher Temperaturanstieg	mäßig	selten	mechanisch / Temperatur	Mengenüberwachung	umgesetzt durch Monitoring	mäßig	sehr selten

Nr.:	Leit-wort	Abweichung auf Parameter	mögliche Ursache	Auswirkung	Risiko-stufe	Häu-figkeit	Art:	Maßnahme die das Risiko minimiert	Verifikation der Maß-nahme	Resultie-rende Risikostufe	Resultie-rende Häufikeit
7/8-1	nicht	Ölförderrohrlei-tung	Leckage	ölhaltiges „Abwasser“	gering	selten	Entsorgung	Ölabscheider	umgesetzt, Typvorgabe	gering	sehr selten
7/8-2				mögliche Moderations-erhöhung	bedeu-tend	selten	Moderation	Überwachung auf Mindestmenge im Be-hälter, Boden mit Ge-fälle für eindeutigen Ablauf	umgesetzt durch Monitoring	bedeutend	sehr selten
7/8-3				Leckageöl als mögliche Brandlast	mäßig	selten	Brandlast	Überwachung auf Mindestmenge im Be-hälter	umgesetzt durch Monitoring	mäßig	sehr selten
8/8-1	nicht	Schleifscheibe	größerer Material-ausbruch	Projektil verlässt Maschinenbereich	mäßig	selten	Projektil	Einhausung	umgesetzt Designvor-gabe Einhau-sung	mäßig	sehr selten

Tab. 2.10 HAZOP-Matrizen für die Funktionseinheit I-5/7: Pufferung Pellets, Sollfunktion: Vorbereitung Wegführung Material vom Schleifprozess

Nr.:	Leitwort	Abweichung auf Parameter	mögliche Ursache	Auswirkung	Risikostufe	Häufigkeit	Art:	Maßnahme die das Risiko minimiert	Verifikation der Maßnahme	Resultierende Risikostufe	Resultierende Häufikeit
1/3-1	kein	Aktorik	keine lokale Stromversorgung	keine Materialförderung	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1/3-2			mechanische Verklemmung	elektrische Kurzschlussgefahr, keine Materialzuförderung	gering	Selten	mechanisch elektrisch	Aktorik kurzschlussfest auslegen	umgesetzt durch Typvorgabe	gering	sehr selten
2/3-1	weniger	Gewicht	noch Kapazität vorhanden	keine kritische Prozessrelevanz	gering	selten	mechanisch	keine	---	gering	selten
3/3-1	mehr	Gewicht	Kapazitätsgrenze erreicht	Überfüllung mit mech. Verklemmungen möglich	mäßig	Selten	mechanisch	weitere Zuförderung stoppen	umgesetzt durch Monitoring	gering	sehr selten

Tab. 2.11 HAZOP-Matrizen für die Funktionseinheit I-6/7: Einreihen Pellets, Sollfunktion: Vorbereitung Wegführung Material vom Schleifprozess

Nr.:	Leitwort	Abweichung auf Parameter	mögliche Ursache	Auswirkung	Risikostufe	Häufigkeit	Art:	Maßnahme die das Risiko minimiert	Verifikation der Maßnahme	Resultierende Risikostufe	Resultierende Häufikeit
1/1-1	kein	Aktorik	keine lokale Stromversorgung	keine Materialförderung	gering	selten	elektrisch	keine	---	gering	selten
1/1-2			mechanische Verklemmung	elektrische Kurzschlussgefahr, keine Materialzuförderung	gering	Selten	mechanisch elektrisch	Aktorik kurzschlussfest auslegen	umgesetzt durch Typvorgabe	gering	ehr selten

Tab. 2.12 HAZOP-Matrizen für die Funktionseinheit I-7/7: Abförderung Pellets, Sollfunktion: Wegführung Material vom Schleifprozess

Nr.:	Leit-wort	Abweichung auf Parameter	mögliche Ursache	Auswirkung	Risiko-stufe	Häu-figkeit	Art:	Maßnahme die das Risiko minimiert	Verifikation der Maß-nahme	Resultie-rende Risikostufe	Resultie-rende Häufikeit
1/3-1	kein	Aktorik	keine lokale Stromver-sorgung	keine Materialförderung	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1/3-2			mechani-sche Ver-klemmung	elektrische Kurzschluss-gefahr, keine Material-zuförderung	gering	selten	mechanisch elektrisch	Aktorik kurzschluss-fest auslegen	umgesetzt durch Typvor-gabe	gering	sehr selten
2/3-1	an-ders als	Gewicht	unvollstän-dige Materi-alabförde-rung	keine kritische Prozess-relevanz	gering	selten	mechanisch	keine	---	gering	selten
3/3-1	an-ders als	Positionierung	mechan. Entriege-lungsposi-tion nicht erreicht	keine Materialabförde-rung	gering	selten	mechanisch	keine	---	gering	selten

Tab. 2.13 HAZOP-Matrizen für die infrastrukturelle Funktionseinheit II-1/2: Raumabluft-Vorfilterung, Sollfunktion: Vorfilterung kontaminierter Raumabluft

Nr.:	Leitwort	Abweichung auf Parameter	mögliche Ursache	Auswirkung	Risikostufe	Häufigkeit	Art:	Maßnahme die das Risiko minimiert	Verifikation der Maßnahme	Resultierende Risikostufe	Resultierende Häufikeit
1/2-1	mehr	Filterbelegung	ausgesprochen hohe Raumluftbelastung, fehlender zyklischer Tausch	Verringerung der Wechselrate der Raumluft, mögliche höhere Raumluft-kontamination	bedeutend	selten	strömungstechnisch	zyklischer Tausch	umgesetzt im Betriebshandbuch	bedeutend	sehr selten
2/2-1	weniger	Filterintegrität	mechanische Zerstörung Filtermembrane	erhöhte kontaminierte Abluft	bedeutend	selten	mechanisch	Schutzgitter	umgesetzt durch Typvorgabe	bedeutend	sehr selten
2/2-2			druckstoßmäßige Zerstörung Filtermembrane	erhöhte kontaminierte Abluft	bedeutend	selten	druckpulstechnisch	stabile Ausführung	umgesetzt durch Typvorgabe, jedoch keine ATEX-Qualität mangels Explo-sionspotential im Raum	bedeutend	sehr selten

Tab. 2.14 HAZOP-Matrizen für die infrastrukturelle Funktionseinheit II-2/2: Brandschutzklappe, Sollfunktion: binäre Regelung Raumabluft

Nr.:	Leit-wort	Abweichung auf Parameter	mögliche Ursache	Auswirkung	Risiko-stufe	Häu-figkeit	Art:	Maßnahme die das Risiko minimiert	Verifikation der Maß-nahme	Resultie-rende Risikostufe	Resultie-rende Häufikeit
1/2-1	nicht	Thermo. Akto-rik (Schmelzsi-cherung)	Verklem-mung	Ausbreitung von Rauch / Feuer	bedeu-tend	selten	Rauch	Einsatz zertifizierter Brandschutzklappen	umgesetzt durch Typvor-gabe	bedeutend	sehr selten
2/2-1	an-ders als	Elektrische Aktorik	kein Strom	keine Funktion	gering	sehr selten	elektrisch	keine, da Schmelzsi-cherung prioritär	---	gering	sehr selten
2/2-2			Fehlfunktion	Ausführung keiner gewollten Funktion	gering	sehr selten	elektrisch / mechanisch	keine, da Schmelzsi-cherung prioritär	---	gering	sehr selten

Das Bisherige kann folgendermaßen zusammengefasst werden: Basierend auf der durchgängigen Einstufung des möglichen Schweregrads mit *gering* und einer möglichen Häufigkeit des Auftretens von *sehr selten* bis *selten*, sind die in ihrer Gänze als risikoarm einzustufenden Funktionseinheiten die Folgenden:

- I-1/7 Auskippen Pellets
- I-2/7 Einreihen Pellets
- I-3/7 Zufördern Pellets
- I-5/7 Pufferung Pellets
- I-6/7 Einreihen Pellets
- I-7/7 Abförderung Pellets

Die Funktionseinheit I-4/7 *Schleifen Pellets* zeigt speziell beim Thema Schleifstaub der Pellets, zu dem Punkt *mangelnde Schleifstaubbindung durch fehlendes Wasser*, ein erhöhtes Kontaminationspotential. Außerdem besteht u. a. auch im Zusammenhang mit dem Schleifwasser ein tendenzielles Risiko hinsichtlich der Verletzung von Moderationsbegrenzungen.

Die infrastrukturelle Funktionseinheit II-1/2 *Raumabluft-Vorfilterung* steht über das Thema *luftgebundener Schleifstaub* in direkter Verbindung zur Schleifmaschine.

Die infrastrukturelle Funktionseinheit II-2/2 *Brandschutzklappe* würde bei einem Versagen der Schmelzsicherung im Anforderungsfall zwar hinsichtlich dem Schweregrad bedeutend sein, die Eintrittswahrscheinlichkeit eines solchen Falls ist jedoch mit der niedrigsten Stufe *sehr selten* gelistet.

Abschließend sei in Bezug auf die Verbindung der beiden Funktionseinheiten I-4/7 *Schleifmaschine und II-1/2 Raumabluft-Vorfilterung* über das Thema *luftgebundener Pellet-Schleifstaub* nochmals explizit darauf hingewiesen, dass bei einer HAZOP-Betrachtung ein Doppelfehler, der beide Funktionseinheiten zugleich beeinträchtigt, nicht abgeprüft wird. Dies ist durch die Anwendung weiterer Störfallanalysen zu überprüfen.

2.4.4.3 Grenzen von HAZOP

Wichtig ist beim Einsatz von Risikoanalysen, auch deren Grenzen zu beachten. Besonders bei einer hohen risikobehafteten Wechselwirkung zwischen mehreren Systemteilen reicht HAZOP alleine nicht aus, und es sind für eine detailliertere Untersuchung weitere Methoden wie die Ereignisbaumanalyse (*Event Tree Analysis*, ETA, siehe Kapitel 2.4.5) und die Fehlerbaumanalyse (*Fault Tree Analysis*, FTA, siehe Kapitel 2.4.6) einzusetzen. Sollen bei HAZOP weitergehende, nicht systemspezifische Eigenschaften oder Aspekte betrachtet werden, kann dies u. U. durch die Einführung zusätzlicher, nicht spezifischer Leitworte realisiert werden, z. B. für Fragen der Zugriffsberechtigung auf ein System oder bei systemspezifische Wartungsanforderungen. Als besonders wichtig ist die bei einer HAZOP-Betrachtung getroffene Grundannahme, dass der auf Abweichungen vom Soll-Zustand betrachtete und anschließend bewertete Ablauf an sich (d. h. innerhalb seiner Soll-Funktion) bereits ein sicherer Prozess ist bzw. ein sicheres Betriebsverhalten besitzt. Die Anwendbarkeit einer HAZOP-Betrachtung gilt unabhängig von den gewählten Funktionskomponenten- oder sonstigen Betrachtungsebenen, da nur innerhalb der gewählten Ebene eine Prüfung auf mögliche Abweichungsszenarien vom Sollzustand erfolgt. Erkannte Abweichungen bilden die nächste, zu betrachtende Ebene.

Wie mit jeder Technik zur Ermittlung von Gefahren oder Funktionsproblemen kann auch bei der HAZOP-Analyse nicht vollständig gewährleistet werden, dass alle Gefahren oder Funktionsprobleme aufgedeckt werden können. Somit sind für eine möglichst umfassende Betrachtung weitere, geeignete Ansätze auszuwählen bzw. durchzuführen.

Vor diesem Hintergrund wurden entsprechend des oben genannten Umstandes in diesem Bericht weitere Methoden wie Deterministische Störfall- und Ereignisbaumanalysen bzw. Fehlerbaum- und probabilistische Sicherheitsanalysen durchgeführt, um u. a. auch an einem konstruierten Ereignis die praktischen Grenzen der grundsätzlich sinnvollen HAZOP Analyse und die – je nach Risikopotential – Wichtigkeit des Einsatzes weiterer Analysemethoden an diesem Beispiel aufzuzeigen. Basierend auf dem Ergebnis der HAZOP-Risikoeinschätzung werden in der Regel im Anschluss Überlegungen zur Wahrung der Verhältnismäßigkeit vorgenommen, ob weitergehende Maßnahmen zur Risikoreduktion erforderlich sind.

2.4.5 Deterministische Störfall- und Ereignisbaumanalyse (DSA und ETA)

Deterministische Störfallanalysen (DSA) werden in der Regel auf Störfallszenarien angewendet, gegen die eine spezielle Anlage auszulegen ist. Dies ist besonders von Bedeutung, wenn z. B. Einzelsysteme zur Gewährleistung der Einhaltung gesetzlich vorgeschriebener Funktionen betrachtet werden müssen. Die dabei auszuführenden Schritte können für den vorliegenden Fall wie folgt zusammengefasst werden: Analyse der Anlagenbedingungen bzw. Identifikation und Kategorisierung von auslösenden Ereignissen, welche zu gefährdenden Material- oder Energiefreisetzungen führen können, gegen die die Anlage auszulegen ist.

Bei den Betrachtungen wird in der Regel von Einzelfehlern ausgegangen. Ein Einzelfehler liegt vor, wenn ein Systemteil seine Funktion bei Anforderung nicht erfüllt. Für eine DSA wird in der Regel auf konservative Annahmen zurückgegriffen. Ein Einfluss menschlicher Fehlhandlungen wird im Allgemeinen nicht detailliert unterstellt bzw. nicht untersucht. Fehler mit gemeinsamer Ursache an mehreren zueinander redundanten Systemteilen (*common cause failure*) sowie Auslegungsfehler werden durch das Einzelfehlerkonzept nicht abgedeckt /GÄN 13/.

Bei der deterministischen Störfallanalyse geht man (wie bei der Ereignisbaumanalyse) nach der induktiven Methode vor, d. h. beginnend von einem Start- bzw. Basisszenario entwickelt man sich zu den sich daraus weiter ergebenden Auswirkungen voran. Als Vorarbeit sind die Ereignisse bzw. das Basisereignis zu benennen sowie in der Folge die sequentiellen Einzelelemente in einer Master-Logik aufzulisten. Bei der deterministischen Störfallanalyse wird, wie im gewählten Beispiel angenommen, ein Einzelfehler unterstellt. Im hier gewählten Beispiel handelt es sich um den mechanischen Integritätsverlust des Hauptlagers des Antriebsgetriebe der Schleifmaschine mit folgendem Verlauf:

- transienter Temperaturgang des Lagers sowie an dessen Fixierungskonstruktion;
- hohe Schwingungsamplituden des Getriebes und Amplitudenübertragung an das Hilfssystem Ölversorgung;
- Resonanzanfachung der Ölzuleitung bis hin zum Bruch;
- weiter fördernde Ölpumpe;

- diffus spritzende Ölaustrittsbruchfläche und Benetzung der umliegenden Oberflächen;
- Selbstentzündung des auf den Hotspot des Getriebekasten spritzenden Öls;
- Zündungsbedingter Druckstoß des Öls bedingt eine Teilzerstörung der primären, rauminternen Filterstufe der Absaugung und Unterdruckerzeugung in der Einhausung;
- allgemeiner Temperaturanstieg und einsetzende Verdampfung des Schleifschmiermittels Wasser;
- Spritzschutz sowie Luftleitfunktion der Polycarbonat-Scheiben der partiellen Einhausungsbereiche verschlechtern bzw. verringern sich;
- Schließen der Brandschutzklappen für die Einhausung der Schleifmaschine und für die Raumluft;
- Abschaltung der Schleifmaschine;
- Aktivierung der CO_2-Löschanlage;
- Löschung des Brands durch Sauerstoffentzug und Kühlung.

In Abb. 2.6 ist die Abfolge dieser Einzelereignisse als *Botton-up* Darstellung inklusive der Kurzbezeichnungen der einzelnen Ereignisse schematisch dargestellt.

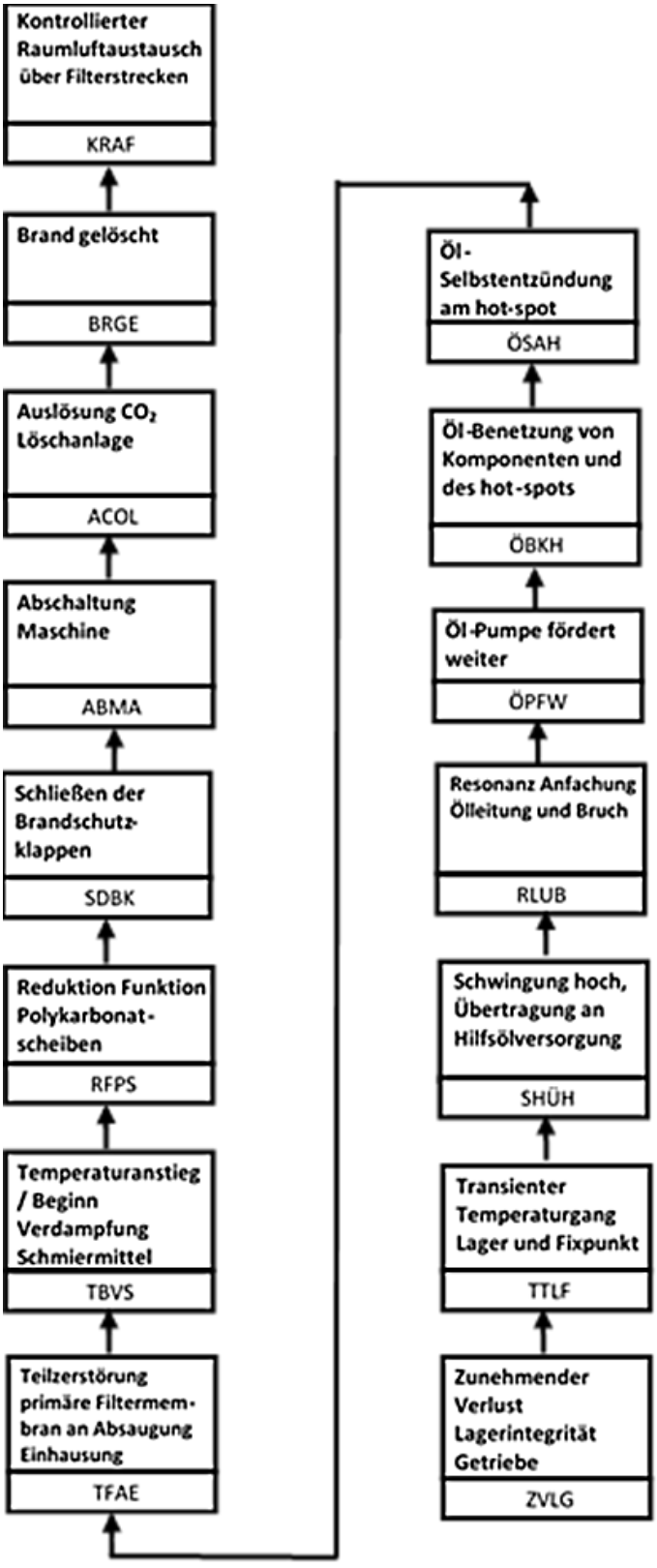

Abb. 2.6 Abfolge der Einzelereignisse als Botton-up-Darstellung inkl. Kurzbezeichnung der einzelnen Ereignisse

Bei der Ereignisbaumanalyse bzw. Event Tree Analysis (ETA) geht man ebenfalls nach der induktiven Methode vor. Das heißt, man geht von einem Startereignis (typischerweise dem interessierenden Fehler) schrittweise voran und ermittelt dabei die möglichen Folgeereignisse. Das Ergebnis wird dann typischerweise in einer binären Baumgrafik dargestellt. Somit ist es möglich, die verschiedenen Pfade bzw. die daraus möglichen Zustände und Folgen aufzuzeigen.

Bei der für das aktuelle Szenario durchgeführten Vorwärtsentwicklung wie in Abb. 2.7 gezeigt werden typischerweise die Elemente der binären Logik verwendet, d. h. als weitere Abfrage wird geprüft, was auf den aktuellen Schritt passiert. Insbesondere können dies Fragen nach einer weiteren Eskalation oder nach dem Eingriff von Sicherheitssystemen sein, die eine deeskalierende Wirkung bedingen.

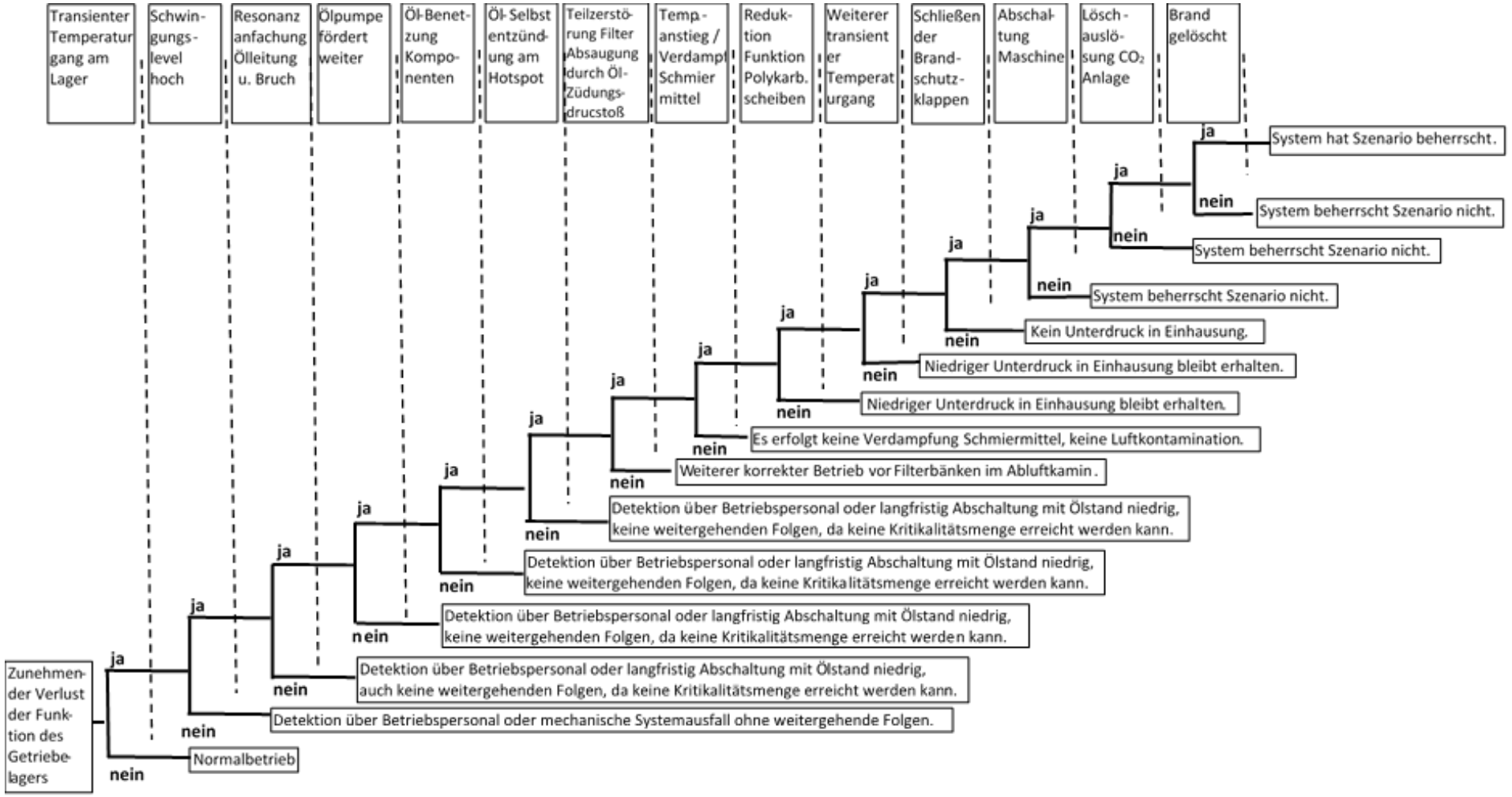

Abb. 2.7 Darstellung des postulierten Ereignisbaums für das ausgewählte Ereignisszenario

Ein Versagen der Leittechnik bzw. der angesteuerten Komponenten bei den letzten drei Schritten, beginnend mit dem Entscheider *Abschalten der Maschine*, *Löschauslösung CO_2-Anlage* und *Brand gelöscht* (d. h. ausreichende Systemperformance der Löschanlage) wären als ernste Systemschwächen einzustufen.

2.4.6 Fehlerbaum- (FTA) und probabilistische Sicherheitsanalyse (PSA)

Im Vergleich zur DSA ist der bei der PSA gewählte Ansatz wesentlich komplexer. Hier werden alle relevanten Ereignisabläufe, d. h. auch anlagendesignbedingte Funktionen, einbezogen bzw. betrachtet. Der Ansatz der PSA für eine Gesamtanlage setzt voraus, dass detaillierte Kenntnisse der Anlage und der darin durchgeführten Prozesse vorhanden sind und die Anlage im Sinne der PSA vollständig abgebildet werden kann. Weiterhin ist mit dieser Herangehensweise die probabilistische Sicherheitsanalyse eines klar abgegrenzten Teilprozesses möglich. Im Vergleich zur DSA finden bei der PSA auch Mehrfachfehler sowie Fehler mit gemeinsamer Ursache (*common cause*) Berücksichtigung. Auch wird bei der PSA i. A. nicht auf konservative Annahmen zurückgegriffen, sondern auf eine möglichst realistische Bewertung der gesamten Anlage abgezielt. Hierbei sollten auch potenzielle menschliche Fehlhandlungen detailliert berücksichtigt werden.

Als weitere Randbedingung ist die Kenntnis aller relevanten Gefahrenquellen/Gefahrstoffe bzw. deren Gefahrenpotential nach Mengen und Auswirkungen zu berücksichtigen. Eine typische Klassifizierung für die bei Störfallereignisanalysen in Frage kommenden Ereignisse sind die drei Klassen *Betriebsstörfälle*, *außergewöhnliche Naturereignisse* und *Einwirkungen von außen*.

Für den vorliegenden generischen Betrachtungsfall ist nur der Punkt Betriebsstörfall relevant, d. h. ein Störfall, der direkt aus Prozessen und Handlungen ableitbar ist, die mit dem Betrieb der Anlage in Zusammenhang stehen /GÄN 13/.

Im Gegensatz zu dem Ereignisbaum stellt die Fehlerbaumanalyse, die als Teil einer PSA zu sehen ist (/LIE 92/), eine deduktive Methode dar, d. h. von einem Schlussszenario ausgehend (Störfall, ggf. postuliert) entwickelt man sich zu der Ursachenseite hin.

In dem hier zugrunde liegenden Beispiel ist von dem unerwünschten Ereignis *Freisetzung radioaktiver Stoffe* im Bereich der Schleifmaschine schrittweise rückwärts auszugehen. In der Folge fächern sich die einzelnen *Rückwärtsschritte* immer breiter auf, d. h.,

dass auch im gewählten Beispiel weitere, weniger auf das eigentliche Szenario fokussierte Nebenäste involviert werden. Basierend auf den aufgeschlüsselten Einzelereignissen kann beim Vorliegen des gesamten Baums die Gesamtwahrscheinlichkeit für eine Freisetzung bestimmt werden. Neben der Freisetzung an der Schleifmaschine (bzw. in deren Aufstellungsraum) ist der Abluftpfad in die Betrachtungen hinsichtlich einer möglichen Freisetzung einbezogen.

Auch sei hier nochmals darauf hingewiesen, dass ein intaktes Pellet im Zustand mechanischer Unversehrtheit, d. h. ohne Bruch- sowie Abriebstäube, (*integres Pellet*), nicht als Freisetzung bewertet wird.

Die Symbole  bzw.  sind als Benennung der Eingangs- bzw. Ausgangstransfers aus untergeordneten bzw. übergeordneten Fehlerbaumelementen mit den entsprechenden Kurzbezeichnungen zu sehen. Als Symbol für eine ODER- Logikgatter-Verknüpfung wurde  , als Symbol für eine logische UND-Verknüpfung  gemäß /IEEE 84/ verwendet.

Zur Identifikation der auslösenden Ereignisse ist im Rahmen einer PSA-Analyse eine generelle Unterteilung des Systems und möglicher Ereignisse hinsichtlich relevanter Einzelvorkommnisse erforderlich. Dabei sind diejenigen Ereignisse zu betrachten, die ausgehend von dem Szenario Freisetzung basierend durch ein Ereignis im Schleifraum, zu dem unerwünschten Finalereignis im betrachteten Prozess führen können.

