Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen

GRS - 646

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen

Udo Weizel

Juni 2021

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Förderkennzeichen 4718R01611 durchgeführt.

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

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

GRS - 646
ISBN 978-3-949088-35-3

Deskriptoren

Anlagensicherung, Drohnen, Einwirkungen, Endlagersicherung, IT-Sicherheit, IT-Sicherheitsvorkommnisse, nukleare Sicherungskultur, Sicherung, Sicherung der Beförderung, sicherungsrelevante Vorkommnisse, Sicherungstechnik, Schnittstelle Sicherheit und Sicherung

Inhaltsverzeichnis

1 Einleitung, Aufgabenstellung und Zielsetzung

Nach dem Atomgesetz (AtG) ist für kerntechnische Anlagen und Einrichtungen (kerntechnische Anlagen) sowie für die Beförderung von Kernbrennstoffen eine Genehmigungsvoraussetzung, dass der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) gewährleistet ist.

Die Sicherung von kerntechnischen Anlagen und bei der Beförderung von Kernbrennstoffen zum Schutz gegen SEWD umfasst Sicherungsmaßnahmen des Genehmigungsinhabers, die in einem Sicherungskonzept festgelegt werden, und darauf abgestimmte Schutzmaßnahmen des Staates. In der Sicherung soll bei der Bewertung und Fortentwicklung von Sicherungskonzepten stets der Stand von Wissenschaft, Technik und Erkenntnis (W,T&E) im gebotenen Umfang berücksichtigt und bundeseinheitlich umgesetzt werden. Der Stand von W,T&E für die Sicherung einschließlich der IT-Sicherheit im nationalen und internationalen Rahmen umfasst u. a. technischen Möglichkeiten und Technologien zur Unterstützung der Sicherung oder als Herausforderung für die Sicherung sowie Erkenntnisse aus Vorkommnissen mit Sicherungsrelevanz und IT-Sicherheitsrelevanz.

Eine zentrale Aufgabe der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH ist die Gewinnung neuer wissenschaftlicher und technischer Erkenntnisse und die Entwicklung neuer wissenschaftlicher Prüf- und Bewertungsmethoden auf dem Gebiet der Sicherung, um die Sicherung deutscher kerntechnischer Anlagen und der Beförderung von Kernbrennstoffen gegen SEWD weiter zu verbessern.

Die GRS als gemeinnützige, technisch-wissenschaftliche Forschungs- und Sachverständigenorganisation stellt ihre Fachkompetenz auf dem Gebiet von Sicherung und IT-Sicherheit insbesondere dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU) zur Verfügung. Als Voraussetzung für eine jederzeit schnelle Unterstützung des Bundes auf einem wissenschaftlich-technisch hohen Niveau ist insbesondere der Erhalt und der Ausbau der Fachkompetenz durch kontinuierliche Verfolgung, Auswertung und Weiterentwicklung des Standes von W,T&E auf nationaler und internationaler Ebene und das Vorhalten fortschrittlicher Prüf- und Bewertungsmethoden erforderlich. Fachkompetenz und Methoden können auch anderen Behörden und Sachverständigen unter Beachtung von Geheimhaltungsanforderungen für einzelne Aspekte zur Verfügung gestellt werden.

Als eine Zielsetzung dieses Vorhabens sollte die Fachkompetenz der GRS auf dem Gebiet der Sicherung erhalten und kontinuierlich ausgebaut werden, um ihre Fähigkeit, Sachverhalte zu aktuellen Fragen der Sicherung einschließlich der Sicherheit der Informationstechnik (IT-Sicherheit) in kerntechnischen Anlagen stets auf der Basis des national und international verfügbaren Wissensstandes auf diesem Gebiet zu bearbeiten, zu gewährleisten und abzusichern. Dazu sollte der Stand von W,T&E im Bereich der Sicherung und IT-Sicherheit systematisch erfasst und ausgewertet werden. Das erfasste Wissen soll auch dazu genutzt werden, um neue Herausforderungen im Bereich der Sicherung und IT-Sicherheit zu identifizieren, generische Lösungsansätze und Anforderungen zur Verbesserung der Sicherung und IT-Sicherheit zu entwickeln und durch den fachlichen und wissenschaftlichen Austausch mit anderen Experten die Weiterentwicklung der wissenschaftlichen und technischen Grundlagen auf nationaler und internationaler Ebene voranzutreiben, auch im Hinblick auf den regulatorischen Bereich. Ereignisse mit Sicherungsrelevanz und IT-Sicherheitsrelevanz sollten analysiert werden.

