Peter Baumann

Betriebliches Sicherheitsmanagement

Band 1

Leitfaden zum Aufbau eines
betrieblichen Sicherheitsmanagements

Baumann Consulting

Dr. Peter Baumann
Laufenburg / Schweiz

Mai 2024

Bildquelle Titelseite: Webseite Kernkraftwerk Leibstadt AG

Peter Baumann

Betriebliches Sicherheitsmanagement

Band 1

Leitfaden zum Aufbau eines betrieblichen Sicherheitsmanagements

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Viele Bücher zum Thema Sicherheitsmanagement, ob sie den Begriff im Titel tragen oder nicht, beginnen mit der Darstellung der grossen Katastrophen der Industriegeschichte. Sie werden zum Anlass genommen weitere, meist ergänzende Theorien zur Katastrophenvermeidung zu entwickeln. Diese nehmen die Regulierungsbehörden immer wieder bereitwillig auf, um die gesetzlichen Anforderungen zu verschärfen. Objektiv betrachtet kann man feststellen, dass es oft ausreichen würde die vorhandenen Gesetze konsequent anzuwenden.

Es liegt natürlich in der Natur des Menschen sich stetig weiterentwickeln und verbessern zu wollen. Deswegen hat bisher noch jede grosse Katastrophe weitere Theorien hervorgebracht, die zu neuen regulatorischen Anforderungen führten. Durch diesen Prozess entsteht mit der Zeit eine Überregulierung, die sich auf die Sicherheit kontraproduktiv auswirken kann. Denn die vorhandenen Theorien bleiben selbstverständlich gültig und werden in der Regel nicht einmal in ihrer Bedeutung relativiert.

Die Gefahr dieser Entwicklung besteht darin, dass der Eindruck erweckt wird, die grossen Katastrophen liessen sich dadurch vermeiden. Doch jede zusätzliche Theorie zur Verbesserung des Sicherheitsmanagements kam erst nach der Katastrophe und hat die folgende Katastrophe nicht verhindert.

Dieses Buch beginnt deshalb bewusst nicht mit dem Aufzeigen von Katastrophen der Industriegeschichte, die mit einem funktionierenden Sicherheitsmanagement vielleicht hätten vermieden werden können. Denn es gilt, wie beispielsweise in der Politik der inneren Sicherheit einer Gesellschaft, nach Katastrophen nicht zuerst neue bzw. verschärfte Regulierungen zu verlangen, sondern die vorhandenen Mittel konsequent anzuwenden.

Die berufliche Praxis zeigt, dass sich das bis heute entwickelte Verständnis von Sicherheitsmanagement bei Weitem nicht in allen Bereichen soweit etabliert hat, dass es zur Vermeidung weiterer Katastrophen bereits hätte wirksam werden können. Woran liegt das eigentlich?

Es zeigt sich, dass in der wissenschaftlichen Fundierung wie auch in der betrieblichen Umsetzung in der Regel keine dem Thema angemessene und vollständige Abbildung des Sicherheitsmanagements enthalten ist.

