Peter Baumann

Betriebliches Sicherheitsmanagement

Band 2

Betriebliches Sicherheitsmanagement für Kernkraftwerke mit Leichtwasserreaktoren in der Schweiz

Baumann Consulting

Dr. Peter Baumann
Laufenburg / Schweiz

Juni 2024

Bildquelle Titelseite: Mit freundlicher Genehmigung der Kernkraftwerk Leibstadt AG

Peter Baumann

Betriebliches Sicherheitsmanagement

Band 2

Betriebliches Sicherheitsmanagement
für Kernkraftwerke mit Leichtwasserreaktoren
in der Schweiz

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Wie schon im Vorwort zum Band 1 ausgeführt, beginnen viele Bücher zum Thema Sicherheitsmanagement mit der Darstellung grosser Katastrophen. Es gibt wohl keinen Industriezweig, der mehr mit grossen Katastrophen in Verbindung gebracht wird, als die Nuklearindustrie. Und hier stehen insbesondere die Kernkraftwerke im Fokus des öffentlichen Interesses. Eine rationale Bewertung dieser Katastrophen zeigt, dass der Auslöser dieser Katastrophen immer das Versagen des Sicherheitsmanagements durch bewusstes Ignorieren von Fakten zu Gunsten eines kurzfristigen, unmittelbaren und scheinbaren Vorteils war, ohne die langfristigen negativen Folgen in eine Risikobewertung einzupreisen. Diesen grossen Katastrophen ist eine Reihe katastrophaler Verletzungen des Sicherheitsmanagements, wie wir es heute verstehen, vorausgegangen. Diese Verletzungen erfolgten zum Teil unbewusst und zum Teil bewusst.

Wenn man unter Sicherheitsmanagement das komplexe Zusammenwirken verschiedener Managementsysteme versteht, welche alle die erfolgreiche Umsetzung von technischen und organisatorischen Sicherheitskonzepten zum Ziel haben, dann ist klar, dass ein Sicherheitsmanagement nur so stark ist wie seine schwächsten Glieder.

Das vorliegende Buch setzt sich zum Ziel, den im Band 1 dieser Reihe dargestellten generischen Leitfaden für die Entwicklung eines betrieblichen Sicherheitsmanagements auf das Sicherheitsmanagement für Kernkraftwerke mit Leichtwasserreaktoren anzuwenden. Das Ziel ist das Verständnis für ein angemessenes betriebliches Sicherheitsmanagement soweit zu stärken, dass zu jeder Zeit jedem Mitarbeiter in einem Kernkraftwerk klar wird, auf welche Glieder in der Kette eines Sicherheitsmanagements er Einfluss hat und wie er sicherstellt, dass diese Glieder durch ihn nicht geschwächt werden. Dafür müssen alle Ebenen des Handelns beleuchtet werden. Von der obersten Ebene der Organisationsstruktur, den Führungskräften, bis zum Mitarbeiter, der Vorort betriebsbedingte Handlungen ausführt.

Diese Aufgabenstellung kann aus unterschiedlichen Perspektiven angegangen werden. Man kann den Neubau eines Kernkraftwerkes betrachten

und aufzeigen, wie sich das betriebliche Sicherheitsmanagement von der Planung, über den Bau bis zur Inbetriebsetzung und den Betrieb entwickelt. Eine weitere Möglichkeit ist, von einem bestehenden Kernkraftwerk auszugehen, welches zeit seines Bestehens kontinuierlich weiterentwickelt und dem jeweiligen Stand von Wissenschaft und Technik angepasst werden muss.

Im vorliegenden Fall wird aufgezeigt, wie das betriebliche Sicherheitsmanagement, nach dem Verständnis des Autors aus über 30 Jahren Erfahrung mit Risiko- und Hochrisikoanlagen, bei Modifikationen in bestehenden Kernkraftwerken mit Leichtwasserreaktoren aussehen sollte und wie die unterschiedlichen Managementsysteme eines solchen Kernkraftwerks zum betrieblichen Sicherheitsmanagement beitragen. Um so viele Mitarbeiter wie möglich zu diesem Thema anzusprechen, wird versucht, eine übergeordnete aber möglichst vollständige Darstellung des Sicherheitsmanagements zu liefern. Es ist aber zu beachten, dass diese Darstellung nie wirklich vollständig sein kann. Dennoch, viele Mitarbeiter bestehender Kernkraftwerke können ihre Rolle in dem so dargestellten betrieblichen Sicherheitsmanagement erkennen, daran spiegeln und allenfalls Impulse zur weiteren Verbesserung ihres Beitrags zum Sicherheitsmanagements erhalten.

Die Entwicklung eines projektbegleitenden betrieblichen Sicherheitsmanagements für ein nukleares Neubauprojekt (z.B. für ein geologisches Tiefenlager oder eine Brennelementverpackungsanlage) muss in einem separaten Band behandelt werden.

Peter Baumann
Sulz AG, im Juni 2024

Anmerkungen des Autors

Aufgrund der besseren Lesbarkeit wird im Text das generische Maskulinum verwendet. Gemeint sind jedoch immer alle Geschlechter.