Die Teilprozesse, bezogen auf die Schleifmaschine, sind in drei Bereiche zu unterteilen:

- Zuführung der Pellets
- Bearbeitung der Pellets
- Abtransport der Pellets

Für die Freisetzung von radioaktivem Material sind prinzipiell folgende Ursachen denkbar:

- Verlust des Pellet-Aggregatszustands *gesintert* mit Zerfall von Pellets
- Pelletbruch mit Freisetzung von Material verschiedenster Größe an der Bruchfläche
- Freisetzung von Pellet-Schleifabrieb

Generell gilt, dass der Zustand *integres Pellet* dabei nicht als eine Freisetzung im Sinne eines schädlichen Zustandes bzw. einer Kontamination klassiert wird. Im hier aufgetretenen Szenario kommt i. W. nur der Fall Freisetzung von Pellets-Schleifabrieb zum Tragen.

Hinsichtlich der Handhabbarkeit müssen die Prozesse in einzelne Teilprozesse bzw. Prozessteile aufgespaltet werden. Dazu werden Ordnungsnummern und Abkürzungsbuchstabenzeichenketten eingesetzt. Die oberste Ebene ist dabei mit *TOP* und der Ordnungsnummer *0* gekennzeichnet. So bildet die Ausgangsgröße in Abb. 2.8 mit dem Ausgangstransfer *1Freisetz-Zuförder* eine Eingangsgröße für Abb. 2.9 mit der Bezeichnung *2Freisetz-Zuförderer*.

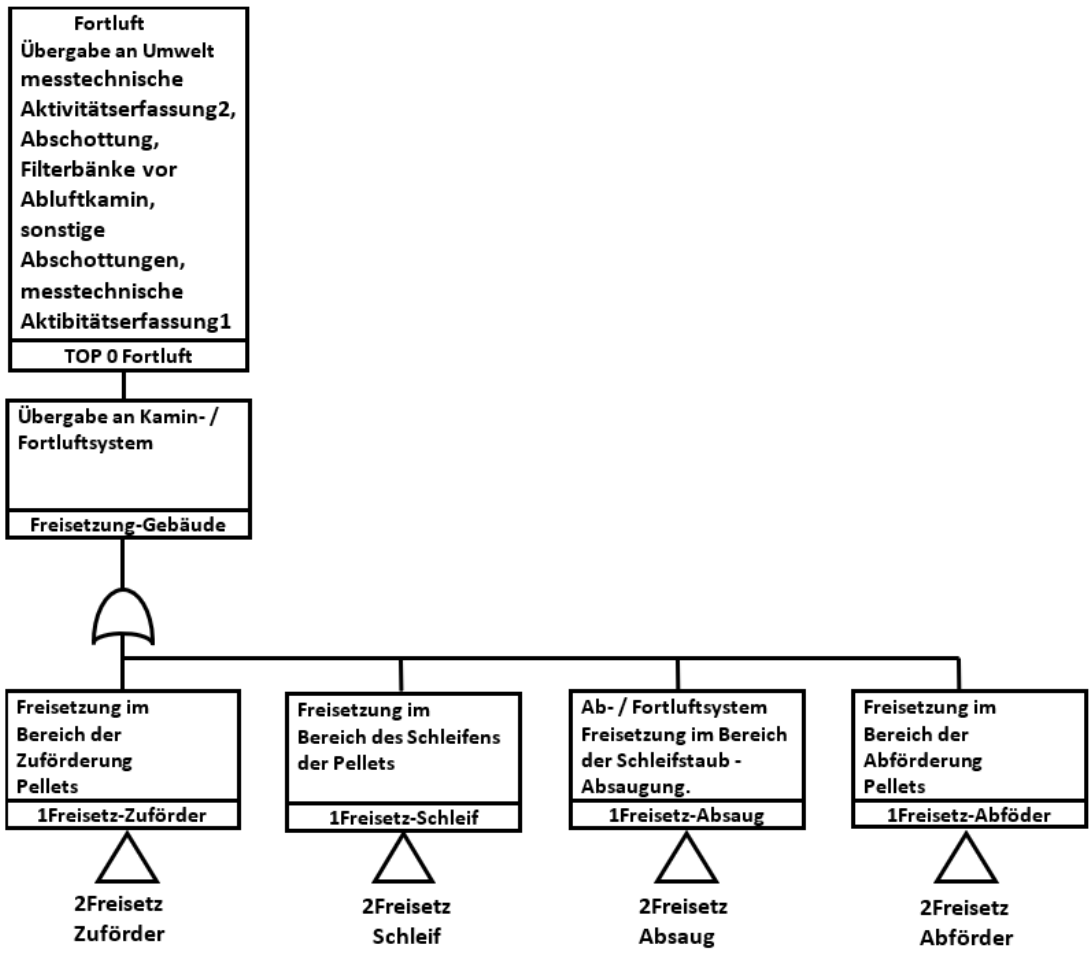

Abb. 2.8 Grobüberblick über die Ereignisse zur Freisetzung radioaktiver Stoffe in der Sektion Schleifmaschine sowie Abluftsystem

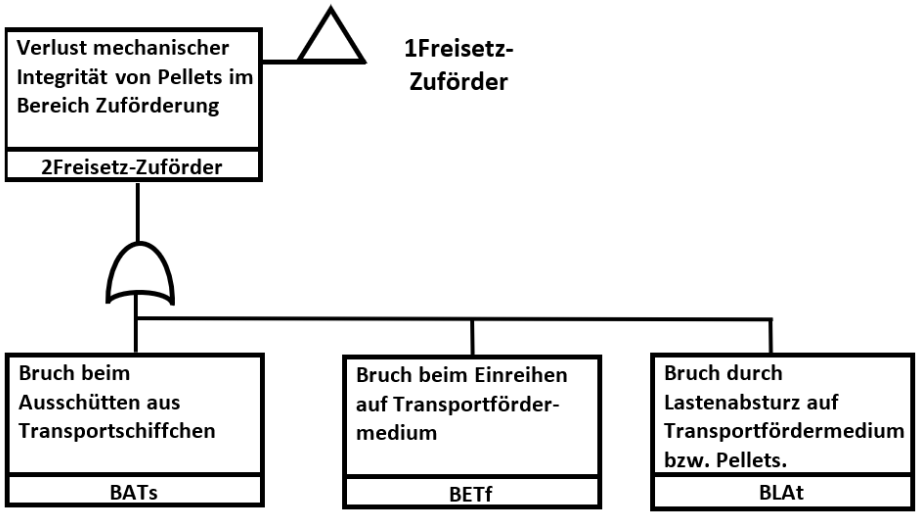

Abb. 2.9 Fortführung zu Abb. 2.8: Ereignisse im Bereich der Pellet-Zuförderung des Schleifprozesses

Zu den einzelnen Prozesszweigen wird folgendes konkretisiert:

Zweig *Verlust mechanischer Integrität von Pellets im Bereich Zuförderung*

Die Zuförderung von Pellets in die Schleifmaschine (siehe Abb. 2.9) ist im Rahmen der Gesamtbetrachtung der erste Prozessschritt. Als zugehörige Basisereignisse wurden folgende drei Ereignisse postuliert:

- Bruch beim Ausschütten aus Transportschiffchen
- Bruch beim Einreihen auf Transportfördermedium
- Bruch bzw. Zerschmettern durch Lastenabsturz auf Transportfördermedium bzw. Pellets

Das **Ausschütten der Pellets aus den Transportschiffchen** erfolgt mit einer geringen kinetischen Energie, so dass den bei der Schleifstation ankommenden Tabletten bei spezifikationsgerechter Konsistenz die notwendige Energie für einen mechanischen Tablettenbruch fehlt. Somit kann dieser Punkt in seiner Wahrscheinlichkeit auf *sehr selten* klassiert werden.

Das **Einreihen der Pellets auf das Transportfördermedium** erfolgt mit einem Förderband auf einer ansonsten passiven Vereinzelungsstrecke. Die Traktionsleistung des Förderbandes ist dabei so gewählt, dass bei einer Verklemmung die Traktionsleistung für einen Gewaltbruch einer Tablette eine zu geringe Energie besitzt. Der für die Traktion zuständige Motor, genauso wie das ihn versorgende Netzteil, ist dabei kurzschlussfest ausgeführt, sodass auch eine länger anhaltende Blockade keinerlei Überhitzung oder mögliche Fehlfunktion auslösen kann.

Ein **Bruch oder ein Zerschmettern durch Lastenabsturz auf das Transportfördermedium bzw. direkt auf die Pellets** wurde postuliert. In den räumlich zuordenbaren Entfernungen sind jedoch keinerlei Lasthebeanlagen angebracht. Ein Absturz von Lampen oder Deckenelementen wird in diesem Betrachtungsszenario durch andere Betrachtungsszenarien abgedeckt (wie z. B. Erdbeben, Flugzeugabsturz, Einwirkung von außen, etc. /LIE 92/).

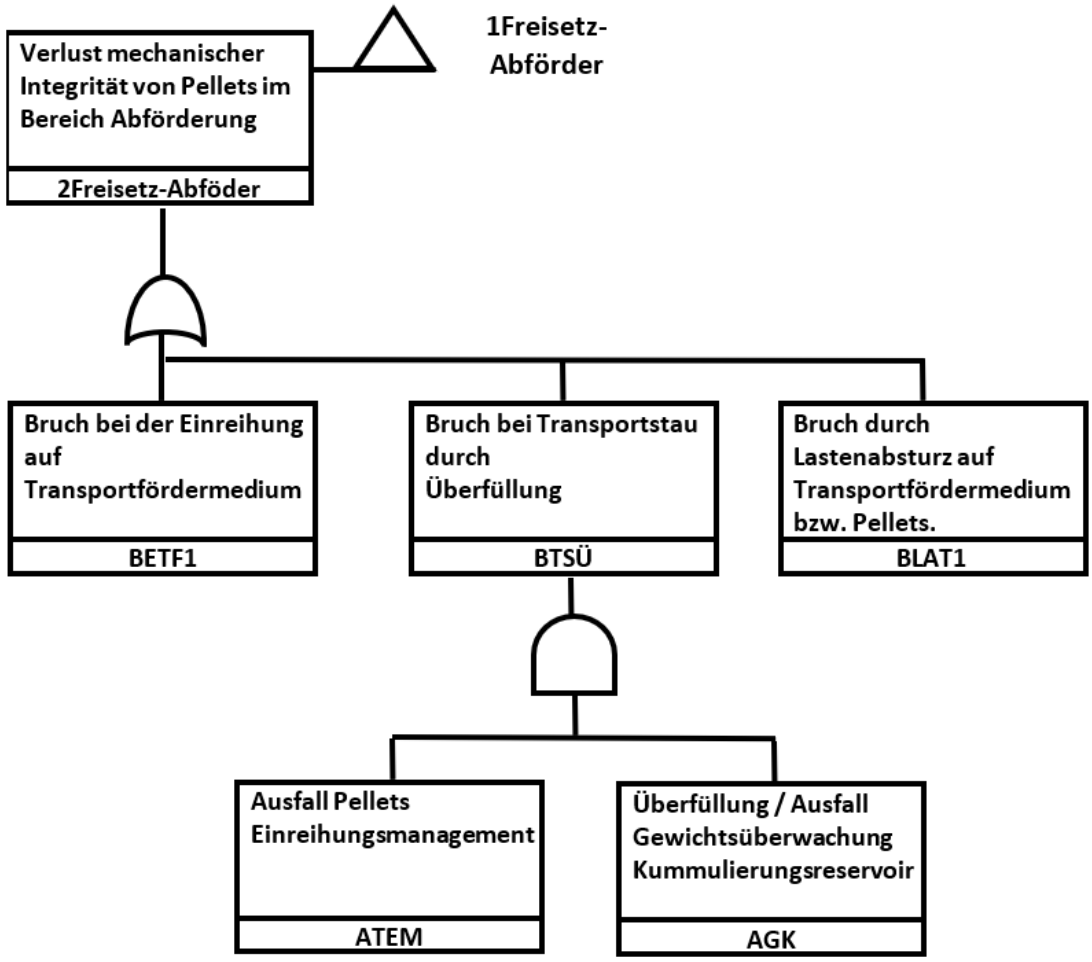

Abb. 2.10 Fortführung zu Abb. 2.8: Verlust mechanischer Integrität von Pellets im Bereich der Abförderung

Zweig *Verlust mechanischer Integrität von Pellets im Bereich Abförderung*

Die Abförderung von Pellets aus der Schleifmaschine (siehe Abb. 2.10) ist im Rahmen der Gesamtbetrachtung der letzte Prozessschritt. Als zugehörige Basisereignisse wurden die folgenden drei Ereignisse postuliert:

1. Bruch bei Transportstau durch Überfüllung
2. Bruch beim Einreihen auf Transportfördermedium
3. Bruch bzw. Zerschmettern durch Lastenabsturz auf Transportfördermedium bzw. Pellets.

Bruch von Pellets bei Transportstau durch Überfüllung des Kumulierungsreservoirs. Die Pellets werden nach ihrer Bearbeitung sequenziell positioniert und in einer definierten Losgröße per Förderband weitertransportiert. Bis zum Erreichen dieser vorgegebenen Losgröße werden die geschliffenen Pellets am Ausgang des Schleifprozesses temporär in einem Behältnis gesammelt. Dieses Behältnis ist zur Mengenerkennung mit einer auf korrekte Funktion überwachten Gewichtsmesseinheit ausgestattet. Bedingt durch die nahezu nur aus passiven oder messtechnischen Komponenten bestehende Anordnung fehlt es an dieser Komponente an entsprechenden energiereichen Elementen, die einen Pelletbruch oder eine *Pulverisierung* bewirken könnten.

Das **Einreihen der Pellets auf das Transportfördermedium** erfolgt mit einem Förderband auf einer ansonsten passiven Vereinzelungsstrecke. Die Traktionsleistung des Förderbandes ist dabei so gewählt, dass bei einer ersten Verklemmung die Traktionsleistung des Systems für einen Gewaltbruch eines Pellets eine zu geringe Leistung besitzt. Der für die Traktion zuständige Motor ebenso wie das ihn versorgende Netzteil, sind dabei kurzschlussfest ausgeführt, sodass auch eine länger anhaltende Blockade keinerlei Überhitzung oder mögliche Fehlfunktion auslösen kann.

Ein **Bruch oder ein Zerschmettern durch Lastenabsturz auf Transportfördermedium bzw. Pellets** wurde postuliert. In den räumlichen zuordenbaren Entfernungen sind jedoch keinerlei Lasthebeanlagen angebracht. Ein Absturz von Lampen oder Deckenelementen wird hier durch andere Betrachtungsszenarien (wie z. B. Erdbeben, Flugzeugabsturz, äußere Einwirkung, etc. /LIE 92/) mit abgedeckt.

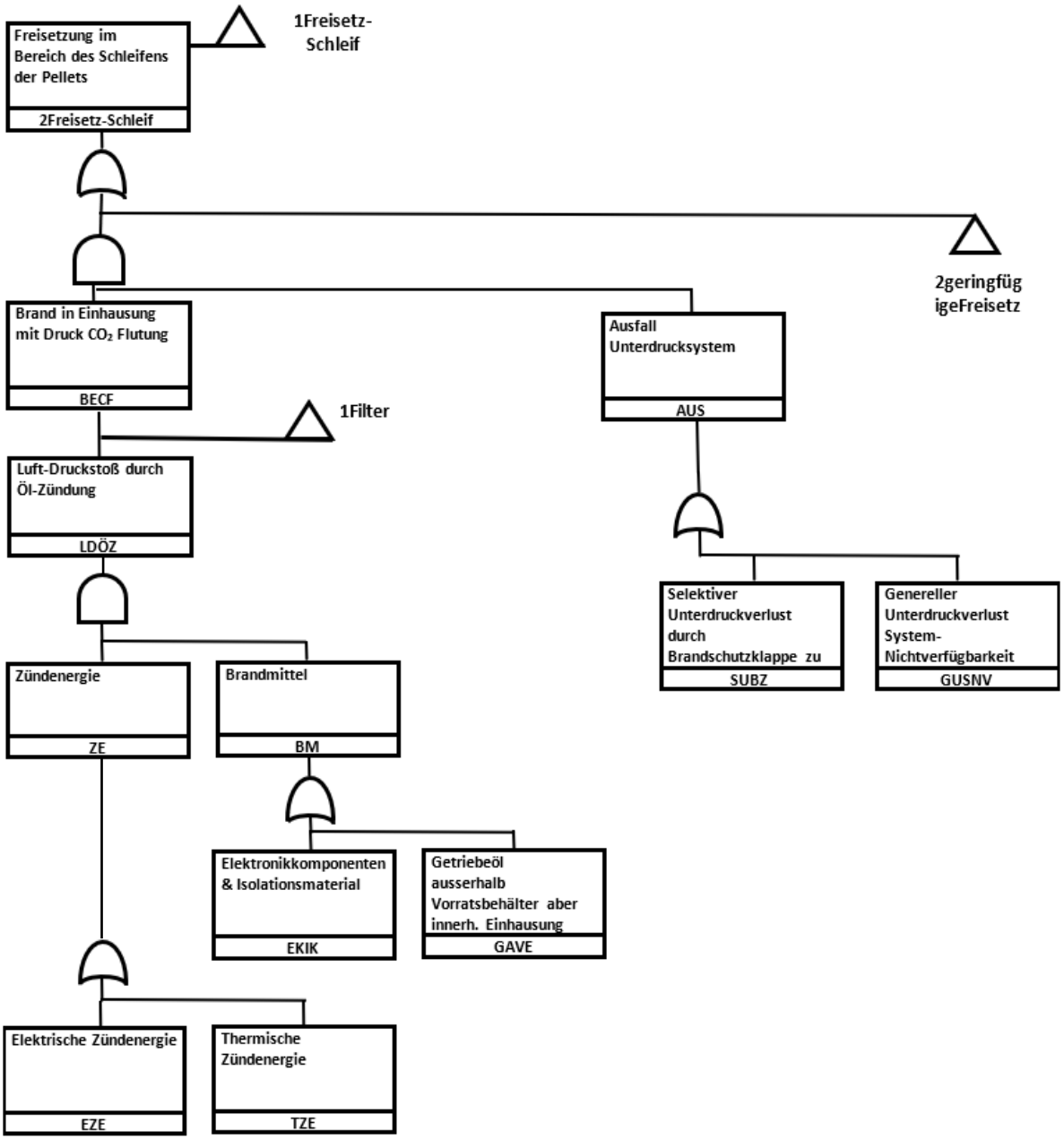

Abb. 2.11. Fortführung zu Abb. 2.8: Freisetzungen im Bereich des Pellet-Schleifens

Parallel zu der Absaugung der Einhausung ist noch eine allgemeine Raumabluft-Absaugung vorhanden, ebenfalls zur Unterdruckgenerierung gegenüber dem Zugangsbereich. Die Druckstaffelung ist so gestaffelt, dass innerhalb der Einhausung der Schleifmaschine ein geringerer Druck als im Schleifraum aufgebaut wird.

Die CO_2-Löschanlage hat im Anforderungsfall die Aufgabe, durch entsprechendes Einblasen von CO_2 und die damit verbundene Verdrängung von Luftsauerstoff einen Brand zu ersticken. Hinsichtlich einer ausreichenden Effizienz muss das Fluten mit CO_2 zügig erfolgen, besonders innerhalb der nicht vollständig abgedichteten Einhausung. Das

Prinzip des gerichteten Unterdrucks muss beim Anforderungsfall *CO_2 Einspeisung* im Umkehrschluss aufgegeben werden, damit die feuererstickende Wirkung des CO_2 nicht durch ein Absaugen verringert bzw. zunichte gemacht wird. Durch die Einspeisung von CO_2 in die Einhausung erfolgt damit eine Umkehr der Druckverhältnisse, d. h. es erfolgt ein Gasstrom vom Inneren der Einhausung nach außen. Somit ist in dem generischen System bei vorhandenen trockenen Schleifstäuben außerhalb der Einhausung mit einer Erhöhung der luftgetragenen Kontamination zu rechnen.

Das Ereignis *Brand in Einhausung* (mit zeitnaher CO_2-Flutung) bedarf als Grundvoraussetzung gemäß dem Verbrennungsdreieck die Komponenten Sauerstoff, brennbarer Stoff und Wärme bzw. Zündenergie. Da beim Betrieb der Schleifanlage im gesamten Raum normale atmosphärische Bedingungen herrschen, sind entsprechend ca. 20 % Raumluftsauerstoff vorhanden. Diese Menge Sauerstoff ist ausreichend für einen Verbrennungsvorgang. Somit kommen den beiden weiteren Größen Zündenergie und Brandmittel entsprechend, eine erhöhte Bedeutung zu. Generell sind als Zündenergie im Ensemble der Schleifmaschine nur elektrische sowie thermische Zündenergie denkbar. Unter elektrischer Zündenergie soll hier ein zeitlich sehr begrenzter Energieeintrag verstanden werden, wie z. B. in Form von Zündfunken. Bei solchen transient gehaltenen Zündpulsen bedürfte es jedoch einem Brandmittel, das mehr zu transienter Zündung neigt. Bei den hier vorliegenden Betriebsmitteln ist ein durch elektrische Zündfunken beginnender Brand auszuschließen, sodass im Folgenden auf eine thermische Zündung fokussiert wird, d. h. Selbstentzündung bedingt durch hohe Kontakttemperatur.

Die einzige Komponente mit ausreichend Energie für eine Temperaturerhöhung ist die Antriebseinheit der Schleifmaschine, respektive der Antrieb der Schleifscheibe. Dies erfolgt durch eine Elektromotor-Getriebe-Kombination. Die Verbindung von Elektromotor, Getriebe und Schleifscheibe erfolgt über starre, kraftschlüssige Kupplungen. Das eingesetzte Getriebe besitzt die Aufgabe eine Drehzahl- respektive eine Drehmomentwandlung durchzuführen. Das Getriebe ist umlaufmäßig ölgeschmiert. Durch seine spezifischen Eigenschaften ist Schmieröl als entsprechendes Brandmittel in der Betrachtung zu klassieren. Die Ölversorgung sowie der Rückfluss erfolgen über einen separaten Ölvorratsbehälter, der auch die Funktion eines Ölkühlers übernimmt. Die Ölumwälzung erfolgt über eine Pumpe im Ablaufbereich des Vorratsbehälters, der Öl-Zulauf zum Vorratsbehälter wird durch den geodätischen Höhenunterschied bewirkt. Ebenfalls werden die beiden ölgeschmierten Hauptlager der Schleifscheibe aus dem Getriebeölsystem mitversorgt.

Als mögliches Szenario wird in Verbindung mit dem Antriebsstrang eine durch den Verlust der mechanischen Integrität bedingter Wärmeeintrag durch Reibung im Allgemeinen bzw. durch einen Lagerschaden im speziellen Szenario gesehen. Neben dem latent vorhandenen Luftsauerstoff muss es zu einer Ölfreisetzung sowie zu einem thermischen Hotspot als Voraussetzung für eine Entzündung kommen. Diese Ausführungen zu einzelnen Basisereignissen werden vorausgeschickt für die Betrachtung des Szenarios *Brand in Einhausung*.

Als zu beachtendes Unterscheidungsmerkmal hinsichtlich der Einbringung von Brandlast ist die Versorgung des Getriebes sowie des Hauptspindellagers der Schleifscheibe mit Schmieröl im Gegensatz zum wasserbasierten Schleifschmiermittel zu sehen.

Ohne Zuführung von Schleifschmiermittel erfolgt das Schleifen der Tabletten trocken mit entsprechender Schleifstaubbildung. Unter ansonsten normalen Betriebsumständen verursacht eine transiente Unterbrechung der Schmiermittelzuführung bedingt durch das Unterdruckkonzept keine relevant erhöhte Kontamination der Raumluft, d. h. der Luft außerhalb der Maschineneinhausung.

Beim Basisereignis *Genereller Unterdruckverlust, System Unterdruck Nichtverfügbarkeit* ist von einem zeitnahen automatischen, bzw. manuell ausgelösten Betriebsstop auszugehen. Beim Basisereignis *Selektiver Unterdruckverlust durch Brandschutzklappe* ist nach der Ausführung bzw. des Vorhandenseins eines Monitoring-Systems zu unterscheiden. Ein unbemerkter Ausfall, d. h. ein nicht erwünschtes Schließen der Brandschutzklappe, kann in der Konsequenz durch das fehlende Unterdruckkonzept zu einer, wenn auch tendenziell begrenzten Kontamination der Raumluft führen. Als *worst case* Szenario wird hier von einem unerkannten, fehlerhaften Schließen der Brandschutzklappe ausgegangen.

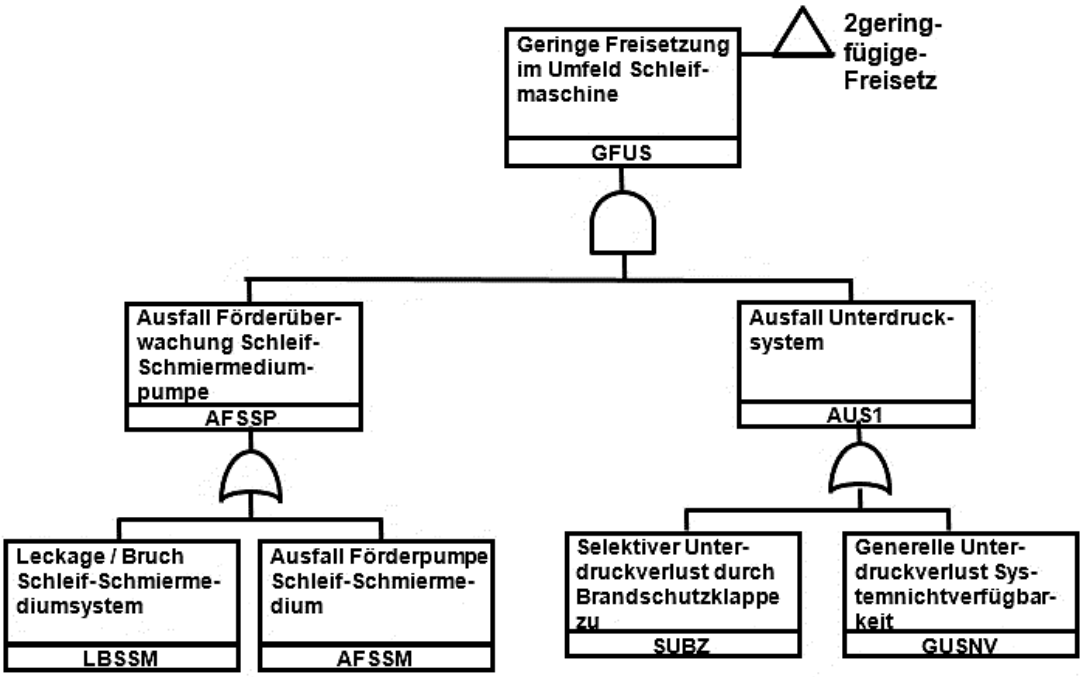

Abb. 2.12 Fehlerbaum mit dem Ausgangsterm *2geringfügige Freisetz* als Verbindung zum gleichnamigen Eingangsterm der Abb. 2.11., rechte Seite

Zweig *Freisetzung im Bereich des Pellet-Schleifens*

Als an Freisetzung im Bereich des Pellet-Schleifens (vgl. Abb. 2.11. und Abb. 2.12) beteiligte Szenarien wirken die postulierten und in engem zeitlichem Zusammenhang stehenden Ereignisse:

- Brand in Einhausung (mit CO_2-Einblasung)
- Ausfall Unterdrucksystem
- Ausfall Förderüberwachung Schleif-Schmiermedium

Das Prinzip der gestaffelten Unterdruckbereiche wird im Wesentlichen, durch die in der Einhausung der Schleifmaschine befindliche Schleifstaub-Absaugung realisiert. Dadurch wird an den temporären bzw. ständigen Öffnungen ein in die Einhausung hinein gerichteter Luftstrom erzeugt, welcher die Vermeidung von sich ausbreitender Kontamination sicherstellt. Diese Eigenschaft ist ein wichtiger Baustein zur Vermeidung von sich ausbreitender Kontamination bei trockenem Schleifabrieb jeglicher Herkunft.

Parallel zu der Absaugung der Einhausung ist noch eine allgemeine Raumabluft-Absaugung vorhanden, ebenfalls zur Unterdruckgenerierung gegenüber dem Zugangsbereich. Die Druckstaffelung ist so organisiert, dass innerhalb der Einhausung der Schleifmaschine ein geringerer Druck als im Schleifraum aufgebaut wird.