Ausserdem versäumen es vorhandene Beiträge oft, die Komplexität der einzelnen Bereiche des Sicherheitsmanagements inkl. der Faktoren Mensch, Technik und Organisation hinreichend miteinzubinden.
Die wissenschaftliche Fundierung des Sicherheitsmanagements wird massgeblich durch die Fakultäten Psychologie und Soziologie geprägt, welche in der betrieblichen Praxis eine äusserst heterogene Umsetzung erfahren.
Es hat sich in den vergangenen 30 Jahren ein Verständnis von Sicherheitsmanagement entwickelt, welches grundsätzlich darauf ausgerichtet ist die menschlichen und organisatorischen Faktoren (HOF) beim Betrieb einer technischen Anlage in den Mittelpunkt zu stellen. Jede Weiterentwicklung hat es jedoch eher versäumt als wichtigsten Teil die Technik einzubeziehen. Man ist davon ausgegangen, dass die Technik sicher genug ist. Es käme demzufolge jetzt darauf an den Menschen und die Organisation als Risikofaktor zu reduzieren.
Ungeachtet dieser Entwicklung versäumt es kein Autor Sicherheitsmanagement als etwas zu definieren, das Mensch, Technik und Organisation gleichermassen einbezieht. Man spricht heute gerne von soziotechnischen Systemen, welche es zu optimieren gilt, und reduziert diesen Ansatz technikseitig allzu oft auf die Frage, wie die Betriebsmittel, sprich die technischen und räumlichen Bedingungen für den Menschen (Operateur), gestaltet sein müssen, um Operateurhandlungen sicher ausführen zu können (Ritz, 2015), Abbildung 20. Dieser Ansatz ist nicht falsch, aber bei Weitem nicht vollständig.
Auf jede grosse Katastrophe reagiert gewöhnlich die Politik bzw. die Gesellschaft als Kollektiv und drückt ihre Betroffenheit aus. Neue Gesetze und Auflagen treten in vielen Fällen in Kraft, ohne dass geprüft worden wäre, ob die vorhandenen Regulierungen bei konsequenter Anwendung nicht bereits ausreichen würden. Die neuen Gesetze werden unter dem Eindruck der Katastrophe zwar gesellschaftlich akzeptiert, aber wir spüren dabei meist keine persönliche Betroffenheit. Eine Katastrophe irgendwo auf der Welt ist bestimmt schrecklich für das Land, die Region und die Menschen, aber eigentlich ist man persönlich nicht betroffen. Und ausserdem: mit dem neuen Gesetz sorgt schon jemand dafür, dass das bei uns nicht passiert.
Es wird vielerorts nicht anerkannt, dass den grossen Katastrophen nicht minder grosse Katastrophen vorausgehen, durch die wir alle und jeden

Tag die persönliche Betroffenheit spüren müssten. Die eigentlichen Katastrophen passieren jeden Tag, vor allem in unseren Büros. Diese Katastrophen haben normalerweise keine unmittelbaren Auswirkungen auf die Sicherheit betrieblicher Prozesse, weil sie nicht an der operativen Front geschehen. Deshalb wird auch dort die unmittelbare Betroffenheit nicht erkannt. Es ist deshalb die Aufgabe, vor allem der Führungskräfte, diese Betroffenheit zu erzeugen. Die lange Zeit vorherrschende Meinung Führungskräfte müssen führen, für das Verständnis der Technik sind die Mitarbeiter zuständig, behindert oft diese Betroffenheit im Bereich Technik zu erzeugen. Auch die Vorstellung, für ein technisches System müsse, sobald einmal in Betrieb genommen, nur die Instandhaltung nach Vorgaben des Lieferanten durchgeführt werden, um Betriebssicherheit zu gewährleisten, führt zu einer Organisation, in der es unmöglich ist Veränderungen von Randbedingungen für den sicheren Betrieb zu erkennen.
Es gibt eine ganze Reihe hervorragender Bücher zum Thema Sicherheitsmanagement, mit dem Fokus Mensch und Organisation (MO). Mit dem vorliegenden Buch soll ein Leitfaden unterbreitet werden, der auf Basis wissenschaftlicher Grundlagen zum Thema Mensch und Organisation die Technik gleichberechtigt einbindet. So entsteht ein Sicherheitsmanagement, das Mensch, Technik und Organisation (MTO), entsprechend den im praktischen Anwendungsfall erforderlichen Schwerpunkten, zusammenführt.
Als wissenschaftliche Grundlage für dieses Buch dient das Buch von Prof. Frank Ritz "Betriebliches Sicherheitsmanagement" (Ritz, 2015). Seine Darstellung der Schnittstellen zwischen Mensch und Organisation auf der einen Seite und Mensch und Technik auf der anderen Seite eignet sich hervorragend, um den Aspekt Technik im beabsichtigten Sinne zu ergänzen.