Danksagung

Das vorliegende Buch ist das Produkt aus 32 Jahren Erfahrung in unterschiedlichen Funktionen der ABB Kraftwerke AG (8 Jahre) und Kernkraftwerk Leibstadt AG (24 Jahre) sowie der Erfahrung aus 20 Jahren Beratungstätigkeit für einschlägige Firmen der Nuklearbranche.
Mein besonderer Dank gilt in erster Linie der Kernkraftwerk Leibstadt AG, meinen Vorgesetzten aus dieser Zeit (Robert Wanner, Reinhard Fuchs und Dr. Johannis Nöggerath) und den Mitarbeitern und Kollegen, die mich mit viel Geduld begleitet und das im vorliegenden Buch dargestellte Verständnis zum betrieblichen Sicherheitsmanagement mitgeprägt haben.

Mein Werdegang wurde ausserdem massgeblich von den herausragenden Experten der Kraftwerksindustrie in den USA Hans Wolff und Ronald Engel (ehemals GE-Licensing Manager) sowie aus der Schweiz Johannes Verdegaal (ehemals Fa. NUCON AG), Dr. Franzisco Blangetti, Ferenc Koronya und Wazlav Svoboda (ehemals ABB Kraftwerke AG) geprägt. In unzähligen Stunden des Wissenstransfers haben sie es mir ermöglicht, das mit diesem Buch vorliegende Verständnis eines betrieblichen Sicherheitsmanagements für ein Kernkraftwerk massgeblich zu schärfen.

Ganz besonders möchte ich unserem ehemaligen Kraftwerksleiter der Kernkraftwerk Leibstadt AG Thomas Franke danken, der mich zum Aufschreiben meiner Sichtweise auf das betriebliche Sicherheitsmanagement motiviert hatte.

Vielen Dank auch meinen Kunden, die ich mit meinen Beratungstätigkeiten unterstützen darf. Jede Beratungstätigkeit hat nicht zuletzt auch mein eigenes Verständnis immer weiter geschärft.

Meiner Tochter Viola Katharina Baumann danke ich für die kritische Durchsicht des Manuskripts.

Zuletzt, aber am allermeisten, danke ich meiner Frau Nataliya, die es mir ermöglichte manche Abend-, Wochenend- und Ferienstunde für dieses Projekt zu verwenden.

1. Einleitung

Das betriebliche Sicherheitsmanagement für ein Kernkraftwerk ist einerseits komplex, wenn man an die Vielzahl der Managementsysteme denkt, welche die zahlreichen Aspekte von Sicherheit abdecken müssen. Andererseits kann man den Zugang zum betrieblichen Sicherheitsmanagement derart mit Struktur versehen, dass die Komplexität sich auflöst und ein klares, für alle Beteiligten verständliches Bild entsteht. Und genau darauf kommt es an: "Ein für alle Beteiligte gleichermassen verständliches Bild erzeugen, sodass sich alle mit einer Sprache verständlich machen können".

Wie im Band 1 dieser Reihe, [1], im Kapitel 7 dargestellt wird, gibt es eine Reihe von Managementsystemen, über welche die Anforderungen eines technischen und organisatorischen Sicherheitskonzepts so eingeführt werden können, dass ein angemessenes, alle Hierarchiestufen und deren Organisationseinheiten umfassendes, betriebliches Sicherheitsmanagement entsteht.

Der Zugang zum betrieblichen Sicherheitsmanagement für Kernkraftwerke soll im vorliegenden Band über das sogenannte Konfigurationsmanagement zur sicherheitsgerichteten Umsetzung von Modifikationen erfolgen. Modifikationen in einem Kernkraftwerk, insbesondere bewilligungspflichtige Modifikationen, können derart vielfältige Anforderungen stellen, dass in die Beschreibung der dafür notwendigen Prozesse und Vorkehrungen ein grosser Teil weiterer Managementsysteme eingebunden werden müssen und so ein Gesamtbild eines betrieblichen Sicherheitsmanagements entsteht.

Modifikationen in einem Kernkraftwerk unterliegen dem Konfigurationsmanagement und müssen top down entwickelt werden. Das bedeutet, die Umsetzung eines technischen Sicherheitskonzepts im Rahmen relevanter regulatorischer Vorgaben in vier Schritten (H1 bis H4), gemäss Band 1, sowie die Entwicklung administrativer und organisatorischer Vorkehrungen, um Menschen und Organisationen auf die erforderlichen sicherheitsorientierten Grundsätze für die Beherrschung der neuen oder veränderten alten Technik auszurichten.