Die CO_2-Löschanlage hat im Anforderungsfall die Aufgabe, durch entsprechendes Einblasen von CO_2 und die damit verbundene Verdrängung von Luftsauerstoff einen Brand zu ersticken. Hinsichtlich einer ausreichenden Effizienz muss das Fluten mit CO_2 zügig erfolgen, besonders innerhalb der nicht vollständig abgedichteten Einhausung. Das Prinzip des gerichteten Unterdrucks muss beim Anforderungsfall *CO_2 Einspeisung* im Umkehrschluss aufgegeben werden, damit die feuererstickende Wirkung des CO_2 nicht durch ein Absaugen verringert bzw. zunichte gemacht wird. Durch die Einspeisung von CO_2 in die Einhausung erfolgt damit eine Umkehr der Druckverhältnisse, d. h. es erfolgt ein Gasstrom vom Inneren der Einhausung nach außen. Somit ist in dem generischen System bei vorhandenen trockenen Schleifstäuben außerhalb der Einhausung mit einer Erhöhung der luftgetragenen Kontamination zu rechnen.

Das Ereignis *Brand in Einhausung* (mit zeitnaher CO_2-Flutung) bedarf als Grundvoraussetzung gemäß dem Verbrennungsdreieck die Komponenten Sauerstoff, brennbarer Stoff und Wärme bzw. Zündenergie. Da beim Betrieb der Schleifanlage im gesamten Raum normale atmosphärische Bedingungen herrschen, sind entsprechend ca. 20 % Raumluftsauerstoff vorhanden. Diese Menge Sauerstoff ist ausreichend für einen Verbrennungsvorgang. Somit kommen den beiden weiteren Größen Zündenergie und Brandmittel entsprechend, eine erhöhte Bedeutung zu. Generell sind als Zündenergie im Ensemble der Schleifmaschine nur elektrische sowie thermische Zündenergie denkbar. Unter elektrischer Zündenergie soll hier ein zeitlich sehr begrenzter Energieeintrag verstanden werden, wie z. B. in Form von Zündfunken. Bei solchen transient gehaltenen Zündpulsen bedürfte es jedoch einem Brandmittel, das mehr zu transienter Zündung neigt. Bei den hier vorliegenden Betriebsmitteln ist ein durch elektrische Zündfunken beginnender Brand auszuschließen, sodass im Folgenden auf eine thermische Zündung fokussiert wird, d. h. Selbstentzündung bedingt durch hohe Kontakttemperatur.

Als einzige mit ausreichend Energie für eine Temperaturerhöhung geeignete Komponente ist hier die Antriebseinheit der Schleifmaschine, respektive der Antrieb der Schleifscheibe, zu identifizieren. Der Antrieb der Schleifscheibe erfolgt im Wesentlichen durch eine Elektromotor-Getriebe-Kombination. Die Verbindung von Elektromotor, Getriebe und Schleifscheibe erfolgt über starre, kraftschlüssige Kupplungen. Das eingesetzte

Getriebe hat als Aufgabe eine Drehzahl- respektive eine Drehmomentwandlung durchzuführen. Das Getriebe ist umlaufmäßig ölgeschmiert. Durch seine spezifischen Eigenschaften ist Schmieröl als entsprechendes Brandmittel in der Betrachtung zu klassieren. Die Ölversorgung sowie der Rückfluss erfolgen über einen separaten Ölvorratsbehälter, der auch die Funktion eines Ölkühlers übernimmt. Die Ölumwälzung erfolgt über eine Pumpe im Ablaufbereich des Vorratsbehälters, der Öl-Zulauf zum Vorratsbehälter wird durch den geodätischen Höhenunterschied bewirkt. Ebenfalls werden die beiden ölgeschmierten Hauptlager der Schleifscheibe aus dem Getriebeölsystem mitversorgt.

Als mögliches Szenario wird in Verbindung mit dem Antriebsstrang eine durch den Verlust der mechanischen Integrität bedingter Wärmeeintrag durch Reibung im Allgemeinen bzw. durch einen Lagerschaden im speziellen Szenario gesehen. Neben dem latent vorhandenen Luftsauerstoff muss es zu einer Ölfreisetzung sowie zu einem thermischen Hotspot als Voraussetzung für eine Entzündung kommen. Diese Ausführungen zu einzelnen Basisereignissen werden vorausgeschickt für die Betrachtung des Szenarios *Brand in Einhausung*.

Als zu beachtendes Unterscheidungsmerkmal hinsichtlich der Einbringung von Brandlast ist die Versorgung des Getriebes sowie des Hauptspindellagers der Schleifscheibe mit Schmieröl im Gegensatz zum wasserbasierten Schleifschmiermittel zu sehen.

Ohne Zuführung von Schleifschmiermittel erfolgt das Schleifen der Pellets trocken mit entsprechender Schleifstaubbildung. Unter ansonsten normalen Betriebsumständen verursacht eine transiente Unterbrechung der Schmiermittelzuführung bedingt durch das Unterdruckkonzept keine relevant erhöhte Kontamination der Raumluft, d. h. der Luft außerhalb der Maschineneinhausung.

Beim Basisereignis *Genereller Unterdruckverlust, System Unterdruck Nichtverfügbarkeit* ist von einem zeitnahen automatischen, bzw. manuell ausgelösten Betriebsstop auszugehen. Beim Basisereignis *Selektiver Unterdruckverlust durch Brandschutzklappe* ist nach der Ausführung bzw. des Vorhandenseins eines Monitoring-Systems zu unterscheiden. Ein unbemerkter Ausfall, d. h. ein nicht erwünschtes Schließen der Brandschutzklappe, kann in der Konsequenz durch das fehlende Unterdruckkonzept zu einer, wenn auch tendenziell begrenzten Kontamination der Raumluft führen. Als *worst case* Szenario wird, hier von einem unerkannten, fehlerhaften Schließen der Brandschutzklappe ausgegangen.

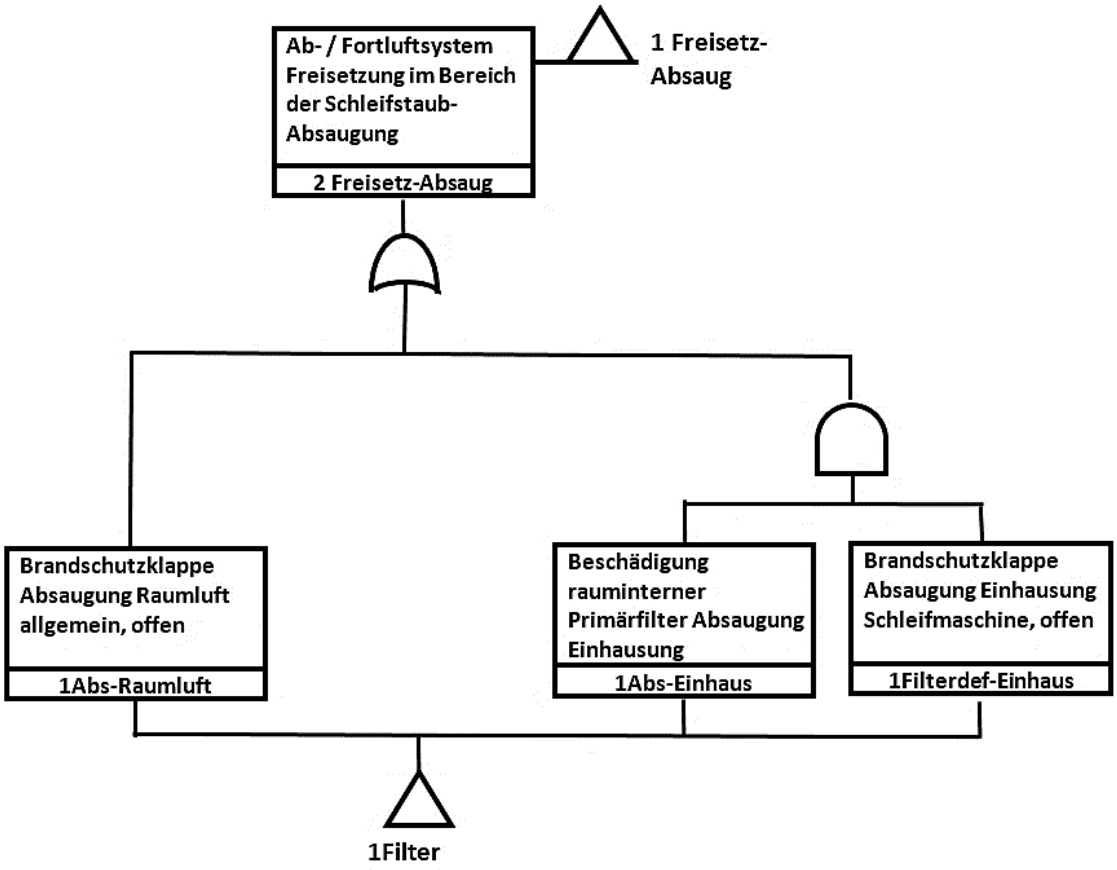

Abb. 2.13 Fortführung zu Abb. 2.11., *1Filter* mit Raumabluft, sowie *Absaugung Einhausung Schleifmaschine* bis Übergabepunkt zum Abluftkamin

Zweig *1Filter mit Raumabluft*, sowie *Absaugung Einhausung Schleifmaschine bis Übergabe*

Als beteiligte Szenarien mit Raumabluft, sowie *Absaugung Einhausung Schleifmaschine* bis Übergabe, vgl. Abb. 2.13 als Fortführung von Abb. 2.11., wirken die in zeitlichem Zusammenhang stehenden Ereignisse:

- Beschädigung des rauminternen Primärfilters der Absaugung / Unterdruckerzeugung der Einhausung der Schleifmaschine durch den Druckstoß der Öl-Entzündung
- Auslösung der Brandschutzklappe *Absaugung Einhausung Schleifmaschine*
- Auslösung der Brandschutzklappe der allgemeinen *Raumluftabsaugung*

Durch die zeitlich nahen beieinanderliegenden Auslösungen der Brandschutzklappen der *Absaugung Einhausung Schleifmaschine* sowie der allgemeinen

Raumluftabsaugung erfolgt eine faktische Abkoppelung des Raumes vom Abluftsystem. Danach erfolgt keine weitere Einspeisung von Schleifstaub bzw. Öl-Ruß in das Abluftsystem, weder durch den defekten Filterpfad der Absaugung Schleifmaschine noch durch die (ungefilterte) allgemeine Raumluftabsaugung.

Der Schadensrelevante Zeitraum lässt sich wie folgt beschreiben:

Die Schleifmaschine ist zunächst im Normalbetrieb, d. h. das Schleifwasser bindet den Großteil des Schleifabriebs. Restlicher luftgetragener Schleifabrieb wird nahezu vollständig über die einhausungsinterne Absaugung erfasst und über die primäre, rauminterne Filterstufe geführt. Danach wird diese Abluft nach dem Durchströmen der Brandschutzklappe mit der eigentlichen Raumabluft vereinigt und dem allgemeinen Abluftstrom zugeführt.

Ab dem Zeitpunkt der Teilzerstörung der Membran des primären Absaugfilters der Einhausung durch den Öl-Zündungsdruckstoß verliert die Filterstufe weitgehend ihre Funktion, d. h. bis zur Schließung der Brandschutzklappe gelangt Schleifabrieb ungefiltert in das Abluftsystem. Zudem gelangt im Augenblick der Teilzerstörung der Filtermembran durch den Druckstoß bereits im Filter zurückgehaltener Schleifabrieb ebenfalls schlagartig in den Abluftstrom.

In Konsequenz ergeben sich bei der mengenmäßigen Betrachtung des Schleifabriebes folgende Phasen:

- **Normalbetrieb**: Es befindet sich ein mengenmäßig unbedeutendes Schleifabriebvolumen im Abluftstrom, der nach der Primärfilterung abgeht.
- **Phase 1** beginnt in dem Augenblick, zu dem durch den Zündungsdruckstoß mit dem dadurch verbundenen Verlust der Filtermembranintegrität bereits im Filter zurückgehaltener Schleifabrieb schlagartig zusätzlich in den Abluftstrom freigesetzt wird, d. h. zunächst erfolgt im Bereich der Einleitung des Abluftstroms des Schleifraums in den Gesamtabluftstrom eine Anstiegsspitze an Schleifabrieb.
- **Phase 2** bildet den Zeitraum, zu dem nach dem Ausspülen der Filterreste die Mengenkonzentration zunächst etwas zurückgeht.
- **Phase 3** bildet die Zeitspanne bis zum Schließen der Brandschutzklappe mit einem langsamen Anstieg der luftgetragenen Aktivität durch Verdampfen des Schleifschmier- und -kühlmittels (Wasser).

Der integrale, luftgetragene Schleifabrieb erreicht die Ausgangsfilterbänke vor dem Abluftkamin mit einer gewissen zeitlichen Verzögerung, die durch den Öl-Entzündungsdruckstoß unbeeinflusst sind. Die vor den Ausgangsfilterbänken installierte redundante Aktivitätsmesstechnik zeigt einen zum geschilderten Verlauf korrespondierenden Anstieg. Die redundante und diversitäre Aktivitätsmessung nach dem Filter bleibt jedoch unauffällig. Mit dem Schließen der Brandschutzklappen normalisieren sich die Werte, während durch die Auslösung der CO_2-Feuerlöschung der Anlagenteil in den Feueralarmmodus übergeht. Ein Anstieg der Aktivitätsabgabe nach dem Abluftfilter bzw. vor Abgabe an die Fortluft würde zu entsprechenden Warnmeldungen bis hin zu einem automatischen Abluftstop führen, um eine Abgabe von Radioaktivität an die Umgebung zu verhindern bzw. zu reduzieren. Somit wird dieser Zweig in die spätere, rechnerische Betrachtung hinsichtlich Aktivitätsabgabe nicht mit eingebunden.

Eine mögliche Überschreitung von Flüssigkeitsmengen im Hinblick auf die Kritikalitätssicherheit, d. h. hier die Einhaltung der mengenmäßigen Sicherheitsparameter, wird basierend auf der integral nur begrenzt vorhandenen Flüssigkeits- und Kernbrennstoffmenge nicht verfolgt. Kritikalitätsrelevante Grenzwerte werden nicht überschritten.

2.4.6.1 Zuverlässigkeitskenngrößen

Zur weiteren Bearbeitung ist eine Datenerhebung der Basiswahrscheinlichkeiten für die einzelnen Schadens- bzw. Fehlerszenarien notwendig. Eine fundierte Berechnung der Eintrittswahrscheinlichkeit bestimmter Szenarien setzt jedoch das Vorhandensein von realistischen, belastbaren Zuverlässigkeits- und Wahrscheinlichkeitsgrößen voraus.

Als mögliche Datenquelle für Wahrscheinlichkeiten steht hier nur die Analyse von meldepflichtigen, anlagenspezifischen Ereignissen zur Ableitung von Zuverlässigkeitskenngrößen zur Verfügung. Basierend auf dem hier konstruierten beispielhaften Maschinensatz mit seinen erheblichen Abweichungen zu existierenden bzw. im kerntechnischen Einsatz befindlichen Lösungen konnten keine realen und ausreichend belastbaren Zuverlässigkeitswerte ermittelt werden. Ebenso gibt es keine realen Datensätze zu den Zuverlässigkeitskenngrößen der unterstellten Schleifmaschine bzw. deren Einzelkomponenten. Somit wurden parallel zu allgemeinen Internetrecherchen grobe Schätzwerte angesetzt. Aufgrund der vorliegenden generischen Untersuchungen zur Demonstration der Methodik stellt dies keine grundsätzliche Einschränkung der erzielten Ergebnisse dar.

Tab. 2.15 Schätzwerte der Eintrittswahrscheinlichkeiten der Funktionsfähigkeit bzw. der Fehlfunktion von Komponenten- / Teilsystemen, sowie des Vorhandenseins von kritischen Einwirkungsfaktoren

Komponente bzw. Teilsysteme	**Eintrittswahrscheinlichkeit**
Ausschütten Pellets ohne Bruch aus Transportschiffchen	$9{,}999 \times 10^{-1}$
Einreihen Pellets auf Transportmedium ohne Bruch	$1{,}000 \times 10^{0}$
Analgenbetrieb ohne Lastenabsturz auf das Pellet-Transportsystem bzw. direkt auf Pellets	$1{,}000 \times 10^{0}$
Anlagenbetrieb ohne Auftreten kritischer elektr. Zündenergie	$1{,}000 \times 10^{0}$
Anlagenbetrieb ohne Auftreten kritischer therm. Zündenergie	$9{,}968 \times 10^{-1}$
Funktionsfähige Elektronikkomponente & Isolationsmaterial	$9{,}997 \times 10^{-1}$
Getriebeöl außerhalb Vorratsbehälter aber innerhalb Einhausung	$1{,}000 \times 10^{-3}$
Fehlerhafter selektiver Unterdruckverlust durch Brandschutzklappe	$1{,}900 \times 10^{-2}$
Genereller Unterdruckverlust/Systemnichtverfügbarkeit	$5{,}800 \times 10^{-3}$
Leckage/Leitungsbruch Schleif-/Schmiermittelsystem	$1{,}300 \times 10^{-2}$
Ausfall Förderpumpe Schleif-/Schmiermittelsystem	$3{,}200 \times 10^{-3}$
Pellet-Einreihungsmanagement funktionsfähig	$9{,}998 \times 10^{-1}$
Überfüllungs-/Gewichtsüberwachung, Kumulierungsreservoir funktionsfähig	$9{,}962 \times 10^{-1}$
Gesamt-Abluftstrang mit Filterbänken und Überwachung funktionsfähig	$9{,}999 \times 10^{-1}$
Beschädigung des rauminternen Primärfilter Absaugung	$1{,}230 \times 10^{-3}$
Brandschutzklappe Absaugung Einhausung Schleifmaschine fehlerhaft offen	$4{,}320 \times 10^{-3}$
Brandschutzklappe Absaugung Raumluft, allgemein, fehlerhaft offen	$2{,}882 \times 10^{-2}$

Als Zeitbasis für die Eintrittswahrscheinlichkeit wurde für die Komponenten ein Betrieb von zwölf Stunden am Tag, bei einer Fünftagewoche und 52 Wochen pro Jahr angesetzt. Somit ergeben sich 3.120 Stunden Betrieb pro Jahr.

2.4.6.2 Abschätzung der Fehlerwahrscheinlichkeiten

Basierend auf den in Tab. 2.15 genannten Werte, wurden für die einzelnen, in den Abbildungen dargestellten Verknüpfungen sowie für das Gesamtsystem, eine rechnerische Abschätzung der Fehlereintrittswahrscheinlichkeit pro Jahr gemäß den dargestellten Gatter-Verknüpfungen mittels Handrechnung durchgeführt. Je nach Bedarf wurde die

aufgelistete Größe Eintrittswahrscheinlichkeit auch als Komplement, d. h. als Nicht-Eintrittswahrscheinlichkeit des genannten Scenarios verwendet.

Für den Zweig in Abb. 2.9 *Ereignisse im Bereich der Pellet-Zuförderung des Schleifprozesses* ergibt sich, basierend auf den oben genannten Werten, eine Eintrittswahrscheinlichkeit einer Fehlfunktion von gerundet $1 \times 10^{-4}\,a^{-1}$. Diese verschwindende Freisetzungswahrscheinlichkeit ist bedingt durch die fast erreichte Fehlerfreiheit hinsichtlich potentieller Freisetzung bei Bruch, d. h. *Bruch beim Ausschütten aus Transportschiffchen* (BATs), bzw. die Fehlerfreiheit bei *Bruch beim Einreihen auf Transportfördermedium* (BETf) und *Bruch durch Lastenabsturz auf Transportfördermedium* (BLAt).

Für den Zweig in Abb. 2.10 mit den Basisereignissen *Bruch bei der Einreihung auf Transportmedium* (BETF1), *Ausfall Pellet Einreihungsmanagement* (ATEM), *Ausfall Gewichtsüberwachung Kumulierungsreservoir* (AGK) und *Bruch durch Lastenabsturz auf Transportfördermedium bzw. Pellet* (BLAT1), ergibt sich für den *Verlust mechanischer Integrität von Pellet im Bereich der Abförderung* (2Freisetz-Abförder) eine Fehlereintrittswahrscheinlichkeit von gerundet $8{,}6 \times 10^{-7}\,a^{-1}$.

Für den Zweig in Abb. 2.12 mit den Basisereignissen *Leckage/Leitungsbruch Schmiermediumsystem* (LBSSM), *Ausfall Förderpumpe Schleif-Schmiermedium* (AFSSM), *Selektiver Unterdruck durch Brandschutzklappe zu* (SUBZ) und *Genereller Unterdruckverlust Systemnichtverfügbarkeit* (GUSNV) ergibt sich eine Fehlereintrittswahrscheinlichkeit von gerundet $4 \times 10^{-4}\,a^{-1}$.

Für den Zweig in Abb. 2.11 mit den Basisereignissen *Elektrische Zündenergie* (EZE), *Thermische Zündenergie* (TZE), *Elektronikkomponenten & Isolationsmaterial* (EKIK), *Getriebeöl außerhalb Vorratsbehälter aber innerhalb Einhausung* (GAVE), *Selektiver Unterdruckverlust durch Brandschutzklappe zu* (SUBZ) und *Genereller Unterdruckverlust Systemnichtverfügbarkeit* (GUSNV) ergibt sich eine Fehlereintrittswahrscheinlichkeit von gerundet $4 \times 10^{-4}\,a^{-1}$.

Für den Zweig in Abb. 2.8 mit den Eingangsereignissen *Freisetzung im Bereich der Zuförderung* (1Freisetz-Zuförder), *Freisetzung im Bereich des Schleifens der Pellets* (1Freisetz-Schleif) und *Freisetzung im Bereich der Abförderung Pellets* (1Freisetz-Abförder) sowie *Freisetzung im Bereich der Schleifstaub-Absaugung* (1Freisetz-Absaug) ergibt sich somit für den Gesamtprozess bis zum Übergabepunkt an das Kamin-Fortluftsystem)

eine Eintrittswahrscheinlichkeit einer Freisetzung mit einer Wahrscheinlichkeit von gerundet 4×10^{-4} a^{-1}.

Sonderfall *Common Cause Failure*

Exemplarisch soll hier als Beispiel für einen Common Cause Failure (CCF) der Ausfall der elektrischen Versorgung der einzelnen Versorgungsnetze erwähnt werden.

Die Pelletschleifmaschine inkl. ihrer Zu- und Abförderungsprozesskomponenten werden in diesem Szenario über das nicht notstromgesicherte, d. h. das betriebliche Stromnetz versorgt. Ein Ausfall der elektrischen Versorgung führt zu einem sofortigen Stillstand der Maschine und hat keinerlei sicherheitstechnische Relevanz. Das notstromgesicherte Brandmeldesystem ist für den relevanten Zeitraum verfügbar.

Da nach der Auslösung der CO_2-Löschanlage die Gas-Flutungsventile selbsthaltend sind, wäre ein Ausfall der Notstromversorgung nach Auslösung der Löschanlage zur Brandbekämpfung unkritisch.

Bei einem Ausfall der Notstromanlage parallel zur betrieblichen Spannungsversorgung und Auftreten des postulierten Brandes würden die Brandschutzklappen über ihre integrierten Feder-Schmelzsicherungen geschlossen, sowie die CO_2-Raumflutung über deren Thermosicherung ausgelöst.

Ohne die betriebliche Spannungsversorgung ist die Relevanz des betrachteten CCF-Szenarios als unerheblich einzustufen, da ohne Betrieb der Maschine die unterstellte Überhitzung und der resonanzbedingte Abriss der Ölleitung nicht eintreten kann.

Ebenfalls ist die kumulative Brandlast innerhalb des Schleifraums so begrenzt, dass bei einer vollständigen exothermen Umsetzung der vorhandenen Brandlast des Raums, baulich für den Raum bzw. dessen Nachbarräume kein relevantes Sicherheitsrisiko ausgeht.

Somit mündet der CCF-Fall in diesem Beispiel in kein besonderes Sicherheitsrisiko.

2.4.7 Schlussfolgerungen zu der generischen Anlage

Ungeachtet von vorhandenen bzw. nicht vorhandenen Ausfallwahrscheinlichkeiten zeigt das entsprechend gewählte generische Szenario, dass hier bedingt durch den Einsatz eines mit Öl geschmierten Getriebes und die damit eingebrachte potenzielle Brandlast eine sicherheitstechnische Schwachstelle vorhanden ist. Dies betrifft insbesondere die postulierte Menge an Schmieröl und den Einsatz eines Vorlagebehälters, der zudem noch über Leitungen mit dem eigentlichen Getriebe verbunden ist. Jede dieser Komponenten erhöht die Ausfallgefährdung dieses hypothetischen Prozessschrittes essenziell.

Eine mögliche Abhilfe wäre in Form einer getriebelosen Maschine oder zumindest einer direkt fettgeschmierten und vollständig gekapselten Drehmomentwandlung zu sehen. Des Weiteren könnte mit verschiedenen leittechnischen Monitoring-Arten wie z. B. einer Überwachung der Leistungsaufnahme des Antriebsstrangs der Schleifmaschine, durch eine Vibrationsüberwachung oder einiger zusätzlicher Temperaturmessstellen, ein anomales Betriebsverhalten frühzeitig erfasst und entsprechende Abschaltmaßnahmen automatisch eingeleitet werden, um eine Eskalation zu verhindern. Als weitere mögliche Konsequenz könnte der Einsatz einer Sauerstoffreduzieranlage sein, wie sie heutzutage bereits oft in IT- und Serverräumen, Archiven oder auch Lagerhallen eingesetzt werden. Durch eine Reduktion des Sauerstoffanteils reduzierte sich die Entzündungsgefahr von brennbaren Materialen erheblich und trüge so zu einer höheren Sicherheit bei. Allerdings wäre der dabei technisch zu betreibende Aufwand, bedingt durch die Anforderungen an den kontrollbereichsbedingten Luftaustausch, hier im Schleifraum mit einer geforderten Luftaustauschrate von $1\,h^{-1}$, unverhältnismäßig hoch.

Abschließend sei nochmals auf den generischen Charakter des beschriebenen Anlagenteils und der bewusst zur Generierung des Fehlerfalls vorhandenen Schwachstellen hingewiesen. Die gewählte Anordnung entspricht nicht dem Einzelfehlerkriterium und wäre aus kerntechnischer Sicht so nicht genehmigungsfähig. Es existieren keine bewussten Parallelen zu bekannten Anlagen.

2.5 Zusammenfassung

Mit Bezug zum Betrieb von Anlagen der nuklearen Ver- und Entsorgung wurde exemplarisch für die Pelletherstellung für Brennelemente ein hypothetisches Störfallszenario aus dem Bereich der Brennstoffpellets und hier bei der mechanischen Pellets-Konfektionierung (Schleifstation) aufgestellt, beschrieben und eine rechnerische Abschätzung der Fehlerwahrscheinlichkeit durchgeführt. Da hier die Demonstration einer Methodik im Fokus liegt, wurde bewusst kein realitätsnaher, sondern vielmehr ein mit bewusst platzierten (und typischerweise in realen Anlagen vermiedenen) Schwachstellen versehener Komponentenaufbau konstruiert.

In einer prinzipiellen Art und Weise wurden anhand dieser postulierten Anordnung die *What-If*, *Hazard and Operability* Analyse (HAZOP) sowie die beiden Methoden der Deterministischen Störfall- und Ereignisbaumanalyse (*Event Tree Analysis*, ETA) und die der Fehlerbaum- und probabilistische Sicherheitsanalyse (*Fault Tree Analysis*, FTA und PSA) angesetzt und deren Ergebnisse exemplarisch aufgezeigt. Besonders für komplexe Systeme, neuartige Sytemauslegungen und Plausibilitätsprüfungen sind die Fehlerbaumanalyse sowie die HAZOP und What-IF Untersuchung geeignet. Quantitative Analysen sind hingegen nur mit der Fehlerbaum- und Ereignisbaumanalyse zu erzielen. Bei Abfolgeabhängigkeiten ist lediglich die Ereignisbaumanalyse dafür geeignet.

Bedingt durch den Charakter eines Postulats sowie einer generell mangelhaften Datenlage hinsichtlich dokumentierter Ausfallwahrscheinlichkeiten der einzelnen, am Prozess beteiligten Komponenten und Systeme, sind die rechnerisch verwendeten Wahrscheinlichkeiten nicht belastbar. Trotzdem wurde, um die generische Vorgehensweise zu zeigen, der Vollständigkeit halber auch eine rechnerische Verknüpfung einzelner Wahrscheinlichkeiten durchgeführt. Vielmehr wird auch durch die Anwendung der einzelnen Verfahren aufgezeigt, dass es sich je nach Fragestellung bzw. Zielsetzung hinsichtlich einer Gesamtbetrachtung des Systems um sich ergänzende Methoden handelt.

Die ermittelte Eintrittswahrscheinlichkeit bzw. das Ergebnis sind, wie Eingangs bereits erwähnt, auf keine der bekannten und in Betrieb befindlichen Anlagen direkt oder indirekt übertragbar.