Peter Baumann
Sulz AG, im Mai 2024

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

Danksagung

Der vorliegende Leitfaden ist das Produkt aus 32 Jahren Erfahrung in unterschiedlichen Funktionen bei der ABB Kraftwerke AG (8 Jahre) und der Kernkraftwerk Leibstadt AG (24 Jahre) sowie der Erfahrung aus 20 Jahren Beratungstätigkeit für einschlägige Firmen aus der Nuklearbranche.
Mein besonderer Dank gilt in erster Linie der Kernkraftwerk Leibstadt AG, meinen Vorgesetzten aus dieser Zeit (Robert Wanner, Reinhard Fuchs und 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) und 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 hat.

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

F. Ritz (Ritz, 2015) hält bei seinen Überlegungen zum Aufbau soziotechnischer Systeme im Kapitel 4.1.2, fest:

Das Anliegen des soziotechnischen Systemansatzes ist die gemeinsame Optimierung von Organisationen, Technikeinsatz und Human Resources. […] Zentrale Fragen, die dabei zu klären sind, betreffen die Anpassung der beiden Teilsysteme, z.B. wie Technik- und Prozessgestaltung menschengerecht umgesetzt werden können und umgekehrt […]

Sicherheit wird nach diesem Verständnis massgeblich durch die Anpassung der Technik an die Fähigkeiten des Menschen, oder die Anpassung der Fähigkeiten des Menschen an die Technik unter Berücksichtigung einer Vielzahl von Umweltfaktoren realisiert.
Dieser Vorstellung folgend entwickelt F. Ritz die Grundlagen für den Aufbau widerstandsfähiger Arbeitssysteme, mit Fokus auf den sicheren Betrieb von Organisationen und Prozessen. Er fasst dies in seinem Buch anschaulich in der Abbildung 20 auf Seite 65 zusammen. Daraus wird ersichtlich, dass die Organisation im Mittelpunkt seiner Überlegungen steht. Das soziotechnische System setzt sich demnach aus dem technischen Teilsystem und dem sozialen Teilsystem zusammen.

Technisches Teilsystem
Es enthält alle für den Menschen erforderlichen Betriebsmittel sowie die vorhandenen technologischen und räumlichen Bedingungen.

Soziales Teilsystem
Es enthält die Organisationsmitglieder, individuelle Bedürfnisse und Qualifikation sowie gruppenspezifische Bedürfnisse.

Beide Teilsysteme dienen der Ausführung der Primär- und Sekundäraufgaben, was der Erfüllung des Systemzwecks gleichkommt.
Dieser Vorstellung liegen Überlegungen zugrunde, die an dieser Stelle unter dem Begriff "**Organisatorisches Sicherheitskonzept**" zusammengefasst werden sollen. Dieses beschreibt die Wechselwirkung zwischen

Mensch und Maschine und hat das Ziel, Sicherheit durch die optimale Organisation dieser Schnittstelle zu gewährleisten.
Ein wesentlicher weiterer Beitrag zur Sicherheit stellt das "**Technische Sicherheitskonzept**" dar. Es stellt sowohl grundlegende technische Anforderungen, die systematisch entwickelt werden müssen, als auch Anforderungen, die im "**Organisatorischen Sicherheitskonzept**" umgesetzt werden müssen, um den sicheren Betrieb einer Anlage gewährleisten zu können.
Technisches und organisatorisches Sicherheitskonzept stehen in vielfältiger Wechselwirkung.

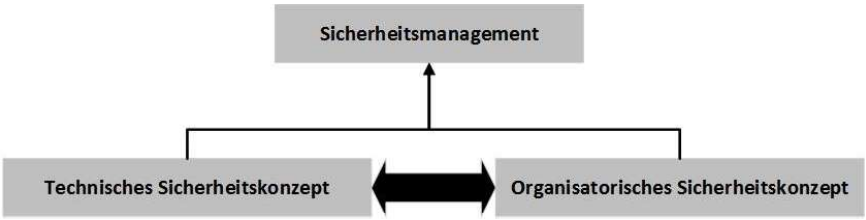

Abbildung 1: Technisches und organisatorisches Sicherheitskonzept: Grundlage des Betrieblichen Sicherheitsmanagements

Die Entwicklung eines Sicherheitsmanagements, welches sich aus den Anforderungen eines technischen **und** organisatorischen Sicherheitskonzepts ergibt, ist Gegenstand des vorliegenden Leitfadens.

