

Textentwurf der RSK-Ad-hoc-Arbeitsgruppe für eine Neufassung des Modul 8 „Anforderungen an das Sicherheitsmanagement“ (Entwurf Revision B Regelwerksaktualisierung)

Diese Unterlage enthält eine Anlage.

Die Arbeitsgruppe hat eine Überarbeitung des Modul 8 begonnen (siehe unten Nr. 2), hierbei sind folgende Aspekte aus der Diskussion der Arbeitsgruppe als Grundlage verwendet worden:

1. Formaler Abgleich von RSK-Anforderungen mit Modul 8:

Nahezu alle Anforderungen, die den Betreiber betreffen, finden sich sinngemäß in Modul 8 wieder (siehe Anlage 1).

2. Allgemeine Kommentare zu Modul 8:

In dem Textentwurf wurde begonnen, alle Passagen, die eine direkte Verknüpfung zur Anforderung an die Qualitätssicherung aufweisen, in einen Anhang zu verschieben (Nummerierung noch nicht durchgängig angepasst).

Insgesamt sind in Modul 8 Entwurf Revision B zu detaillierte Anforderungen und auch Wiederholungen von Textbausteinen enthalten. Eine Kürzung wäre sinnvoll. Es sind großflächig Texte mit Inhalten aus Regelwerken zu QM-Systemen enthalten, diese sollten wenn überhaupt in einem Anhang zusammengefasst werden. Anforderungen an die „Sicherheitskultur“ sollten im Modul 1 konkretisiert werden.

Die Diskussionen, ob das Darstellungskonzept des Moduls grundsätzlich geändert werden sollte, wurden nicht abgeschlossen, da sich die Arbeitsgruppe nicht einigen konnte. Der Textentwurf wurde von einem Mitglied der Arbeitsgruppe eingereicht, die Bearbeitung des Textes durch die Arbeitsgruppe wurde bis zum Abschnitt 3.5(2)3 vorgenommen. Die Beiträge von Herrn Prof. Wilpert konnten nicht alle ausdiskutiert werden. Ein Abschluss fehlt z. B. für die Aspekte, ob

- die Aufbau- und Ablauforganisation, die sich stark an ISO 9000 orientiert, in einer neuen KTA-Regel konkretisiert werden könnte,
- die Gewährleistung der Qualität in KTA 1401 berücksichtigt werden sollte, und
- die „Auswertung der Betriebserfahrungen...“ am besten bei der Fortschreibung der AtSMV zu berücksichtigen sein sollte.

Anlage 1

Abgleich der RSK-Anforderungen mit Modul 8

herangezogene Unterlage:

„Anlage 2 zum Ergebnisprotokoll der 352. Sitzung der Reaktor-Sicherheitskommission am 13.06.2002

RSK - STELLUNGNAHME

13.06.2002

Memorandum der RSK zur Gewährleistung einer angemessenen Sicherheitskultur“

RSK-Memorandum

behandelt in Modul 8

4.2 Strukturänderungen und Personalabbau

- Die Veränderungen betreffen teilweise langjährig bewährte Organisationsstrukturen, die eine der Voraussetzungen für den sicheren Betrieb darstellen. Die Veränderung von Weisungslinien und Informationswegen sowie die neue Zuordnung von Verantwortung und Kompetenzen beeinflussen die organisatorische Basis der Sicherheit. Abschnitt 3.1, Seite 6
- Durch den Personalabbau wird die für alle in einem Kraftwerk anfallenden Tätigkeiten zur Verfügung stehende Personalstärke reduziert. Dabei ist zu beachten, dass die Personalressourcen zur Erfüllung aller sicherheitstechnischer Aufgaben nicht unterschritten werden. Auch wenn in den ausgewiesenen sicherheitsrelevanten Bereichen kein Personalabbau vorgenommen wird könnte infolge von Umverteilung von Aufgaben und einer daraus resultierenden größeren Aufgabenlast für das verbleibende Personal die Sicherheit dennoch negativ beeinflusst werden. Abschnitt 3.3
- Personalabbau, insbesondere durch Vorruhestandsregelungen, betrifft überwiegend betriebsbewährtes Personal und Know-how-Träger. Erfolgt die Freistellung dieser Mitarbeiter zu schnell oder wird sie nicht von geeigneten Maßnahmen zum Know-how-Transfer begleitet, geht wertvolles Erfahrungswissen verloren. Abschnitt 3.3 (2) 2, Seite 12
- Einer der wichtigsten Garanten für den sicheren Betrieb sind die Motivation und das Engagement der Mitarbeiter. Unsicherheit über den Erhalt des Arbeitsplatzes im Zuge von Stilllegungen, Fusionen und Umstrukturierungen können diese Erfolgsfaktoren empfindlich beeinflussen. Abschnitt 3.3 (3), Seite 12

4.3 Outsourcing und Zentralisierung

- Es muss sichergestellt werden, dass die organisatorischen Voraussetzungen hinsichtlich eindeutiger Verantwortungsstrukturen weiterhin gegeben und dass Verantwortung, Fachkunde und Kompetenzen der verantwortlichen Personen

- kongruent sind.
- In der Anlage müssen weiterhin diejenigen Kompetenzen verbleiben, die notwendig sind, in Anspruch genommene Leistungen zu spezifizieren, deren Ausführung qualifiziert zu überwachen und die Ergebnisse der erbrachten Fremdleistungen zu bewerten.
- 4.4 Kompetenz- und Wissenserhalt**
Um auch weiterhin den hohen Sicherheitsstandard halten zu können, müssen die erworbenen Kompetenzen erhalten werden. Als drängendstes Problem zeigt sich hier die Frage des Generationenwechsels.
...
...
Durch extensive Vorruhestands- und Altersteilzeitregelungen wird diese Entwicklung vor allem dadurch verstärkt, dass die für einen geordneten Wissenstransfer erforderlichen Zeiten oft nicht mehr zur Verfügung gestellt werden. Die Nachwuchssituation leidet außerdem darunter, ...
- 4.5 Wissenschaftlich-technische Infrastruktur**
In der Vergangenheit haben die Betreiber auf Grund einer vorhandenen guten Infrastruktur von Herstellern, Fachfirmen und Dienstleistern bestimmtes Know-how und Dienstleistungen nicht selbst aufgebaut bzw. ausgelagert. Inzwischen haben fehlende Neubauprojekte im Inland, ...
... Nukleargeschäft ab. Damit ist auch ein Know-how-Verlust verbunden, der von den Betreibern kerntechnischer Anlagen nur durch den Aufbau eigenen Know-hows kompensiert werden könnte. Dies steht allerdings im Widerspruch zu der beobachteten Entwicklung, Eigenpersonal abzubauen.
- 5 Schlussfolgerungen und Empfehlungen**
- Konkretisierung der Sicherheitspolitik
Die Grundvoraussetzung für eine Weiterentwicklung der Sicherheitskultur ist eine aktive Sicherheitspolitik der Betreibergesellschaft. Diese Sicherheitspolitik sollte in einem klaren, deutlichen und öffentlichen Bekenntnis zur Sicherheit festgeschrieben werden. Dabei sollten die Sicherheitsverantwortung der Unternehmensleitung zum Ausdruck gebracht werden und die daraus resultierenden Anforderungen in konkrete Aussagen und Vorgaben umgesetzt werden.
- Die Aufsichtsbehörden sollten diese Festschreibung und Konkretisierung der Sicherheitspolitik von den Unternehmen einfordern und die Umsetzung begleiten. Im Sinne eines offenen vertrauensvollen Dialogs zwischen Betreiber und Behörde sollte die Behörde die von ihr diesbezüglich gestellten Anforderungen definieren und offen mit dem Betreiber diskutieren.

Abschnitt 3.2 (1) 1,
Seite 11Abschnitt 3.3 (2) 2,
Seite 12Abschnitt 3.3 (4) 3
ist durch Abschnitt 3.3
(2) abgedeckt