3 Anwendung der generischen Störfallanalyse auf einen exemplarischen Störfall: Freisetzung von UF_6 in der Brennelementfertigung

In diesem Kapitel wird die Anwendung der Störfallanalyse auf einen zweiten, möglichst unterschiedlichen Teilprozess der nuklearen Versorgung betrachtet. Hierfür wird die Freisetzung von UF6 mit einer möglichen gasförmigen Freisetzung und seinem hohen chemotoxischen Potential herangezogen, damit sich der Störfall deutlich von dem in Kapitel 2 betrachteten Brand in der Tablettenschleifmaschine unterscheidet. Dazu wird allgemein ein generischer Teilprozess einer konstruierten Brennelementfertigung beschrieben und dafür ein hypothetischer Störfall konstruiert. An diesem Beispiel werden die Methoden der Störfallanalyse exemplarisch angewendet werden.

In dem Dokument „Sicherheitsanforderungen für Kernbrennstoffversorgungsanlagen“ /BMUV 05/ sind bei der Handhabung von gasförmigem UF_6 stets zwei Barrieren gegenüber der Umgebung gefordert, bei der Handhabung von flüssigem UF_6 (wie bei der Abfüllung), drei Barrieren. Die Gefahr großer Freisetzungen von Uranhexafluorid aus den aufgeheizten Behältern ist in deutschen Anlagen durch die eingesetzten Autoklaven, die als eine zweite Barriere fungieren, im ordnungsgemäßen Betrieb gewährleistet. Die Entleerung des UF_6-Zylinders erfolgt über einen Aufheiz- bzw. Ausdampfprozess in der Betriebshalle. Relevante Rohrleitungssysteme sind doppelwandig asugeführt, mit zusätzlich in der zweiten Rohrumhüllung integrierten Leckageerkennungen. Die Betriebsstätte wirkt durch die Gewährleistung einer Unterdruckerhaltung mit entsprechender Lüftungstechnik als eine weitere Barriere gegen Freisetzung in die Umgebung. Per Vorschrift ist festgelegt, dass keinerlei Arbeiten an der UF_6-Absperrarmatur oder der Verbindungsleitung durchgeführt werden dürfen, solange ein aufgeheizter und mit UF_6 gefüllter Behälter zur Entladung, bzw. Teilentladung angeschlossen ist.

Zur Orientierung sind im Folgenden die bislang in Deutschland aufgetretenen, meldepflichtigen Ereignisse im spezifischen Bereich der UF_6 Entladung, bzw. des ersten Verarbeitungsschrittes aufgelistet.

- UF_6-Undichtigkeit im Ausdampfautoklaven.
- Überschreitung der 30B-Behältertemperatur von 115 °C.
- Versagen einer UF_6-Verbindungsleitung.

- Undichtigkeit der Restentleerungspumpe eines UF_6- Zylinders.
- Ausfall der Auswerteeinheit der Temperaturüberwachung eines Reaktionsbehälters in der Trockenkonversionsanlage.
- Unkontrollierte Abgabe von Fluorwasserstoff mit der Fortluft der Trockenkonversionsanlage.
- Abschalten der UF_6 Verdampfung aufgrund des fehlerhaften Ansprechens einer Sicherheitsverriegelung.

Diese Aufzählung dient lediglich einer groben Orientierung, welche Ereignisse in Realität bereits aufgetreten sind.

Daneben gibt es verschiedene potenzielle UF_6-Freisetzungsszenarien, die für eine Anlage des Kernbrennstoffkreislaufs postuliert werden können. Eine der möglichen Aufsplittungen ist die Einteilung in vier übergeordnete Basisszenarien /SIM 84/:

- Ausfälle von UF_6-Zylindern
- Ausfälle der UF_6-Prozessausrüstung
- nukleare Kritikalitätsereignisse und
- Bedienungsfehler

Die meisten der darunterfallenden Szenarien finden innerhalb eines Gebäudes statt.

3.1 Beschreibung der generischen Handhabungsprozesse von UF_6

Der hier beschriebene Prozess gilt für eine hypothetische Brennelementfabrik, die zum Zweck dieser Störfallanalyse konstruiert wurde, und die entsprechend postulierte Mängel im Prozessablauf enthält. Eventuelle Ähnlichkeiten zu real existierenden Anlagen sind rein zufällig.

Den Ausgangspunkt der Analyse bildet das Behälterzwischenlager einer Brennelementfabrik, in dem angereichertes Uran als Hexafluorid (UF_6) in 30B Behältern gelagert wird. Es wird definiert, dass das Behälterzwischenlager aus einer wettergeschützten Halle besteht. Somit ist abgesehen von der Luftfeuchtigkeit, kein Wasser in der unmittelbaren Umgebung der Behälter vorhanden. Leckagen aller Art, d. h. besonders auch Gase,

können durch die Raumumschließung noch sensitiver erfasst werden, als diese bei reiner Outdoor-Lagerung möglich wäre. Ab dem Behälterzwischenlager erfolgt der weitere Transport der Behälter schienengebunden, d. h. mittels schienengeführten Transportwägen. Dies wird durch zwei unterschiedliche Schienensysteme realisiert. Das erste Schienensystem läuft von der Behälterzwischenlagerhalle in die Betriebshalle und dort bis in den Autoklav Bereich. Danach wird der Behälter vom Transportwagen auf den Autoklav-Einfahrschlitten umgesetzt.

Der 30B Transportbehälter verfügt über ein entsprechenden Ventilanschluss, über den die flüssige Befüllung in der Anreicherungsanlage, sowie die gasförmige Entleerung über einen Ausdampfprozess in der Brennelementefabrik erfolgen kann. Die hier unterstellten Transfer-Autoklaven haben die Aufgabe, das UF_6 bis zum Erreichen des Dampfzustands zu erhitzen und dadurch eine Entladung des UF_6 im gasförmigen Zustand zu ermöglichen. Hierzu ist der Behälter so zu drehen, dass sich das Ventil als Entnahmestelle zur sicheren Dampfentnahme oben befindet, d. h. auf der 12 Uhr Position. Der Anschluss des Behälters an das UF_6-Leitungssystem des Autoklavs respektive der Anlage, erfolgt mittels eines sogenannten Pigtails an das Behälterventil. Der Pigtail ist ein flexibles, bewegliches Leitungsteil des UF_6 Anlagenrohrleitungssystems, welches sich innerhalb des Autoklavs und daher im Aufheizbereich befindet. Somit benötigt das Pigtail, im Gegensatz zum restlichen UF_6-Rohrleitungssystem, keine eigene Rohrheizung. Die mechanische Verbindung zwischen dem Pigtail als Teil der Autoklavtechnik und dem Ventilstutzen des Behälters erfolgt über eine Gewindemuffe, die nach dem Einfahren des Behälters übergeworfen und angezogen wird. Des Weiteren verfügt der Autoklav über eine mechanische Spindelverlängerung nach außen, die das Öffnen des Ventils bei geschlossener Autoklavtür durch eine Spindel-Mitnehmerkonstruktion ermöglicht. Nach erfolgtem Anschluss des Pigtails wird die Spindel-Mitnehmerkonstruktion eingehängt. Danach kann der Autoklav geschlossen werden. Ab diesen Zeitpunkt ist das Behälterventil von außen per Spindel bedienbar.

Basierend auf dem Ist-Parameter Temperatur, können bei geöffnetem Behälterventil über den gemessenen Druck Rückschlüsse auf mögliche Fremdgase gezogen werden, die sich zusätzlich im Behälter befinden.

Durch entsprechende Türkontakte wird sichergestellt, dass die Aufheizphase erst bei geschlossener, bzw. verriegelter Autoklavtür gestartet werden kann. Zur sicherheitstechnischen Begrenzung ist die technisch maximal mögliche Wärmezufuhr begrenzt. Dies wird durch die Art der eingesetzten Heizspiralen umgesetzt. Diese Maßnahme eines

langsamen Aufwärmens stellt sicher, dass der Behälter möglichst gleichmäßig durchwärmt wird.

Während der Verweilzeit des Behälters im Autoklav werden die Temperaturen redundant überwacht, um eine mögliche Überhitzung auszuschließen. Dazu kommt ein betriebliches, sowie ein ausschließlich zu Schutzzwecken dienendes Sicherheitssystem zum Einsatz. Der folgende Prozessschritt wird erst dann freigegeben, wenn die vorgegebene Zieltemperatur sicher erreicht ist und man von einer gleichmäßigen Durchwärmung des Behälters ausgehen kann. Die Weiterleitung des gasförmigen UF_6 in den Reaktionsbehälter des Folgeprozesses erfolgt durch ein angeschlossenes und beheiztes Rohrleitungssystem. Damit soll sichergestellt werden, dass die gasförmige Phase des UF_6 erhalten bleibt und somit Ablagerungen und Verstopfungen ausgeschlossen werden können, die auf dem Übergang zu festen UF_6 basieren. Die Steuerung der Weiterleitung des UF_6 erfolgt durch Regelventile. Der Mengendurchfluss wird durch installierte Messeinrichtungen erfasst.

Im Folgeprozess erfolgt die sogenannte Konversion. Dort wird im Reaktionsbehälter das kontinuierlich einströmende, gasförmige UF_6 mittels überhitzten Wasserdampfs und Wasserstoff in einem kontinuierlichen Prozess in pulverförmiges Uranoxid und gasförmigen Fluorwasserstoff umgewandelt. Das beim chemischen Prozess anfallende Gas wird zur Weiterbehandlung in Kühlkondensatoren eingespeist. Basierend auf der Abkühlung findet ein Auskondensieren des vorhandenen Wasserdampfes sowie des Fluorwasserstoffs (Siedepunkt 19,51 °C) statt. Durch den Einsatz von Kalksteinfiltern können vorhandene, gasförmige HF-Restanteile zu Flussspat (CaF_2) gebunden werden.

Das anfallende Uranoxidpulver wird dem Prozess kontinuierlich per mechanischer Ausförderung entnommen. Durch die Konversion endet die Existenz des Materials UF_6. Die Entleerung des Behälters wird über Gewichtssensoren, aber auch über den Verlauf der Behältertemperatur und des Behälterdrucks, sowie über den gemessenen Massenfluss kontinuierlich verfolgt. Wenn der Ausgasvorgang erschöpft ist, wird das Ventil im Rohrleitungssystem zum Prozessbereich geschlossen. Noch ausgasende Materialreste werden über ein Unterdruckpumpsystem abgezogen. Zur Vermeidung der Bildung fester Materialanteil werden noch im aufgeheizten Zustand die Leitungen mit Stickstoff gespült. Durch das Schließen des Behälterventils wird der Entladevorgang beendet.

Grundsätzlich kann flüssiges UF_6 in Kontakt mit Kohlenwasserstoffen eine explosive Reaktion auslösen. Daher muss im Prozessablauf dafür gesorgt werden, das Kohlenwasserstoffe aus Zylindern mittels Vakuumpumpen und anderen Prozessgeräten entfernt werden, damit sichergestellt werden kann, dass kein Kontakt von flüssigem UF_6 und Kohlenwasserstoffen auftreten kann (/MES 09/).

Eine, wie in der Störfallannahme definierte, zu betrachtende gasförmige und in nennenswerter Menge vorhandene Freisetzung von UF_6 bedarf daher, basierend auf den bereits zuvor angesprochenen bestehenden hohen Sicherheitsvorkehrungen, einer Postulierung von besonderen Umständen bzw. System-Schwachstellen.

3.2 Ablauf des hypothetischen Störfalls mit Freisetzung von Uranhexafluorid

Nach der Anlieferung und Kontrolle der Frachtbriefe, speziell auf Gewicht und Anreicherungsgrad des UF_6 durch den Verarbeiter bzw. die Brennelementfabrik, erfolgt zunächst eine Lagerung der angelieferten 30B Behälter. Bei betrieblichem Bedarf erfolgt die Umsetzung einzelner 30B Zylinder in die Behälterzwischenlagerhalle, wo die Behälter durch eine weitere, betriebseigene Kontrolle hinsichtlich ihres Füllgewichtes sowie auf die UF_6 Qualität überprüft werden. Je nach betrieblichem Bedarf werden im Anschluss die Transportbehälter von der UF_6 Behälterzwischenlagerhalle in die Verarbeitungshalle gebracht. Dies geschieht in der Regel durch einen schienengebundenen Transport mittels eines speziellen Transportwagens. In der Verarbeitungshalle werden die Transportbehälter auf einen weiterhin schienengebundenen Einfuhrschlitten für den Transfer-bzw. Ausdampf-Autoklaven geladen.

Der Transfer-Autoklav, von dem drei Stück parallel betrieben werden können, hat die Aufgabe das UF_6 bis zum Erreichen des Dampf-Zustands zu erhitzen und dadurch eine Entladung des UF_6 im gasförmigen Zustand zu ermöglichen. Die Weiterleitung des gasförmigen UF_6 an den Folgeprozess erfolgt durch ein angeschlossenes und beheiztes Rohrleitungssystem, zur Beibehaltung der gasförmigen Phase.

Bei Normaldruck und einer Temperatur von 56,5 °C geht Uranhexafluorid durch Sublimation direkt vom festen in den gasförmigen Zustand über. Auch reagiert UF_6 sehr sensitiv mit Wasser, d. h. für eine Reaktion reicht in der Regel die in der Luft vorhandene Luftfeuchtigkeit.

Der zu postulierende UF_6 Störfall kann somit nur im Zeitfenster des größten Gefahrenpotentials von UF_6, also im heißen Zustand definiert werden. Somit hat ein Szenario zwangsweise im Bereich des Autoklavs und im bereits aufgeheizten Zustand stattzufinden.

Autoklaven an sich sind dabei gemäß Herstellerangeben entsprechend druckstabil ausgelegt. Neben einer massiven Konstruktion wird dies speziell durch den Umstand unterstützt, dass der Autoklav über ein wesentlich größeres Innenvolumen als der 30B Behälter verfügt. Bei einem Behälterversagen im Autoklav herrscht demnach ein wesentlich geringeres Druckniveau bzw. entsprechendes Gefahrenpotential. Wie im Regelproduktionsbetrieb üblich, wurde im hier konstruierten Beispiel wurde ein 30B Behälter in einen Transfer-Autoklaven eingefahren. Nach ordnungsgemäßem Behältereinfahren, Anschließen und Verschließen des Autoklavs, kam es während der nachgeschalteten Aufheizphase des Behälters zu einer begrenzten, aber sich vergrößernden Inkonsistenz infolge einer Fehlfunktion der Temperaturanzeige. Bei einem Anzeigewert des betrieblichen Systems von ca. 95 °C erfolgte aus Sicherheitsbedenken eine Systemumschaltung auf manuellen Betrieb, die Heizelemente wurden abgeschaltet und die weitere Prozesssteuerung für eine mögliche Entladung zurückgesetzt.

Die weitere Vorgehensweise wurde von der Betriebsmannschaft nach Vorgabe in der Betriebsanweisung verfolgt. Demnach müssen teilentladene Zylinder erst auf unter 54 °C abgekühlt werden, bevor diese wieder entnommen werden dürfen.

Es wurde noch kein UF_6 entnommen, da der Prozess vor dem Erreichen der Endtemperatur abgebrochen wurde. Daher wurde der Vorgang von der Betriebsmannschaft nicht als Teilentladung eingestuft. Diese Sicht, dass noch keine Teilentladung vorliegen würde, wurde dadurch verstärkt, dass das Prozess-Übergabeventil sowie das Pigtail noch geschlossen waren, da die Endtemperatur noch nicht erreicht war. Es wurde der übliche Kühlprozess für entleerte bzw. teilentleerte Zylinder gestartet. Durch das vollständige Behälterinventar des Zylinders besitzt dieser im Gegensatz zu leeren bzw. teilentleerten Zylinder eine sehr hohe Wärmekapazität, benötigt demnach also einen entsprechend hohen Wärmeabtransport, was eine entsprechend lange Abkühlzeit zur Folge hat. Im Rahmen des betrieblichen Ablaufs werden die drei vorhandenen Autoklave von der zentralen Kühlgas-Prozesseinheit versorgt. Dem Betriebsablauf entsprechend, erfolgt dies in der Regel in sequenziellen Anforderungsfällen.

Durch den Quasi-Ausfall eines Autoklavs steht für den normalen Nennbetrieb keine ausreichend große Menge UF_6 zur Verfügung. Um den Produktionsprozess nicht stoppen zu müssen, wurde die Ausdampf- bzw. die Entnahmemenge zunächst reduziert. In der Folge stellte sich heraus, dass ein Abkühlen eines weiteren Autoklavs / respektive eines entleerten Zylinders, parallel zu dem heißen Autoklav 2 nicht möglich bzw. auch ein 2 Schicht Autoklav-Betrieb mit verringertem Durchsatz mittelfristig nicht durchführbar erschien.

Um die Wärmeabfuhr aus dem Autoklav 2 zu unterstützen, d. h. die Abkühlzeit zu verringern, sollte die Beladeklappe des Autoklavs, parallel zu einem engmaschigen Monitoring Programm hinsichtlich der atmosphärischen Innenwerte im Autoklav, schrittweise geöffnet werden. Da es keine Hinweise auf sonstige Anomalien gab, erschien das Risiko der Aufgabe der Sicherheitsbarriere Autoklav als akzeptabel einstufbar, da es sich auch noch um keine Teilentleerung gemäß (fiktivem) Anlagenhandbuch handelte. Nachdem dies von der technischen Seite umgesetzt war, sollte zur weiteren Unterstützung der einsetzenden Naturkonvektion die Abkühlung des hinteren Behälterteils verbessert werden. Dazu sollte der Zylinder im Rahmen der Toleranz des noch angeschlossenen Pigtails, bzw. unter Beibehaltung der vollen Auflageflächen der Schlittenkufen auf den Autoklavschienen, wenige Zentimeter nach vorne gezogen werden.

Nach Ankoppelung der elektrisch betriebenen Schub-/ Zieheinheit und des Anfahrens, verklemmte sich ein bei der Beladung unbemerkt mit in den Autoklaven eingefahrener, magnetischer Fremdkörper zwischen Oberseite des Transportzylinders und der Autoklaven Innenhaut. Bei der angeforderten Vorschubbewegung des Transportzylinders verletzte der keilförmige und mit scharfen Bruchkanten ausgestattete Fremdkörper lokal die Zylinderumschließung. Dieser Vorgang wurde durch die hohe zur Verfügung stehende Traktionsleistung der Schub- /Zieheinheit möglich. Bedingt durch den immer noch hohen Innendruck des UF_6 Zylinders kam es in der Folge an der geschwächten Behälterstelle zur Ausbildung eines begrenzten Lochs in der Zylinderhaut. Bedingt durch das Loch an der Oberseite und der hohen Behältertemperatur, führte dies zu einer kontinuierlichen UF_6 Dampf-Freisetzung. Das dabei austretende UF_6 reagiert sofort mit der vorhandenen Luftfeuchtigkeit zu einer entsprechenden Wolkenbildung. Der in Richtung des Inneren des Autoklavs gerichtete Dampfstrom wurde durch die noch in ähnlicher Größenordnung vorhandene Innentemperatur nicht wesentlich in Temperatur oder Aggregatszustand beeinflusst.

Die automatische Raumüberwachung löste zeitnah einen entsprechenden Alarm aus, inklusive einer Umschaltung in den Notlüftungsbetrieb. Neben dem freigesetzten Uran ist besonders das sich in der Luft bildende und stark ätzend wirkende HF zu betrachten, eine höchst toxische Substanz.

Im Vergleich zu dem hier konstruierten hypothetischen Störfall sind Autoklaven in reell existierenden Anlagen typischerweise so ausgelegt, dass ein Bersten eines normal befüllten aber auch eines überfüllten 30B Zylinders von ihm sicher abgefangen wird. Eine Überfüllung kann im Rahmen von vorherigen Gewichtsüberprüfungen ermittelt werden. Für eine Beschädigung seiner Barrierefunktion müsste mindestens ein Doppelfehler, d. h. eine nicht erkannte massive Überfüllung in Kombination mit einer substanziellen Überhitzung vorliegen, um eine solche Druckerhöhung nur ansatzweise zu erreichen.

3.3 Anwendung der generischen Störfallanalyse auf das postulierte Störfallereignis

Für die Störfallanalyse wurden drei geeignete Analysemethoden ausgewählt, um den Störfall umfänglich zu beschreiben. Für jede der drei Analysemethoden fließen, die über eine Literaturrecherche ermittelten, aktuellen Erkenntnisse und Entwicklungen bezüglich der jeweiligen Gefahrenanalysen in Wissenschaft und Technik, in eine detaillierte Durchleuchtung sämtlicher Abläufe des betrachteten Teilprozesses nach möglichen Gefahren und die Ermittlung der möglichen zugrundeliegende Ursachen mit ein. Die Analysen beinhalten zur Demonstration, je nach Art der Methode, die Schritte Untersuchungen zu auslösenden Ereignissen, Eintrittswahrscheinlichkeiten und mögliche (probabilistisch) Konsequenzen, bzw. sicher eintretende (deterministisch) Konsequenzen.

3.3.1 Flussdiagramm des zeitlichen Ablaufplans des postulierten Prozesses

Um die Fehleranalyse Methoden möglichst zielgenau und detailliert anwenden zu können, ist eine entsprechende kompakte Aufteilung der Vorgänge, Randbedingungen und Entscheidungen auf Einzelschritte, linear über der Zeit notwendig. Daher wird eine dem zeitlichen Ablauf entsprechende Darstellung hinsichtlich einer besseren Überschaubarkeit erstellt. Die einzelnen Schritte bzw. Phasen werden mit der Abkürzung S für Schritt sowie einer folgenden Ordnungsnummer für eine bessere Orientierung innerhalb des Ablaufgeschehens versehen, siehe Tab. 3.1.

Tab. 3.1 Flussdiagramm des zeitlichen Ablaufplans des postulierten Prozesses

	Vorgang	**Besondere Randbedingungen**	**Entscheidungen**
S1	Nach Freigabeerteilung durch den Leitstand aufladen des 30B-Zylinders per Kransystem auf das Transport-Schienensystem von der Behälterzwischenlagerhalle zum Betriebsgebäude	Zylinderventil in 12 Uhr Stellung, Gewichtsüberprüfung.	Bei vorliegenden positiven Überprüfungschecks, Freigabe Einleitung Transport
S2	Überprüfung der Vorgaben der Aufladeanweisung, besonders der Sicherstellung, dass das Zylinderventil in der 12 Uhr Stellung, also oben, steht. Erfassung des Gesamtgewichtes des Transportbehälters und Über-prüfung auf Zulässigkeit bzw. den Sollwert, als Bedingung einer Freigabe.		
S3	Freigabeerteilung des Transportprozesses nach optischer Kontrolle, dass der Transportweg frei ist.	Kontrolle Fahrweg	Freigabe, wenn Kontrolle durchgeführt
S4	Freigabeerteilung zur Öffnung des Tores Lagerhalle und Öffnung äußeres Tor Schleusenbereich Betriebsgebäude, nur wenn Innentor Schleuse zu ist und Schleuse leer und betriebsbereit ist.	Überprüfung auf mögliche Störmeldungen	Freigabe, wenn alles OK
S5	Durchführung des Transports	Begleitung durch Aufsicht vor Ort	
S6	Eintreffen des Transportes in der Schleuse der Betriebshalle. Schließen des Einfahrtors.	Vor Öffnung Innentor, Außentor geschlossen, befundfreie Messergebnisse	Freigabe Innentor, Freigabe Transport
S7	Messung auf mögliche UF_6 Anhaftungen sowie HF-Verdunstungsspuren.		
S8	Nach Freigabe und Außentor sicher zu, Ausschleusen des Transportes in die Betriebshalle.		
S9	Weiterfahrt des Transportes bis zu Übergabestelle an das zweite Schienensystem, d. h. zur elektrischen Einfahrbrücke mit Hubsystem.	Weitere Freigaben erforderlich, Vorbereitung Einfahren, mechanische Sicherung bis zur Einfahrt	
S10	Mit Abstellsicherungen / Unterlegkeile Transport zunächst sichern, bis die Übergabestelle freigegeben wird.		
S10	Mit Abstellsicherungen / Unterlegkeile Transport zunächst sichern, bis die Übergabestelle freigegeben wird.		
S11	Einleiten der Zylinderübergabe auf den Einfahrschlitten. D.h. es erfolgt zunächst durch eine elektrische-pneumatische Unterstützung ein Anheben des Zylindertransportgestells. Beim Erreichen des Niveaus (des noch außerhalb stehenden Einfahrschlittens des Autoklavs), wird der Zylinder elektrisch von der Schub- Zieheinheit auf den außerhalb des Autoklavs stehenden Einfahr-Schlitten aufgeschoben. Dieser Vorgang wird durch mechanische und optische Sensoren gesteuert und überwacht. Auch wird überprüft, ob sich das Behälterventil weiterhin in der 12 Uhr Stellung befindet.	Systemanzeige OK um Zylinder auf Niveau zu bringen und auf Einfahrschlitten zu positionieren	Freigabe

	Vorgang	Besondere Randbedingungen	Entscheidungen
S12	Die korrekte Position des Einfahrschlitten wird auch nach dem Aufschieben des Zylinders weiterhin über verschiedene mechanische und optische Positionserfassungssensoren kontinuierlich überwacht. Bei richtiger Positionierung erfolgt OK Anzeige vom System	Überwachung	Freigabe, wenn alles OK
S13	Nach Freigabe der Position des Einfahrschlittens sowie der Schub- Zieheinheit, wird die Tür des vorher überprüften Autoklavs, elektrohydraulisch geöffnet. Wenn Tür gesichert offen ist, d. h. die Sensoren freigeben, wird der Einfahrschlitten per Gleitreibung durch die Schub- Zieheinheit auf seinen Kufen in den Führungsschienen des Autoklavs eingeschoben.	Überwachung	Freigabe
S14	Wenn Sensorik die korrekte Positionierung des Einfahrschlittens innerhalb des Autoklavs bestätigt, Freigabe für den nächsten Schritt abwarten.	Wenn alles OK	Freigabe
S15	Die Schub- Zieheinheit wird vom Einfahrschlitten mechanisch abgekoppelt, zurückgesetzt und mechanisch gesichert.	Wenn alles OK	Freigabe
S16	Mechanischer Anschluss des Pigtails an das, in der 12 Uhr befindliche Behälterventil, so die Autoklaven-Innenraum-Überwachung auf HF unauffällig.	Dichtigkeit des Anschlusses	Freigabe
S17	Nach Fertigmeldung und Freigabe erfolgt „rückwärts“ d. h. von den Autoklaven aus, eine Stickstoffbeaufschlagung als Druckdichtigkeitsprüfung des Anschlusses und des Pigtails, als Voraussetzung für eine Freigabe für den nächsten Arbeitsschritt.		
S18	Bei bestätigter und dokumentierter Dichtigkeit des Anschlusses und der Leitung, kann am Behälterventil die mechanische Spindelmitnahme angebracht werden. Im Anschluss daran wird die Autoklaventür wieder zugefahren und verriegelt. Zur Sicherstellung, dass die Verriegelungsbolzen auch komplett eingefahren sind, ist dies optisch von außen zu überprüfen, d. h. es darf nur noch der grüne und nicht mehr der rote Bolzenanteil sichtbar sein. Dies ist parallel zur elektronischen Erfassung zu dokumentieren.	Spindel eingehängt, Türverriegelung erfolgreich.	Freigabe, wenn alles OK
S19	Start der Aufheizphase nach erfolgter Freigabe. Neben der zugeführten elektrischen Heizleistung erfolgt eine Überwachung durch ein betriebliches, sowie durch ein sicherheitsgerichtetes Temperaturmesssystem. Parallel dazu wird der Druck im Inneren des Autoklavs, sowie die innere Atmosphäre auf mögliche Freisetzungsspuren von UF6 oder HF überwacht.	Wenn keine Auffälligkeiten.	Freigabe elektrische Aufheizung
S20	Basierend auf der begrenzten Wärmezufuhr pro Zeiteinheit, ist die eine Sicherstellung einer möglichst homogenen Durchwärmung des Zylinders gewährleistet. Bedingt dadurch, dauert der Aufheizprozess über 10 Stunden, bis zum Erreichen der Zieltemperatur von 110°C. Zur Sicherstellung, dass diese Temperatur nicht verändert werden kann, ist sie im Steuersystem fest einprogrammiert. Bedingt durch diese, meist 2 Arbeitsschichten umfassende Prozedur, erfolgt der Prozess automatisch gesteuert. Zusätzlich sind diverse Überwachungsprozeduren, wie z. B. der Temperaturgradienten aktiv.	Bes. Randbedingung	

	Vorgang	Besondere Randbedingungen	Entscheidungen
S21	Ab ca. 90 °C wurde eine erste, sonst unübliche Differenz zwischen der betrieblichen und der Sicherheitstemperaturanzeige im Leitstand festgestellt. Eine weitere Beobachtung zeigte eine stetige, nichtlineare Zunahme der Differenz beider Werte. Beide Systeme gingen, auch bis zu diesem Zeitpunkt, nicht auf Störung.		
S22	Als Konsequenz aus der ad-hoc nicht erklärbaren und sich vergrößerten Messdifferenz, erfolgte ein Abbruch des Aufheizvorgangs bei ca. 97 °C, indem eine Systemumschaltung auf manuelle Steuerung durchgeführt wurde.	Abbruch Aufheizen wegen inkonsistente Temperaturanzeigen.	Umschaltung auf manuellen Systemsteuerung, Abbruch des Erhitzungsvorgangs Aktivierung der Kühlfunktion.
S23	Parallel dazu wurde, die ausschließlich über einen Gaskreislauf wirkende innere Kühlfunktion des Autoklavs aktiviert.		
S24	Die durchgeführten Fehleranalysen zu den divergenten Temperaturanzeigen brachten ad-hoc keine weiteren Erkenntnisse. Bedingt durch das noch vollständige Behälterinventar erfolgt der eingeleitete Abkühlvorgang extrem langsam.	Nach Formulierungen Handbuch liegt bei noch nicht geöffneten Zylinderventil kein Zustand „Teilentladung eines Behälters“ vor. Keinerlei sonstige Auffälligkeiten bzgl. Möglichen UF6 Austritt aus dem Zylinder in den Autoklaven-Innenraum.	Entscheidung zur weiteren Fehlersuche und Parametervalidierung.
S25	Das 30B-Behälterventil war, da die Entnahmetemperatur noch nicht erreicht wurde, noch geschlossen. Das Pigtail sowie die angeschlossene Leitung waren noch im Zustand der Stickstoff-Inertisierung. Somit war es, zumindest interpretierbar, dass es sich bei diesem Zustand, gemäß Handbuch, noch um keine Behälter-Teilentladung handelt und die dazu geltende Verfahrensanweisung, dass für ein Ausschleusen des Behälters, dieser unter 54 °C haben muss, damit keine Relevanz bekommen würde. Sowohl während des Aufheizvorgangs, während des Abbruchs des Vorgangs und auch danach, waren die Messwerte des Innendrucks im Autoklav unauffällig. Ebenso lagen keine Hinweise auf Undichtigkeiten des Zylinders vor, die auf ausgetretenes UF6, oder sonstige Anomalien hinweisen würden.		
S26	Da das Produktionsgeschehen in der Fabrik durch mehrere Autoklave bedient wird, wurde zunächst eine Reduzierung der Produktionsmenge eingesteuert, um den Gesamtprozess nicht anhalten zu müssen.	Keine sicherheitsrelevanten Auffälligkeiten.	Weiterführung eines reduzierten Produktionsprozesses
S27	Die Abkühlung eines nun entleerten anderen 30B-Zylinders als Bedingung für ein Ausfahren aus einem anderen Autoklav stand betrieblich an. Bei der Kühlung handelt es sich aus Sicherheitsgründen um ein mit Gas als Trägerelement laufendes zentrales Kühlsystem, bei dem für die einzelnen Autoklaven, einzelne Stränge binär zu oder abgeschaltet werden können. Die Abkühlung eines vollen Behälters ist jedoch eine um Größenordnungen höhere Anforderung an das Kühlsystem als die Abkühlung eines entleerten Behälters. Als die Kühlfunktion für den oben benannten, ausgedampften Autoklaven zugeschaltet wurde, geriet das Kühlsystem, durch die noch hohe Temperatur im Autoklav 2, jenseits seiner Kapazitätsgrenze. So wurde entschieden, den Autoklaven mit dem noch vollen UF6 Zylinder aus dem Kühlsystem auszusteuern, um den schon reduzierten Betriebsprozess nicht zu gefährden.	Kühlsystem nicht selektiv steuerbar überlastet für den Fall einer erweiterten Anforderung, d.h. für eine Abkühlung eines vollen und eines entleerten Behälters, mangels regelbarer Drosselventile. Es kam zu einer Systemüberlastung.	Aussteuerung des Autoklavs mit dem vollen Behälter aus dem Kühlsystem.