2. Begriffsdefinition

Die Definition wichtiger Begriffe erfolgt im Weiteren als Storytelling. Die folgenden Begriffe werden erklärt und dargestellt, welches die wichtigen Zusammenhänge sind.
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 (Wikipedia, 2020) ist sehr gut geeignet, um den Rahmen, der mit dem vorliegenden Leitfaden aufgespannt wird, abzudecken. Sicherheitsmanagement ist dort wie folgt definiert:

Das Sicherheitsmanagement führt, lenkt und koordiniert eine Organisation in Bezug auf alle Sicherheitsaktivitäten.
Sicherheitsmanagement ist synonym zu Risikomanagement (RM), welches 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.

Wikipedia stellt ausserdem Definitionen wichtiger Elemente des Sicherheitsmanagements zur Verfügung. Diese werden im Rahmen dieses Leitfadens entweder unverändert übernommen oder dem Zweck dieses Leitfadens entsprechend angepasst.

2.2. 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 auf Wikipedia (Wikipedia, 2020) wie folgt definiert:

Zentraler Bestandteil eines Sicherheitsmanagements ist ein Sicherheitskonzept. Hier werden alle relevanten Rahmenbedingungen, die definierten Sicherheitsziele des Unternehmens sowie Massnahmen zur Zielerreichung beschrieben bzw. definiert. Das Sicherheitskonzept stellt entsprechend 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.

Damit ist die Bedeutung zweier Begriffe festgelegt, die gleich zu Beginn dieses Leitfadens von Bedeutung sind. Wie im nächsten Kapitel gezeigt wird, soll ein allgemein gültiger Begriff von Sicherheitskonzept so entwickelt werden, dass er soziotechnische Systeme vollständig umfasst. Ziel ist es der Technik den Raum zu geben, der ihrer Bedeutung im Sicherheitsmanagement angemessen ist.
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.

2.3. 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 bestimmt. Unterschiedliche Technologien resultieren in unterschiedlichen Ereignisspektren.
Das Ereignisspektrum bildet die Grundlage zur Bestimmung der schwerwiegendsten Ereignisse, die wir als **auslegungsbestimmende Ereignisse** oder Auslegungsstörfälle bezeichnen.

2.4. Auslegungsbestimmende Ereignisse (Auslegungsstörfälle)

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 Auslegungsstörfälle bilden die wichtigste Grundlage zur Entwicklung der Auslegungsanforderungsspezifikation, zur Steuerung der Auslegungsprozesse und zur Entwicklung der Auslegungsspezifikationen.

2.5. Beherrschungskonzept (Schutzsequenzen)

Zur Beherrschung der auslegungsbestimmenden Ereignisse müssen Beherrschungskonzepte entwickelt werden, mit denen sichergestellt werden kann, dass keine Akzeptanzkriterien und Akzeptanzgrenzwerte verletzt werden. Dazu müssen technische Systeme und sonstige (auch organisatorische) Vorkehrungen entwickelt werden, die bei Abweichungen vom bestimmungsgemässen Betrieb eingreifen können und die Folgen des Ereignisses regelwerkskonform begrenzen können.
Systeme oder sonstige Vorkehrungen, die Abweichungen vom bestimmungsgemässen Betrieb begrenzen können, werden als **sicherheitsrelevante Systeme** oder Vorkehrungen bezeichnet.

2.6. Sicherheitsrelevante Systeme

Sicherheitsrelevante Systeme werden unterschieden nach sicherheitsbezogenen Systemen zur Begrenzung der Eskalation von Ereignissen auf der Sicherheitsebene 2 (Begrenzungssysteme) und Sicherheitssysteme zur Beherrschung eines Ereignisses auf der Sicherheitsebene 3, falls die Begrenzungssysteme auf Sicherheitsebene 2 versagt haben sollten.