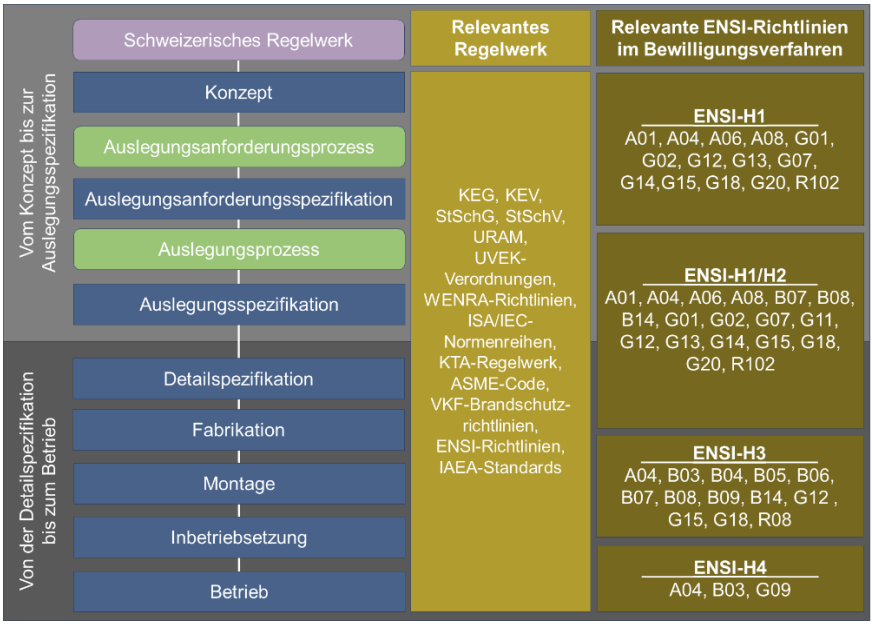

Abbildung 1: Top-Down-Entwicklung der nuklearen Sicherheit, relevantes Regelwerk und ENSI-Richtlinien auf den Hierarchiestufen des Bewilligungsverfahrens

Diese Top-Down-Entwicklung beginnt mit der Identifikation der relevanten Regelwerksanforderungen und dem daran anschliessenden Auslegungsanforderungsprozess. Er führt weiter über den Auslegungsprozess zur Auslegungsspezifikation, Detailspezifikation, Herstellung, Montage, Inbetriebsetzung und zum Betrieb.
Abbildung 1 zeigt diesen Ablauf und stellt diesem das für Kernkraftwerke mit Leichtwasserreaktoren relevante Schweizer Regelwerk und die Hierarchiestufen des Bewilligungsverfahrens gegenüber. Entlang dieses Ablaufs werden am Beispiel einer Modifikation und der Anwendung des dafür erforderlichen Konfigurationsmanagements alle Managementsysteme eingebunden, welche dazu beitragen, die Anforderungen des technischen und organisatorischen Sicherheitskonzepts angemessen umzusetzen. Dabei handelt es sich im Wesentlichen um folgende Managementsysteme:

a) Konfigurationsmanagement
b) Risikomanagement
c) Alterungsmanagement
d) Dokumentationsmanagement
e) Betriebsdauermanagement
f) Anforderungsmanagement
g) Qualitätssicherungsmanagement
h) Ersatzteilmanagement
i) Betriebserfahrungsmanagement
j) Ausbildungsmanagement und Wissensmanagement
k) IT- und OT-Sicherheitsmanagement
l) Sicherungsmanagement
m) Notfallmanagement

Der vorliegende Band beschreibt das erforderliche betriebliche Sicherheitsmanagement für Kernkraftwerke mit Leichtwasserreaktoren, deren wesentliche Merkmale in Kapitel 3 beschrieben werden.
Jede Industrie muss für ihr betriebliches Sicherheitsmanagement die für sie spezifischen Aspekte der Sicherheit einbinden. Auf die Aspekte der Sicherheit für Kernkraftwerke mit Leichtwasserreaktoren wird in Kapitel 4 eingegangen.
Dem Prozess gemäss Abbildung 1 folgend muss zu allererst geklärt werden, welches Regelwerk zur Anwendung kommen muss. In Kapitel 5 wird deswegen auf das für Kernkraftwerke mit Leichtwasserreaktoren anzuwendende Regelwerk eingegangen und die Regelwerkspyramide zu den einzelnen Aspekten der Sicherheit gemäss Kapitel 4 dargestellt.
Ebenfalls der Logik des Prozesses aus Abbildung 1 folgend, muss geklärt werden, wie für diesen Prozess das Bewilligungsverfahren gesteuert werden muss, um sicherzustellen, dass für alle Aspekte der Sicherheit eine Modifikation im Kernkraftwerk regelwerkskonform und damit sicherheitsgerichtet erfolgt. Dies führt zum Konfigurationsmanagement (wie in

Kapitel 6.1.1 beschrieben), welches zu allen Aspekten der Sicherheit die o.g. Managementsysteme zusammenführt und das betriebliche Sicherheitsmanagement bildet.
Dem Leitfaden gemäss Band 1 folgend [1] werden dann in Kapitel 6 & 7 das technische und organisatorische Sicherheitskonzept, spezifisch für Kernkraftwerke mit Leichtwasserreaktoren, entwickelt und in den weiteren Kapiteln 8 bis 13 dargestellt, wie diese im Konfigurationsmanagement für Modifikationen im Rahmen eines Bewilligungsverfahrens angewendet werden.
Kapitel 14 bis 16 gehen auf den Zusammenhang zwischen Sicherheitsmanagement und Sicherheitskultur, auf die durch die Sicherheitskultur sichtbar werdenden Merkmale eines nicht funktionierenden Sicherheitsmanagements sowie auf diesbezüglich gemachte Erfahrungen aus der Praxis ein.

2. Begriffsdefinitionen und Erläuterungen

Die Definition bzw. Erläuterung wichtiger Begriffe erfolgt im Weiteren in einer Art Storytelling. Die folgenden Begriffe werden erklärt und es wird erzählt, welches die wichtigen Zusammenhänge im Bewilligungsverfahren, gemäss Abbildung 1, im Bereich der Hierarchiestufen 1 und 2 sind. Also vom Schweizer Regelwerk bis zur Auslegungs- bzw. Detailspezifikation.
Ein betriebliches Sicherheitsmanagement muss den sicheren Gebrauch der folgenden Begriffe im Kontext zueinander, z.B. bei allen an einem Bewilligungsverfahren beteiligten Personen, gewährleisten. Damit wird ein gemeinsamer Mindset erzeugt, der für das gegenseitige Verständnis, insbesondere über Organisationseinheiten hinaus, von entscheidender Bedeutung ist.