Abschnitt 3.2 (1) 1

Abschnitt 3.2 (1) 1

RSK-Memorandum**behandelt in Modul 8**

- In gleicher Weise sollten Genehmigungs- und Aufsichtsbehörden für ihre Tätigkeiten ein **übergeordnetes Sicherheitsleitbild** festschreiben und Aufsichtleitlinien im Sinne der Sicherheitskultur definieren.
- Nachvollziehbarkeit von **Organisationsänderungen**
Organisatorische Änderungen bergen Chancen und Risiken. Im Sinne einer ausgeprägten Sicherheitskultur **muss bei organisatorischen Veränderungen der Nachweis geführt werden, dass damit keine Beeinträchtigung der Sicherheit verbunden ist.** Dies bedingt Vergleiche ...
durch Abschnitt 3.2 (1) 1 und Abschnitt 3.1 abgedeckt
 - Konzepte zum **Kompetenzerhalt**
Zur Gewährleistung des gegenwärtigen Sicherheitsniveaus in den Anlagen und zum Qualitätserhalt der erforderlichen behördlichen Aufsicht hält es die RSK für erforderlich, **ein Gesamtkonzept zum Kompetenzerhalt zu entwickeln. Das Management von Wissen**, insbesondere des Erfahrungswissens der in der Kerntechnik tätigen Personen kann diesem Kompetenzverlust entgegensteuern, neue Kompetenzen aufbauen und somit dazu beitragen, ...
Abschnitt 3.3 (2) 2
Im Zusammenhang mit den zuvor beschriebenen Veränderungen der Rahmenbedingungen sind daher **Maßnahmen zum Erhalt und Transfer des in der Reaktorsicherheit vorhandenen Wissens und ein effizienter Umgang mit der Ressource Wissen in einem auch finanziell enger werdenden Umfeld von allen Beteiligten gefordert.**
Alle beteiligten Institutionen sollten Anreize und Perspektiven entwickeln, **um qualifizierte Nachwuchskräfte für einen beruflichen Einstieg in die Kerntechnik zu motivieren.**
indirekt abgedeckt durch Abschnitt 3.3 (4) 3
 - Erhalt und Weiterentwicklung der Sicherheit
... notwendig. Die Verwendung von europäischem und internationalem Know-how und Hardware verlangt eine **Öffnung des bislang durch sehr spezifische Regelwerke abgegrenzten deutschen Marktes für ausländische Anbieter.** Die RSK unterstreicht deshalb die **Notwendigkeit einer Vereinheitlichung der sicherheitstechnischen Anforderungen und des Regelwerks auf europäischer Ebene.** Dabei ist darauf zu achten, ...
keine Anforderung
 - **Verhältnis zwischen Betreiber und Behörde**
Erforderliche Anpassungen der Anlage an den Stand von Wissenschaft und Technik sowie Maßnahmen zum Erhalt des Sicherheitsniveaus sollten zum einen hinsichtlich der zu erfüllenden Anforderungen, den Nachrüstumfängen und für die Nachweisführung für den Betreiber mit einer hinreichenden Planungssicherheit verbunden sein, zum anderen
Abschnitt 3.2 (1) 1

sollte das Bewusstsein und der Wille der Betreiber vorhanden sein, derartige Anpassungen vorzunehmen. Divergierende Meinungen sollten sachbezogen und offen diskutiert werden. Nach Feststellung der Zulässigkeit der beantragten Maßnahmen sollten diese zügig umgesetzt werden. Bei der Bewertung der Zulässigkeit ist die Verträglichkeit der Änderungsmaßnahmen mit dem bestehenden Sicherheitskonzept der Anlage sicherzustellen.

Die Sicherheitskultur des Anlagenbetreibers zeigt sich im Verhältnis zu der Behörde auch dadurch, dass er der Aufsichtsbehörde (und den hinzugezogenen Gutachtern) rechtzeitig alle erforderlichen Informationen zukommen lässt, so dass diese den sicheren Betrieb der Anlage beurteilen und bei Erfordernis aufsichtlich eingreifen kann. Dazu gehört auch, dass die Erkenntnisse aus Forschung und Entwicklung und aus der Betriebserfahrung (Meldewesen, Ereignisse unterhalb der Meldeschwelle, Alterungsmanagement etc.) analysiert, dokumentiert und kommuniziert werden.

Abschnitt 3.2 (1) 1

... Bei der Festlegung und Umsetzung der Maßnahmen sollten die Behörden ihrerseits die Förderung der Sicherheitskultur durch transparentes Handeln und vertrauensvolle Kommunikation im Auge haben.

Abschnitt 3.2 (1) 1

- Einbindung der Öffentlichkeit
Neben der Beteiligung der Öffentlichkeit auf der Grundlage gesetzlicher Verpflichtungen sind die angemessene Information der Öffentlichkeit durch Betreiber und Behörden und die Transparenz des sicherheitsgerichteten Handelns aller Beteiligten ein wesentlicher Teil der Sicherheitskultur.

Abschnitt 3.3 (1) 1

- Verfolgung der Sicherheitsleistung (Safety Performance)
... auf die Sicherheit der Anlagen müssen auch durch zeitnahe Verfolgung der Safety Performance verhindert werden. Hierzu sind ...

Abschnitt 3.0

... Eine solche Beurteilung sollte nach Ansicht der RSK auf einem Selbsteinschätzungsprozess des Betreibers basieren. Eine Unterstützung durch externen Sachverstand im Auftrag des Betreibers kann dabei hilfreich sein. Dieser Prozess der Selbstbewertung sollte in regelmäßigen Abständen wiederholt und zu einer festen Einrichtung innerhalb einer kerntechnischen Anlage/Organisation werden. Dadurch lässt sich die Wirksamkeit der ergriffenen Maßnahmen zur Gewährleistung der Sicherheit überprüfen oder das Nachlassen der Sicherheitsleistung erkennen.

Abschnitt 3.1 (3)

Abschnitt 3.5 (4) 3

Die Aufsichtsbehörden müssten solche

Selbsteinschätzungsprozesse der Betreiber einfordern, begleiten und überprüfen. Dabei ist dem Zielkonflikt zwischen der notwendigen aufsichtlichen Überwachungstiefe der Sicherheitskultur einerseits und der Förderung der Eigenverantwortung der Betreiber für die Weiterentwicklung der Sicherheitskultur andererseits Rechnung zu tragen. Die Überwachung der Vorgehensweise des Betreibers sollte sich primär auf die Einrichtung des Prozesses und die Bewertung seiner Ergebnisse fokussieren. Zur Verfolgung der Safety Performance sollten bundeseinheitlich geeignete Instrumente, Kriterien und Vorgehensweisen entwickelt werden.

Textentwurf der AG 4

Gliederung

1	Zielsetzung und Geltungsbereich	8
2	Grundsätzliche Anforderungen an das Sicherheitsmanagement	8
3	Anforderungen an das Sicherheitsmanagementsystem.....	9
3.0	Sicherheitsmanagementsystem.....	9
3.1	Managementzyklus.....	11
3.2	Sicherheitspolitik und Sicherheitsziele.....	12
3.3	Ressourcenbereitstellung	14
3.4	Aufbauorganisation.....	16
3.5	Ablauforganisation	17
3.6	Dokumentation.....	26
4	Anforderungen an die Gewährleistung der Qualität und den Erfahrungsrückfluss.....	28
4.1	Gewährleistung der Qualität	28
4.2	Auswertung von Betriebserfahrung und anderen Erkenntnissen, Erfahrungsrückfluss und Informationsaustausch.....	30

1 Zweck und Geltungsbereich

1.1 Dieser Regeltext konkretisiert die Anforderungen der „Sicherheitsanforderungen für Kernkraftwerke: Grundlegende Sicherheitsanforderungen“ (Modul 1), Abschnitt 1, an das Sicherheitsmanagement in Kernkraftwerken. Dargestellt werden die Anforderungen

- an das Sicherheitsmanagement,
- an die einzelnen Prozesse und
- an den Nachweis der Wirksamkeit.

Im Folgenden werden ausschließlich Anforderungen formuliert, die die kerntechnische Sicherheit betreffen. Sie gelten analog bei Integration des Sicherheitsmanagements in ein integriertes Managementsystem.

1.2 Die nachfolgenden Anforderungen gelten unabhängig von der Organisationsstruktur des Betreibers für alle Organisationseinheiten des Unternehmens, die auf die Sicherheit des Kernkraftwerks Einfluss haben können.

2 Grundsätzliche Anforderungen an das Sicherheitsmanagement

2.1 Der sichere Betrieb von Kernkraftwerken erfordert ein Sicherheitsmanagement, das die Ziele und Aktivitäten aller Unternehmensbereiche zur Gewährleistung eines sicheren Betriebs zusammenfasst.

Das Sicherheitsmanagement umfasst die Gesamtheit der Tätigkeiten zu sachgerechten Planung, Organisation, Leitung und Kontrolle von Personen und Arbeitsaktivitäten. Die Zielsetzungen des Sicherheitsmanagements sind die

- Gewährleistung der Sicherheit, die
- stetige Verbesserung der Sicherheit sowie die
- Förderung der Sicherheitskultur.

Dies erfordert die Gewährleistung einer hohen Qualität der sicherheitsrelevanten Infrastruktur, Prozesse und Tätigkeiten.

Hinweis Die sicherheitsrelevanten Prozesse umfassen zum Beispiel: Betreiben der Anlage, Betriebsbereithaltung der Anlage (einschließlich Instandhaltung und Durchführung von Änderungsmaßnahmen), Bereitstellen von Brennelementen, Behandlung radioaktiver Abfälle, Entwicklung von Unternehmenszielen, Alterungsmanagement, Wissensmanagement, Unternehmenskommunikation sowie Anlagenüberwachung, Personalauswahl und -ausbildung, Ereignismeldung und -analyse, Dokumentenhandhabung, Beschaffung und Lagerung sowie den Prozess Sicherheitsmanagement.

Die aus dem Sicherheitsmanagement abgeleiteten Anforderungen und die Anforderungen, die aus anderen Zielen des Unternehmens erwachsen, werden in einem integrierten Ansatz und in nachvollziehbarer und transparenter Weise unter Berücksichtigung der Priorität der Sicherheit abgeglichen, gewichtet und eindeutig festgelegt.