	Vorgang	Besondere Randbedingungen	Entscheidungen
S28	Es wurde eine weitere Überprüfung der Messwerte des Autoklavs respektive der Werte aus dem Innenraum auf Hinweise auf Druck oder Gas-Anomalien durchgeführt. Alle Ergebnisse waren im Normalbereich. So entschied man sich, über eine Messleitung zunächst den Druck im Autoklaven-Innenraum auf atmosphärische Hallen-Verhältnisse anzupassen. Diese Messleitung wurde parallel zu einem weiteren Sicherheitsmonitoring schrittweise geöffnet.	Keine Anomalien feststellbar.	Erneute Überprüfung auf Anomalien. Öffnung einer Messleitung, um atmosphärische Druckverhältnisse im Innenraum des Autoklavs zu erhalten.
S29	Zur weiteren Abkühlung des UF_6 Zylinders wird nun, da alle Messwerte erwartungsgemäß waren, eine Wärme-Naturkonvektion eingeleitet, d. h. die Autoklavetür, unter ständiger Beobachtung aller vorhandenen Messwerte, geöffnet.	Engmaschige Überwachung aller Messwerte.	Vorsorgliche Räumung der Halle. Einleitung einer Naturkonvektion durch öffnen der Autoklavetür.
S30	Bei der Türöffnung an sich und beim Zustand danach zeigten sich keine Hinweise auf Abnormalitäten. Aufkommende Überlegungen zur weiteren Unterstützung der Naturkonvektion ergaben, dass die Behälter-Transportschlitten-Kombination im Rahmen der Möglichkeit etwas nach vorne gezogen werden sollte. Dazu wurde die Frage der Standsicherheit der Behälter-Transportschlitten-Kombination im Autoklav betrachtet. Die Überdeckung des Abstands des Endes des Zylinderschlittens bis zum Ende der Autoklavkufe wurde mit 12 cm angegeben.	Engmaschige Überwachung aller Messwerte. Bewertung der Standsicherheit des Zylinderschlittens im Autoklav. Bis 12 cm Bewegung nach vorne, noch vollflächige Auflage von Behälterschlitten auf Autoklavkufen.	Lösung des Pigtails, um bei einer Behälterverschiebung weder das Behälterventil noch die UF6 Anschlussleitung zu gefährden. Festlegung, dass der gesicherte Zylinderschlitten, nicht mehr als 6 cm nach vorne bewegt werden darf.
S31	Entscheidung den Transportschlitten bei abgekoppelten Pigtail um max. 6 cm unter weiteren Sicherungsbedingungen nach vorne zu ziehen.		Halle war weiterhin geräumt.
S32	Ankoppeln Behälterschlitten an Traktionseinheit. Programmierung der Fahrstrecke und zusätzlich mechanische Sicherung der maximal vorgegebenen Fahrstrecke durch Bremskeile hinter der Traktionseinheit im Abstand von 6 cm. Halle blieb weiterhin vorsorgliche geräumt.	Elektronische und mechanische Absicherung der Einhaltung der Verschiebevorgabe.	Halle war weiterhin geräumt. Betreten nur mit Vollschutzanzug und Pressluftatmung zum reinen Ankoppeln.

	Vorgang	Besondere Randbedingungen	Entscheidungen
S33	Nahezu parallel zum Start des Traktionsvorgangs erfolgte die HF-Alarmauslösung des Sensors im Autoklaven-Inneren.	Auslösung des Störfallmanagement. Entweichung Zylinderinhalt in Betriebshalle.	Auslösung Störfallmanagement. Auslösung Steuerimpuls zum Schließen der Autoklavtüre bei angekoppelter Traktionseinheit nicht möglich.
S34	Typisches Anzeichen für eine UF6 Heißentweichung. Erste Hinweise und Messergebnisse deuten jedoch auf eine tendenziell überschaubare Leckage-Rate des im Autoklav befindlichen Zylinders hin. Durch den angekoppelten Zustand ist kein Schließen der Türe möglich. Durch das noch relativ heiße Autoklaven-Innere erfolgt auch keinerlei nennenswerter Kondensationsprozess.	Vorbereitung einer Rettungs- und Bekämpfungsmannschaft mit Vollausrüstung (Pressluft etc.)	Störfallszenario aktiviert, wie Türsteuerungen, Anforderung Filter-Lüftungssystem, etc.
S35	Nach einer Rüstzeit von ca.15 Minuten trifft die Bekämpfungsmannschaft am Autoklav ein, löst die Kupplung zur Traktionseinheit, entfernt die beiden Bremskeile und rangiert die Traktionseinheit ausreichend nach hinten. Der noch anstehende Steuerimpuls für Schließen Autoklavetür“ wird angenommen und der elektrohydraulische Schließvorgang für die Autoklavetür wird durchgeführt. Doch bereits bis zum Eintreffen der Rettungsmannschaft war der Ausströmvorgang weitgehend durch Verdampfung des Inhaltes zum Ende gekommen. Das Schließen der Türe brachte somit keinen nennenswerten Beitrag zur Expositionsbegrenzung in der Halle.	Mechanische Handeingriffe zur Entkoppelung Traktionseinheit, Entfernung Bremsklötze, Rücksetzen Traktionseinheit.	Störfallszenario weiterhin aktiv.
S36	Alle anderen Sicherheits- und Begrenzungssystem funktionierten einwandfrei.		

Eine spätere Ursachenuntersuchung ergab, dass ein scharfkantiges metallisches und magnetisches (vermeintliches) Bruchstück unbekannter Herkunft, unbemerkt im oberen Bereich des Zylinders anhaftete und mit in den Autoklaven einfuhr. Beim Rückrangieren kam es, basierend auf der geometrischen Form des Fremdkörpers zu einer Verklemmung und in der Folge zu einem „sich hineindrücken“ des Fremdkörpers, sowohl in die Behälter- als auch die Autoklavewand. Durch die Schwächung der Zylinderummantelung kam es, zusammen mit dem herrschenden Innendruck, zu einer Leckausbildung. Unterstützend ist beim Unfallverlauf auch der Umstand, dass beim Hineinschieben, bzw. beim Herausziehen des Transportschlitten ein größeres Losbrechmoment von Haft- auf Gleitreibung von Nöten ist, so dass hier auch genügend Energie zur Verfügung stand, die Zylinderhaut mit dem scharfkantigen Fremdkörper zu verletzen. Diese Schwächung war ausreichend, um zusammen mit dem hohen Innendruck, den Durchbruch der Behälterwand zu bewirken, der zu der Leckage führte.

3.3.2 Zusammenfassung der aus dem Flussdiagramm abgeleiteten Fragestellungen

Basierend auf dem in Kapitel 3.3.1 dargestellten Flussdiagramm mit dem zeitlichen Ablaufplan des postulierten Prozesses werden einzelne Punkte, bzw. Handlungen hinterfragt. Ziel ist es, die Fehlerart bzw. die Fehlerkette herauszustellen.

- Unterschiedliche Werte bei Temperaturanzeigen:
  Die unterschiedlichen Temperaturanzeigen im Autoklav Innenraum waren nicht erklärbar, da kein System auf „Störung“ ging. Ungeachtet der eigentlichen Ursache ist der Abbruch des Aufheizvorgangs durch eine Umschaltung auf manuelle Steuerung als sicherheitsgerichtet zu bezeichnen. Auch ist diese korrekte Handlung von den später folgenden Eingriffen entkoppelt zu sehen.

- Vorschrift zu teilentladenen Behältern
  Die Vorschrift, dass teilentladene Behälter erst auf unter 54 °C abgekühlt werden müssen, bevor sie wieder entladen werden dürfen, beinhaltet einerseits Aspekte der Teilentladung selbst, sowie der Handhabung des heißen UF_6 bei dem Prozess der Teilentladung. Übergeordnet dient aber auch der Autoklav prinzipiell für den Fall des risikoreicheren Behälterzustands heiß als eine weitere, effektive Sicherheitsbarriere. Diesem Umstand wurde im Handlungsablauf nicht ausreichend Rechnung getragen. Es wurde mehr auf die Frage, ob eine Teilentladung vorlag, fokussiert, als auf die allgemein höhere Gefahr, die von einem heißen Behälter ausgeht. Gerade der Schutz des heißen Behälters bei einer unerklärlichen Situation wurde hier nicht beachtet.

- Zeitpunkt der Leckbildung
  Wenn es zu einer Leckbildung bei einer spätere Behälterentnahme im entleerten oder abgekühlten Zustand gekommen wäre, wäre der weitere Verlauf betrieblich handhabbar gewesen. Der Konjunktiv bei der Leckbildung wurde dahingehend gewählt, da der hohe Innendruck des gefüllten und heißen Behälters die letzte Phase des Aufreißens der Zylinderhaut gefördert hat.
  Der Worstcase bei einer Leckbildung bei einem entleerten Behälter ist, bedingt durch die zuvor durchgeführte Entleerung mit Vakuumabsaugung etc. als betrieblich handhabbar einzuordnen. Durch den Unterdruck im entleerten Behälter, ist bei einer Leckbildung die Strömungsrichtung bis zum Druckausgleich sicherheitsgerichtet nach innen, d. h. in den Behälter gerichtet.

- Geringe Kühlkapazität, mangelnde selektive Regelbarkeit
  Die sich aus den Umständen / Randbedingungen ergebende Handlungskette einer zu geringen Kapazität der Autoklav-Innenkühlung lenkte die Aktivitäten der Betriebsmannschaft weiter Richtung unsicherer Zustand. Dieser Umstand wurde primär durch die begrenzte Kühlkapazität, aber auch durch den Umstand unterstützt, dass keine regelbare Kapazitätsverteilung der Leistung des Kühlsystems auf den einzelnen Autoklaven möglich war.

- Öffnen der Autoklavtür im Behälterzustand heiß.
  Hier ist im Wesentlichen auf die Ausführungen zu dem Bullet zu teilentladenen Behälter zu verweisen. Auch wenn der Vorgang zunächst ohne Vorkommnis ablief, wurde in diesen Augenblick eine der wichtigsten Sicherheitsbarrieren aufgegeben.

- Rangieren des Behälters im Zustand heiß.
  Eine Vorprüfung über erkennbare Risiken zum Vorgang des Rangierens wurde nur vermeintlich durchgeführt. Der danach eingetretene Fall einer Verklemmung wurde nicht als eine potenzielle Ausgangsbasis für einen Schadensverlauf in Betracht gezogen. Somit zeigt sich, dass bei einem unbekannten Problem, bzw. noch unbekannten Randbedingungen, eine Fehler- / Risikobetrachtung per Definition nicht umfänglich möglich ist. In dieser, auch stressbedingten Situation, verlor sich der notwendige, nüchterne Breitbandfokus, zugunsten einer schnellen Situationsklärung.

Zusammenfassend ist eine Suche in Detailfragen und an welcher Stelle genau bei dieser Systemkonstellation ein Fehler begangen wurde, wenig zielführend. Der übergeordnete Hauptsatz dazu lautet das der geschlossene Autoklav, solange der Behälter eine Temperatur über 54 °C hat, eine unverzichtbare Barrierefunktion ausübt. Ein solcher Eingriff in einer unklaren Situation, d. h. mit auch potenziell vorhandenen Ungewissheiten wie denen der unterschiedlichen Temperaturmessungen, ist dennoch ein Eingriff unter unklaren Umständen.

Basierend auf diesen postulierten Abläufen und Erkenntnissen sind für diese generische Anlage, technische Verbesserungsmöglichkeiten im Rahmen einer verbesserten Risikominimierung sowohl auf technischer wie auch auf administrativer Basis notwendig.

Das betrifft z. B. eine Außenprüfung des Behälters vor dem Einfahren in den Autoklaven auf mögliche Anhaftungen und allgemein auf Beschädigungen der Zylinderhaut. Dies können, wie hier im Beispiel, magnetische Anhaftungen aber auch ganz allgemein Eindrückungen, anhaftendes Material oder eine punktuell geschwächte Zylinderaußenhaut

sein. Diese fehlende Kontrolle zum Zeitpunkt des Einfahrens in den Autoklav müsste im Rahmen einer Betrachtung zu den möglichen Fehlern bzw. zu Fehlervermeidungsstrategien, mit in die Systemhandhabung aufgenommen werden.

Auch ist die Optimierung der möglichen Optionen der Behälterkühlung, die im Gefahrenfall eine schnelle Druckentlastung im Autoklav bewirken kann, aufzugreifen. Basierend auf der hohen Wärmekapazität eines vollen Zylinders, ist die mögliche Kapazität des Kühlsystems für das Autoklavinnere eine wichtige Größe zur Beherrschung von kritischen Situationen. Beim elektrischen Aufheizen geht es in der ersten Linie um die Sicherstellung einer homogenen Durchwärmung des Behälters bei gleichzeitiger Reduzierung einer Überhitzungsgefahr durch eine technisch bzw. konstruktiv begrenzte Wärmezufuhr. Bei der Kühlfunktion für einen noch nicht leeren Behälter, liegt der Fokus nicht zwangsweise auf einer homogenen Kühlung des gesamten Inventars. Hier hilft, in transienten Situationen und in gewissen Grenzen, bereits ein abgekühlter Außenbereich. Die technische Herausforderung liegt dabei im Bereich der Wärmeabfuhr. Da bedingt durch Kritikalitätsbetrachtungen, ein flüssigkeitsbasierter Kühlkreislauf im Autoklav ausscheidet, ist auf eine gasbasierte Kühlung auszuweichen. Dabei sind die entsprechend notwendigen hohen Kühlkapazitäten jedoch schwerer zu erreichen. Auch sollte das Kühlmanagement hinsichtlich Kompaktheit versus vielfältiger Konfigurationsmöglichkeiten für gezielte Eingriffe, sowie nach einer möglichen Systemredundanz betrachtet werden. Anstelle von einem einzelnen Aggregat könnten Lösungen mit zwei Aggregaten mit jeweils 50 % Leistung sowie einer Zusatzreserve von weiteren 50 % Leistung angedacht werden. Diese wären primär der Kühlung beladener oder nur geringfügig teilentladener Zylinder bevorzugt zugedacht.

3.3.3 Ereignisbaum

Für die Darstellung eines Störfalls wird typischerweise die Darstellung als Ereignisbaum gewählt, da dies eine zeitlich stringente Darstellung des Ablaufs erlaubt. Dazu wird eine Liste der auslösenden Ereignisse und der Handlungsschritte erstellt, die den Prozess entwickeln bzw. den Gefährdungszustand beeinflussen. Zudem wird dargestellt bzw. untersucht, ob die bei den Ablaufschritten getroffenen Maßnahmen, seien diese systeminitiiert oder manuell bedingt, erfolgreich waren oder sich eine Fehlfunktion bzw. eine Fehlreaktion einstellt. Dies erfolgt durch eine klassische ja / nein Abfrage. Die Verästelung erfolgt dabei Richtung Zukunft. Die Strukturierung ist so vorzunehmen, dass das Zielereignis bzw. der unerwünschte Zustand mit den dafür bestimmenden bzw. den auslösenden Umständen abgebildet wird. Bei der Anwendung der Ereignisbaumanalyse ist neben

der traditionellen, quantitativen Betrachtung auch eine qualitative Betrachtung möglich. Die Umsetzung dieses Ansatzes in der breiten Praxis, die binären Verästelungen mit einer parallelen Hinterlegung von Wahrscheinlichkeiten nun auch konsequent numerisch anzugehen und auszuwerten, wird zunehmend zum Standard bei solchen Ereignisbaum-Untersuchungen. Dabei werden die Wahrscheinlichkeiten des Startereignisses mit denen von unabhängigen Abzweigungen der Pfade multipliziert, um die spezifischen Eintrittswahrscheinlichkeit zu erhalten.

Als innovative Komponente werden zunehmend im Ereignisbaum verbale Beschreibungen von z. B. Fehlerschweren etc., zur Unterstützung des nicht technischen Managements eingesetzt. Diese, in Klassen unterteile Einschätzung, soll auf Basis einfacher Schlagwörter das entscheidende Management in verständlicher Art und Weise unterstützen. Somit wurde zu den einzelnen Schritten, neben den Eintrittswahrscheinlichkeiten der korrekten Funktionsweise, eine Schadensschwere (*call them like you see them*) für den Fehlerfall hinzugefügt. Als Kriterien wurde hier für die technische Schadensschwere, fünf Schadensschwere-Klassen gewählt und in den Ereignisbaum integriert:

- keine
- gering
- mittel
- hoch
- sehr hoch

Die Einklassierung bzw. Benennung erfolgt, wie zuvor ausgeführt, auf der Basis *call them like you see them,* gepaart mit dem pragmatischen Ressourcenverständnis der Analysten. Wie im Ereignisbaum in Folge ersichtlich, ist die Aufgabe der Barriere *umschließender Autoklav* im Behälterzustand *heiß* mit einer Schadensschwere von *sehr hoch* klassifiziert, so dass auch nicht-Techniker dies als risikoreichen, vermeidbaren Punkt erkennen können.

Als Aufsatzpunkt für den Ereignisbaum wird hier der Punkt der Übergabe des Zylinders auf den Einfahrschlitten *Schritt 11* gewählt. Wenn alles nach Plan verläuft, geht es mit dem nächsten Ast weiter. Treten Fehler auf bzw. läuft etwas schief, ist der entsprechende Ast zu bedienen bzw. weiter zu verfolgen.

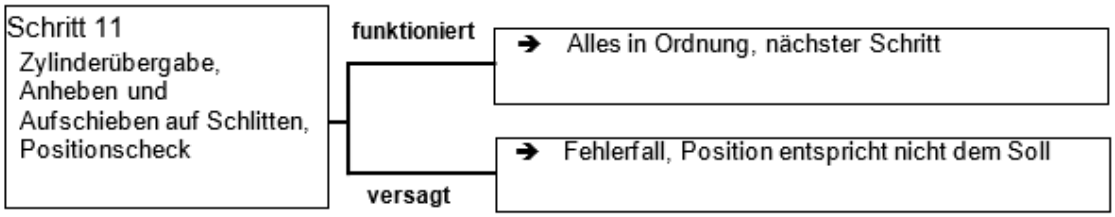

Abb. 3.1 Beispiel einer Verzweigung im Ereignisbaum

Im hier vorliegenden Beispiel wird dies gemäß Ablaufliste dargestellt. Mangels veröffentlichter Daten bzw. aufgrund der für diese generische Analyse konstruierten Gerätschaften und Prozessschritten, wurden geschätzte Wahrscheinlichkeiten angenommen. Auch sind einzelne Entscheidungen nicht von der Zuverlässigkeit der Technik, sondern von der Qualität der zur Entscheidungsfindung (human error) herangezogenen Basisinformation abhängig.

So bedeutet die prinzipielle Entscheidung, bei einem heißen 30B-Zylinder die Autoklavtür zu öffnen, die Aufgabe einer Sicherheitsbarriere. Erst dies ermöglicht den Eintritt des Freisetzungsszenarios in Form von Austritt, von heißem UF_6 in die Betriebshalle. Die Aufgabe einer Sicherheitsbarriere ist nicht zu rechtfertigen. Dies zeigt die Entscheidung, den Zylinder-Schlitten zu rangieren, d. h. einen mechanischen Eingriff zuzulassen. Dies wurde für den weiteren Vorgang zu einem Fehler mit unabsehbaren Risiken. Für eine Betrachtung der reinen technischen Fehlerwahrscheinlichkeiten wurde die Entscheidung, dass es sich noch nicht um eine Teilentladung handelt (Schritt 25) und somit auch eine Abkühlung innerhalb des geschlossenen Autoklavs zwangsweise wäre, außer Betracht gelassen. Diese Aufgabe einer Sicherheitsbarriere, mit einem als sehr hoch einzuschätzenden Fehler-Wahrscheinlichkeitswert, sowie der mechanische Eingriff, dominiert die gesamte Betrachtung für eine Austrittswahrscheinlichkeit von UF_6 in die Halle. Abb. 3.2 und Abb. 3.3 zeigt den entsprechenden Ereignisbaum. Dabei werden folgende Abkürzungen verwendet:

- SSK: Schadensschwere-Klasse
- WdfF: Wahrscheinlichkeit der fehlerfreien Funktion