Dafür verfolgte dieses Eigenforschungsvorhaben mehrere fachliche Einzelziele, die im Rahmen der folgenden Arbeitspakete (AP) bearbeitet wurden:

- AP 1: Erfassung und Auswertung des Standes von Wissenschaft Technik und Erkenntnis bei der Sicherung hinsichtlich der
  - Entwicklung technischer Hilfsmittel zur Einwirkung und Systeme zum Schutz (Sicherung und IT-Sicherheit)
  - generischen Anforderungen für Endlagerkonzepte
  - Schnittstellen zwischen Sicherheit und Sicherung
  - nuklearen Sicherungskultur
  - Identifizierung von Themen der Sicherung und IT-Sicherheit mit Forschungs- und Entwicklungsbedarf
- AP 2: Analyse von Ereignissen mit Sicherungsrelevanz und IT-Sicherheitsrelevanz zur
  - Identifizierung von Lücken bei Sicherung und IT-Sicherheit
  - Entwicklung von Lösungsansätzen

- AP 3: Weiterentwicklung von Sicherungsstandards im Rahmen der internationalen Zusammenarbeit wie
  - bilateraler Expertenaustausch
  - Expertentreffen der internationalen Atomenergiebehörde (IAEO)

Die zugehörigen Arbeiten erfolgten auf einer generischen Ebene und haben zugleich Modellcharakter für einzelne Anlagentypen.

Die Erkenntnisse aus dem Vorhaben und konkrete Ergebnisse dienten u. a. im Rahmen des Vorhabens 4718R01610 als Grundlage für die Weiterentwicklung des Regelwerks zur Sicherung und der Fachberatung des BMU.

Zum Erkenntnisgewinn der Sachverständigen sowie zum Erkennen aktueller Trends und Schwerpunkte im Sinne des Standes von W,T&E auf dem Gebiet der Sicherung werden verschiedene Möglichkeiten genutzt, die alle einen Beitrag zum Erhalt und Ausbau der Fachkompetenz liefern. Dazu gehören u. a. die gutachterliche Tätigkeit, informative Diskussionen zu speziellen Sicherungsaspekten, Teilnahmen als Beobachter an Übungen, Kontaktaufbau und -pflege zu anderen Experten auf dem Gebiet der Sicherung etc.

Im Rahmen dieses Vorhabens wurden Arbeiten durchgeführt, die der systematischen Erfassung und Auswertung des Standes von W,T&E im Bereich der Sicherung einschließlich der IT-Sicherheit auf nationaler und internationaler Ebene durch dessen kontinuierliche Verfolgung, Auswertung und Weiterentwicklung dienen. Dazu gehörten die Beobachtung des Marktes, die Teilnahme an nationalen und internationalen Fachtagungen, Konferenzen und Trainingskurse zu verschiedenen Themen der Sicherung mit besonderer Aktualität und Praxisnähe der Themen sowie mit Bezug zu aktuellen Entwicklungen der Technik etc., der fachliche Austausch mit internationalen Experten über Erfahrungen und aktuelle Erkenntnisse auf dem jeweiligen Gebiet, aber auch gezielte Recherchen zu ausgewählten Aspekten der Sicherung und Analysen von sicherungsrelevanten Ereignissen.

Das Vorhaben hatte eine Laufzeit von 17.12.2018 bis zum 30.06.2021.

2 Stand von Wissenschaft, Technik und Erkenntnis

Arbeiten im Rahmen des AP 1: Erfassung und Auswertung des Standes von Wissenschaft, Technik und Erkenntnis bei der Sicherung

Systementwicklungen für den Bereich der Sicherung und die am Markt verfügbaren technischen Möglichkeiten und Technologien für die Sicherung und auch für Einwirkungen sollten spezifisch verfolgt und ausgewertet werden, um Trends und Neuerungen in der Sicherungstechnik sowie geänderte Möglichkeiten für Einwirkungen rechtzeitig erkennen zu können. Dabei sollten auch weitere spezifische Fragestellungen zu Sicherungsbelangen identifiziert werden.