2.3 Zur Realisierung des Sicherheitsmanagements wird ein Sicherheitsmanagementsystem eingerichtet, das alle Festlegungen, Regelungen und organisatorischen Hilfsmittel zur Planung, Durchführung, Überprüfung und stetigen Verbesserung sicherheitsrelevanter Tätigkeiten und Prozesse zusammenfasst.

3 Übergeordnete Anforderungen an das Sicherheitsmanagementsystem

3.1 Sicherheitsmanagementsystem

3.1 (1) Die Ziele des Sicherheitsmanagementsystems sind, einen sicheren Betrieb zu gewährleisten sowie eine stetige Verbesserung der Sicherheit und des Sicherheitsbewusstseins der Mitarbeiter herbeizuführen. Deshalb fördert das Sicherheitsmanagementsystem die Bereitschaft zum stetigen Lernen und einen offenen Informationsaustausch in Sicherheitsfragen innerhalb des Unternehmens über alle Hierarchieebenen.

3.1 (2) Das Sicherheitsmanagementsystem gibt frühzeitig Hinweise auf mögliche Beeinträchtigungen der Sicherheit.

3.1 (3) Das Sicherheitsmanagementsystem ist prozessorientiert aufgebaut. Um zu gewährleisten, dass die sicherheitsrelevanten Aufgaben sicher geplant,

abgewickelt sowie die Zielerreichung kontrolliert und verbessert werden, wird im Sicherheitsmanagementsystem der geschlossene Managementzyklus (auch PDCA-Zyklus genannt, für „Plan – Do – Check – Act“) angewandt. Dieser besteht aus den Phasen Planen, Durchführen, Überprüfen und Verbessern.

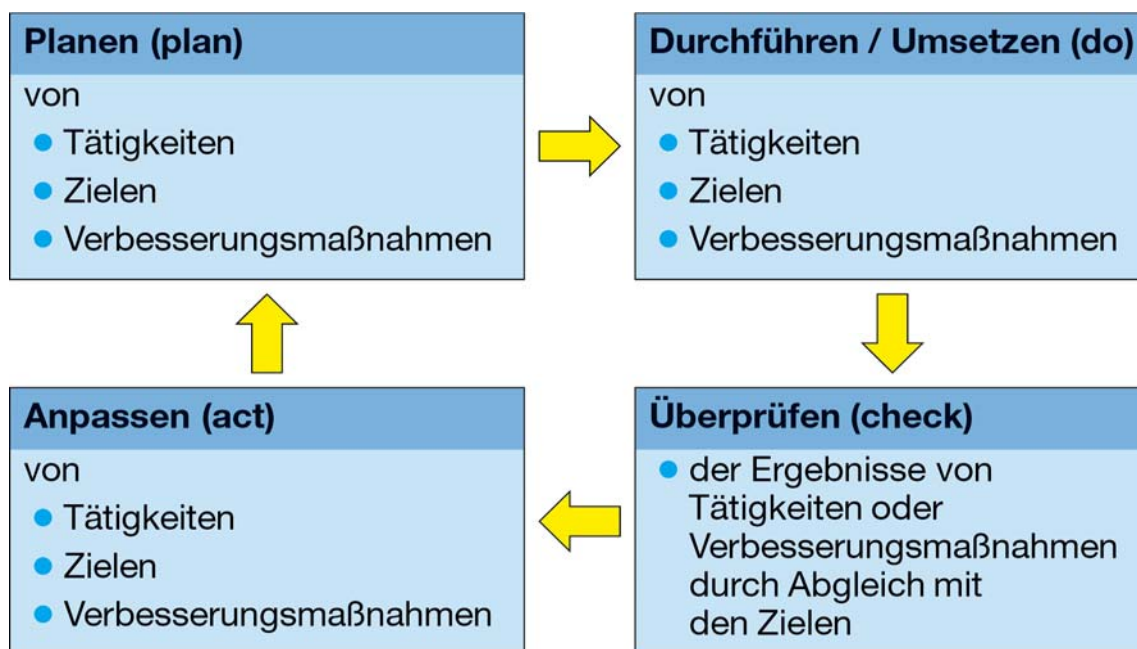


Abb. 1: Beispiel eines PDCA-Zyklusses

Das Organisieren des Sicherheitsmanagementsystems ist ein eigenständiger Prozess, auf den der Managementzyklus ebenfalls angewandt wird.

Hinweis: Das Organisieren des Sicherheitsmanagementsystems wird im Folgenden als „Prozess Sicherheitsmanagement“ bezeichnet. Dieser Prozess ist im Anhang xx beschrieben.

Sicherheitsziele sind mit anderen Unternehmenszielen abgestimmt, wobei die Sicherheitsziele oberste Priorität haben. Das Sicherheitsmanagementsystem ist mit anderen Managementsystemen abgestimmt. (Hinweis: Bezüge zu Strahlen-/Arbeitsschutz)

3.1 (4) Die Einführung, Aufrechterhaltung und Verbesserung des Sicherheitsmanagementsystems liegt in der Verantwortung der Unternehmensführung.

Die Unternehmensführung hat dabei insbesondere folgende Aufgaben:

- Koordination der Entwicklung und Einführung des Sicherheitsmanagementsystems
- Verfolgen der Umsetzung des Sicherheitsmanagementsystems einschließlich seines Einflusses auf die Sicherheit und die Sicherheitskultur sowie der nötigen Verbesserungen
- Koordination der Überprüfung und der kontinuierlichen Verbesserung des Sicherheitsmanagementsystems
- Lösen der Zielkonflikte zwischen verschiedenen Anforderungen und innerhalb der sicherheitsrelevanten Prozesse.
- Vorleben und aktive Unterstützung von sicherheitsgerichtetem Handeln und Förderung der Sicherheitskultur.

3.2 Managementzyklus

In der prozessorientierten Unternehmenslenkung wird der PDCA-Zyklus auf folgenden verschiedenen Ebenen im Unternehmen angewendet: Tätigkeitsebene, Prozessebene und Managementebene (siehe Abb. 2).

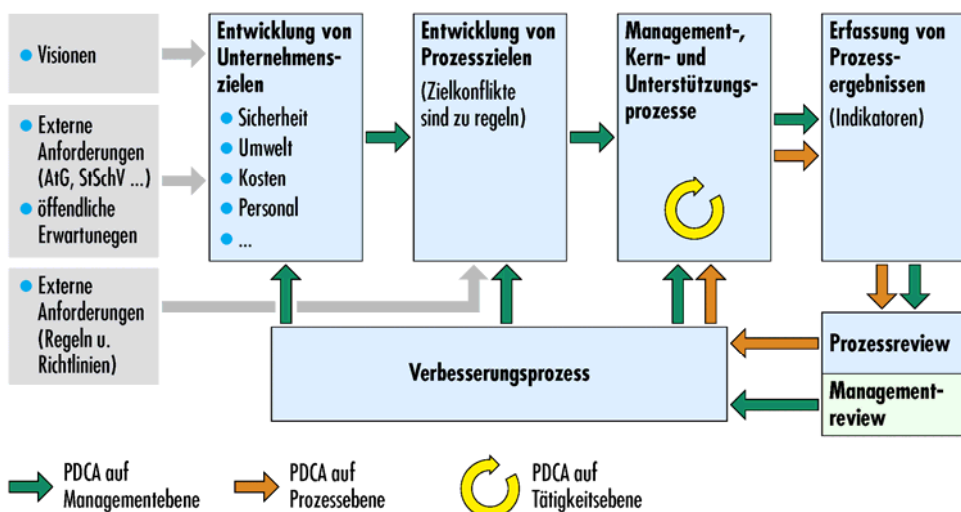


Abb. 2 Integriertes Managementsystem

Hinweis In Anhang ist der Prozess Sicherheitsmanagement beispielhaft beschrieben.

4 Anforderungen an die Elemente des Sicherheitsmanagementsystems

4.1 Sicherheitspolitik und Sicherheitsziele

4.1 Die Unternehmensführung legt eine Sicherheitspolitik fest, welche der Sicherheit oberste Priorität einräumt. Aus der Sicherheitspolitik werden für alle Funktionsbereiche und Hierarchieebenen des Unternehmens, die Einfluss auf die Sicherheit haben können, eindeutige, messbare und hinsichtlich der Sicherheitspolitik sowie untereinander widerspruchsfreie Sicherheitsziele abgeleitet.

4.1 (1) Grundsätze der Sicherheitspolitik

Die Sicherheitspolitik wird als integraler Bestandteil der gesamten Unternehmenspolitik betrachtet und beinhaltet mindestens folgendes:

- Eine unternehmensspezifische Sicherheitskultur ist auszugestalten, zu fördern und weiter zu entwickeln.
- Die Einhaltung der Sicherheitsziele hat Vorrang vor allen anderen Unternehmenszielen wie Unternehmensgewinn, Produktivität und Termineinhaltung.
- Die Sicherheit der Anlagen wird überprüft und kontinuierlich verbessert.
- Die Anlage wird in Übereinstimmung mit den gesetzlich und behördlich vorgegebenen sicherheitsrelevanten Anforderungen betrieben.
- Die für die Umsetzung der Sicherheitspolitik erforderlichen Ressourcen werden bereitgestellt.