2.1. Sicherheitsmanagement

Die Definition von Sicherheitsmanagement der Wikipedia [2] deckt bereits gut das für uns wichtige Verständnis von Sicherheitsmanagement ab. Es ist dort wie folgt definiert:

Das Sicherheitsmanagement führt, lenkt und koordiniert eine Organisation in Bezug auf alle Sicherheitsaktivitäten.
Sicherheitsmanagement ist synonym zu Risikomanagement (RM), das sämtliche Massnahmen zur systematischen Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken umfasst.
Unter Sicherheitsmanagement wird im Folgenden der Prozess zum Aufbau, der kontinuierlichen Prüfung, Steuerung und Fortentwicklung des Sicherheitsniveaus eines Unternehmens verstanden. Sicherheitsmanagement bezieht sich auf das Gesamtunternehmen, seine Geschäftsprozesse und Ressourcen. Es erstreckt sich über alle Bereiche der Sicherheit, vom Objektschutz über die Geschäftsprozesse, die Arbeitssicherheit bis hin zum Personenschutz.

2.2. Sicherheit und Sicherheitsmanagement

Es muss zunächst die Bedeutung von Sicherheit für komplexe Primäraufgaben definiert werden. Es stellt sich also die Frage: "Ab wann ist die für eine komplexe Primäraufgabe eingesetzte Technik hinreichend sicher und durch den Menschen hinreichend sicher bedienbar"?
Unterschiedliche Sichtweisen können verschiedene Antworten auf diese Frage hervorbringen. Es erscheint aber logisch, davon auszugehen, dass die Gestaltung der einzusetzenden Technik zur Beherrschung einer komplexen Primäraufgabe eine zentrale Rolle spielt. Wir beantworten die oben gestellte Frage deswegen wie folgt:

Die Sicherheit beim Betrieb einer komplexen Primäraufgabe ist dann gegeben, wenn die Auslegungsgrenzen der eingesetzten Technik unter allen denkbaren sowie wahrscheinlichen Betriebsbedingungen nicht verletzt werden. Das bedeutet, dass im bestimmungsgemässen Betrieb Betriebsgrenzen eingehalten werden und genügend Sicherheitsabstand zu den Auslegungsgrenzen besteht sowie die Anforderungen an die Auslegung, Herstellung, Montage, Inbetriebsetzung sowie den Betrieb und die Instandhaltung dieser Technik die Fähigkeiten der dafür eingesetzten Organisation und des dafür eingesetzten Personals nicht übersteigen.

Dieses Verständnis von Sicherheit stellt die Einhaltung des übergeordneten Sicherheitszieles sicher:
Der Schutz von Menschen und Umwelt

2.3. Sicherheitsmanagement und Sicherheitskultur

Sicherheitsmanagement darf nicht mit Sicherheitskultur verwechselt werden. Es muss sich der komplexeren Aufgabe der Entwicklung eines technischen Sicherheitskonzepts und dessen Unterstützung durch ein organisatorisches Sicherheitskonzept widmen.
Konkret bedeute dies, die Erstellung von verbindlichen Regeln im technischen und organisatorischen Sicherheitskonzept, die den Menschen, die Technikentwicklung, die Instandhaltung und den Betrieb der Technik sowie die dafür erforderliche Organisation auf die sichere Beherrschung der

Technik ausrichten. Wenn diese Ausrichtung gelingt, kann man von einer guten Sicherheitskultur in der Unternehmung ausgehen.
Sicherheitskultur ist also immer etwas, was in Bezug auf etwas gefördert werden muss. Demnach dürfen Programme zur Förderung der Sicherheitskultur nicht einfach nur sich selbst genügen, sondern müssen im Hinblick auf den sicheren Betrieb einer Technik entwickelt werden. Die Entwicklung dieser Sicherheitskulturprogramme bedingt also u. A. detaillierte Kenntnisse über die zu beherrschende Technik als solche und die damit verbundenen gesellschaftlich akzeptierten Rahmenbedingungen.

Die Effektivität eines Sicherheitsmanagements, also die Güte der Sicherheitskultur, hängt deswegen massgeblich davon ab, wie gut das gegenseitige Verständnis und die Zusammenarbeit von jenen, die den Menschen verstehen und jenen, die die Technik verstehen ist. Die Aufgabe ist es beide Welten zusammen zu bringen, um ein betriebliches Sicherheitsmanagement effektiv in die Praxis umsetzen zu können.