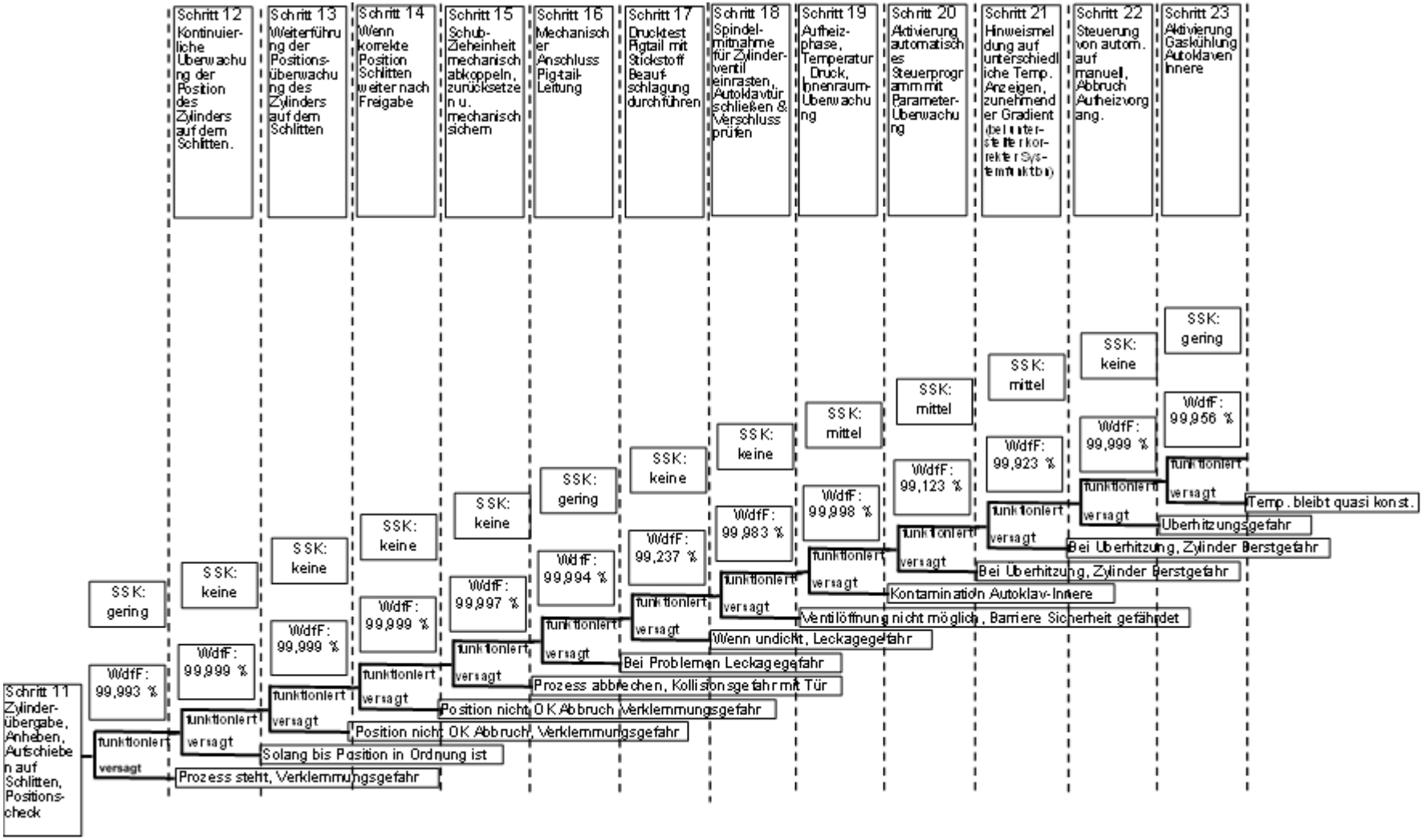

Abb. 3.2 Darstellung des Ereignisbaums: Schritt 12 bis 23

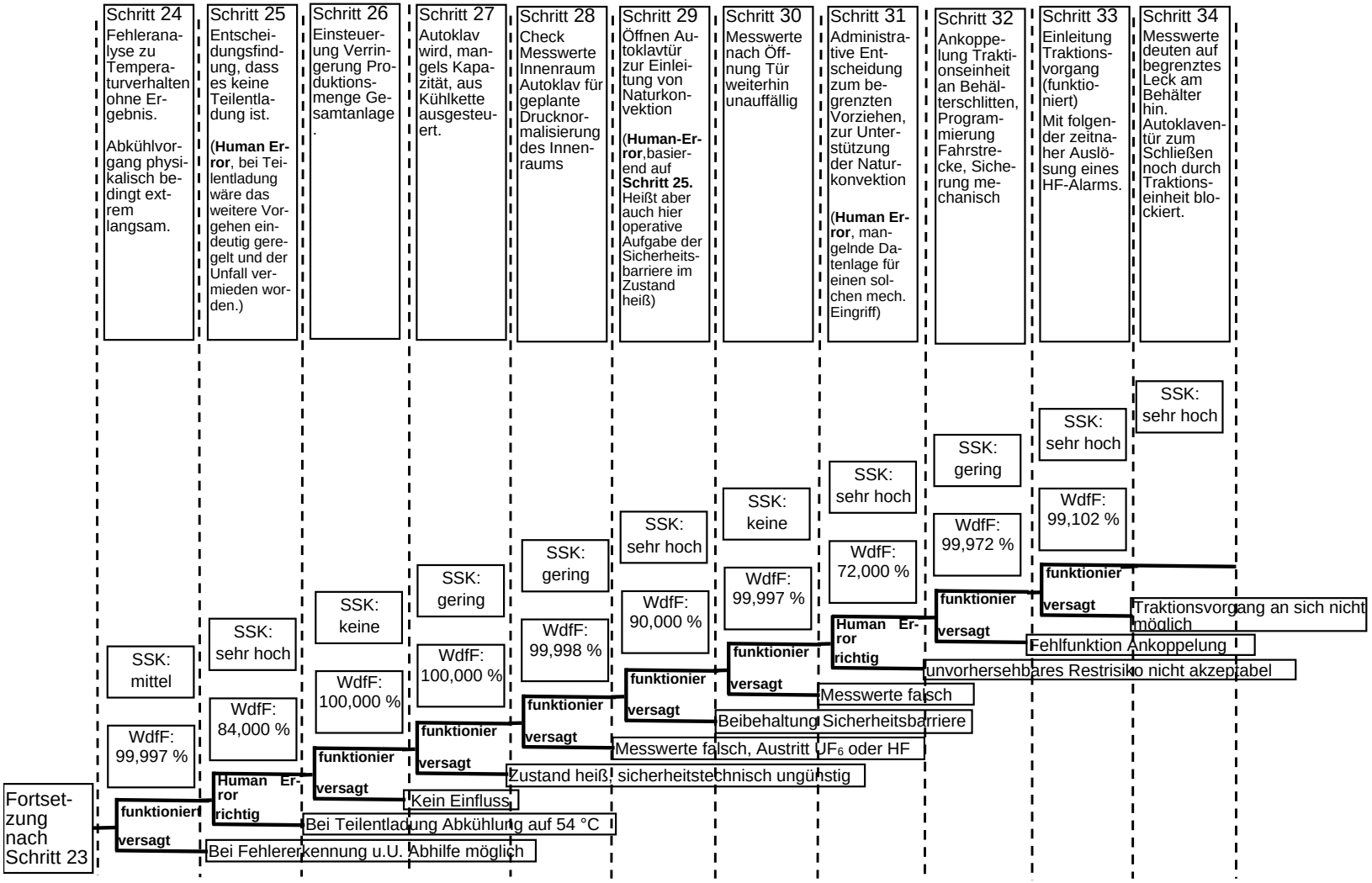

Abb. 3.3 Darstellung des Ereignisbaums: Schritt 24 bis 34

Der letzte Schritt (Nummer 34) ist nur noch im Zusammenhang mit einer anzustrebenden Begrenzung der Austrittsmenge zu sehen. Das Ergebnis des kompletten Ausdampfens bei dem benötigten zeitlichen Vorlauf der Einleitung von Sicherungs- und Rettungsmaßnahmen, ist dabei vorhersehbar. Dazu wurde eine Abschätzung zur Dauer des UF_6 Austritts für ein Loch mit ca. 5 cm Durchmesser in zwei Schritten durchgeführt. Der erste Schritt beinhaltet die Abkühlung des Behälters durch den ausströmenden Dampf bis auf den Tripelpunkt des beinhalteten UF_6. Dies erfolgt in einer Zeitspanne von ca. 75 Sekunden, bei einer Freigabe von ca. 240 kg UF_6. Der zweite Schritt ist die Abkühlung bis auf den Sublimationspunkt, an dem der Dampfdruck von UF_6 dem atmosphärischen Druck entspricht und der Ausdampfvorgang endet. Dieser Vorgang dauert ca. 400 Sekunden, die verdampfte Menge liegt dabei bei ca. 961 kg. Somit ist der integrale Vorgang nach insgesamt ca. 5 Minuten unter der Freigabe von ca. 1.200 kg UF_6 beendet.

Im Folgenden wird noch auf die quantitative Ermittlung der eintretenden Wahrscheinlichkeit eingegangen. Sind die Einzelereignisse, die dem Startereignis folgen, das Versagen bzw. der Fehlerfall mit einer Wahrscheinlichkeit $P_{Fehler\text{-}Schritt\text{-}X}$, so kann die Wahrscheinlichkeit des Endzustandes P_{Ende}, durch die Multiplikation der Einzelwahrscheinlichkeiten der einzelnen Schritte ermittelt werden. Die Bedingung dazu ist jedoch, dass die Schritte voneinander unabhängig sind (also z. B. nicht alle von derselben Stromversorgung gespeist werden etc.), da ansonsten bedingte Wahrscheinlichkeiten als Werte einzusetzen sind.

Für die Schritte 11 bis 24 wird die Wahrscheinlichkeit der korrekten Funktion zu 0,98 bzw. die Fehlerwahrscheinlichkeit zu 0,02 bestimmt. Entsprechend wird für die Schritte 26 bis 30 und 32 bis 33 die korrekte Funktion zu 0,90 und 0,99 bzw. die Fehlerwahrscheinlichkeiten zu 0,10 und 0,01 bestimmt. Die Fehlerwahrscheinlichkeiten für die Schritte 25 und 31 als human-error-administrativ-Fehler wurden mit dem Komplement der korrekten Funktion von 0,84 und 0,72 zu 0,16 und 0,28 angesetzt. Somit ergibt sich die Gesamtwahrscheinlichkeit für das Szenario am Ende des Fehlerbaums für die obere *funktioniert*-Verästelung zu 0,53, bzw. zu 0,47 für deren Komplement *versagt*.

3.3.4 Fehlerbaum

Fehlerbaumanalysen oder Fault Tree Analysis (FTA) werden bevorzugt für die Vorbereitung probabilistischer Analysen erstellt. Die Fehlerbaumanalyse wird als eine systematische Zuverlässigkeitsanalyse eingesetzt und dient der Wahrscheinlichkeitsbestimmung des Systemausfalls bzw. einer Systemfehlfunktion in Abhängigkeit seiner Komponenten.

Bei einigen Komponenten ist die Ausfallwahrscheinlichkeit auch eine Funktion ihrer Betriebsdauer bzw. ihres Lebenszyklus. Zielsetzung ist in der Regel eine Aufdeckung von notwendigen Ausfallkombinationen um das definierte, ungewünschte Ereignis eintreten zu lassen. Parallel dazu soll die Zuverlässigkeit bzw. der korrekte Betrieb des Systems in Zahlenwerten erfasst werden. Die Darstellung des Fehlerbaums basiert dabei auf Elementen von Logik-Gattern sowie Tor- und Zwischenergebnis-Elementen. Der Startpunkt TOP beginnt mit dem definierten, unerwünschten Ereignis als oberstes Element.

Die Neuerungen im Bereich der Fehlerbaumanalysen betrifft weniger die Methodik an sich, sondern mehr den zunehmend breiteren Einsatz in der Technik. Dies wird besonders durch die am Markt immer besser werdenden und zunehmend kostengünstigeren Software-Pakete bedingt. Von Kleinanwendungen bis hin zu komplexen Systemen werden hier besonders administrative Hilfestellungen gegeben, beginnend bei der Definitionsphase, stringenter Anwendung gewählter Bezeichnungen, bis hin zu zyklischen, korrekt nummerierten Dokumentationsversionen der Projektentwicklung etc. Im hier vorliegenden Fall wird das TOP Ereignis als Freisetzung von Behälterinventar im Zustand heiß benannt. Unter dem Begriff Freisetzung soll das Austreten von UF_6 Material aus einem Loch im Zylinder, respektive die Freisetzung in den Bereich der Raumluft der Betriebshalle, verstanden werden.

In Tab. 3.2 sind die für diese spezifische Betrachtung als Basis-Elemente definierten Zustände und Ereignisse mit ihrer jeweiligen Referenznummer aufgelistet.

Tab. 3.2 Nummerierung und Beschreibung der verwendeten Basis-Ereignisse

Nummer des Basis-Ereignisses	Beschreibung
1	Temperaturwerte sicherheits- u. betriebliche Temperaturüberwachung zunehmend divergent
2	Fehlerevaluierung zur Temperaturüberwachung ohne Ergebnis
3	Aktivierung Kühlprozess des vollen 30B-Behälters mit hoher Wärmekapazität
4	Parallele, betriebliche Anfouz77777rderung Abkühlung eines weiteren entleerten B30 Behälters
5	Totalausfall des Zentralkühlaggregates zur Behälterkühlung
6	Reduzierte Leistung des Zentralkühlaggregates zur Behälterkühlung
7	Start von Behälterkühlversuch im thermodynamisch abgekoppelten Zustand, jenseits der normalen Betriebsfunktionen
8	Überprüfung Standsicherheit über Verschiebeweg des Einfahrschlitten
9	Pigtail-Leitung abkoppeln, Ventil / Anschluss auf Leckagen prüfen
10	Verschiebestrecke Schlitten mechanisch und elektrisch gemäß Vorgabe begrenzen

Nummer des Basis-Ereignisses	Beschreibung
11	Betriebshalle räumen
12	Leckage-Monitoring im Autoklav läuft
13	Entscheidung Verschiebung Transportschlitten im Autoklav zur bes. Kühlung
14	Schwächung Zylinderhaut durch Verklemmung u. Eindrückung Fremdkörper
15	Temperaturgemäßer Innendruck im 30B-Behälter
16	Versagen Führungsschiene im Autoklav
17	Falsche Positionierung von Behälter oder Schlitten im Autoklav
18	Bruch oder Versagen der 30B-Behälteraufnahme mit Abrutschen und Abriss des Pigtails
19	Mechanischer Fehler Schlittenaufnahme bei heißem Autoklav oder Behälter
20	Werkstoffversagen heißer Behälter
21	Ausfall Heizungssteuerung zur unsicheren Seite (Dauerbetrieb)
22	Fehlfunktion Temperaturerfassung Sicherheitssystem
23	Versagen oder Leckage des Behälter-Ventils
24	Unbemerkter Ausfall Sicherheits-Überwachung Temperatur
25	Unbemerkter Ausfall Redundanz Sicherheits-Überwachung Temperatur
26	Unbemerkter Ausfall betriebliche Temperaturerfassung
27	Unbemerkter Ausfall lokale Temperatur-Überwachung am Autoklav
28	Versagen Abschalteinrichtung Heizelemente
29	Defekt atmosphärische Messleitung Autoklav
30	Defekt, bzw. Blockade offene Tür, bzw. Türbereich Autoklav
31	Gewichtsüberprüfung durch eigene Erfassungseinheit
32	Transport in Behälterzwischenlager zur Überprüfung
33	Betriebliche Materialanforderung
34	Freigabe Transport in Behälterlager
35	Überprüfung Lieferschein Behälternummer u. Konsistenz der Angaben
36	Materialannahme u. Eingangskontrolle 30B-Behälter
37	Anreicherungsüberprüfung durch eigene Erfassungseinheit
38	Freisetzung über Produktionsleitung außerhalb des Autoklavs

Diese Basisereignisse sind entsprechend ihrer Nummerierung im aufgestellten Fehlerbaum zu finden.

Auch im Bereich der Fehlerbaumanalyse werden zunehmend Keywords zur Schadensschwere der einzelnen Prozessschritte mit aufgenommen. Die Ermittlung der möglichen Schadensschwere-Klasse erfolgt dabei nach dem Grundsatz *call them like you see them*. Diese unterteilte Einschätzung soll das Management hinsichtlich der Bewertung und der Frage der Dringlichkeit von möglichen Verbesserungen unterstützen.

Als Kriterien wurde für die technische Schadensschwere die 5 folgenden Schadenschwere-Klassen (SSK) gewählt und in den Fehlerbaum integriert:

- Kein
- Gering
- Mittel
- hoch
- sehr hoch

Den gesamten Fehlerbaum zeigen die Abb. 3.4 bis Abb. 3.9 . Der für den hier betrachteten Störfall im Fehlerbaum eingetretene Fehlerweg ist für eine einfachere Nachverfolgung durch blaue Elemente gekennzeichnet. Neben den klassischen Prozess Startpunkten werden, die für die aktuelle Fragestellung nicht relevante Seitenäste nur verkürzt als Basis-Elemente dargestellt.

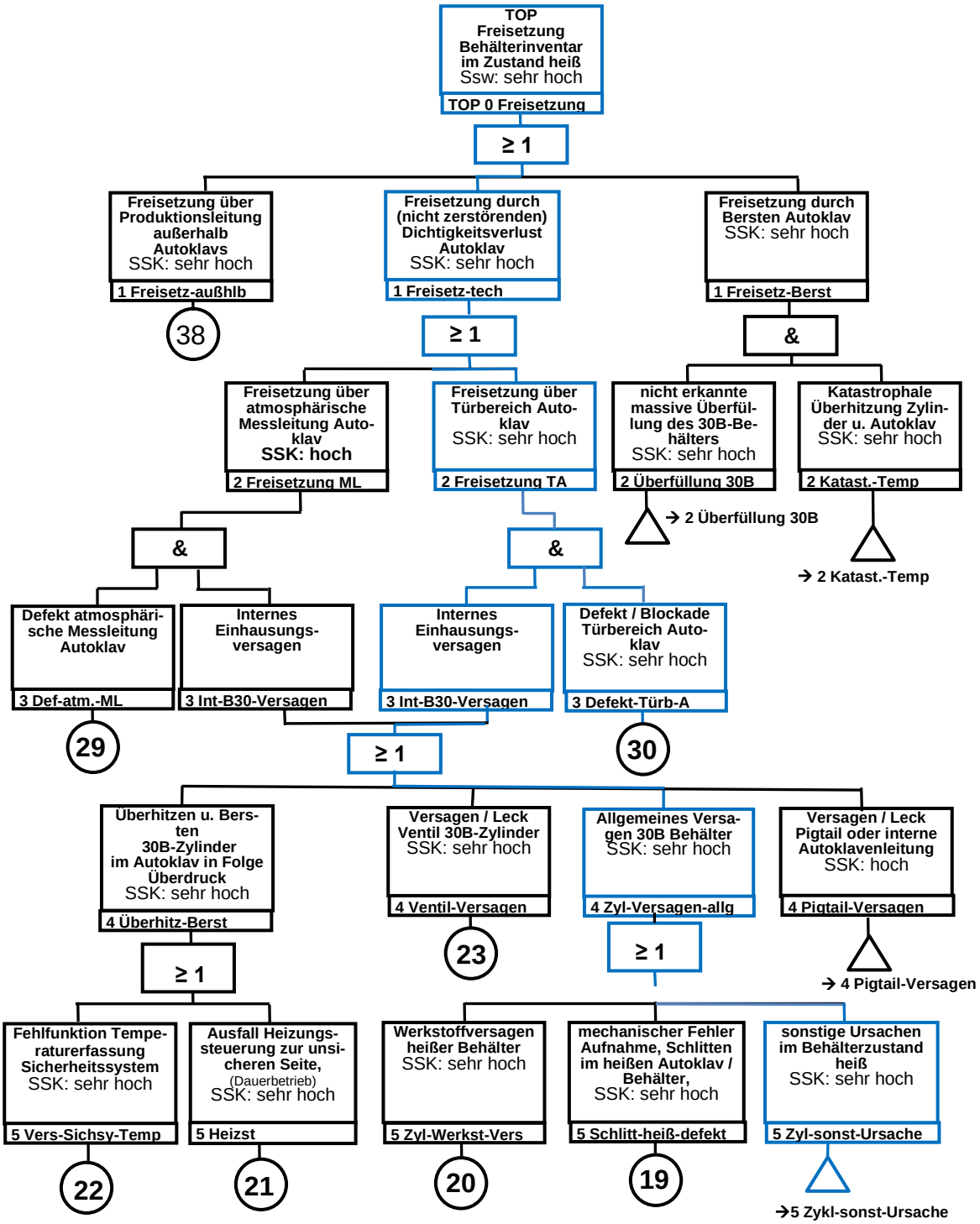

Abb. 3.4 Darstellung des Fehlerbaums, Teil 1

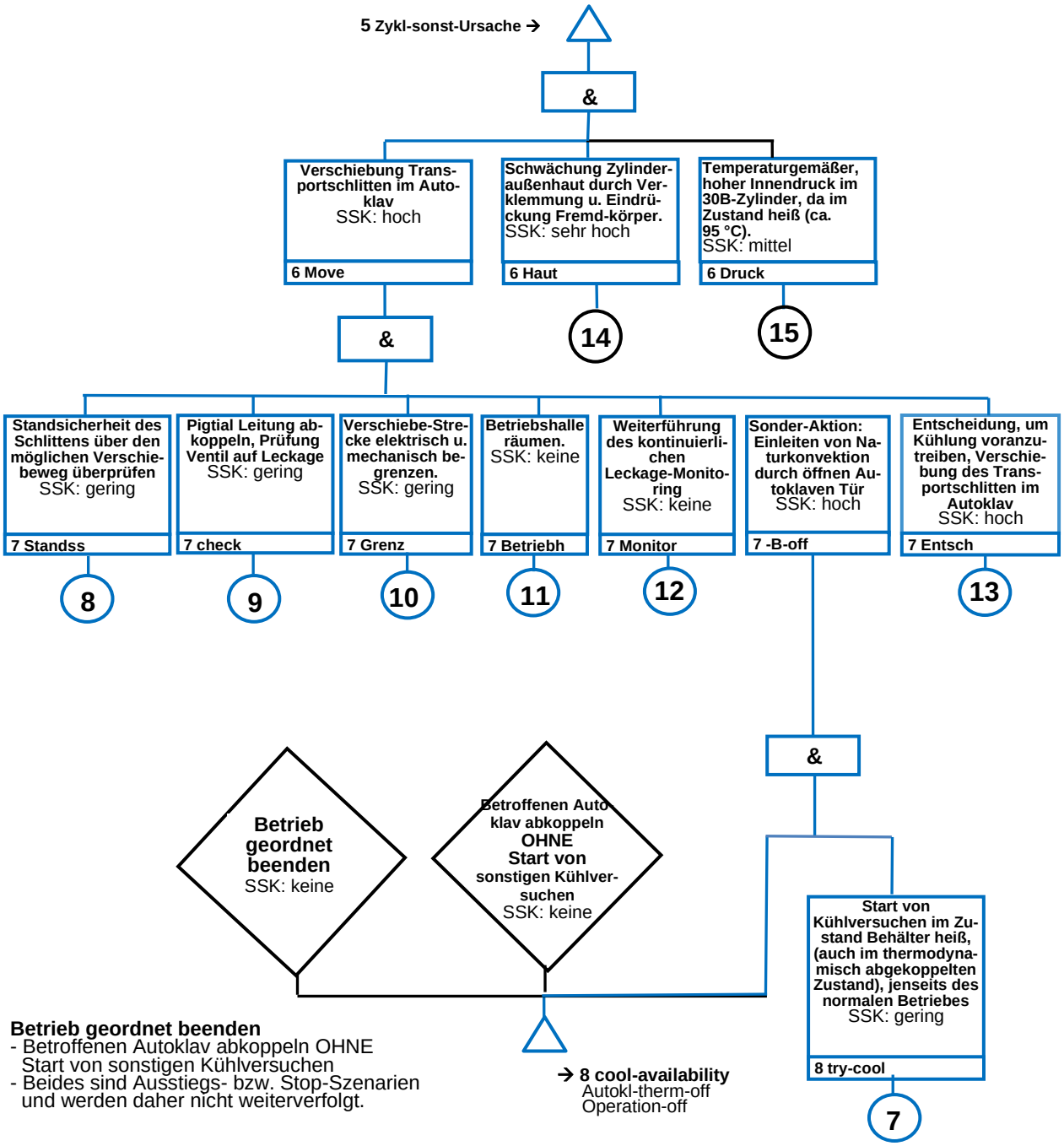

Abb. 3.5 Darstellung des Fehlerbaums, Teil 2: Fortsetzung mit Übergabepunkt *5 Zyl-sonst-Ursache*

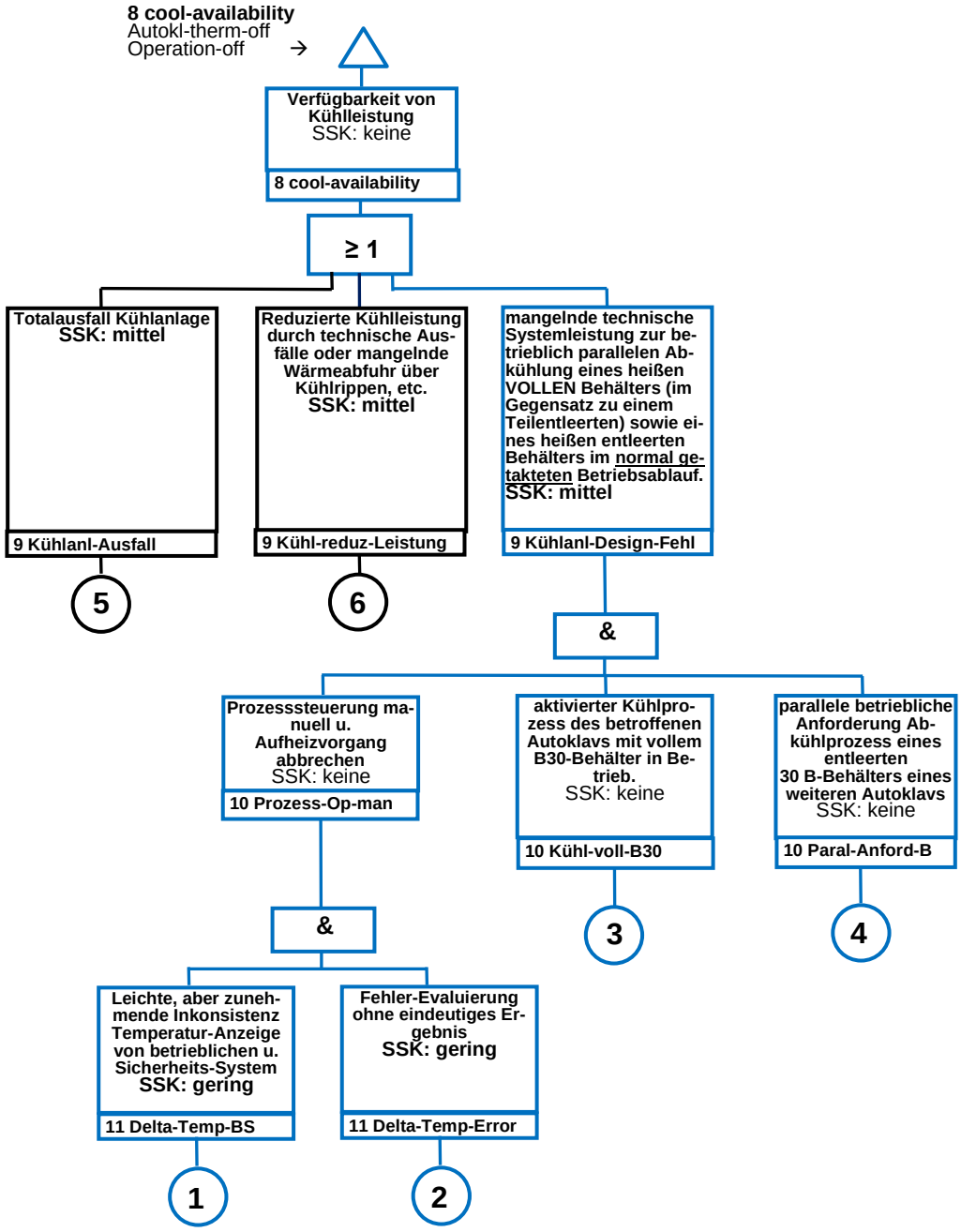

Abb. 3.6 Darstellung des Fehlerbaums, Teil 3: Fortsetzung mit Übergabepunkt *8 cool-availability*

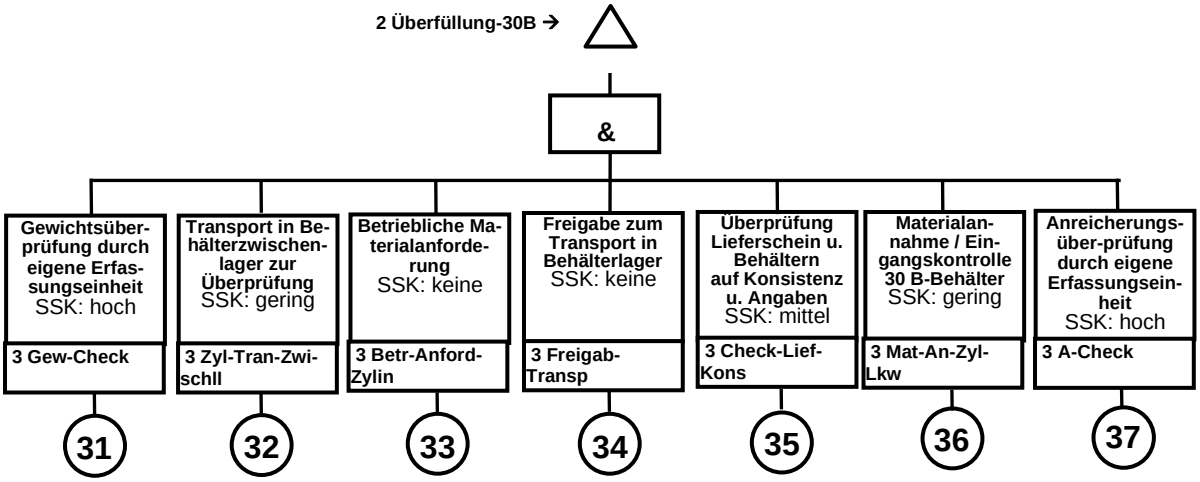

Abb. 3.7 Darstellung des Fehlerbaums, Teil 5: Fortsetzung mit Übergabepunkte *2 Überfüllung 30B*

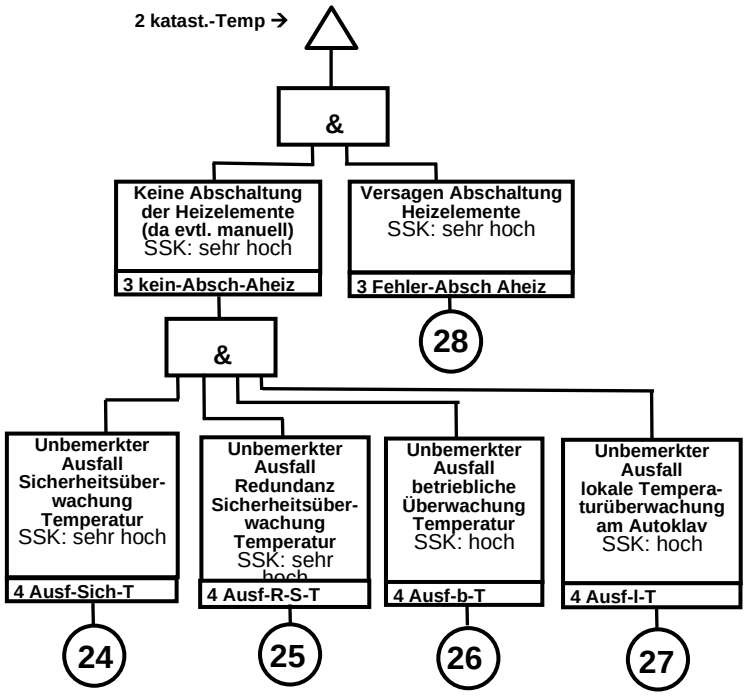

Abb. 3.8 Darstellung des Fehlerbaums, Teil 4: Fortsetzung mit Übergabepunkte *2 katast-Temperatur*

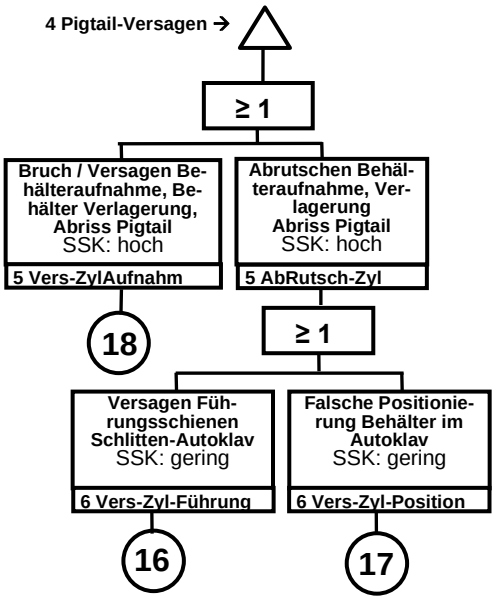

Abb. 3.9 Darstellung des Fehlerbaums, Teil 6: Fortsetzung mit Übergabepunkte 4 *Pigtail-Versagen*

Zur weiteren Auswertung des Fehlerbaums können sogenannte Minimalschnitte erstellt werden. Diese geben darüber Auskunft, wie viele Einzelereignisse auftreten müssen, um das TOP Ereignis des Fehlerbaums zu erreichen. In diesen Fall wurde bereits bei der Konstruktion des Beispiels ausgeführt, dass es die beiden administrativen Entscheidungen waren, den Autoklav zu öffnen (Wegfall einer Sicherheitsbarriere), sowie diesen zu rangieren. Somit liegt der Initialfehler im Bereich Human Error. Aus diesem Beispiel ist sicherheitstechnisch abzuleiten, dass aus systemtechnischer Sicht eine unumgehbare temperaturgesteuerte Entriegelungssperre am Autoklav fehlt.