4.1 (2) Festlegung der Sicherheitsziele

Die Sicherheitsziele werden aus der Sicherheitspolitik abgeleitet. Mit der Festlegung von Sicherheitszielen wird die Sicherheitspolitik in operative Vorgaben für sicherheitsrelevante Prozesse (z. B. Betrieb der Anlage, Instandhaltung der Anlage, Erfahrungsrückfluss, Personalmanagement etc.) umgesetzt.

4.1 (3) Umsetzung der Sicherheitspolitik und der Sicherheitsziele

Die Unternehmensführung und die Führungsebene der Anlage leben sicherheitsgerichtetes Handeln vor, um die Sicherheitskultur zu stärken und zu fördern sowie Sicherheitspolitik und Sicherheitsziele durchzusetzen. Dazu gehören:

- Die Unternehmensführung und die Führungsebene der Anlage identifizieren sich mit der Sicherheitspolitik des Unternehmens und unterstützen diese aktiv.
- Die Unternehmensführung und die Führungsebene der Anlage nehmen eine Vorbild- und Kontrollfunktion wahr.

Die Unternehmensführung ergreift die erforderlichen Maßnahmen dafür , dass alle Mitarbeiter, die Inhalte und Aussagen der Sicherheitspolitik in ausreichendem Maß verstehen und sich ihrer eigenen Funktion bei der Gewährleistung der Sicherheit bewusst sind.

4.1 (4) Überprüfung der Sicherheitspolitik und Sicherheitsziele

Das Unternehmen überprüft die Sicherheitspolitik und die Sicherheitsziele in angemessen Abständen und bei besonderen Anlässen hinsichtlich ihrer Wirksamkeit und Vollständigkeit. Die Zielerreichung wird nachvollziehbar überprüft.

3.2 (4) Verbesserung der Sicherheitspolitik und Sicherheitsziele

Das Unternehmen leitet aus den Ergebnissen der Überprüfung Verbesserungsmaßnahmen für die Sicherheitspolitik und die Sicherheitsziele ab.

3.3 **Ressourcenbereitstellung**

Der Leiter der Anlage ist insbesondere verantwortlich für die Ermittlung der erforderlichen Ressourcen, die zur Einführung, zur Umsetzung, zum Aufrechterhalten und zur stetigen Verbesserung aller sicherheitsrelevanten Prozesse. Er ermittelt die erforderlichen Ressourcen auf Basis eines geeigneten Verfahrens. Die Unternehmensführung stellt ihre Verfügbarkeit sicher. Die erforderlichen Ressourcen umfassen

- eine ausreichende Infrastruktur,
- ausreichendes und qualifiziertes Personal einschließlich Fremdpersonal (personelle Ressourcen),
- finanzielle Ressourcen,
- Information und Wissen, Unterstützung durch externe Organisationen,
- angemessene Arbeitsumgebung und Arbeitsbedingungen,
- geregelte Zusammenarbeit mit externen Organisationen.

3.3 (1) Infrastruktur

Die für den sicheren Betrieb der Anlage, für die Umsetzung der Sicherheitspolitik und das Erreichen der Sicherheitsziele erforderliche Infrastruktur wird ermittelt, festgelegt, bereitgestellt und erhalten. Zur Infrastruktur zählen die Anlage selbst einschließlich der Ausrüstungen (Hard- und Software), Werkzeuge, Hilfsstoffe sowie unterstützende Tätigkeiten und Prozesse (Information, Kommunikation, Transport).

Die Methoden der Instandhaltung werden festgelegt, um die erforderliche Wirksamkeit und Zuverlässigkeit der Einrichtungen sicherzustellen, so dass die Infrastruktur stets der Sicherheitspolitik und den Sicherheitszielen entspricht. Die Art und Häufigkeit der Instandhaltung sowie die Verifizierung der anforderungsgerechten Funktionsfähigkeit der Infrastruktur (z.B. durch wiederkehrende Prüfungen) richten sich nach deren sicherheitstechnischen Bedeutung.

3.3 (2) Personelle Ressourcen

Die Anzahl von Mitarbeitern und ihre Kompetenz, die für die Umsetzung der Sicherheitspolitik, für das Erreichen der Sicherheitsziele und zur Durchführung sicherheitsrelevanter Tätigkeiten und Prozesse erforderlich sind, werden ermittelt, bereitgestellt und erhalten. Dabei werden auch die Anzahl von Mitarbeitern und ihre Kompetenz berücksichtigt, die aus den sicherheitstechnischen Anforderungen an Stellvertreter- und Bereitschaftsregelungen folgen. Die Festlegung der personellen Ressourcen berücksichtigt auch die Anforderungen, die sich aus den Erfordernissen des Wissenstransfers und -erhalts ergeben. Die Anzahl von Mitarbeitern und ihre Kompetenz werden regelmäßig überprüft und erforderlichenfalls angepasst.

3.3 (3) Arbeitsumgebung und Arbeitsbedingungen

Alle zur Durchführung von sicherheitsrelevanten Arbeiten erforderlichen Einrichtungen, Hilfsmittel und schriftlichen Anweisungen sind nach arbeitswissenschaftlichen Grundsätzen der Ausgestaltung von Arbeitsplätzen und der Informationsdarbietung gestaltet.

Die Arbeitsumgebung und die Arbeitsbedingungen

- sind den menschlichen Fähigkeiten und den sicherheitstechnischen Erfordernissen angepasst,
- sind, wie die Hilfsmittel und schriftlichen Anweisungen, situationsgerecht gestaltet,
- beeinflussen die Motivation, Zufriedenheit und Leistung der Mitarbeiter positiv,
- ermöglichen die Durchführung der geplanten Arbeiten auf eine sichere Art und Weise ohne unangemessene physische und mentale Belastungen für die Mitarbeiter.

3.3 (4) Zusammenarbeit mit externen Organisationen

Die Zusammenarbeit mit Behörden und Sachverständigen sowie sonstigen externen Organisationen (z.B. Hersteller, Zulieferer, Fremdfirmen) ist geregelt und koordiniert. Die Schnittstellen zu externen Organisationen sind für die durchzuführenden Arbeiten definiert

- 3.3 (4) 1 Für die Zusammenarbeit mit Behörden und Sachverständigen sind Prozesse etabliert.
- 3.3 (4) 2 Die Abgrenzung und die Schnittstellen sowie das Zusammenwirken und die Wechselwirkungen mit sonstigen externen Organisationen sind unter Berücksichtigung der sicherheitstechnischen Bedeutung definiert.

Die Aufgaben der Hersteller, Zulieferer und Fremdfirmen sind festgelegt und die von ihnen zu erfüllenden Qualitätsanforderungen spezifiziert.

Die Tätigkeiten des Fremdpersonals werden durch Mitarbeiter der Anlage kontrolliert und überwacht, um zu gewährleisten, dass die spezifizierten Qualitätsanforderungen eingehalten werden (siehe Ziffer 3.5 (3)). Das Betreiberpersonal ist für diese Aufgaben qualifiziert und geschult, damit es mögliche sicherheitstechnisch bedeutsame Abweichungen erkennen und korrigieren kann. Der Personalbedarf zur Spezifikation und Abnahme von Leistungen sowie zur Überwachung von Fremdpersonal durch Betreiberpersonal wird ermittelt, festgelegt, überwacht und ggf. modifiziert.

- 3.3 (4) 3 Das Unternehmen trifft Vorkehrungen, um die kompetente ingenieurtechnische und technische Unterstützung, die durch externe Organisationen bereitgestellt wird, in allen sicherheitsrelevanten Bereichen für die gesamte Betriebsdauer der Anlage zu erhalten.

3.4 Aufbauorganisation

- 3.4 (1) Die Unternehmensführung legt eine Organisationsstruktur fest, die mit der Sicherheitspolitik und den Sicherheitszielen im Einklang steht. Aufgaben, Verantwortung und Befugnisse (Entscheidungs- und Weisungsbefugnisse) sind innerhalb des Unternehmens von der Führungsebene bis zur Ausführungsebene eindeutig zugeordnet, mit den Betroffenen abgestimmt und bekannt gemacht. Die Aufgaben und Zuständigkeiten der einzelnen Organisationseinheiten sind

überschneidungsfrei zugeordnet und die Schnittstellen geregelt. Dabei sind auch die Schnittstellen zu externen Organisationen einbezogen.

Position, Aufgaben, Verantwortung und Befugnisse von Organisationseinheiten und Personen sind eindeutig spezifiziert. Die Übereinstimmung von Aufgaben, Befugnissen und Verantwortung ist gewährleistet. Aufgaben sind so zugeordnet, dass für den Einzelnen keine Interessenkonflikte entstehen. Grundsätzlich ist die interne Überwachung der Wirksamkeit des Sicherheitsmanagements unabhängig von den ausführenden Organisationseinheiten gestaltet.

Hinweis Siehe auch die Anforderungen aus der Strahlenschutzverordnung und der Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung.

Der Leiter der Anlage hat die übergeordnete Steuerung und Verantwortung für alle sicherheitsrelevanten Tätigkeiten. In der Wahrnehmung seiner Verantwortung wird der Leiter der Anlage von der Unternehmensführung unterstützt. Dazu gehört auch, dass in Übereinstimmung mit dem Leiter der Anlage die sicherheitsrelevante Planungen und Entscheidungen des Unternehmens getroffen werden.