Als vorbereitender Schritt zur Bearbeitung des AP 1 wurden geeignete Quellen und Medien für Recherchen, wichtige Konferenzen, Workshops, Fachforen etc. eruiert.

2.1 Verfolgen der Entwicklungen mit Relevanz für die Sicherung

Das Ziel der Arbeiten bestand darin, relevante Trends technischer und methodischer Entwicklungen in Bezug auf deren Verwendung für mögliche Einwirkungen und zur Sicherung gegen derartige Einwirkungen zu identifiziert, generisch zu bewerten und ggf. Handlungsbedarf zu erkennen. Die Arbeiten umfassten grundsätzlich die Schritte Sichtung, Erstbewertung und vertiefte Auswertung auf generischer Ebene bei Bedarf.

Ein Aspekt der Recherche umfasst die Entwicklung von technischen Systemen, Werkzeugen, Fahrzeugen und anderen Hilfsmitteln, die von Tätern genutzt werden können, ein anderer Aspekt die aktuelle technische Entwicklung von Sicherungsmaßnahmen.

Das bereits in den Vorläufervorhaben begonnene regelmäßige Verfolgen der technischen Entwicklung von typischen marktgängigen Werkzeugen u. ä., die als Hilfsmittel für Einwirkungen verwendet werden können, im Internet, auf Fachveranstaltungen, bei Herstellern etc. wurde fortgesetzt. Die Dokumentation der Rechercheergebnisse erfolgt durch die Pflege einer bestehenden Excel-Datei. Die Rechercheergebnisse können bei Bedarf ausgewertet werden, um Schlussfolgerungen für die Sicherung und die Fortschreibung des SEWD-Regelwerks, insbesondere der Lastannahmen, zu ziehen. In diesem Zusammenhang werden auch interessante Neuentwicklungen mit Potential als Hilfsmittel für Einwirkungen identifiziert, z. B.:

Betonkettensäge, Zusammenfassung gemäß /THW 21/
Das Technische Hilfswerk (THW) verwendet bei Bergungseinsätzen Betonkettensägen um Beton, Stein und Glas zu zerschneiden. Betonkettensägen unterscheiden sich in drei wesentlichen Punkten von normalen Kettensägen: Ihre Zähne sind kleine Steine, die aus einem gebrannten Diamantgemisch bestehen. Damit können sie problemlos durch Stahlbeton und Glas schneiden. Im Freilauf beschleunigt die Kette auf rund 85 km/h. Die Kette wird dabei nicht wie bei einer normalen Kettensäge mit Öl geschmiert, sondern mit einem Wasserstrahl, der während dem Betrieb der Säge ständig über ihre Kette fließt. Da beim Schneiden von Beton eine große Reibungshitze entsteht, kühlt das Wasser das gesamte Schneideblatt ab und bindet Staub und Splitter. Ein Nachteil der Betonkettensägen ist, dass sie pro Minute 15 Liter Wasser verbrauchen, weshalb sie für ein 60 mal 70 cm großes Loch in etwa 900 Liter Wasser benötigt. Angetrieben wird die Betonkettensäge von einem Hydraulikaggregat.
siehe:
https://www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/betonkettensaege.html

Die Recherche zu aktuellen Entwicklungen von Sicherungsmaßnahmen erfolgt vor allem in Fachmagazinen für Sicherungstechnik. Ausgewählte Erkenntnisse mit Relevanz für die Sicherung sind nachfolgend zusammengestellt:

- Detektionssystem für Drohnen, Zusammenfassung gemäß /PRO 19a/
  Die Firma Securiton hat für den Perimeterschutz eine Systemlösung für die Detektion von Drohnen bis zu einer Entfernung von sieben Kilometern entwickelt. Die Systemlösung mit dem Namen „SecuriLocate“ wird dazu verwendet schon das Einschalten einer Drohnen-Fernbedienung zu detektieren. Sowohl die Drohne als auch die Fernbedienung lassen sich lokalisieren und auf einem Lageplan anzeigen.
  Die Drohnen samt Fernsteuerung werden anhand ihrer HF-Signale erkannt, welche sie zur Kommunikation nutzen. So können Richtung und Position von Drohne und Fernsteuerung, aber auch Marke und Modell sowie Traglast und Reichweite der Drohne bestimmt werden.
  siehe:
  https://www.securiton.de/produkte/drohnendetektionssysteme/securilocate-drone.html