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.

2.7. Schutzzielfunktionen der sicherheitsrelevanten Systeme

Die Schutzzielfunktionen sicherheitsrelevanter Systeme sind Funktionen oder Teilfunktionen von Systemen, die auf der Sicherheitsebene, auf der sie wirksam sein sollen, die Einhaltung der Schutzziele sicherstellen, indem sie dafür sorgen, dass das Barrierenkonzept nicht verletzt wird und die dafür erforderlichen Akzeptanzgrenzwerte bzw. Akzeptanzkriterien nicht verletzt werden.
Die Schutzzielfunktionen sicherheitsrelevanter Systeme bestehen aus Strukturen und Komponenten, die besondere Auslegungsmerkmale haben müssen. Ein wichtiges Auslegungsmerkmal dieser Strukturen und Komponenten ist die **Klassierung**.
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.

2.8. Klassierung für Strukturen und Komponenten sicherheitsrelevanter Systeme

Für Strukturen und Komponenten sicherheitsrelevanter Systeme gelten spezifische Anforderungen im Auslegungsanforderungsprozess (siehe Abbildung 4). 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.

2.9. Leittechnische Kategorisierung der im Beherrschungskonzept erforderlichen Schutzzielfunktionen

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

3. Grundsätze zur Entwicklung eines betrieblichen Sicherheitsmanagements

Ein angemessenes betriebliches Sicherheitsmanagement wird in der Regel in Abhängig von der in Ritz (Ritz, 2015) beschriebenen Primäraufgabe eines Unternehmens entwickelt. Die Primäraufgaben von Unternehmen können entweder ein sehr einfaches und übersichtliches, oder aber auch ein äusserst komplexes Sicherheitsmanagement erforderlich machen. Dies ist von der Komplexität der eingesetzten bzw. zu beherrschenden Technik abhängig.
Ist die Primäraufgabe beispielsweise Stromproduktion, so wird die Komplexität des zu entwickelnden betrieblichen Sicherheitsmanagements sehr von der Komplexität der eingesetzten Technik und dem von ihr ausgehenden Gefahrenpotential für das Betriebspersonal, die Bevölkerung und die Umwelt abhängig sein:

Art der eingesetzten Technik	**Anforderungen an ein betriebliches Sicherheitsmanagement**
Photovoltaik	Gering
Windmühlen	Gering
Wasserkraftwerk	Mittel
Kohlekraftwerk	Hoch
Kernkraftwerk	Sehr Hoch
Fusionskraftwerk	Sehr Hoch

Auch wenn die Ausprägung eines Sicherheitsmanagements, abhängig von der eingesetzten Technik, sehr unterschiedlich sein kann, so sind alle Sicherheitsmanagementsysteme doch strukturell zumindest ähnlich.
Diese strukturelle Ähnlichkeit erlaubt es, einen Leitfaden für den Fall des Einsatzes sehr komplexer Technik zu entwickeln, der dann auf Primäraufgaben, welche weniger komplexe Technik, oder gänzlich andere Primäraufgaben erfordert, herunter gebrochen werden kann.

Zum Aufbau eines angemessenen betrieblichen Sicherheitsmanagements müssen die erforderlichen Sicherheitskonzepte im Wesentlichen über drei Ebenen entwickelt werden. F. Ritz (Ritz, 2015) beschreibt diese im Kapitel 4.2.3 "Ebenen technischen Handelns" mit:

1. Makroebene
2. Mesoebene
3. Mikroebene

Gemäss F. Ritz (Ritz, 2015) gilt:
*Auf der **Makroebene** werden zum Schutz von Menschen und Umwelt unter dem Einfluss gesellschaftlicher Akzeptanz und öffentlicher Meinung durch Regierungen Gesetze zur Regulierung der Gestaltung von Mensch-Maschine-Systemen verabschiedet.*