In der Aufbauorganisation sind die Verantwortlichkeiten für die Tätigkeiten und Prozesse festgelegt. Die Abhängigkeiten zwischen den verschiedenen Arbeitsabläufen werden berücksichtigt

- 3.4 (2) Behördlich geforderte „Beauftragte“ (z.B. Strahlenschutzbeauftragte nach StrlSchV, Sicherheitsbeauftragter nach AtSMV) sind entsprechend ihrer Aufgabenstellung und Zuständigkeit in der Aufbauorganisation berücksichtigt.
- 3.4 (3) Die Organisationsstruktur mit den zugehörigen Festlegungen ist dokumentiert. Hierzu gehören u. a. ein Organisationsplan und Stellenbeschreibungen für alle Stellen/ Stellengruppen der Organisation.

3.5 Ablauforganisation

- 3.5 (1) Die Ablauforganisation ist in einer Weise festgelegt, dass die sicherheitsrelevanten Prozesse und Tätigkeiten auf allen Sicherheitsebenen gemäß den Anforderungen des Sicherheitsmanagements (Kapitel 2) realisiert werden, d. h. sie werden systematisch mit hoher Qualität geplant, durchgeführt,

überprüft und verbessert. Hierzu werden alle sicherheitsrelevanten Prozesse und Tätigkeiten einschließlich des Prozesses Sicherheitsmanagement identifiziert, ihre Abfolge, ihr Zusammenwirken und ihre Wechselwirkungen werden definiert. Dabei werden die Abhängigkeiten zwischen den verschiedenen Arbeitsabläufen berücksichtigt. Im Anhang sind die wesentlichen Anforderungen aufgeführt.

3.5 (2) Anforderungen an die Realisierung sicherheitsrelevanter Tätigkeiten und Prozesse

3.5 (2) 1 Planung von Tätigkeiten und Prozessen

Das Unternehmen gewährleistet bei der Planung der Tätigkeiten und Prozesse:

- Die Sicherheitsziele und Anforderungen an Prozessdurchführung und Prozessergebnisse sind ermittelt, festgelegt und dokumentiert.
- Die Anforderungen werden vor ihrer Einführung bewertet, um sicherzustellen, dass sie klar definiert und erfüllbar sind.
- Bei Änderungen von Anforderungen werden die betroffenen Dokumente angepasst.
- Die Anforderungen aus den Prozessen anderer Managementsysteme sind einbezogen. Konkurrierende Anforderungen sind derart geregelt, dass der Vorrang der sicherheitsrelevanten Anforderungen eindeutig definiert und nachvollziehbar ist.
- Die Vorbeugungsmaßnahmen zur Verhinderung von Fehlern bzw. zur Verhinderung der Auswirkungen auftretender Fehler sind festgelegt.
- Die erforderlichen Verifizierungs-, Validierungs-, Überwachungs- und Prüfschritte mit den dazugehörigen Kriterien zur Bewertung der Prozesse und Prozessergebnisse sind festgelegt.
- Die erforderlichen Aufzeichnungen, um nachzuweisen, dass die Prozesse und Prozessergebnisse die Anforderungen erfüllen, sind festgelegt.
- Die erforderlichen Ressourcen für die Erreichung des angestrebten Prozessergebnisses sind festgelegt.

- Die Vorkehrungen, die vorgesehen werden müssen, um bei der Durchführung der Tätigkeiten die z.B. Anforderungen des Strahlenschutzes und des Arbeitsschutzes einzuhalten sowie die kerntechnischen Sicherheit sicherzustellen, sind festgelegt.
- Für alle Tätigkeiten sind die jeweils zuständigen Organisationseinheiten spezifiziert, ggf. erforderliche Bezüge zu detaillierten Arbeitsanweisungen, zu anderen Tätigkeiten oder Prozessen sind hergestellt.

Bei der Planung der Tätigkeiten und Prozesse ist sichergestellt, dass die sicherheitstechnische Bedeutung jeder Maßnahme angemessen bewertet und berücksichtigt wird.

3.5 (2) 2 Durchführung von Tätigkeiten und Prozessen

Der Betreiber (Das Unternehmen?) führt die sicherheitsrelevanten Tätigkeiten und Prozesse unter kontrollierten Bedingungen durch. Kontrollierte Bedingungen enthalten, falls zutreffend,

- die Verfügbarkeit von internen und externen Anforderungen (Angaben zu Sicherheitszielen sowie Prozessvorgaben und Prozessergebnissen),
- die Verfügbarkeit von Arbeitsanweisungen,
- den Gebrauch geeigneter Hilfsmittel.

Der Betreiber legt für sicherheitsrelevante Tätigkeiten und Prozesse Regelungen fest, die eine Statuskennzeichnung des Durchführungsstands der Tätigkeiten sicherstellen. Der Ablauf der Tätigkeiten wird kontrolliert und koordiniert, der Fortschritt der Tätigkeiten wird dokumentiert und die Rückverfolgbarkeit der Tätigkeiten wird gewährleistet.

Es ist sichergestellt, dass Tätigkeiten, die ungeplant unterbrochen wurden, erst dann wieder aufgenommen werden, wenn unter den gegebenen Randbedingungen die relevanten Sicherheitsanforderungen eingehalten sind.

3.5 (2) 3 Überwachung von Tätigkeiten und Prozessen

Der Betreiber überwacht alle sicherheitsrelevanten Tätigkeiten und Prozesse. Dazu gehören

- die Verfügbarkeit und der Gebrauch geeigneter Überwachungs- und Messmittel,
- die Durchführung von Überwachungen und Messungen sowie Freigabe des Prozessergebnisses.

Sämtliche sicherheitsrelevanten Tätigkeiten und Prozesse, deren Ergebnisse nicht durch nachfolgende Überwachung verifiziert werden können, werden validiert.

3.5 (2) 3a Korrekturmaßnahmen

Der Betreiber ergreift Korrekturmaßnahmen zur Beseitigung der Ursachen von unzureichenden Prozessergebnissen, um Wiederholungen zu vermeiden. Die Entwicklung und Umsetzung geeigneter Korrekturmaßnahmen werden durch Terminüberwachung und Überprüfung der Maßnahmen sichergestellt. Die Planung von Korrekturmaßnahmen ist den sicherheitstechnischen Anforderungen angemessen.

3.5 (2) 4 Verbesserung von Tätigkeiten und Prozessen

Der Betreiber führt ein Verfahren zur ständigen Verbesserung der sicherheitsrelevanten Tätigkeiten und Prozesse ein. Dieses Verfahren stellt sicher, dass auf der Basis der Ergebnisse von Überprüfungen die erforderlichen Maßnahmen identifiziert und umgesetzt werden. Der Betreiber fördert das Engagement des Personals, aktiv an der Entwicklung von Verbesserungsmaßnahmen mitzuwirken.

Es werden Regelungen getroffen, um die verschiedenen Verbesserungsprozesse zu koordinieren und um Prioritäten und Ressourcen festzulegen. Die Festlegung der Prioritäten von Verbesserungsmaßnahmen erfolgt auf Basis sicherheitstechnischer Überlegungen unter Nutzung der Ergebnisse von Prozessüberwachung, Audits, Reviews und anderer relevanter Informationsquellen.

3.5 (3) Spezifische Anforderungen an Prozesse

3.5 (3) 1 Änderungen (Neuentwicklungen und Änderungsmaßnahmen)

Jede Änderung an Einrichtungen, von Verfahren, von Methoden, der Aufbau- und Ablauforganisation, von Anweisungen oder von Überprüfungsverfahren wird bewertet, hinsichtlich ihrer sicherheitstechnischen Bedeutung eingeordnet und gerechtfertigt. Dazu werden

- die Entwicklungsphasen einschließlich der Umsetzungsphase und des Umsetzungsplans festgelegt,
- für jede Entwicklungsphase eine angemessene Bewertung, Verifizierung und Validierung gewährleistet,
- die verantwortlichen Organisationseinheiten, ihre Aufgaben und Befugnisse für die Planung, Entwicklung und Durchführung von Änderungen sind festgelegt. Die Schnittstellen zwischen den beteiligten Organisationseinheiten werden unter Berücksichtigung einer wirksamen Kommunikation definiert und beschrieben.

Es ist sichergestellt, dass sich durch Änderungsmaßnahmen

- keine Einschränkungen der Sicherheit ergeben,
- die Wirksamkeit des Sicherheitsmanagementsystems erhalten bleibt und damit die vorgesehenen Ziele erreichen lassen.

Für die Planung, Durchführung und Prüfung dauerhafter und vorübergehender Änderungen ist ein Prozess etabliert, der unter Berücksichtigung deren sicherheitstechnischen Bedeutung Folgendes sicherstellt:

- Machbarkeitsbetrachtung,
- Begründung und Rechtfertigung der Änderung,
- Auslegungsrandbedingungen,
- Sicherheitsbetrachtung,
- Aktualisierung der Dokumentation und der Schulungen,

- Umsetzung, Installation und Prüfung.

Detailierungsgrad und Umfang der Planung und Prüfung der Änderungsmaßnahmen entsprechen der sicherheitstechnischen Bedeutung der Änderung. Die Änderungsmaßnahmen werden dokumentiert.