Der Wegfall der Sicherheitsbarriere Autoklav durch eine Türöffnung im Zustand heiß, darf auch bei einer Umschaltung der Systemtechnik auf manuellen Betrieb nicht möglich sein. Solche Schwachstellen können bei einer HAZOP Untersuchung aufgedeckt und dann im Rahmen einer Verbesserung unterbunden werden, siehe Kapitel 3.3.5.

Wie in dem Fehlerbaum ersichtlich, setzt sich das *TOP*-Ereignis, d. h. *eine Freisetzung von UF_6* aus den mittels einer ODER-Funktion verknüpften 3 Ereignissen *Freisetzung über Produktionsleitung außerhalb des Autoklavs (1 Freisetz-außhlb)*, *Freisetzung durch (nicht zerstörenden) Dichtigkeitsverlust Autoklav (1 Freisetz-tech)*, sowie einer möglichen *Freisetzung durch das Bersten des Autoklavs (1 Freisetz-Berst)* zusammen.

Gemäß der technischen Schreibweise wird das ODER-Gatter durch eine Addition ausgedrückt.

0-TOP = 1 Freisetz-außhlb + 1 Freisetz-tech + 1 Freisetz-Berst (3.1)

Dabei ist hier der Fall einer Freisetzung über Produktionsleitung außerhalb des Autoklavs nicht Gegenstand der weiteren Betrachtung. Somit wurde dieser Fall als ein Basisereignis mit der Ordnungsnummer 38 definiert. Durch eine Umformulierung des grafischen Fehlerbaums in die technische Schreibweise, kann der gesamte Fehlerbaum durch entsprechende Gleichungssysteme dargestellt werden. Durch nachfolgendes, konsequentes Einsetzen der Gleichungen kann der Gesamte Baum auf die Kombination der Basis-Ereignisse zurückgeführt werden.

Bei entsprechenden Randbedingungen kann somit *1 Freisetz-außhlb* als Basisereignis Nr. 38, *1 Freisetz-tech* als die Verknüpfung der Summe der Basis-Ereignisse [16 + 17 + 18 + 19 + 20 +21 + 22 +23 + (8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 * (1 * 2 * 3 * 4 *7 + 5*7 + 6*7))] * (29 + 30) und *1 Freisetz-Berst* als Multiplikations-Verknüpfung von 24 * 25 * 26 * 27 * 28 * 31 * 32 * 33 * 34 * 35 * 36 *37 aufgelöst werden. Durch weitere Anwendung von Wahrscheinlichkeiten der Basis-Ereignisse kann somit die Gesamtwahrscheinlichkeit des Eintretens von *0-TOP* bestimmt werden.

Der Term von *1 Freisetz-Berst* ist ein reiner Multiplikationsterm. Wenn ein Ereignis nicht eintritt, d. h. mit einem Wert Null abgebildet wird, ist auch die Gesamteintrittswahrscheinlichkeit Null. Der Term von *1 Freisetz-tech* besteht letztendlich aus 8 mittels ODER-Gatter verknüpften Einzeltermen. Der Eintritt eines dieser Szenarien würde somit *0-TOP* bedingen. Für eine erleichterte Betrachtung bzw. weitergehende Bewertung werden oft Ereignisse zu Gruppen oder Modulen zusammengefasst, wie das im Folgenden für *1 Freisetz-tech* exemplarisch gezeigt werden soll.

1 Freisetz-tech = (16 + 17 + 18 + 19 + 20 +21 + 22 +23) ***29** +
(16 + 17 + 18 + 19 + 20 +21 + 22 +23) ***30**+
1 * 2 * 3 * 4 *7 *8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 ***29** +
1 * 2 * 3 * 4 *7 *8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 ***30** +
5 * 7 * 8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 * **29** +
5 * 7 * 8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 * **30** +

6 * 7 * 8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 * **29** +
6 * 7 * 8 * 9 * 10 * 11 * 12 * 13 * 14 * 15 * **30**

Hier wird erkenntlich, dass sich identische und oft wiederholende Elemente zur vereinfachten Darstellung anbieten. Insbesondere sind die beiden Basis-Ereignisse 29 und 30 zentral vertreten. Basis-Ereignis 29 beschreibt den Defekt der atmosphärischen Messleitung in den Autoklav, also eine konstruktiv nicht vermeidbare Durchführung durch die Autoklaven-Umschließung. Basis-Ereignis 30, der Defekt bzw. Blockade der offenen Tür bzw. Türbereich des Autoklavs ist, wie in der Szenario-Beschreibung ausgeführt, die absichtliche und aktive Aufgabe einer Sicherheitsbarriere im Behälterzustand heiß. Somit wurde dies auch über die Darstellung innerhalb des Fehlerbaums deutlich, was bereits beim Aufbau des Szenarios klar war.

Die dritte Möglichkeit einer Freisetzung im Behälterzustand heiß ist *1 Freisetz-Berst*. Dazu wurde weiter oben bereits ausgeführt, dass bedingt durch die Vielzahl der UND Verknüpfungen (Multiplikation) der Zustand bzw. Prozess, als sehr robust einzuschätzen ist.

3.3.5 HAZOP-Analyse

Bei der HAZOP-Systemanalyse (Hazard and Operability) handelt es sich um eine Technik der Risiko- und Funktions-Problemidentifizierung (siehe /GRS 19/). Die Zielsetzung dabei ist, bei eintretenden Abweichungen die daraus folgenden Auswirkungen zu erfassen. Operativ soll dies durch ein systematisches Hinterfragen möglicher Abweichungen erfolgen, die von nicht planmäßigen Abläufen von Einzel- oder Untersystemen bedingt werden können. Die für ursprünglich kontinuierliche Prozesse entwickelte Technik wird heutzutage auch auf die verschiedensten Formen von diskontinuierlichen Prozessen angewendet. Die Vorgehensweise ist dabei auch normentechnisch in der IEC-61882, 2016 /DEU 16/ beschrieben. Wie bei den meisten Analyse-Methoden wird auch hier, als Erweiterung der Analyse zunehmend versucht, konsequent eine gewisse Quantifizierung mit in die Betrachtung mit aufzunehmen. Dies geschieht in der Regel durch die Hinzunahme von einfachen Klassifizierungsworten vordefinierter Risikostufen. Damit soll je nach Anwendungsfall, z. B. nach erwarteter Häufigkeit oder nach der Schwere, von nicht gewünscht eintretenden Ereignissen klassifiziert werden können. Dies ist besonders für den aus den Analyseergebnissen ableitbaren Handlungsbedarf wichtig, z. B. im Rahmen der Selektion von umzusetzenden Risikominimierungsmaßnahmen.

Mit der HAZOP-Methodik können Analysen möglicher Gefahren zu unterschiedlichsten Systemlebens- bzw. Zyklusphasen durchgeführt werden. Ein weiterer Vorteil der HAZOP-Analyse ist, dass diese einen weitaus höheren Detaillierungsgrad im Vergleich zu der What-If-Analyse bietet.

Gemäß der Norm IEC 61882 soll der Ablauf in die vier folgenden Aufgabenblöcke strukturiert werden:

- Planung mit den notwendigen Festlegungen
- Vorbereitungen
- Untersuchungen
- Dokumentation, Ergebnisbewertung und Folgeaktivitäten

Das Thema Untersuchungen beinhaltet die eigentlichen Analysen und beginnt damit, zunächst eine Unterteilung des Systems z. B. in Subsysteme vorzunehmen. Die Auswahl bzw. Unterteilung kann dabei nach operativen sequenziellen Systemteilen oder nach logischen Funktionsblöcken vorgenommen werden. Dabei ist es wichtig, die Unterteilung nach deren Zweck bzw. Ziel vorzunehmen, um nachfolgend eine möglichst zielgenaue Identifizierung von Abweichungen mittels der Frage- und Leitwörter, Bestimmung deren Ursachen und Folgen, sowie Festlegung von Maßnahmen und Aktionen vornehmen zu können.

Im Arbeitsblock Dokumentation und Folgeaktivitäten werden die Ergebnisse aufgezeichnet, Aktionen nachverfolgt, Nachuntersuchungen durchgeführt, sowie der Abschlussbericht erstellt. In diesem Themenblock ist auch die Dokumentation und Aufbereitung der bereits weiter oben beschriebenen, und aktuell für die Managementbewertung zunehmend relevanten Bewertungskriterien integriert. Dies kann, je nach Größe des Projektes, von einer visuellen Hervorhebung der Risiko-Bewertungsworte bis hin zu kompakten Neuzusammenstellungscharts aller erkannten hohen oder höchsten Risikostufen erfolgen.

Die Qualität der Ergebnisse hängen maßgebend von der Treffgenauigkeit der vorbereiteten Frageworte, und somit auch vom Erfahrungsschatz des durchführenden Teams ab. Der Detaillierungsgrad der Unterteilung des Systems in Subsysteme oder Funktionsblöcke ist dabei abhängig von der gewünschten Betrachtungstiefe. Diese ist in der Regel selbst wiederum eine Funktion des erwarteten Risikos. Das Ergebnis sind die, mit den

Fragen eruierten Parameterabweichungen vom Soll- bzw. Erwartungswert. Diese sollen möglichst alle denkbaren Abweichungen umfassen. Im Bedarfsfall können weitere, über die Norm hinausgehende Leitworte eigenständig definiert werden. Wichtig dabei ist, dass die Leitworte in ihrer Eigenschaft eindeutig festgelegt und entsprechend dokumentiert werden, damit alle Beteiligten das gleiche Verständnis für die Leitworte entwickeln. Beispielhaft zeigt die nachfolgende Tab. 3.3 typische Frage, bzw. Leitworte mit ihren zugehörigen Erklärungen.

Tab. 3.3 Typische Frage / Leitworte der HAZOP-Analyse

Frage, bzw. Leitworte	**Erklärung**
nein, nicht, kein	Sollverhalten tritt nicht ein
falsch	allgemein nicht vorgesehene Größe
mehr	qualitativer Zuwachs der Größe, zu viel
weniger	qualitative Abnahme der Größe, zu wenig
sowohl als auch	zusätzliche Ereignisse zum Soll-Verhalten
teilweise	Soll-Verhalten nur unvollständig erreicht
Umkehrung	gegenteiliges Verhalten zur Soll-Funktion
anders als	etwas anderes als das Soll-Verhalten
Ausfall	undefiniertes Verhalten
früher	Soll-Verhalten tritt zu früherem Zeitpunkt ein
später	Soll-Verhalten tritt zu späterem Zeitpunkt ein
zuvor/danach	Soll-Verhalten in anderer Reihenfolge
schneller	nicht erwarteter Anstieg der Ablauf-/Ausführungsgeschwindigkeit
langsamer	nicht erwartete Abnahme der Ablauf-/Ausführungsgeschwindigkeit

Allgemein ist dabei nochmals betont, dass es sich neben den formalisierbaren Fragewörten und der systematischen Abarbeitung der System- bzw. Prozesseigenschaften um einen kreativen Prozess handelt, dessen Erkenntnisgewinn auch von den Erfahrungen der beteiligten Spezialisten abhängt.

Zur Optimierung der Ergebnisse der Analysen werden diese typischerweise in system- oder prozessspezifischen Tabellen zusammengefasst. Diese Tabellen enthalten neben einer Spalte für die Ordnungsnummer auch Spalten für die Leitworte, die Abweichung z. B. auf Parameterebene, die möglichen Ursachen, und die sich speziell für die einzelnen selektiv genannten Parameterabweichungen ergebenden Auswirkungen. Dem folgt die damit verbundene Risikostufe und die Eintrittshäufigkeit (beides gemäß: call them

like you see them), die Art und die Maßnahmen, die das Risiko minimieren, mögliche Verifikationen der Maßnahmen, die daraus resultierende Risikostufe und die zu erwartende Häufigkeit.

Bei der Anzahl der in der Methodik zu benutzenden Risikostufen und Häufigkeiten muss zwischen einer ausreichenden Auflösung und einer mit ihrer Anzahl zunehmenden Komplexität abgewogen werden. Die Anzahl soll so gewählt werden, dass das Aufspüren von Schwachstellen sicher gewährleistet wird. Für weitere Detailfragen können im Anschluss die als auffällig selektierten Systeme einer weiteren separaten Analyse unterzogen werden.

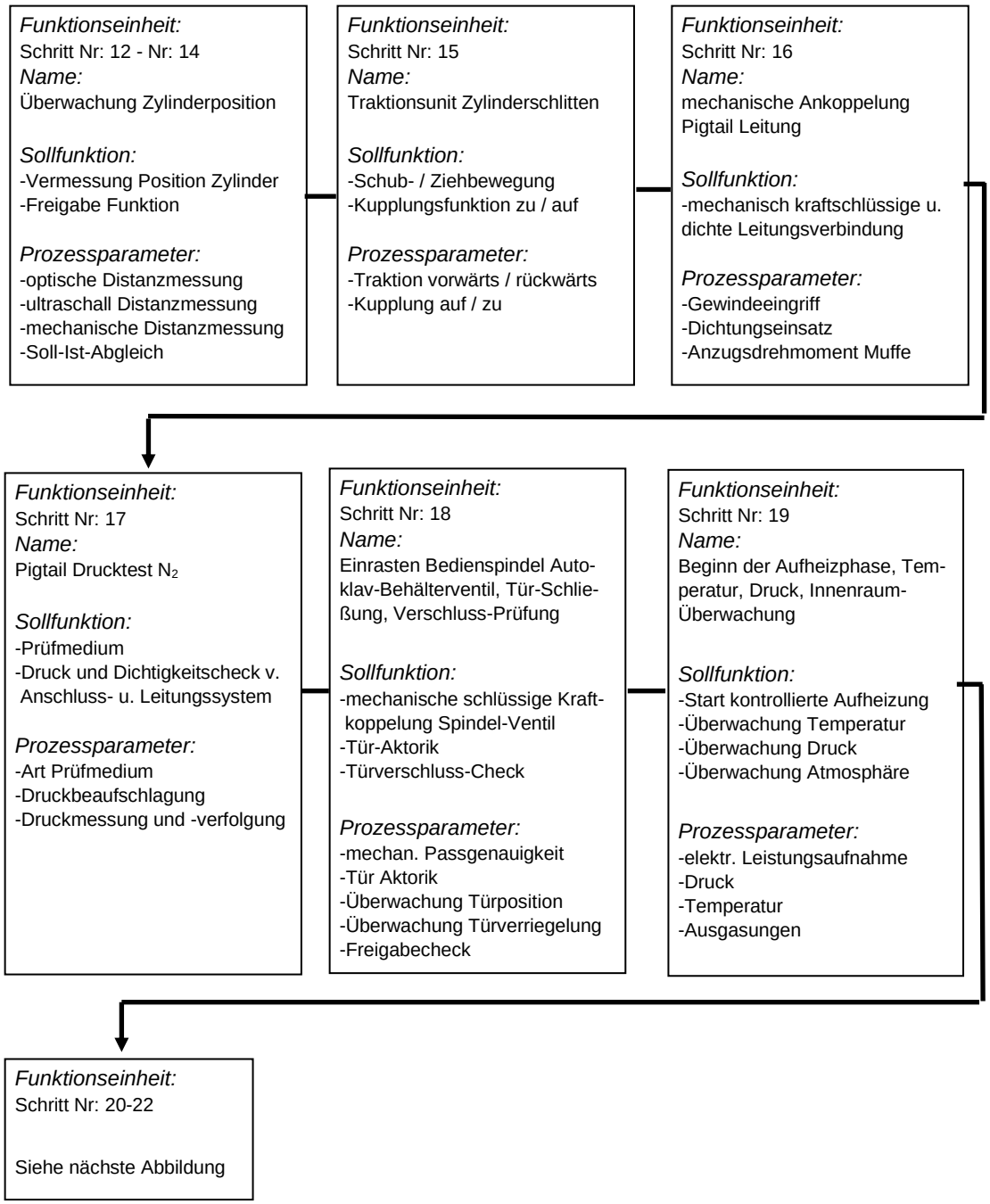

Abb. 3.10 Prozessuntergliederung in Funktionseinheiten Schritt 12 bis 19 aus dem Flussdiagramm Tab. 3.1

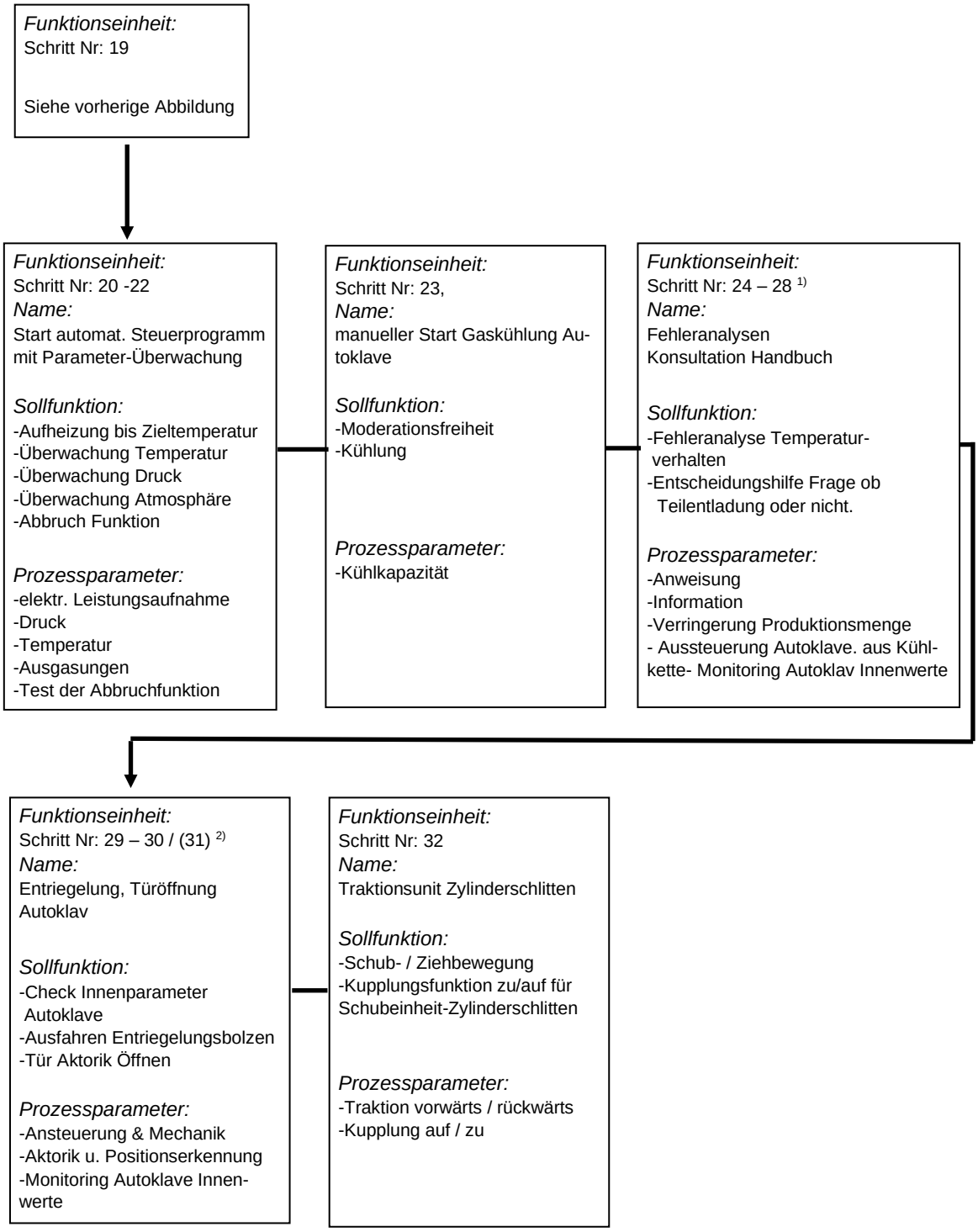

Abb. 3.11 Prozessuntergliederung in Funktionseinheiten Schritt 20 bis 32 aus dem Flussdiagramm Tab. 3.1

Details zu 1) (Schritt 24 – 28), und Schritt 2) (29 – 30 / (31)), siehe nächste Seite.

[1] Details zu Schritt 24 – 28:
Schritt 24 bis 28, also die durchgeführte Fehleranalyse zum Temperaturverhalten sowie die Behandlung der Frage, ob es sich um eine Behälter-Teilentladung handelt, ist in dem hier gewählten Beispiel tendenziell eine systemexterne Aktivität, bzw. Bewertung. Da dies allerdings, mangels einer technischen Verriegelung des Autoklavs gegen Öffnen, den entscheidenden Beitrag zum weiteren Verlauf ergab, wurden diese in die Betrachtung aufgenommen.

[2] Details zu Schritt 29 – 30 / (31):
Bei Schritt 29 bis 31 sind neben dem systemtechnischen Ablauf, der ein Teil der originären Systembetrachtungen ist, administrative Komponenten vorhanden, die als Systemtechnik eher Richtung Betriebsanweisungen, bzw. System-Handhabung gehen.

Als Kriterien für das Risiko werden fünf Risikostufen angesetzt, d.h. von keinem Risiko bis sehr hohes Risiko. Diese werden in die Analyse-Fragetabelle integriert:

- kein
- gering
- mittel
- hoch
- sehr hoch

In gleicher Art und Weise werden für die unterstellte Schadenshäufigkeit vier Klassen von sehr selten bis oft für die Analyse-Fragetabellen festgelegt:

- sehr selten
- selten
- mittel
- oft

Auch wenn ein Punkt mit einer Eintrittswahrscheinlichkeit *sehr selten* klassifiziert wurde, heißt das nicht, dass hier nicht durchaus noch Maßnahmen zur weiteren Verhinderung des Eintretens des Ereignisses möglich oder sinnvoll sind. So wurden bei einigen der

Betrachtungen, trotz einer Eintrittswahrscheinlichkeit *sehr selten*, weitere Maßnahmen vorgeschlagen, um die Eintrittswahrscheinlichkeit oder die Auswirkung des Ereignisses zu reduzieren. Diese Vorgehensweise der Verwendung von nur einer begrenzten Anzahl von Stufen wird in der Regel angewendet, um den Vorteil einer übersichtlichen Klassifizierung beizubehalten, d. h. ein einfaches und klares Bild zu liefern.

Wie in der Einleitung zum Thema HAZOP ausgeführt, handelt es sich bei dieser Technik um eine Risiko- und Funktions-Problemidentifizierung. Sie basiert auf dem Einsatz von standardisierten Frageworten zu den einzelnen Prozessschritten, um die Risiken und Funktionen möglichst umfangreich zu hinterfragen und mit entsprechenden Tabellen zu dokumentieren. Diese sehr umfangreiche und detaillierte Betrachtung ergab z. B. auch die beiden Punkte der Prüfung, dass sowohl der Einfahr- als auch der Ausfahrraum des Zylinders bezüglich des Autoklavs frei von Objekten jeglicher Art ist, als einen unbedingt zu betrachtenden Punkt, wie in den nachfolgenden Tabellen ersichtlich wird. Im Detail soll mit dieser Betrachtung ausgeschlossen werden, dass Fremdkörper das Ein- und Ausfahren des Zylinders in den Autoklav behindern bzw. prinzipiell fremde Gegenstände vorhanden sind, die als Schadensverursacher auftreten könnten. Die dabei unterstellte Schadenspalette reicht von Marginalien über mögliche Schäden an wesentlichen Einrichtungen, wie z. B. der Pigtail-Anschlussleitung bzw. dem UF_6-Leitungssystem, bis zu Beschädigungen des Autoklave-Innenraums im Allgemeinen bzw. des UF_6-Zylinders selbst. Daher wird als Risikoreduzierung vor jeder einzuleitenden Bewegung des UF_6-Zylinders, bzw. vor Bewegung des Transportschlittens, die Abwesenheit von störenden Objekten in dessen Bewegungsraum gefordert. Genau diese fehlende, infolge aber detailliert vorzunehmende Überprüfung, wurde hier zum Schadensauslöser.

Subjektiv kann zwar eine Überprüfung der Abwesenheit von störenden Objekten beim Ausfahren von entleerten Behältern als überzogen gesehen werden, dabei eintretende Schäden an der installierten Technik sind jedoch mit Sicherheit nur mit größerem Aufwand zu beheben, als dies z. B. entsprechende 100-Prozent Sichtprüfungen ausmachen. Um den operativen Aufwand für die Betriebsmannschaft zu begrenzen, wären u. a. auch vorinstallierte Kameras mit einem Standardprocedere denkbar.

Die betrachteten Analysetabellen der HAZOP-Analyse beginnen mit der Positionierung des 30B-Zylinders vor dem Einfahren in den Autoklav, Schritt 12 im Flussdiagramm Tab. 3.1 aus Kapitel 3.3.1.

Die in diesem Kapitel angewendete Systematik wird anhand des ersten, mittels Leitwort-Abfrage betrachteten Schritts betrachtet, der Positionierung vor und während des folgenden Einfahrens des 30B-Zylinders in den Autoklav. Exemplarisch erfolgt zunächst für die ersten Schritte eine Darstellung der Ermittlung der Einträge der Tabelle. Die Sollfunktion basiert auf optischen, Ultraschall- sowie mechanischen Distanzmessungen, wobei ein Soll-Ist Zielabgleich durch das System mit dem Funktionsnamen *Überwachung Zylinderposition* zu erfolgen hat. Dabei liegt der Fokus auf dem Messignal als allgemeine Größe. Als Möglichkeiten wurden dafür die drei Szenarien *kein Messsignal*, *falsches Messsignal*, sowie *Ausfall Messsignal* (im allgemeinsten Sinn als undefiniertes Verhalten) aus der Fragewortliste ausgewählt.

Die Parameterabweichung *kein Messsignal* wird z. B. auf einen sehr punktuellen Ausfall der Stromversorgung des Messsystems zurückgeführt. Die Auswirkung äußert sich darin, dass kein Messsignal, bzw. keine Positionsangabe vorhanden ist. Da dieser Fall durch das Auswertesystem eindeutig erkennbar ist, wird die daraus resultierende Risikostufe für eine solche Fehlfunktion als gering eingeschätzt. Basierend auf der eingesetzten Technikart und in der Anlage gesammelter Erfahrungswerte, wird die Häufigkeit als sehr selten eingeschätzt. Als Maßnahme, die das Risiko weiter reduzieren kann, wurde angeregt, dass nicht nur der Prozess wie im ursprünglichen Design vorgesehen stehen bleibt, sondern die Auslösung eines aktiven Stop-Prozesses abgesetzt und signalisiert wird. Da man sich bereits in den beiden untersten Klassen, d. h. Risikostufe gering und Häufigkeit sehr selten bewegt, soll hier, gemäß *call them like you see them*, auch keine weitere Veränderung stattfinden. Nicht jede Maßnahme, die das Risko vermindert, wird sich sofort in einer Veränderung der Risikostufe auswirken. Ähnliches gilt für die diskretisierte Häufigkeit.

Die nächste denkbare Parameterabweichung *Random Signal* kann auf einem Teilausfall des Sensors oder der Signalaufbereitungseinheit basieren. Die Auswirkung wäre eine falsche Positionsangabe und damit eine weitaus komplexere Situation für die Selbstüberwachung der eingesetzten Technik gegenüber dem Fall *kein Messsignal*. Daher erfolgte die Zuordnung der Risikostufe *mittel* und durch die Einschätzung der eingesetzten Technik mit einer konservativ angesetzten Häufigkeit von *mittel*. Als Abhilfemaßnahme werden diversitäre und redundante Signalverknüpfungen und Plausibilitätschecks der Messgrößen untereinander vorgeschlagen. Diese Maßnahme, verknüpft mit einem dezidierten Steuersignal *stopp Prozess* bei Abweichungen, minimiert das Risiko. Durch

diese Verbesserungen wird das Risiko einer falschen Positionierung *gering* eingeschätzt, bei einer effektiv eintretenden Häufigkeit von nur *sehr selten*.