Für die Entwicklung eines allgemein anwendbaren Leitfadens ist diese Aussage jedoch etwas zu eng gefasst. Tatsächlich verabschiedet der Gesetzgeber, insbesondere bei der Anwendung komplexer Technik mit hohem Gefahrenpotential, deutlich mehr Regulierungen als nur zur Gestaltung eines Mensch-Maschine-Systems. Dies kann damit beginnen, dass bestimmte Techniken für eine Primäraufgabe ausgeschlossen werden. Dass bei der Verwendung gewisser Techniken ganz bestimmte Akzeptanzkriterien und Akzeptanzgrenzwerte eingehalten werden müssen. Dass die Art der Nachweisführung zur Einhaltung der geforderten Akzeptanzgrenzwerte vorgeschrieben wird, etc.
Mit diesem Vorgehen schafft der Gesetzgeber eine Art Grundsicherheit, die immer dann verlangt wird, wenn er aufgrund des Gefahrenpotentials mit gesellschaftlichen Folgen aufgrund eines Grossereignisses oder vieler Kleinereignisse rechnen muss. Der gesetzlich festgelegte Verzicht auf den Bau neuer Kernkraftwerke soll ein von einer solchen Anlage möglicherweise ausgehendes Grossereignis verhindern. Die im Arbeitsgesetzt festgelegten Vorgaben sollen viele Kleinereignisse vermeiden helfen, die in ihrer Summe ebenfalls gesellschaftliche Relevanz erlangen würden.

Gemäss F. Ritz (Ritz, 2015) gilt weiter:
*Auf der **Mesoebene** werden die gesetzlichen Vorgaben (aus der Makroebene) in Organisationen durch Gestaltungsmassnahmen umgesetzt.*

Bei dieser Aussage ist es von entscheidender Bedeutung, dass die Gestaltungsmassnahmen im gesamten Entwicklungsprozess zum Aufbau einer Anlage entwickelt werden müssen. Dieser Entwicklungsprozess beinhaltet:

1. Konzept
2. Auslegung
3. Fertigung
4. Montage
5. Inbetriebsetzung
6. Betrieb

Gemäss F. Ritz (Ritz, 2015) gilt ausserdem:
*Auf der **Mikroebene** läuft die operative Mensch-Maschine-Interaktion zur Aufgabenerfüllung ab. Erfahrungen, die auf der Mikroebene gemacht werden, können durch Erfahrungsrückfluss zu Anpassungen auf der Mesoebene genutzt werden.*

Ein betriebliches Sicherheitsmanagement muss alle für die Sicherheit relevanten Prozesse eines technischen und organisatorischen Sicherheitskonzepts enthalten. Dies gilt insbesondere auch für die Aufbauphase, weil dort, z.B. durch geschickte technische Auslegung, sichergestellt werden kann, dass eine sichere Mensch-Maschine-Interaktion im Betrieb möglich gemacht oder inhärente Sicherheit vorgesehen wird, sodass spezifische Gefahren von vorne herein ausgeschlossen werden können.
F. Ritz (Ritz, 2015) beschreibt diese Aufbauphase im Kapitel 4.2.4 "Gestaltung der Mensch-Maschine-Interaktion", für welche im Rahmen dieses Leitfadens das technische und organisatorische Sicherheitskonzept als

tragende Säulen eines betrieblichen Sicherheitsmanagements konkretisiert und so erweitert werden, dass sich daraus für viele Primäraufgaben ein angemessenes betriebliches Sicherheitsmanagement ableiten lässt.

3.1. Sicherheit und Sicherheitsmanagement

Bevor das oben genannte technische und organisatorische Sicherheitskonzept konkretisiert werden kann, muss 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 sicher und durch den Menschen 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, 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.

So einfach und einleuchtend dieser Satz auch klingen mag, so kompliziert sind die sich daraus ergebenden Beziehungen zwischen Menschen, Technik und Organisation (MTO). Dies umso mehr, je komplexer sich die Primäraufgabe darstellt. Es ist möglich ein scheinbar perfektes technisches und organisatorisches Sicherheitskonzept zu haben, welches die Sicherheit jedoch nur ungenügend oder gar nicht gewährleistet.