3.5 (3) 2 Zusammenarbeit mit externen Auftragnehmern

Externe Auftragnehmer (z.B. Hersteller, Zulieferer, Fremdfirmen) werden nach festgelegten Kriterien bewertet und ausgewählt. Die Anforderungen an die Kompetenz des Personals und an das Qualitätsmanagement der externen Unternehmen werden definiert. Die Bewertung der externen Unternehmen wird dokumentiert.

Externe Auftragnehmer werden in das Sicherheitsmanagementsystem einbezogen. Die entsprechenden Schnittstellen sind im Sicherheitsmanagementsystem ausgebildet. Wichtige Aspekte dabei sind ein ausreichender Informationsaustausch, Schulung und Einweisung, Überwachung der Fähigkeiten und Beurteilung sowie Anerkennung für erfolgreiche Bemühungen und Leistungen bezüglich der Sicherheit.

Der Betreiber überzeugt sich, dass das Fremdpersonal für die ihm zugewiesenen Aufgaben über die notwendige Kompetenz und Qualifikation verfügt. Der Betreiber verfolgt kontinuierlich die Erfahrungen mit externen Unternehmen hinsichtlich Einhaltung der Sicherheits- und Qualitätsanforderungen. Bei Abweichungen reagiert er entsprechend. Der Betreiber überzeugt sich, dass ein externes Unternehmen in der Lage ist, die Anforderungen zu erfüllen, die an zu beschaffende Ressourcen (Dienstleistungen, Hilfsstoffe, Hard- und Software) zu stellen sind.

3.5 (3) 3 Kommunikation

Der Betreiber stellt sicher, dass geeignete Prozesse zur Kommunikation innerhalb des Unternehmens vorhanden sind. Die Kommunikationsprozesse werden gepflegt und ihre Nutzung gefördert. Die Kommunikation kann in

Abhängigkeit der Bedeutung der vermittelten Informationen in formeller und informeller Art erfolgen. Sowohl der Kommunikationsweg von den Führungskräften zu den Mitarbeitern als auch der umgekehrte Kommunikationsweg sind systematisiert. Folgende Aspekte werden hinsichtlich der Kommunikation insbesondere berücksichtigt:

- Die Sicherheitspolitik wird im Unternehmen kommuniziert, so dass jeder Mitarbeiter im Unternehmen sie verstehen kann und sich über seine Rolle bei der Gewährleistung der Sicherheit im Klaren ist.
- Die aus der Sicherheitspolitik abgeleiteten Sicherheitsziele sowie die detaillierten Prozessziele für Prozessdurchführung und Prozessergebnisse werden kommuniziert.
- Die organisatorischen Festlegungen sind im Unternehmen bekannt gemacht.
- Allen Mitarbeitern werden Kenntnisse der gesetzlichen und behördlichen Anforderungen, der sicherheitsrelevanten betrieblichen Vorschriften der Anlage, der Regelungen zur Durchführung sicherheitsrelevanter Tätigkeiten sowie neuer Erkenntnisse auf dem Gebiet der Sicherheit vermittelt, wobei sich der Umfang der vermittelten Kenntnisse am Aufgabenbereich des jeweiligen Mitarbeiters orientiert. Der Informationsaustausch zwischen Führungskräften und ihren Mitarbeitern, zwischen Arbeitsgruppen sowie den Schichten ist systematisiert.
- Die für die Durchführung sicherheitsrelevanter Tätigkeiten notwendigen Informationen werden weitergegeben.
- Die Bereitschaft der Mitarbeiter zu Rückmeldungen von Sicherheitsbedenken wird gefördert.
- Das Unternehmen pflegt Kommunikationsbeziehungen zu Externen (z.B. Zulieferern, Aufsichtsbehörden, Sachverständigen, anderen Kernkraftwerken, Betreiberorganisationen), die über definierte und wirksame Kommunikationswege stattfinden.

3.5 (4) 1 Wirksamkeitsprüfung

Die Wirksamkeit sämtlicher sicherheitsrelevanter Prozesse wird überprüft. Die Wirksamkeitsprüfung umfasst:

- die Festlegung des Überwachungsumfangs,
- eine Untersuchung der Eignung der im Sicherheitsmanagementsystem vorhandenen Prozesse für die Erreichung der Sicherheitsziele,
- eine Untersuchung der Eignung der Indikatoren für die Überprüfung der Sicherheit,
- die Untersuchung der Eignung der genutzten Messmethoden für die Erfassung sicherheitsrelevanter Informationen (z.B. Anlagenparameter, Audits, Ereignisanalyseverfahren),
- die Eignung der Verbesserungsmaßnahmen und der Maßnahmen zur stetigen Verbesserung der Sicherheit.

3.5 (4) 2 Der Überwachungsumfang ergibt sich aus den Sicherheitszielen und berücksichtigt insbesondere:

- sämtliche Ebenen des Unternehmens (Unternehmensführung, Führungsebene, Mitarbeiterebene) sowie deren Wechselwirkungen;
- alle Schnittstellen (sowohl innerbetrieblich zwischen verschiedenen Organisationseinheiten als auch außerbetrieblich zu Fremdfirmen);
- Schnittstellen mit der Behörde und Gutacherorganisationen.

Die erste Überwachung wird während der Prozessabarbeitung von den beteiligten Mitarbeitern vorgenommen.

Alle weiteren Überwachungsmaßnahmen sind unabhängig von den an der Prozessdurchführung beteiligten Mitarbeitern zu gestalten. Die dafür verantwortlichen Organisationseinheit oder Organisationseinheiten sind in der Ablauforganisation festgelegt. Diese Organisationseinheiten sind nicht an der Durchführung der zu überwachenden Prozessen beteiligt. Zusätzlich zu diesen internen Überwachungsmaßnahmen sind gegebenenfalls auch externe Überwachungsmaßnahmen vorzusehen.

Die Unternehmensführung wertet die Ergebnisse der Überwachungsmaßnahmen geeignet aus und leitet gegebenenfalls Verbesserungsmaßnahmen ein.

3.5 (4) 3 Die Eignung des Sicherheitsmanagementsystems zur Gewährleistung der Sicherheit wird geprüft bezüglich

- des gewählten Ansatzes,
- der Festlegung der Verantwortlichkeiten innerhalb der Unternehmenshierarchie und
- der wirksamen Abstimmung der Sicherheitsziele mit anderen Zielen des Unternehmens.

Dies kann durch unabhängige Überprüfungen sowie anhand der Überprüfung von Indikatoren erfolgen. Die Überprüfungsansätze sind für den jeweiligen Aspekt aus dem Überwachungsumfang, für den sie eingesetzt werden, geeignet.

Bei der unabhängigen Überprüfung werden insbesondere folgende Ansätze unterschieden:

- Interne Überprüfung (internes Audit)
- Überprüfung durch externe Sachverständige (externes Audit)
- Systematischer Vergleich mit anderen Betreibern (Benchmarking, Peer Reviews).

Bei der Überprüfung durch Indikatoren, werden z.B. folgende Ansätze unterschieden:

- Erreichung von Prozesszielen,
- Trendverfolgungen.

3.5 (4) 4 Indikatoren und Messmethoden werden so festgelegt, dass sie

- eine gültige Aussage darüber erlauben, ob die Ziele des Sicherheitsmanagementsystems erreicht werden,
- sich zur Überprüfung des Erreichens der Sicherheitsziele eignen,
- vollständig sind.

Es stehen ausreichende Ressourcen und Methoden für die Datenerhebung, die Durchführung von Messungen sowie die Auswertung von Messergebnissen zur Verfügung.

3.5 (4) 5 Die Eignung der Messung ist dokumentiert (Verlässlichkeit der Datenerhebung). Erhobene Daten sind auf ihre statistische Qualität geprüft. Gezeigt sind:

- die Qualität der Messung (Stabilität und Konsistenz),
- die Eignung für Trendverfolgungen,
- die angemessene Qualifikation des Personals für die sachgerechte Durchführung der Messung.

3.5 (4) 6 Die Eignung des Sicherheitsmanagementsystems zur Identifikation von Verbesserungspotentialen ist für alle sicherheitsrelevanten Prozesse dokumentiert. Die sicherheitsfördernde Wirkung von Verbesserungsmaßnahmen ist gezeigt über

- die vollständige Einbeziehung der durch die Maßnahme bewirkten Auswirkungen,
- deren systematische Herleitung aus gewonnenen Erkenntnissen und
- die Konsistenz der Ergebnisse aus allen sicherheitsbezogenen Auswertungsprozessen (z.B. Audits, Ereignisanalyse, PSA).

Belegt sind entsprechende Ressourcen und Prozesse insbesondere für

- die Auswertung der Erkenntnisse aus der Datenerhebung,
- das Vorgehen bei Verdachtsmomenten und
- die Auswertung des Standes von Wissenschaft und Technik.

3.6 ***Dokumentation***

Hinweis Die grundsätzlichen Anforderungen an die Dokumentation sind in "Sicherheitsanforderungen für Kernkraftwerke: Anforderung an Nachweisführungen und Dokumentation" (Modul 6), Abschnitt 7 behandelt.