- Videodetektion mit KI-Technologie, Zusammenfassung gemäß /PRO 19b/
  Die Softwarelösung Unusual Motion Detection Technology (UMD) der Firma Avigilon ermöglicht es die Bewegungen von Personen und Fahrzeugen zu detektieren und

dabei normale und abnormale Bewegungen und Aktivitäten voneinander zu unterscheiden. Die Ungewöhnliche Bewegungserkennung ist Teil der Videomanagementsoftware Avigilon Control Center (ACC). Die UMD-Technologie basiert auf Künstlicher Intelligenz und nutzt diese zum Extrahieren von Informationen.
siehe:
http://avigilon.com/de-de/products/video-analytics/umd/

- Videodetektion, automatische Verfolgung, Zusammenfassung gemäß /PRO 19c/
  Die Axis Communications Analyseanwendung „AXIS Perimeter Defender“, die zur Erfassung von Eindringlingen dient, unterstützt auch eine PTZ[1]-Autotracking-Funktion. Dadurch können unter anderem eine feste Wärmebild- oder normale Kamera mit einer PTZ-Kamera zusammenarbeiten. Die feste Kamera gibt die Positionsdaten der Alarmobjekte an die PTZ-Kamera und steuert dadurch die Richtung und Zoomstufe der PTZ-Kamera.
  siehe:
  https://www.axis.com/de-de/products/axis-perimeter-defender-ptz-autotracking

- Metallschäume, Zusammenfassung gemäß /LAB 21/
  Im Bereich der Materialforschung wurde ein Weg gefunden, Metallschäume als Sprengschutz oder Hitzeschild einzusetzen. Die Metallschäume sind dabei dem Vorbild von Knochen nachempfunden. Sie haben eine geringe Dichte und ein kleines Volumen, weisen dabei aber eine große Oberfläche auf, dadurch sind sie im Verhältnis zu ihrem Gewicht äußerst steif und fest. Durch ihre Eigenschaften eignen sie sich als mobile Schutzwände um Stoßwellen bei Explosionen abzufangen, aber auch tragende Teile in Fahrzeugen lassen sich aus Metallschäumen herstellen. Im Artikel wird auch auf weiterführende Informationen in der Publikation zur Beschichtung von Metallschäumen “Modelling and Simulation of the Coating Process on Open Porous Metal Foams” verwiesen.
  siehe:
  https://www.laborpraxis.vogel.de/stahlharte-schaeume-als-sprengschutz-a-810633/

[1] **P**an, **T**ilt and **Z**oom

2.2 Bewertung spezieller Hilfsmittel

2.2.1 Drohnen

Die Recherchen im Vorläufervorhaben zum Stand von W,T&E im Hinblick auf unbemannte Fahrzeuge, insbesondere auf Luftfahrzeuge (unmanned aerial vehicle – UAV, umgangssprachlich Drohnen), wurden fortgesetzt und vervollständigt. Die fortschreitende Entwicklung und Verfügbarkeit stetig leistungsfähigerer Fahrzeuge führt dazu, dass sich die Attraktivität für Nutzer ständig erhöht. Das beinhaltet auch den Aspekt, dass insbesondere Drohnen auch verstärkt im Zusammenhang mit Anforderungen an die Sicherung von zu schützenden Objekten betrachtet werden müssen.

Die zunehmende Bedeutung und Weiterentwicklung unbemannter Systeme und deren stetig steigende Verbreitung machen es erforderlich, bei der Erfassung des Standes von W,T&E für die Sicherung auch solche unbemannten Systeme zu berücksichtigen. Dabei wurde besonders betrachtet, welche unbemannten Systeme aktuell erhältlich sind und in welchem Maße deren Einsatz- und Leistungsfähigkeiten aus Sicht der Sicherung relevant sind.