Wie im Vorwort bereits angemerkt:
Grossen Katastrophen gehen eine Reihe nicht minder grosser Katastrophen voraus.

Von den vorausgehenden Katastrophen - und wir können absolut sicher sein, dass sie immer auch erkannt wurden - hat sich nur niemand betroffen gefühlt. Wenn aber ein perfektes technisches und organisatorisches Sicherheitskonzept vorhanden war, was führte dann zum Versagen des betrieblichen Sicherheitsmanagements? Es ist die Führung. Es ist der Mangel an "Mut zur Verantwortung", es ist der Mangel an Wahrhaftigkeit.

Erklärungsversuche, die den kulturellen Hintergrund der Gesellschaft und die Sozialisierung der Menschen in diesen Gesellschaften heranziehen, verschleiern lediglich den Blick auf das eigentlich ganz einfache Problem und unterstützen ausserdem Aussagen wie: "Was da in Japan passiert ist, das kann hier bei uns in Europa nicht passieren". Es ist immer die Führung, die täglich im Büro beim Erkennen und Beherrschen der vorausgehenden Katastrophen versagt und erst recht dann, wenn eine Katastrophe sich weit über die Bürogrenzen hinaus entwickelt.
Sicherheit zu gewährleisten ist eine komplexe Aufgabe. Sie muss interdisziplinär, getragen vom gemeinsamen Willen das Beste erreichen zu wollen, organisiert werden. Der erste Schritt zur Gewährleistung von Sicherheit muss deswegen darin bestehen komplexe Zusammenhänge zu vereinfachen. Dies gelingt, indem man Struktur erzeugt. Die ersten beiden wichtigen Strukturelemente sind das technische Sicherheitskonzept und das organisatorische Sicherheitskonzept. Sie bilden die beiden wichtigen Säulen des betrieblichen Sicherheitsmanagements.
Demnach verstehen wir betriebliches Sicherheitsmanagement als Gesamtheit aller Vorkehrungen zum Aufbau, Betrieb und zur Weiterentwicklung technischer und organisatorischer Sicherheitskonzepte. Beide sollen gleichwertig nebeneinanderstehen.
Abbildung 2 zeigt den grundsätzlichen Aufbau eines betrieblichen Sicherheitsmanagements, ohne auf die darunterliegenden Details einzugehen.

Technisches Sicherheitskonzept
Der Grundsatz für die Entwicklung eines technischen Sicherheitskonzepts besteht in der *Ausrichtung der technischen Auslegung auf sicherheitsorientierte Grundsätze für die Beherrschung von Technik*

Organisatorisches Sicherheitskonzept

Der Grundsatz für die Entwicklung eines organisatorischen Sicherheitskonzepts besteht in der *Ausrichtung von Menschen &* Organisation *auf sicherheitsorientierte Grundsätze für die Beherrschung von Technik*