- 3.6 (1) Die Dokumente des Sicherheitsmanagementsystems werden den betroffenen internen oder externen Mitarbeitern bekannt gemacht und gegebenenfalls erläutert, insbesondere nach Aktualisierung oder Änderung der Dokumente.
- 3.6 (2) Das Sicherheitsmanagementsystem ist hinsichtlich folgender Punkte dokumentiert:
- Anwendungsbereich des Sicherheitsmanagementsystems,
 - Sicherheitspolitik des Unternehmens,
 - Sicherheitsziele zur Erreichung der Politik,
 - Herleitung der Sicherheitsindikatoren und Prozesse aus der Sicherheitspolitik und den Sicherheitszielen,
 - Beschreibung der Prozesse und Verantwortlichkeiten zur Erreichung der Sicherheitsziele einschließlich deren Begründung („know-why“),
 - Prozesse zur Entscheidungsfindung bei Abgleich von Sicherheitszielen mit anderen Unternehmenszielen,
 - Aufzeichnungen zum Nachweis der Konformität mit den Anforderungen des Sicherheitsmanagementsystems,
 - Wechselwirkungen der sicherheitsrelevanten Prozesse sowie ggf. Schnittstellen und Abgrenzungen zu anderen Managementsystemen.
- 3.6 (3) Die Dokumentation der Ressourcen wird auf dem aktuellen Stand gehalten. Sie beinhaltet
- die Dokumentation des jeweils aktuellen Anlagenzustandes einschließlich der Unterlagen zur Genehmigung der Anlage mit Nachweisen, technische Beschreibungen sowie allen durchgeführten Änderungsmaßnahmen,
 - die Festlegungen für die sonstige Infrastruktur,
 - regelmäßige Dokumentation des Personalbestandes und der Arbeitskapazitäten,
 - die Festlegungen zu Arbeitsumgebung und Arbeitsbedingungen und
 - die Regelungen zur Zusammenarbeit mit externen Organisationen.

- 3.6 (4) Wesentliche Regelungen zu Aufbau- und Ablauforganisationen sind z.B. in den Betriebshandbüchern, Notfallhandbüchern und Prüfhandbüchern enthalten (siehe „Sicherheitsanforderungen für Kernkraftwerke: Grundlegende Sicherheitsanforderungen“ (Modul 1), Abschnitt 8). Detailregelungen sind in sonstigen schriftlichen Anweisungen zur Durchführung von Prozessen und Tätigkeiten (Ablauf- und Arbeitsanweisungen) niedergelegt. In den Regelungen - insbesondere in den Ablaufregelungen - sind neben den technischen Abläufen auch jeweils die Zuständig- und Verantwortlichkeiten, Überprüfungsmaßnahmen und Qualitätsanforderungen eindeutig festgelegt.
- 3.6 (5) Die Dokumentation des Betriebs enthält alle sicherheitsrelevanten Erfahrungen und vorhandenen Ressourcen. Sie umfasst insbesondere die Betriebsaufzeichnungen, Analysen zu eigenen oder fremden Ereignissen und Erkenntnissen, Unterlagen zu Instandhaltungserfahrungen und -ergebnissen, das Schichtbuch und Änderungsanzeigen. Die Auswertung der Betriebsdokumentation erfolgt systematisch und nachvollziehbar. Die Ergebnisse der Auswertung fließen in die Planung und Verbesserung des sicheren Betriebs einschließlich des Sicherheitsmanagementsystems ein.

4 Anforderungen an die Gewährleistung der Qualität und den Erfahrungsrückfluss

4.1 Gewährleistung der Qualität

- 4.1 (1) Alle sicherheitsrelevanten Einrichtungen, Prozesse und Tätigkeiten weisen eine hohe Qualität auf. Die hohe Qualität wird durch ein systematisches Qualitätsmanagement gewährleistet.

4.1 (2) Qualitätsmanagement

Sämtliche Ziele, Grundsätze, Systeme und Methoden des Qualitätsmanagements stehen im Einklang mit den Zielen, Grundsätzen, Systemen und Methoden des Sicherheitsmanagements bzw. des integrierten Managementssystems.

- 4.1 (2) 1 Das Qualitätsmanagement ist darauf ausgerichtet, die kerntechnische Sicherheit durch kontinuierliche Verbesserung der Maßnahmen zur Gewährleistung der Qualität zu erhöhen.
- 4.1 (3) 1 Das Qualitätsmanagement wird auf alle sicherheitsrelevanten Einrichtungen, Prozesse und Tätigkeiten angewendet. Es umfasst auch die sicherheitsrelevanten Aktivitäten und Produkte, die durch externe Auftragnehmer bereitgestellt werden.
- 4.1 (3) 2 Alle Mitarbeiter des Unternehmens und von externen Auftragnehmern, die mit sicherheitsrelevanten Aufgaben betraut sind, sind verpflichtet, die Maßgaben des Qualitätsmanagements einzuhalten.
- 4.1 (3) 3 Bei der Identifizierung der Einrichtungen, Prozesse und Tätigkeiten, auf die das Qualitätsmanagement anzuwenden ist, werden die Vorgaben zur Klassifizierung gemäß „Sicherheitsanforderungen für Kernkraftwerke: Grundlegende Sicherheitsanforderungen“ (Modul 1), Ziffer 2.1 (10), herangezogen.
- 4.1 (4) Die Verantwortlichkeiten für die Planung und Umsetzung der Maßnahmen des Qualitätsmanagements sind so festgelegt, dass andere Erwägungen (z.B. Zeitplanung) keinen Vorrang vor der Sicherheit erhalten.
- 4.1 (5) 1 Die Prüfung der Qualität ist durch unabhängige Maßnahmen gewährleistet. Art und Umfang der unabhängigen Qualitätsprüfung spiegeln die Sicherheitsrelevanz und die Komplexität der jeweiligen Aufgabe wider.
- 4.1 (5) 2 Falls Abweichungen von Qualitätszielen während der Durchführung von Prozessen oder Tätigkeiten, im Rahmen unabhängiger Prüfungen oder auf Grund sonstiger Informationen festgestellt werden, wird Folgendes ermittelt:
- mögliche Auswirkungen auf die Sicherheit,
 - die Dringlichkeit von Korrekturen unter Berücksichtigung der Sicherheitsrelevanz,
 - die Ursache der Abweichungen,

- die Korrekturen, die zu planen und nachzuweisen sind, um die Abweichung zu korrigieren und Wiederholungen ähnlicher Ereignisse zu vermeiden.

Die Ergebnisse der Untersuchungen sind dokumentiert. Die Umsetzung der Korrekturen wird überwacht und dokumentiert. Festgestellte Abweichungen und die getroffenen Korrekturmaßnahmen gehen in den Erfahrungsrückfluss ein.

- 4.1 (5) 3 Das Qualitätsmanagement stellt sicher, dass Tätigkeiten, die aus Qualitätsgründen unterbrochen wurden, erst dann wieder aufgenommen werden, wenn unter den gegebenen Randbedingungen die relevanten Qualitätsmerkmale eingehalten werden.

4.2 Auswertung von Betriebserfahrung und anderen Erkenntnissen, Erfahrungsrückfluss und Informationsaustausch

Hinweis Ein maßgeblicher Bestandteil der Verbesserung des Sicherheitsmanagementsystems ist durch die Auswertung der Betriebserfahrungen gegeben (siehe Ziffer 3.1 (4)).

4.2 (1) Prozesse und Verantwortung

- 4.2 (1) 1 Der Betreiber entwickelt Prozesse und führt diese durch, um meldepflichtige Ereignisse gemäß AtSMV, Störungen, Betriebserfahrungen, Erkenntnisse zu sicherheitstechnisch relevanten Aspekten der Auslegung der eigenen und anderer Anlagen, Änderungen des Standes von Wissenschaft und Technik und der internationalen Sicherheitsstandards einschließlich der hierzu behördlich veranlassten Informationen auf systematische Weise unter Berücksichtigung der Anforderung des Sicherheitsmanagementsystems (siehe Kap. 3) zu sammeln, zu sichten, auszuwerten und diese Schritte zu dokumentieren.

- 4.2 (1) 2 Die Betriebserfahrung wird ausgewertet, um bisher unerkannte sicherheitstechnisch bedeutende Ereignisse, mögliche Precursor-Ereignisse und Tendenzen zur Veränderung der Sicherheit oder von Sicherheitsmargen zu erkennen.

- 4.2 (1) 3 Der Betreiber stellt ausreichend qualifiziertes Personal zur Durchführung dieser Prozesse, zur Kommunikation der sicherheitstechnisch wichtigen Ergebnisse und - soweit angebracht - zur Empfehlung von Abhilfemaßnahmen bereit.

Bedeutende Erkenntnisse (Hinweise, Verdachtsmomente, Ergebnisse und Trend) werden dem Leiter der Anlage gemeldet.

4.2 (1) 4 Das für die gemäß Ziffer 4.2 (1) 1 geforderten Tätigkeiten verantwortliche Personal erhält eine angemessene Aus- und Weiterbildung, ausreichende technische und finanzielle Ressourcen und Unterstützung der Unternehmensführung.