In analoger Weise wird die Parameterabweichung *falsches Signal* durch einen Defekt, bzw. durch eine mögliche Verschmutzung betrachtet. Dabei wird eine Risikostufe *mittel* bei einer Häufigkeit *selten* angesetzt. Die wie oben bereits ausgeführten Maßnahmen zur Verringerung des Risikos einer falschen Positionierung werden vom Analysten als besonders wirkungsvoll eingeschätzt. Daher wird das Risiko auch für diesen Fall bei einer falschen Positionierung als *sehr gering* und *sehr selten* eingeordnet.

Abschließend wird noch das Leitfragewort *Ausfall* abgefragt, im Sinne eines undefinierten Verhaltens des Messsignals. Durch die bereits oben ausgeführten Maßnahmen, die das Risiko minimieren, wird die Risikostufe einer falschen Positionierung (bzw. die noch übrigbleibende mögliche Auswirkung) neu als *gering* eingestuft, bei einer gleich gebliebenen Häufigkeit von *sehr selten*.

Bei jeder dieser Betrachtungen handelt es sich um ein eigenes Szenario, mit einer individuellen Risikostufe. Nach diesem Muster werden die Tabellen Tab. 3.4 bis Tab. 3.14 für die einzelnen Schritte des Prozessablaufs erstellt.

Tab. 3.4 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 12-14

Funktionsname: Überwachung Zylinderposition

Sollfunktion: optische-, Ultraschall-, mechanische-Distanzmessung, Soll-Ist-Ziel-Abgleich

Überwachung Zylinderposition											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko minimiert**	**Verifikation der Maß-nahme**	**Resultie-rende Risikostufe**	**Resultieren-de Häufigkeit**
optische-, Ultraschall-, mechanische-Distanzmessung											
1-1	kein	Messsignal	keine lokale Stromversor-gung	keine Positions-angabe	gering	sehr selten	elektrisch	Auslösung eines aktiven Stop-Pro-zesses	---	gering	sehr selten
1-2			Ausfall	falsche Position	mittel	mittel	physikalisch	diversitäre & redundante Signaverknüpfung, Plausibilitätscheck	---	gering	sehr selten
2-1	falsch		Defekt, Verschmutzung	falsche Position	mittel	selten	physikalisch		---	sehr gering	sehr selten
3-1	Ausfall		Defekt, Verschmutzung	falsche Position	mittel	selten	physikalisch		---	gering	sehr selten
Soll-Ist-Ziel-Abgleich											
4-1	kein	Messsignal	Elektronik Defekt	keine Position	mittel	selten	elektrisch		---	sehr gering	sehr selten
4-2				falsche Position	mittel	selten		Redundanz	---	sehr gering	sehr selten
5-1	Ausfall			mittel	mittel	selten		Redundanz	---	sehr gering	sehr selten

Tab. 3.5 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 15

Funktionsname: Traktionsunit Zylinderschlitten

Sollfunktion: Schub- / Ziehbewegung, Kupplungsfunktion zu / auf

Traktionsunit Zylinderschlitten											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko minimiert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Schub- / Ziehbewegung											
1-1	keine	Traktion Schub-/Ziehbewe-gung	keine lokale Stromversor-gung	keine Traktion	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1-2			Defekt Antrieb	keine Traktion	gering	selten	elektrisch / mechanisch	keine	---	gering	selten
2-1	Um-keh-rung		falscher Steuerbefehl	falsche Richtung Rammgefahr im Traktionsbereich	sehr hoch	selten	physikalisch	diversitäre, zusätzli-che Richtungser-kennung, Prellbock in Rich-tung Einfahrt mit zus. Lichtschranke	täglicher Test	sehr hoch	sehr selten
Kupplungsfunktion (zu / auf)											
3-1	nein	Kupplungs-funktion zu / auf	Elektronik Defekt, mechanischer Defekt	kein Einkuppeln	gering	selten	elektrisch / mechanisch	Logische Verknüp-fung Änderung Kupplungszustand, Position und Trakti-onsrichtung	---	gering	selten
3-2				kein Auskuppeln	mittel	selten			---	mittel	sehr selten
4-1	Um-keh-rung			gegenteilige Funktion	mittel	selten			---	mittel	sehr selten

Tab. 3.6 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 16

Funktionsname: Ankoppelung Pigtail Leitung

Sollfunktion: mechanisch kraftschlüssige und dichte Leitungsverbindung

Ankoppelung Pigtail Leitung											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
mechanisch kraftschlüssige und dichte Leitungsverbindung											
1-1	keine	Gewinde-eingriff Überwurf-mutter	kaputtes Ge-winde zylinderseitig	kein Anschluss	gering	selten	mechanisch	keine	---	gering	selten
1-2			kaputtes Ge-winde leitungsseitig	kein Anschluss	gering	selten	mechanisch	keine	---	gering	selten
1-3			Fremdkörper /falsche Dich-tung	kein Anschluss	gering	selten	mechanisch	keine	---	gering	selten
2-1	kein	Dichtungs-einsatz	human error	Nachgeschaltete Dichtheitsprü-fung unzu-reichend	gering	selten	mechanisch	Nur eine Art von Dichtung in der tool-box vorhalten	---	gering	selten
3-1	weni-ger	Anzugs-drehmo-ment Muffe	Verbindung un-dicht	Leckage	gering	selten	mechanisch	Drehmoment-schlüssel verwen-den	---	gering	selten
4-1	mehr		Gewinde ge-schädigt	Gewinde ge-schädigt	mittel	selten			---	mittel	selten

Tab. 3.7 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 17

Funktionsname: Pigtail N_2 Drucktest

Sollfunktion: Prüfmedium, Druck u. Dichtigkeitscheck von Anschluss- u. Leitungssystem, N_2 Inertisierung

Pigtail N_2 Drucktest											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Ri-sikostufe**	**Resultie-rende Häufigkeit**
Prüfmedium											
1-1	kein	Gas Art und Feuchte	falsche Gas Art und hohe Feuchte	Reaktion von UF_6 mit Feuch-teanteil	mittel	sehr selten	physikalisch	fest installierte Versorgung, vor-gelagerte zentrale Prüfung	administrativ	gering	sehr selten
Druck u. Dichtigkeitscheck von Anschluss- u. Leitungssystem											
2-1	keine	Druckbe-aufschla-gung	defektes Ein-speisesystem	kein Druckauf-bau, kein Test-beginn	gering	sehr selten	physikalisch	keine	---	gering	sehr selten
2-2			selektiv ge-schlossenes Re-gelstrecke	kein Druckauf-bau, kein Test-beginn	gering	sehr selten	physikalisch	keine	---	gering	sehr selten
3-1	mehr	Druckbe-aufschla-gung	Infrastruktur falsch konfigu-riert	im Extremfall Berstgefahr Lei-tung	gering	sehr selten	physikalisch	Drucksicherheits-ventil versor-gungsseitig		gering	sehr selten

Pigtail N_2 Drucktest											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Ri-sikostufe**	**Resultie-rende Häufigkeit**
Druckmessung / Druckverfolgung auf Konstanz											
4-1	kein	Druckmes-sung	Ausfall Mess-kette	Abbruch	gering	sehr selten	physikalisch	keine	---	gering	sehr selten
5-1	anders als	unplau-sible Werte (spez. beim Start Messung)	Defekt / Teilde-fekt Messkette	Abbruch	gering	sehr selten	physikalisch	keine	---	gering	sehr selten
6-1	kein	Druck-konstanz	Leckage an Be-hälterankoppe-lung oder Lei-tungssystem	Austritt von UF_6 aus Behälter / Leitung in Auto-klaven (als zweite Barriere)	mittel	sehr selten	physikalisch	kontinuierliche Prüfung Atmo-sphäre im Auto-klav	Analysetech-nik werktäglich prüfen	gering	sehr selten
N_2 Inertisierung											
7-1	anders als	Inertisie-rung Gas Art an Messstel-len	falsches Gas, unzureichende Spülung	Wiederholung oder Abbruch bis OK	gering	sehr selten	physikalisch	Optimierung Messtechnik	---	gering	sehr selten

Tab. 3.8 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 18

Funktionsname: Einrasten Bedienspindel Autoklav-Behälterventil, Tür Schließung, Verschluss-Prüfung

Sollfunktion: mechanisch schlüssig Kraftkoppelung Spindel-Behälterventil, Tür-Aktorik, Türverschluss-Check

Einrasten Bedienspindel Autoklav-Behälterventil, Tür Schließung, Verschluss-Prüfung											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
mechanisch schlüssig Kraftkoppelung Spindel-Behälterventil											
1-1	kein	mechani-sche Pass-genauig-keit	falscher Spin-deleinsatz, fal-sches Behälter-ventil, verbogene Kom-ponenten	Kein Eingriff, Verbiegung, bis maximal Abriss Behälterventil	hoch	sehr selten	mechanisch	Spindeleinsatz nicht veränderbar, Sichtprüfung Be-hälterventil auf richtigen Typ und Integrität.	---	hoch	sehr selten
Tür Aktorik											
2-1	keine	Tür Aktorik schließen	Keine lokale Stromversor-gung, Antrieb defekt	Prozess stoppt, keine Auswir-kung	gering	sehr selten	physikalisch	keine	---	gering	sehr selten
2-2			mechanische Verklemmung	Prozess stoppt, keine Auswir-kung	gering	sehr selten	mechanisch	keine	---	gering	sehr selten

Einrasten Bedienspindel Autoklav-Behälterventil, Tür Schließung, Verschluss-Prüfung											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Türverschluss-Check											
3-1	keine	Verriege-lungsfunk-tion Tür	kein Antrieb, Bolzen verbo-gen, Fremdkör-per im Sackloch	Prozess stoppt, keine Auswir-kung	gering	sehr selten	mechanisch	keine	---	gering	sehr selten
4-1	keine	automati-sierte Ver-schluss-Prüfung	Positions-End-schalter ausge-fallen	Prozess stoppt, keine Auswir-kung	gering	sehr selten	physikalisch	keine	---	gering	sehr selten
5-1	keine	human op-tical check	Nicht durchgeführt	Prozesskette geht weiter, möglicher Ver-lust 2-te Sicher-heitsbarriere	hoch	sehr selten	human	abgezeichnete Checkliste zur Fortsetzung Pro-zess nötig	durch Schicht-leiter	hoch	sehr selten

Tab. 3.9 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 19

Funktionsname: Start Aufheizphase, Temperatur, Druck, Innenraum-Überwachung

Sollfunktion: Start Aufheizphase, Überwachung Temperatur, Druck, atmosphärische Prozessparameter

kontrolliertes Aufheizen bis Zieltemperatur, Überwachung Temperatur, Druck, atmosphärische Prozessparameter											
Nr.:	**Leitwort**	**Abweichung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risikostufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko minimiert**	**Verifikation der Maßnahme**	**Resultierende Risikostufe**	**Resultierende Häufigkeit**
Start Aufheizphase											
1-1	kein	Start Aufheizphase	Ausfall Energieversorgung	keine Erhitzung	hoch	sehr selten	mechanisch			hoch	sehr selten
1-2			Komplettausfall des elektr. Heizkreises	keine Erhitzung	gering	sehr selten	physikalisch			gering	sehr selten
1-3			Ausfall Soll/Ist Vergleichs oder sonst. Selbstüberwachung	potenzielle Gefahr Überhitzung	sehr hoch	sehr selten	elektrisch / physikalisch	Redundanz, Abgleich Sicherheitssystem mit betrieblichem System, Überwachung durch Wartenpersonal	Sammlung Erfahrungswerte und Nachbesserung	sehr hoch	sehr selten
2-1	weniger		Ausfall einzelner Heizschlangen	zu langsame Erhitzung	gering	sehr selten	mechanisch			gering	sehr selten
3-1	mehr		Steuerungs- / Leittechnikprobleme	Gefahr Überhitzung	sehr hoch	sehr selten	physikalisch	Integration gemessene Wärmemenge und deren Begrenzung nach Menge und Zeit	kontinuierlicher Check	sehr hoch	sehr selten

kontrolliertes Aufheizen bis Zieltemperatur, Überwachung Temperatur, Druck, atmosphärische Prozessparameter											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Ri-sikostufe**	**Resultierend Häufigkeit**
Überwachung Druck, atmosphärische Prozessparameter (Gas Art)											
4-1	keine	Druck Atmosphä-renart	Ausfall Mess-technik	Prozess nicht steuerbar	hoch	sehr sel-ten	elektrisch			hoch	sehr selten
5-1	anders als		Defekt Mess-technik	Prozess nicht steuerbar	hoch	sehr sel-ten	elektrisch			hoch	sehr selten
Überwachung Temperatur											
6-1	weni-ger	Temperatur Anzeige zum Ist-Wert	Defekt in Mess-kette	falsche Prozess-steuerung	sehr hoch	sehr sel-ten	elektrisch	elektrische / physi-kalische Redun-danz	kontinuierli-cher Check	sehr hoch	sehr selten
7-1	mehr		Defekt in Mess-kette	falsche Prozess-steuerung	hoch	sehr sel-ten	elektrisch	elektrische / physi-kalische Redun-danz	kontinuierli-cher Check	hoch	sehr selten

Tab. 3.10 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 20 – 22

Funktionsname: Start autom. Steuerprogr. mit Param-Überwachung

Sollfunktion: Aufheizen bis Zieltemperatur, Überwachung Temperatur, Druck, atmosphär. Prozessparameter, Abbruch Funktion

Start automatisches Steuerungsprogramm mit Parameter-Überwachung											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Aufheizen bis Zieltemperatur											
1-1	kein	Aufheizen bis Ziel-temperatur	Ausfall Energie-versorgung	keine Erhitzung	hoch	sehr selten	mechanisch			hoch	sehr selten
1-2			Komplettausfall des elektr. Heiz-kreises	keine Erhitzung	gering	sehr selten	physikalisch			gering	sehr selten
1-3			Ausfall Soll/Ist Vergleichs oder sonst. Selbst-überwachung	potenzielle Ge-fahr Überhitzung	sehr hoch	sehr selten	elektrisch / physikalisch	Redundanz, Ab-gleich Sicherheits-system mit be-trieblichem System, Überwachung durch Wartenper-sonal	Sammlung Er-fahrungswerte und Nachbesse-rung	sehr hoch	sehr selten
2-1	weni-ger		Ausfall einzelner Heizschlangen	zu langsame Erhitzung	gering	sehr selten	mechanisch			gering	sehr selten
3-1	mehr		Steuerungs- / Leittechnikprob-leme	Gefahr Überhit-zung	sehr hoch	sehr selten	physikalisch	Integration Wär-memenge & Be-grenzung nach Menge und Zeit	kontinuierli-cher Check	sehr hoch	sehr selten

Start automatisches Steuerungsprogramm mit Parameter-Überwachung											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Überwachung Druck, atmosphärische Prozessparameter (Gas Art)											
4-1	keine	Druck Atmosphä-renart	Ausfall Mess-technik	Prozess nicht steuerbar	hoch	sehr selten	elektrisch			hoch	sehr selten
5-1	anders als		Defekt Mess-technik	Prozess nicht steuerbar	hoch	sehr selten	elektrisch			hoch	sehr selten
Überwachung Temperatur											
6-1	weni-ger	Tempera-tur An-zeige zum Ist-Wert	Defekt in Mess-kette	falsche Prozess-steuerung	sehr hoch	sehr selten	elektrisch	elektrische / physi-kalische Redun-danz	kontinuierli-cher Check	sehr hoch	sehr selten
7-1	mehr		Defekt in Mess-kette	falsche Prozess-steuerung	hoch	sehr selten	elektrisch	elektrische / physi-kalische Redun-danz	kontinuierli-cher Check	hoch	sehr selten
Test Abbruch Funktion											
8-1	anders als	Abbruch Funktion	blockierte Leit-technik, „hän-gender“ Leistunsgs-schütz	Überhitzung möglich	sehr hoch	sehr selten	elektrisch	manuell bedienba-rer Leistungs-schütz auf „aus“	zyklische Funktions-probe	sehr hoch	sehr selten
9-1	anders als	Abbruch Funktion	Leittechnik gibt selbst essenzi-elle Schutzfunk-tionen für manu-elle Eingriffe frei	Öffnen Autoklav im Zustand heiß möglich	sehr hoch	sehr selten	elektrisch / manuell	Einführung v. Hochsicherheits-funktionen die auch manuell, bei Autoklav heiß, nicht außer Kraft gehen	zyklische Funktions-probe	sehr hoch	sehr selten

Tab. 3.11 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 23

Funktionsname: manueller Start Gaskühlung Autoklav

Sollfunktion: Moderationsfreiheit, Kühlung

Moderationsfreiheit, Kühlung											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Moderationsfreiheit											
1-1	keine	Moderati-onsfreiheit	Flüssigkeit an-stelle von Gas im Kühlkreislauf	erhöhtes Risiko	gering	sehr selten	technisch	administrativ		hoch	sehr selten
1-2			Sonstiger Flüs-sigkeitseintrag in Autoklav	erhöhtes Risiko	hoch	sehr selten	technisch	administrativ		gering	sehr selten
Kühlung											
2-1	keine	Kühlung	Ausfall Kühlkette	Kühlung setzt nicht ein, Zeit-management ge-fährdet	gering	sehr selten	physikalisch			hoch	sehr selten
3-1	weni-ger		Verschmutzung Kühllamellen, mangelnde Kompression Verdichter Sonstiges	Kühlung setzt nicht ein, Zeit-management ge-fährdet	gering	sehr selten	physikalisch			hoch	sehr selten
4-1	mehr		falsch ange-schlossene Rohrleitungen	Keinerlei Küh-lung, Zeitma-nagement ge-fährdet	mittel	sehr selten	technisch	QM	double -Check	mittel	sehr selten

Tab. 3.12 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 24 – 28

Funktionsname: Fehleranalysen, Konsultation Handbuch

Sollfunktion: digitale und analoge Abfrage Messpunkte, Anleitung, Entscheidungshilfe

Konsultation Handbuch											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko mini-miert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Anleitung, Entscheidungshilfe											
1-1	kein	System-checkliste mit Prüf-größen	Aktuelle Abwei-chungen nicht ausreichend sig-nifikant oder analoge / digi-tale Prüfgrößen unvollständig	Betriebssicher-heit gefährdet	hoch	selten	technisch	Verbesserung Checkliste, vor al-len auch mit An-gabe von Fehlerto-leranzen für unklare Sachlagen	Fehlereffek-tanalyse	hoch	sehr selten
2-1	anders als	Behälter voll, Zu-stand heiß	vollständige ent-leerter Behälter	Verfahrensan-weisung, *voll-ständig entleer-ter Behälter*	gering	sehr selten	technisch			gering	sehr selten
2-2			teilentleerter Be-hälter	Verfahrensan-weisung, teil*ent-leerter Behälter*	gering	sehr selten	technisch	a		gering	sehr selten
3-1	kein		Zustand / Vorge-hensweise in Betriebshand-buch nicht be-rücksichtigt	divers	sehr hoch	sehr selten	technisch	keine Maßnah-men, die nicht durch das Be-triebshandbuch dezidiert gedeckt sind ergreifen	Arbeitsauftrag mit mindes-tens doppelter Gegenzeich-nung	mittel	sehr selten

Tab. 3.13 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 29 – 30

Funktionsname: Entriegelung Türöffnung Autoklav

Sollfunktion: Check Innenparameter Autoklav, Ausfahren Entriegelungsbolzen, Tür-Aktorik: öffnen

Entriegelung Türöffnung Autoklav											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko minimiert**	**Verifikation der Maß-nahme**	**Resultie-rende Ri-sikostufe**	**Resultie-rende Häufigkeit**
Check Innenparameter Autoklav											
1-1	kein	Innenpara-meter Au-toklav	Ausfall Mess-technik	Unbekannter oder zumindest nicht abgesi-cherter Innenzu-stand	sehr hoch	sehr selten	technisch	keine Türfreigabe		mittel	sehr selten
2-1	anders als		mögliche Le-ckage	Temperaturab-hängig zuneh-mende Kontami-nationsgefahr	sehr hoch	sehr selten	technisch	Störfallplan akti-vieren		hoch	sehr selten
Ausfahren Entriegelungsbolzen											
3-1	kein	Ausfahren Entriege-lungsbol-zen	Ausfall elektro/hydrauli-sche Steue-rungstechnik	Autoklav bleibt verschlossen	gering	sehr selten	technisch			gering	sehr selten
4-1	falsch	Ausfahren Entriege-lungsbol-zen im Zu-stand heiß	Fehlfunktion Steuerungs- / Verriegelungs-technik	Autoklav könnte geöffnet werden	hoch	sehr selten	technisch	Verbesserung Steuerungstechnik	zyklische Prü-fung	hoch	sehr selten

Entriegelung Türöffnung Autoklav											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko minimiert**	**Verifikation der Maß-nahme**	**Resultie-rende Ri-sikostufe**	**Resultie-rende Häufigkeit**
Tür-Aktorik: öffnen											
5-1	kein	Tür-Akto-rik:öffnen	Ausfall elektro/hydrauli-sche Steue-rungstechnik	Tür nur bedingt oder nicht offen	gering	sehr selten	technisch			gering	sehr selten
6-1	teil-weise				gering	sehr selten	technisch			gering	sehr selten

Tab. 3.14 HAZOP-Matrizen für die Funktionseinheit Schritt Nr. 32

Funktionsname: Traktionsunit, Zylinderschlitten

Sollfunktion: Schub-/Ziehbewegung, Kupplungsfunktion zu/auf für Schubeinheit-Zylinderschlitten

Traktionsunit Zylinderschlitten											
Nr.:	**Leit-wort**	**Abwei-chung auf Parameter**	**Mögliche Ursache**	**Auswirkung**	**Risiko stufe**	**Häufigkeit**	**Art**	**Maßnahme die das Risiko minimiert**	**Verifikation der Maß-nahme**	**Resultie-rende Risi-kostufe**	**Resultie-rende Häufigkeit**
Schub- / Ziehbewegung											
1-1	kein	Traktion Schub-/Ziehbewe-gung	keine lokale Stromversor-gung	keine Traktion	gering	sehr selten	elektrisch	keine	---	gering	sehr selten
1-2			Defekt Antrieb	keine Traktion	gering	selten	elektrisch / mechanisch	keine	---	gering	selten
2-1	Um-keh-rung		falscher Steuerbefehl	falsche Richtung Rammgefahr im Traktionsbereich	Sehr hoch	selten	physikalisch	diversitäre, zusätz-liche Richtungser-kennung, Prellbock in Rich-tung Einfahrt mit zus. Lichtschranke	täglicher Test	sehr hoch	sehr selten
Kupplungsfunktion (zu / auf)											
3-1	nein	Kupp-lungsfunk-tion zu / auf	Elektronik Defekt, mechanischer Defekt	kein Einkuppeln	gering	selten	elektrisch / mechanisch	Logische Verknüp-fung Änderung Kupplungszu-stand, Position und Traktionsrich-tung	---	gering	selten
3-2				kein Auskuppeln	mittel	selten			---	mittel	sehr selten
4-1	Um-keh-rung			gegenteilige Funktion	mittel	selten			---	mittel	sehr selten

Im Weiteren sind nun, basierend auf den Analysetabellen, besonders die Spalte *Maßnahme, die das Risiko minimiert* zuerst von der für das System-Design verantwortlichen Stelle und infolge vom verantwortlichen Management zu bewerten. Darauf basierend sind bei Bedarf weitere Schritte in Richtung Risikominimierung einzuleiten.

Ergebnis der gesamten HAZOP-Analyse ist, dass besonders die Handlungsanweisungen, die nur auf die Aufrechterhaltung der vorgesehenen Produktionssequenz abzielt, keinerlei Sicherheit-reduzierende Maßnahmen im möglichen Entscheidungspool enthalten darf, wie z. B. die Aufgabe einer Sicherheitsbarriere. Dieser Umstand war der ursprüngliche Auslöser, dass die Kühltechnik für die reguläre Abkühlung eines vollen und heißen Behälters zu wenig Kühlleistung besaß und man durch Interpretationen der Anweisungen versuchte, dennoch einen Weg zu finden die kontinuierliche Produktion nicht zu unterbrechen. Außerdem sind weitere Schutzmaßnahmen erforderlich, die das Öffnen eines Autoklavs im heißen Zustand prinzipiell unterbinden.

Literaturverzeichnis

/BUN 18/ Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung (AtSMV) zuletzt geändert 31. Dezember 2018; (Art. 20 VO vom 29. November 2018).

/BUN 21/ Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz, AtG) zuletzt geändert 31. Oktober 2021; (Art. 2 G vom 10. August 2021).

/DIN 05/ DIN: Zuverlässigkeitsmanagement - Teil 3-1: Anwendungsleitfaden - Verfahren zur Analyse der Zuverlässigkeit - Leitfaden zur Methodik. DIN EN 60300-3-1:2005-05, 2005.

/DIN 16a/ DIN: Kunststoffe - Dynamische Differenz-Thermoanalyse (DSC). DIN EN ISO 11357:2016, 2016.

/DIN 16b/ Deutsches Institut für Normung (DIN) e.V.: HAZOP-Verfahren (HAZOP-Studien) Anwendungsleitfaden. DIN EN 61882:2016-02, Beuth Verlag: Berlin, 2016.

/GAB 20/ Gabrielli Cossellu Mario, Mayerhöfer Jan: ATEX 2014/34/EU LEITLINIEN, Leitlinie zur Anwendung der Richtlinie 2014/34/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechstvorschriften der Mitgliederstaat für Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen, ATEX 2014/34/EU Leitlinien - 3. Ausgabe - Mai2020. Hrsg.: Europäische Union (EU), 3. Aufl.: Brüssel, Stand vom Mai-2020, erreichbar unter https://www.bgrci.de/fileadmin/BGRCI/Downloads/DL_Praevention/Explosionsschutzportal/Dokumente/ATEX_2014-34-EU-Guidelines_3rd-Edition_dt_Fassung_2020.pdf, 2020.

/GÄN 13/ Gänßmantel, G., Mayer, G., Wehrfritz, M.: Probabilistische Sicherheitsanalysen für Anlagen der Brennelementfertigung und der Anreicherung: Exemplarische Analyse eines repräsentativen Teilprozesses der Brennelementfertigung, Abschlussbericht zum Vorhaben 3610R03350. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A-3702, 243 S., Juli 2013.

/GEU 09/ Geupel S., Ellinger A., Wehrfritz M., Haider C.: Grundlagen für Störfallanalysen in nuklearen Versorgungsanlagen. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A-3530, Oktober 2009.

/GRS 19a/ Sommer, F.: Handbuch zur Störfallanalyse von nuklearen Ver- und Entsorgungseinrichtungen, Teil A - Grundlagen der Störfallanalyse. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-507, ISBN 978-3-946607-92-2: Garching b. München, April 2019.

/GRS 19b/ Sommer, F.: Handbuch zur Störfallanalyse von nuklearen Ver- und Entsorgungseinrichtungen, Teil B - Physikalisch-chemische Grundlagen der Störfallanalyse. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-508, ISBN 978-3-946607-93-9: Garching b. München, Juli 2019.

/GRS 19c/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH: Handbuch zur Störfallanalyse, Teil C, Auswertung der Betriebserfahrung von Vorkommnissen. GRS-509, ISBN 978-3-946607-94-6: Garching b. München, Juli 2019.

/IEEE 84/ IEEE: IEEE Standard Graphic Symbols for Logic Functions. 91/91a-1984:1984, DOI 10.1109/IEEESTD.1984.7896954, IEEE: Piscataway, NJ, USA, 1984.

/LIE 92/ Liemersdorf H., S. L., Thomas W.: Störfallanalyse und Restrisiko-Ereignisse bei kerntechnischen Anlagen des nuklearen Brennstoffkreislaufes. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A-1943, August 1992.

/NRC 99/ Nuclear Regulatory Commission (NRC): Nuclear Fuel Cycle Facility Accident Analysis Handbook. NUREG/CR-6410, 1999.

/PRE 17/ Preiss, R.: Methoden der Risikoanalyse in der Technik, Systematische Analyse komplexer Systeme. TÜV AUSTRIA, 2. Aufl., ISBN 978-3-901942-76-1, TÜV AUSTRIA AKADEMIE GMBH: Wien, 2017.

Abbildungsverzeichnis

Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-946607-95-3