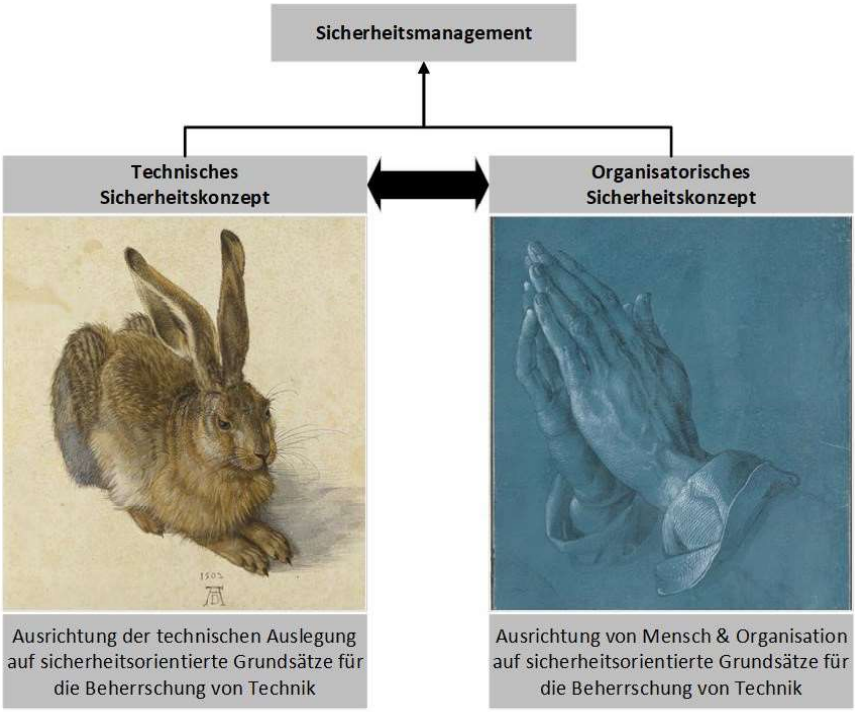

Abbildung 2: Anforderungen an Technische und Organisatorische Sicherheitskonzepte

Im ersten Fall sind besonders die technischen und naturwissenschaftlichen Disziplinen gefordert, die mit ihrer Kunst das Bild einer technischen Auslegung so exakt wie möglich zeichnen müssen. Je besser wir "den Hasen" erkennen umso mehr können wir darauf vertrauen, dass es sich wirklich um einen Hasen handelt und sich dieser nicht irgendwann wie ein Wildschwein verhält.

Im zweiten Fall sind besonders die psychologischen und soziologischen Disziplinen gefordert, die mit ihrer Kunst das Bild einer Ausrichtung von

Mensch und Organisation zur Unterstützung der technischen Auslegung zeichnen müssen. Wenn die oben genannte Ausrichtung von Menschen und Organisation gelingt, kann man von einer guten Sicherheitskultur in der Unternehmung ausgehen. Die Etablierung einer guten Sicherheitskultur ist jedoch keine leichte Aufgabe, an der auch nach dem Aufbau und der Inbetriebnahme eines organisatorischen Sicherheitskonzepts kontinuierlich weitergearbeitet werden muss. Genauso, wie am technischen Sicherheitskonzept, bspw. durch Instandhaltung der Technik, kontinuierlich gearbeitet werden muss.
In beiden Fällen ist bereits während der Entwicklung der Sicherheitsmanagementkonzepte ein reger Austausch zwischen den beiden Disziplinen erforderlich. Nur so kann garantiert werden, dass das betriebliche Sicherheitsmanagement als Ganzes die Sicherheit bei der Erfüllung der Primäraufgabe des Betriebs gewährleistet.
Für unsere Gesellschaft bilden die Gemälde von Albrecht Dürer, jedes für sich alleine, einen immensen Wert. Für ein betriebliches Sicherheitsmanagement ist der Wert seiner einzelnen Komponenten jedoch nahezu unbedeutend. Das betriebliche Sicherheitsmanagement kann erst im Zusammenwirken aller seiner Faktoren zur Entfaltung kommen.
Ein schlechtes Sicherheitsmanagement zeichnet sich dadurch aus, dass nicht klar wird, was betende Hände mit einem Feldhasen zu tun haben. Nun, der erfahrene Leser wird sicher Beispiele aus der eigenen betrieblichen Praxis finden, die ihm genau diese Offenbarung bestätigen.
Insbesondere für den Betrieb hochriskanter Produktions- und Dienstleistungsprozesse unter Einsatz komplexer Technik muss es gelingen, ein betriebliches Sicherheitsmanagement zu entwickeln, das scheinbar nicht in Zusammenhang stehende Dinge in die richtige Beziehung stellt und so dazu beiträgt, den Schutz von Menschen und Umwelt kontinuierlich aufrechtzuerhalten. Damit ist auch schon das über allen Zielen stehende oberste Ziel vorgegeben.

Das übergeordnete Sicherheitsziel:
Der Schutz von Menschen und Umwelt
Diesem Sicherheitsziel dienen alle Anstrengungen und Vorkehrungen, die im Rahmen eines betrieblichen Sicherheitsmanagements organisiert werden müssen.