4.2 (1) 5 Der Betreiber stellt sicher, dass Ergebnisse erzielt, Schlüsse gezogen und Abhilfemaßnahmen rechtzeitig und angemessen getroffen werden, um eine Wiederholung von Ereignissen zu vermeiden und die Sicherheit der Anlage zu erhalten oder zu verbessern.

4.2 (1) 6 Der Betreiber informiert die zuständigen Behörden umfassend über die relevanten abgeleiteten Ergebnisse und Maßnahmen.

4.2 (2) Meldung und Verbreitung sicherheitstechnisch bedeutsamer Informationen

Hinweis Anforderungen an die Meldung von Ereignissen sind in der AtSMV geregelt.

4.2 (2) 1 Der Betreiber verpflichtet das gesamte Personal, sicherheitstechnisch bedeutende meldepflichtige Ereignisse, Störungen und Beinaheereignisse den zuständigen Stellen im Kraftwerk anzuzeigen.

4.2 (2) 2 Der Betreiber stuft alle meldepflichtigen Ereignisse in die INES-Skala ein und meldet sie dem INES-Officer.

4.2 (2) 3 Der Betreiber etabliert Prozesse, um sicherheitstechnisch wichtige Betriebserfahrungen und Erkenntnisse dem zuständigen Personal innerhalb der Anlage, den zuständigen staatlichen Stellen und den von diesen benannten Sachverständigenorganisationen in geeigneter Weise mitzuteilen sowie mit anderen Betreibern, Betreiberorganisationen, und internationalen Gremien angemessen auszutauschen.

Der Betreiber unterstützt die Behörden beim internationalen Austausch von Betriebserfahrungen.

4.2 (2) 4 Der Betreiber etabliert Prozesse, um die Erkenntnisse aus Ereignissen, Betriebserfahrungen sowie Änderungen des Standes von Wissenschaft und Technik angemessen in den Schulungsprogrammen zu berücksichtigen.

4.2 (3) Dokumentation und Archivierung von Betriebserfahrung

Der Betreiber dokumentiert und archiviert die aufbereiteten Betriebserfahrungen sowie andere sicherheitstechnisch relevante Informationen so, dass sie einfach aufzufinden und systematisch durchsucht, sortiert und bewertet werden können.

4.2 (4) Auswertung von Ereignissen

4.2 (4) 1 Sicherheitstechnisch bedeutsame Ereignisse werden unverzüglich ausgewertet, damit gegebenenfalls erforderliche Sofortmaßnahmen umgehend getroffen werden können.

4.2 (4) 2 Der Betreiber stellt sicher, dass angemessene Auswertemethoden für die Betriebserfahrungen sowohl für technische als auch für personell/organisatorische Aspekte verwendet werden.

4.2 (4) 3 Die Ereignisauswertung wird entsprechend der sicherheitstechnischen Bedeutung des Ereignisses durchgeführt. Die Auswertung

- zeigt den gesamten Ereignishergang auf,
- bestimmt die Abweichungen vom Sollzustand,
- identifiziert und analysiert Fehler, Ursachen und beitragende Faktoren,
- bestimmt die sicherheitstechnische Bedeutung mit den potentiellen Auswirkungen,
- untersucht die Übertragbarkeit auf andere Randbedingungen und andere Einrichtungen und Verfahrensweisen,
- entwickelt die Abhilfemaßnahmen.

4.2 (4) 4 Der Betreiber erhält angemessene Verbindungen zu den Organisationen aufrecht, die mit der Auslegung und Errichtung der Anlage bzw. von Anlagenteilen befasst waren und/oder sind, um den Rückfluss von

Betriebserfahrungen sicherzustellen und sich gegebenenfalls von diesen Organisationen beraten zu lassen.

- 4.2 (4) 5 Als Ergebnis der Auswertung von Betriebserfahrungen werden die Abhilfemaßnahmen rechtzeitig getroffen, um die Sicherheit wiederherzustellen oder zu verbessern, das wiederholte Auftreten von Ereignissen zu vermeiden und sicherheitsgerichtete Trends zum Beispiel von Indikatoren zu unterstützen.

Die Abhilfemaßnahmen werden nach den Anforderungen des Sicherheitsmanagementsystems und des Qualitätsmanagements geplant, durchgeführt, überprüft und dokumentiert.

- 4.2 (5) Überprüfung und kontinuierliche Verbesserung der Prozesse zur Auswertung von Betriebserfahrungen

Nach den Anforderungen des Sicherheitsmanagementsystems (siehe insbesondere Ziffern 3.1 (3) und 3.2 (3)) werden die Prozesse zur Auswertung von Betriebserfahrungen und anderen Erkenntnissen in regelmäßigen Abständen auf ihre Wirksamkeit überprüft. Dies kann auch durch geeignetes anlagenfremdes Personal geschehen. Die Ergebnisse der Überprüfungen werden dokumentiert.

In den Anhang verschoben:

3.2 (1) In der Phase der Planung bezieht das Unternehmen insbesondere folgende Aspekte ein:

- Sicherheitspolitik und Sicherheitsziele.
- Schnittstellen zu anderen Managementsystemen und Prozessen.
- Methoden und Prozesse zur Überprüfung der Wirksamkeit hinsichtlich der Erfüllung der Sicherheitsziele. Die Überprüfungsmethoden müssen abdeckend und ausgewogen sein (siehe Ziffer 3.5 (4)).
- Prozesse zur Verbesserung.

3.2 (2) In der Phase der Durchführung wird das Sicherheitsmanagementsystem eingeführt, etabliert und aufrechterhalten. Dabei bezieht das Unternehmen insbesondere folgende Aspekte ein:

- Es werden Tätigkeiten und Prozesse zur Umsetzung der Sicherheitspolitik sowie für das Erreichen der Sicherheitsziele etabliert.
- Es werden Tätigkeiten und Prozesse zur Überwachung der Wirksamkeit der Sicherheitsziele etabliert.
- Es werden Maßnahmen getroffen, um die Sicherheitspolitik, die Sicherheitsziele und das Sicherheitsmanagementsystem allen Mitarbeitern auf allen Ebenen des Unternehmens oder externer Organisationen, die mit sicherheitsrelevanten Aufgaben befasst sind, zu vermitteln, damit diese von den Mitarbeitern verstanden, umgesetzt und gelebt werden.
- Es werden Maßnahmen getroffen, die sicherstellen, dass alle sicherheitsrelevanten Tätigkeiten und Prozesse in hoher Qualität durchgeführt werden.
- Die erforderlichen Dokumente und Arbeitsanweisungen werden bereitgestellt.

3.2 (3) In der Phase der Überprüfung wendet das Unternehmen die Überwachungs-, Mess- und Analyseprozesse an, die erforderlich sind, um

- die Umsetzung der Sicherheitspolitik und das Erreichen der Sicherheitsziele bzw. der Prozessergebnisse aufzuzeigen,
- die Wirksamkeit des Sicherheitsmanagementsystems und seiner Tätigkeiten und Prozesse sicherzustellen,
- die Wirksamkeit des Sicherheitsmanagementsystems und seiner Tätigkeiten und Prozesse zu verbessern.

Dazu führt das Unternehmen in geplanten Abständen interne Überprüfungen mit geeigneten Methoden durch, um zu ermitteln, ob das Sicherheitsmanagementsystem die festgelegten Anforderungen erfüllt, ob es wirksam verwirklicht ist und aufrechterhalten wird.

Bei den Überprüfungen werden folgende Aspekte berücksichtigt:

- die Ergebnisse der Überwachung der Prozesse,
- der Status von Korrektur- und Verbesserungsmaßnahmen,
- der Status und die Ergebnisse der Maßnahmen, die aus vorangegangenen Bewertungen gefolgt sind,
- Rückmeldungen von externen Organisationen (Behörden, Sachverständige, Auftragnehmer etc.),
- Änderungen mit Auswirkungen auf das Sicherheitsmanagement (technische, organisatorisch-administrative Änderungen) sowie
- Änderungen interner und externer Anforderungen.

Bei der Festlegung von Anlässen, Umfang, Häufigkeit und Methoden der Überprüfungen ist die Bedeutung der zu prüfenden Tätigkeiten und Prozesse für die Sicherheit zu berücksichtigen.

Das Unternehmen lässt zusätzlich Überprüfungen durch unabhängige Organisationen in angemessenen Abständen und zu besonderen Anlässen durchführen, um die Effektivität und Effizienz des Sicherheitsmanagementsystems im Vergleich zum Stand von Wissenschaft und Technik bewerten zu können.

3.2 (4) Das Unternehmen verbessert stetig das Sicherheitsmanagementsystem und seine Tätigkeiten und Prozesse insbesondere durch

- Umsetzung der Ergebnisse aus den in Absatz 3.1 (3) genannten Überprüfungen.
- Umsetzung von neuen Erkenntnissen, die sich insbesondere aus der Auswertung von Ereignissen und sonstigen Erfahrungen sowie aus der Verfolgung des Standes von Wissenschaft und Technik und der internationalen Sicherheitsstandards ergeben.

Bei allen Verbesserungsmaßnahmen werden die Rückwirkungen auf das Sicherheitsmanagementsystem, die Tätigkeiten und Prozesse sowie die Schnittstellen berücksichtigt.