2.4. Gefährdungsannahmen und Sicherheitskonzept

Jedes betriebliche Sicherheitsmanagement muss sich über die von seiner Unternehmung ausgehenden Gefahren bewusst sein. Für sogenannte Risiko- und Hochrisikounternehmungen legen bereits der Gesetzgeber und seine Aufsichts- und Vollzugsbehörden Gefährdungsannahmen fest, die mindestens in Betracht gezogen und bewertet werden müssen und für die ein Sicherheitskonzept entwickelt werden muss. Diese Gefährdungsannahmen betreffen alle Aspekte der Sicherheit.
Von übergeordneter Bedeutung ist der Begriff "Sicherheitskonzept". Dieser wird wie folgt definiert [2]:

Zentraler Bestandteil eines Sicherheitsmanagements ist ein Sicherheitskonzept. Hier werden alle relevanten Rahmenbedingungen, die definierten Sicherheitsziele des Unternehmens sowie Massnahmen zur Zielerreichung (Beherrschung der Gefahren) beschrieben bzw. definiert. Das Sicherheitskonzept stellt die Basis für die Planung und Durchführung einzelner Sicherheitsmassnahmen dar. Ziel der Erstellung und Umsetzung eines Sicherheitskonzepts ist das Erreichen eines geplanten Sicherheitsniveaus

und die Minimierung identifizierter Risiken, die sich aus den Gefährdungsannahmen ergeben.

Die Gefährdungsannahmen sind die Grundlage für die Entwicklung daraus potentiell resultierender Ereignisse (dem **Ereignisspektrum**) und für die Bewertung von damit einhergehenden Risiken, die den sicheren Betrieb gefährden könnten.

2.5. Ereignisspektrum

Das Ereignisspektrum ist die Summe aller denkbaren Ereignisse, die sich aus den Gefährdungsannahmen entwickeln könnten.
Das Ereignisspektrum wird massgeblich durch die an den Betriebsprozessen verwendeten Technologien und den Eingriffen durch den Menschen bestimmt. Unterschiedliche Technologien von Leichtwasserreaktoren resultieren auch in unterschiedlichen Ereignisspektren.
Das Ereignisspektrum bildet die Grundlage zur Bestimmung der schwerwiegendsten Ereignisse (**auslegungsbestimmende Ereignisse**), die wir, abhängig von der erwarteten Häufigkeit, als auslegungsbestimmende Betriebsstörungen, Auslegungsstörfälle oder auslegungsüberschreitende Störfälle bezeichnen.

2.6. Auslegungsbestimmende Ereignisse

Die auslegungsbestimmenden Ereignisse werden aus dem Ereignisspektrum entwickelt und stellen als solche die höchsten Ansprüche an die am **Beherrschungskonzept** für die Ereignisse beteiligten Systeme, Strukturen und Komponenten (SSK).
Die auslegungsbestimmenden Ereignisse bilden die wichtigste Grundlage zur Entwicklung der Auslegungsanforderungsspezifikation, zur Steuerung der Auslegungsprozesse und zur Entwicklung der Auslegungsspezifikationen.

2.7. Beherrschungskonzept (Schutzsequenzen)

Zur Beherrschung der auslegungsbestimmenden Ereignisse müssen Beherrschungskonzepte entwickelt werden, mit denen sichergestellt wer-

den kann, dass keine Akzeptanzkriterien und Akzeptanzgrenzwerte verletzt werden. Dazu müssen technische Systeme und sonstige (auch organisatorische) Vorkehrungen entwickelt werden, die bei Abweichungen vom ungestörten bestimmungsgemässen Betrieb eingreifen können und die Folgen des Ereignisses regelwerkskonform begrenzen können.
Systeme oder sonstige Vorkehrungen, die Abweichungen vom ungestörten bestimmungsgemässen Betrieb begrenzen können, werden als **sicherheitsrelevante Systeme** oder Vorkehrungen bezeichnet.

2.8. Sicherheitsrelevante Systeme

Sicherheitsrelevante Systeme werden unterschieden nach sicherheitsbezogenen Systemen zur Begrenzung der Eskalation von Ereignissen auf der Sicherheitsebene 2 (Begrenzungssysteme und ihre Begrenzungsfunktionen) und Sicherheitssysteme und ihre Sicherheitsfunktionen zur Beherrschung eines Ereignisses auf der Sicherheitsebene 3, falls die Begrenzungssysteme auf Sicherheitsebene 2 versagt haben sollten, siehe Kapitel 7.3.
Die sicherheitsbezogenen Systeme erfüllen dabei **Schutzzielfunktionen** auf Sicherheitsebene 2 und die Sicherheitssysteme erfüllen Schutzzielfunktionen auf Sicherheitsebene 3.
Die Sicherheitsebenen sind Bestandteil des Konzepts der gestaffelten Sicherheitsvorsorge im technischen Sicherheitskonzept des betrieblichen Sicherheitsmanagements.

2.9. Schutzzielfunktionen

Grundsätzlich kann man alle Funktionen für alle Sicherheitsebenen (SE 1 bis SE 4) im Konzept der gestaffelten Sicherheitsvorsorge als Schutzzielfunktionen bezeichnen, wenn sie einem Schutzziel dienen (vergleiche mit Kapitel 7.1).
Die Schutzzielfunktionen sicherheitsrelevanter Systeme sind Funktionen oder Teilfunktionen von Systemen, die auf den Sicherheitsebenen 2 und 3, auf der sie wirksam sein sollen, die Einhaltung der Schutzziele sicherstellen, indem sie dafür sorgen, dass vorhandene Barrieren (vergleiche mit Kapitel 7.2) und die dafür erforderlichen Akzeptanzgrenzwerte und damit die Akzeptanzkriterien nicht verletzt werden.

Die Schutzzielfunktionen sicherheitsrelevanter Systeme bestehen aus Strukturen und Komponenten, die besondere Auslegungsmerkmale haben müssen. Ein wichtiges Auslegungsmerkmal dieser Systeme, Strukturen und Komponenten ist die **Klassierung**.