Die Recherchen umfassten eine Betrachtung von unbemannten Systemen im generellen Sinn, deren Einteilung nach Einsatzumgebung und die aktuellen Leistungsparameter. Der rechtliche Rahmen, der die Nutzung solcher unbemannten Systeme in Deutschland regelt, wurde betrachtet.

Die Entwicklung unbemannter Systeme unterliegt einem hochdynamischen Prozess. Für die verschiedene Umgebungen Land, Luft und Wasser werden unbemannte Fahrzeuge entwickelt, die unterschiedliche Eigenschaften aufweisen müssen und sich damit auch in ihren Einsatzmöglichkeiten unterscheiden:

- UGV – Unmanned Ground Vehicle: unbemanntes, ggf. autonomes Landfahrzeug
- UAV – Unmanned Aerial Vehicle: unbemanntes, ggf. autonomes Fluggerät
- USV - Unmanned Surface Vehicle: unbemanntes, ggf. autonomes Überwasser-Fahrzeug
- UUV - Unmanned Underwater Vehicle: unbemanntes, ggf. autonomes Unterwasser-Fahrzeug

Insbesondere die Leistungsfähigkeit unbemannter Fluggeräte stieg in den letzten Jahren um ein Vielfaches, was die Verwendung im privatem, gewerblichem, aber auch staatlichem Gebrauch signifikant steigerte. Dabei muss zwischen Modellflugzeugen mit starren Flügeln und Multikoptern (sog. Drohnen) mit Drehflügeln mit verschiedenen Flugeigenschaften und Einsatzzwecken unterschieden werden. Die Verbreitung von Drohnen ist deutlich höher, da mit ihnen auch Schwebeflüge (Stehen in der Luft) möglich sind. So werden Drohnen durch staatliche Einsatzkräfte wie z. B. Polizei oder Feuerwehr für die Lageerkundung genutzt, andere Einsatzszenarien werden angedacht oder sind bereits etabliert. Die Verwendung im gewerblichen Sektor als Arbeitsgerät umfasst bereits die Vermessung, das Ausbringen von Insektiziden oder die Erkundung von schwer zugänglichen örtlichen Gegebenheiten. Auch das Ausliefern von Paketen zur Entlastung der Verkehrssituation in dicht besiedeltem Gebiet ist im Versuchsstadium.

Der Fokus der Recherchen zu unbemannten Systemen und deren Bewertung lag auf den luftgestützten Systemen. Recherchiert wurden der rechtliche Rahmen für den Gebrauch von unbemannten Luftfahrzeugen, die Leistungsfähigkeit in Verbindung mit technischen Ausführungen und die bereits verfügbaren Möglichkeiten zum Erkennen und zur Abwehr von unbemannten Flugsystemen. Für ausgewählte Drohnen wurden z. B. technische Auslegung sowie die Leistungsparameter flugfertiges Gewicht, Geschwindigkeit, Flugdauer, Übertragungsreichweite und Nutzlast gegenübergestellt.

Auf Basis der recherchierten und systematisch zusammengestellten Informationen wurde bewertet, welche dieser Systeme am wahrscheinlichsten und in welcher Form für die Sicherung relevant sein können. Auch die zur Verfügung stehende Detektions- und Abwehrmaßnahmen wurden näher betrachtet. Die Bewertungen mit Bezug zur Sicherung kerntechnischer Anlagen werden als VS-NfD eingestuft.

Die Ergebnisse der Recherche und der Bewertung wurden im technischen Bericht „Möglichkeiten zum Einsatz von Drohnen bei SEWD, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis“ /GRS 21a/ dargestellt. Im Rahmen dieses Vorhabens wurde zusätzlich auch die Beantragung des Vorhabens 4720R01600 unterstützt, mit dem Informationen zur weiteren Entwicklung von unbemannten Systemen erfasst und deren Einsatzmöglichkeiten für SEWD aber auch im Bereich der Nuklearen Gefahrenabwehr (NGA) abgeschätzt und bewertet werden sollen.