2.10. Klassierung sicherheitsrelevanter Systeme, Strukturen und Komponenten

Für Strukturen und Komponenten sicherheitsrelevanter Systeme gelten spezifische Anforderungen im Auslegungsanforderungsprozess. Daraus ergibt sich unter anderem die Klassierung der SSK, entsprechend ihrer Sicherheitsrelevanz.
Die Klassierung der SSK legt deren Qualifikationsanforderungen und die **Kategorisierung** der für den Betrieb der SSK erforderlichen **leittechnischen Funktionen** fest.

2.11. Leittechnische Kategorisierung der im Beherrschungskonzept erforderlichen Schutzzielfunktionen

Die Kategorisierung der für den Betrieb der Strukturen, Systeme und Komponenten erforderlichen leittechnischen Schutzzielfunktionen ist eng verknüpft mit der Klassierung dieser Strukturen, Systeme und Komponenten. Sie bilden eine wesentliche Grundlage für die Entwicklung der Auslegungsspezifikationen der Strukturen, Systeme und Komponenten.

3. Kernkraftwerke mit Leichtwasserreaktoren in der Schweiz

In der Schweiz werden zwei Typen von Leichtwasserreaktoren betrieben:

1. Druckwasserreaktoren: Kernkraftwerke Beznau und Gösgen
2. Siedewasserreaktoren: Kernkraftwerke Leibstadt und Mühleberg. Mühleberg befindet sich seit 2019 im Rückbau.

Entsprechend ist das Regelwerk zum Betrieb von Kernkraftwerken auf den Typ Leichtwasserreaktoren ausgerichtet.

Im Folgenden wird der prinzipielle Aufbau von Kernkraftwerken mit Druckwasser- und Siedewasserreaktoren dargestellt [3].

3.1. Grundsätzlicher Aufbau eines Kernkraftwerks mit Druckwasserreaktoren

Der Druckwasserreaktor hat zwei getrennte Kreisläufe: den Primär- und den Sekundärkreislauf. Im Primärkreislauf durchfließt das Wasser den sogenannten Reaktorkern. Dort wird es über die von den Brennelementen erzeugte Energie aus der Kernspaltung von 291 °C auf 326 °C erhitzt (im sog. Reaktordruckbehälter). Da das Wasser unter einem Druck von 157 bar steht, siedet es auch bei diesen hohen Temperaturen nicht (im Unterscheid zum Siedewasserreaktor (SWR).

Das erhitzte Wasser aus dem Reaktordruckbehälter wird in die Heizrohre des sogenannten Dampferzeugers geleitet. Der Dampferzeuger stellt die Schnittstelle zwischen Primär- und Sekundärkreislauf dar. Die Wärme wird so an das Wasser im Sekundärkreislauf abgegeben, welches die Heizrohre umgibt. Dadurch kann das kontaminierte Wasser des Primärkreislaufes nicht in den Sekundärkreislauf gelangen. Nach der Wärmeübertragung im Dampferzeuger wird das abgekühlte Wasser im Primärkreislauf zurück in den Reaktordruckbehälter gepumpt. Da der Druck auf der Sekundärseite des Dampferzeugers nur 64,5 Bar beträgt, verdampft

das Wasser dort bei 280,5 °C. Der entstehende Dampf wird durch Turbinen geleitet. Ein nachgeschalteter Generator wandelt die dort erzeugte Energie in elektrischen Strom um. Danach wird der Dampf abgekühlt, in einem Kondensator niedergeschlagen und als Wasser wieder in den Dampferzeuger zurückgeleitet.

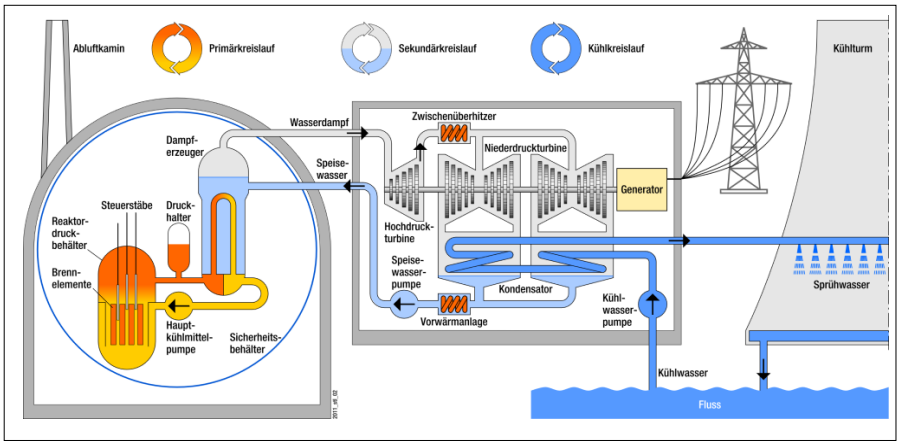

Abbildung 2: Kernkraftwerk mit Druckwasserreaktor

3.2. Grundsätzlicher Aufbau eines Kernkraftwerks mit Siedewasserreaktoren

Der Siedewasserreaktor verfügt über einen geschlossenen Wasser-Dampf-Kreislauf. Das Kühlmittel des Kühlkreislaufs durchströmt den Reaktorkern. Dort erhitzt die bei der Kernspaltung in den Brennelementen entstandene Wärme das Wasser soweit (bis circa 286 °C), dass es direkt im Reaktordruckbehälter siedet. Dabei herrscht im Reaktordruckbehälter ein Druck von circa 70 bar. Das Sieden und Verdampfen des Kühlmittels im Reaktordruckbehälter stellen das besondere Merkmal des Siedewasserreaktors dar, das ihn vom Druckwasserreaktor unterscheidet.

Der beim Siedevorgang entstehende Dampf durchströmt im oberen Teil des Reaktordruckbehälters (oberes Plenum) spezielle Vorrichtungen (Zyklone und Dampftrockner), die seinen Wasseranteil reduzieren. Danach wird der „getrocknete“ Dampf zur Turbine geleitet. Ein nachgeschalteter

Generator wandelt die Rotationsenergie der Turbine in elektrische Energie um. Hinter der Turbine wird der Dampf in grossen Kondensatoren abgekühlt, wieder zu Wasser kondensiert und in den Reaktordruckbehälter als Speisewasser zurückbefördert.

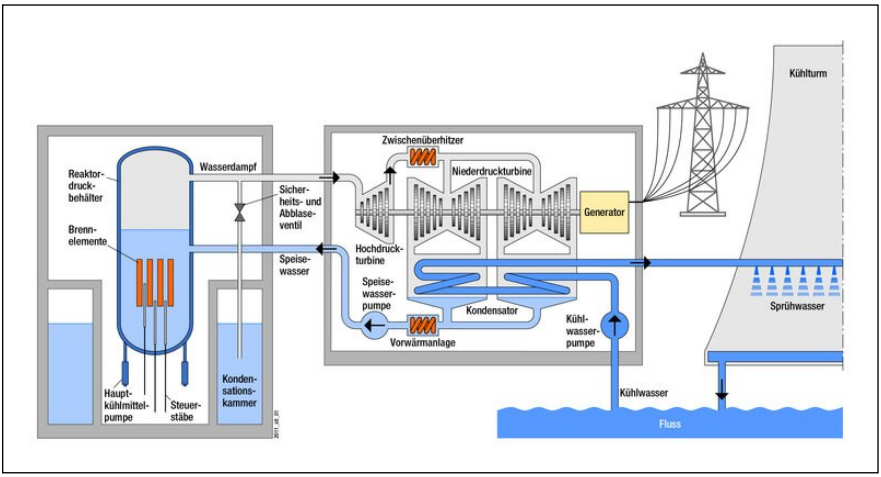

Abbildung 3: Kernkraftwerk mit Siedewasserreaktor

4. Aspekte der Sicherheit für Kernkraftwerke mit Leichtwasserreaktoren

Das betriebliche Sicherheitsmanagement für ein Kernkraftwerk muss eine Reihe von Sicherheitsaspekten berücksichtigen. Um welche es sich dabei handelt, lässt sich z.B. sehr umfassend aus den Empfehlungen der WANO zum Risikomanagement ableiten [4]. Diese sind:

1. Betriebliche Sicherheit

   Potential für unerwünschte Auswirkungen auf die Anlage, wie die einer Anlagentransiente, Schäden an Komponenten, Verlust von redundant und diversitär ausgelegten Sicherheitssystemen, Überschreiten zulässiger Nichtverfügbarkeitszeiten (zeitlich eingeschränkter begrenzter Betriebsbedingungen).

2. Nukleare Sicherheit

   Es besteht das Potential für die Verletzung von Schutzzielen durch Kernschäden und die signifikante Freisetzung von Radioaktivität durch den Verlust der zum Schutz des Betriebspersonals und von Menschen und Umwelt vorgesehenen Rückhalte-Barrieren für radioaktive Spaltprodukte.

3. Radiologische Sicherheit

   Es besteht das Potential für gesundheitliche Auswirkungen durch interne oder externe ionisierende Direktstrahlung oder für eine Kontamination der Umwelt als unmittelbare Konsequenz der Freisetzung von radioaktivem Material. Der operationelle Strahlenschutz sieht Vorkehrungen zur Gewährleistung der radiologischen Sicherheit des Betriebspersonals, als Teil der Arbeitssicherheit, vor. Weitere Vorkehrungen zur Überwachung der radiologischen Abgaben durch Abwässer, Emissionen und Abfälle dienen der Umweltsicherheit.

4. Arbeitssicherheit

   Potential für Schäden an Leib und Leben durch Gefahren des Arbeitsplatzes (nur konventionelle Gefahren).

5. Umweltsicherheit

   Potential für schädliche Auswirkungen auf lebendige Organismen in der Umwelt durch Abwässer, Emissionen, Abfälle (nur konventionelle Gefahren).

Ausser den für diese Gefahren aufgeführten Risiken werden auch noch das Projektrisiko und das Unternehmensrisiko aufgeführt. Auf diese wird im weiteren Verlauf nicht eingegangen. Diese Risiken werden als im Wesentlichen eliminiert betrachtet, solange ein betriebliches Sicherheitsmanagement alle anderen aufgeführten Sicherheitsaspekte abdeckt. Das erfolgreiche Abschliessen von Projekten und der Erhalt der Unternehmensreputation wird mit dem beabsichtigten betrieblichen Sicherheitsmanagement massgeblich unterstützt.

Die Sicherheit und damit die Wirtschaftlichkeit beim Betrieb eines Kernkraftwerkes ist dann gegeben, wenn die Auslegungsgrenzen der eingesetzten Technik unter allen denkbaren sowie wahrscheinlichen Betriebsbedingungen nicht verletzt werden, im bestimmungsgemässen Betrieb die Betriebsgrenzen eingehalten werden und genügend Sicherheitsabstand zu den Auslegungsgrenzen besteht. Ausserdem dürfen die Anforderungen an die Auslegung, Herstellung, Montage, Inbetriebsetzung sowie den Betrieb und die Instandhaltung dieser Technik die Fähigkeiten der dafür eingesetzten Organisation und des dafür eingesetzten Personals nicht übersteigen.

Tabelle 1 zeigt für die einzelnen Aspekte der Sicherheit auf, welches Ziel verfolgt wird und welche Schutzkonzepte erforderlich sind. Diese Listen sind nicht abschliessend, geben aber einen Überblick, auf was es ankommt.

Für die weitere Entwicklung des betrieblichen Sicherheitsmanagements werden wir für die Sicherheitsaspekte aufzeigen, welches Managementsystem bei der Umsetzung der Anforderungen eines technischen und organisatorischen Sicherheitskonzepts so unterstützt, dass ein angemessenes, alle Hierarchiestufen umfassendes Sicherheitsmanagement entsteht.

Damit werden die wichtigsten Sicherheitsaspekte für den Leistungsbetrieb und den Stillstand eines Kernkraftwerks behandelt. Auf das betriebliche Sicherheitsmanagement für die Abfallbehandlung wird hier nicht eingegangen.

Aspekt	Ziel	Beherrschungskonzepte
Nukleare Sicherheit	Beherrschung interner und externer Einflüsse im Rahmen regulatorischer Vorgaben Auslegung von SSK und administrative Vorkehrungen stellen die Erfüllung der regulatorischen Akzeptanzkriterien sicher	**Interne Einflüsse:** Schutzsequenzen für Anlagentransienten, Brandschutz, Flutschutz, etc. **Externe Einflüsse:** Brandschutz, Blitzschutz, Flutschutz, Seismik, Geologie, Flugzeugabsturz, etc. Betriebs-, Störfall- und Notfallorganisation Betriebs-, Störfall- und Notfallanweisungen
Radiologische Sicherheit	Beherrschung radiologischer Konsequenzen aus internen und externen Einflüssen im Rahmen regulatorischer Vorgaben Auslegung von SSK und administrative Vorkehrungen stellen die Erfüllung der regulatorischen Akzeptanzkriterien sicher	**Interne Einflüsse:** Schutzsequenzen für Anlagentransienten, Strahlenschutz, etc. **Externe Einflüsse:** Brandschutz, Blitzschutz, Flutschutz, Seismik, Geologie, Flugzeugabsturz, etc. Betriebs-, Störfall- und Notfallorganisation Betriebs-, Störfall- und Notfallanweisungen
Betriebliche Sicherheit	Störungsfreier Betrieb, Betriebsgrenzen mit Sicherheitsabstand innerhalb der Auslegungsgrenzen der SSK und Freisetzung von Radioaktivität innerhalb der	Qualifikationskonzepte für Strukturen, Systeme und Komponenten (SSK) Instandhaltungskonzept, Prüfungskonzepte, etc. für SSK

Aspekt	Ziel	Beherrschungskonzepte
	regulatorischen Grenzwerte	Anlagenfahrvorschriften
Arbeitssicherheit	Personen- und Gesundheitsschutz Arbeitsbedingungen innerhalb der regulatorischen Akzeptanzkriterien	Spezifische, tätigkeitsbezogene Vorkehrungen des Arbeitsplatzes und persönliche Schutzausrüstungen aus Gefährdungsannahmen und Risikobewertungen ermittelt
Umweltsicherheit	Beherrschung des Umgangs mit Gefahrstoffen im Rahmen der regulatorischen Vorgaben Auslegung von SSK und administrative Vorkehrungen stellen die Erfüllung der regulatorischen Akzeptanzkriterien sicher	Schutzsequenzen für Anlagentransienten Schutzkonzepte für den Umgang mit Gefahrstoffen, die die Umwelt gefährden könnten Tätigkeitsbezogene spezifische Vorkehrungen beim Umgang mit Gefahrstoffen aus Gefährdungsannahmen und Risikobewertungen ermittelt

Tabelle 1: Ziele und Vorkehrungen für die Aspekte der Sicherheit

Wie aus der Tabelle 1 hervorgeht, besteht die Aufgabe darin, für jeden Sicherheitsaspekt ein technisches und organisatorisches Sicherheitskonzept derart umzusetzen, dass daraus Schutzkonzepte abgeleitet werden können. Das Ziel ist, für alle möglichen Anlagenzustände die regulatorischen Akzeptanzkriterien erfüllen und die erforderlichen Akzeptanzgrenzwerte einhalten zu können.

Wie im Band 1 [1] dargestellt wird, bilden das technische und organisatorische Sicherheitskonzept zusammen die Grundlage für das betriebliche Sicherheitsmanagement. Ziel ist es, die technische Auslegung und auch die Anforderungen an Mensch und Organisation auf sicherheitsgerichtete Grundsätze auszurichten.