Die wesentlichen Ergebnisse, ohne die entsprechend dem Handbuch für den Geheimschutz in der Wirtschaft als Verschlusssache einzustufenden Aspekte, sind im techni-

schen Bericht „Möglichkeiten zum Einsatz von Drohnen für Belange der Sicherung, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis“ /GRS 21i/ enthalten.

2.2.2 Halligan-Tool

Im Rahmen des Vorhabens wurden Recherchen zu effektiven mechanischen Hilfsmitteln zum Öffnen von Öffnungsverschlüssen wie Türen in Barrieren, die für die Sicherung von Bedeutung sein können, durchgeführt. Als ein solches Hilfsmittel wurde das sogenannte Halligan-Tool als Hebel- und Brechwerkzeug identifiziert, das ursprünglich zur gewaltsamen Öffnung von Türen von Feuerwehrmännern in den USA entwickelt und eingesetzt wurde. Es findet immer noch hauptsächlich Anwendung bei der Feuerwehr.

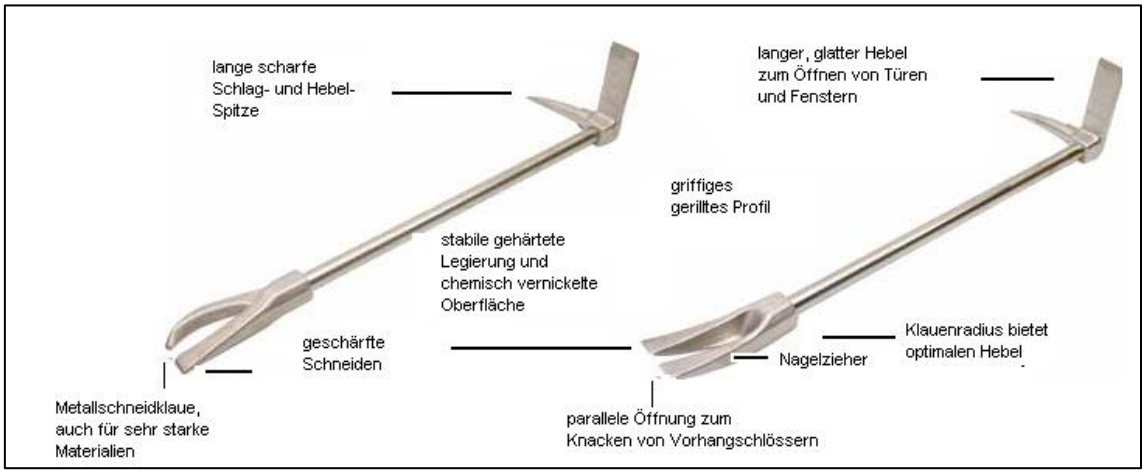

Abb. 2.1 Schematische Darstellung des Halligan-Tools als Standardvariante und mit Metallschneideklaue[2]

Zum Halligan-Tool wurde neben den Parametern mit typischen Bauweisen und Ausführungsformen vor allem die möglichen Einsatz- und Verwendungsmöglichkeiten recherchiert. Die Konstruktion besteht aus einer Stahlstange mit einer Klinge und einem Dorn an einem Ende und einem Kuhfuß am anderen Ende. Zumeist wird das Halligan-Tool zusammen mit einem Spalthammer oder einer Axt eingesetzt. Als manuelles Hebel- und Brechwerkzeug ist es demnach sehr flexibel und effektiv einsetzbar. So kann z. B. eine Klinge in enge Spalte geschlagen werden, um diese durch die Flankenkräfte des Keils aufzuweiten. Ein Dorn kann verwendet werden, um Löcher in Bleche und weichere

[2] Quelle: http://www.medirescue.com/html/body_e-hooligan.html, Abgerufen 17.06.2021

Baustoffe zu schlagen. Eine Klaue wird vor allem zum Metallschneiden und mit ihrem Mittelspalt als eine Art Nageleisen eingesetzt. Typische Anwendungstechniken bei Rettungseinsätzen der Feuerwehr sind auf den Einsatz durch zwei Personen oder auch nur eine Person zugeschnitten und wirken wahlweise auf die die Tür selbst, deren Befestigung und deren Verschluss.

Die Anwendungsmöglichkeiten wurden hinsichtlich ihrer Wirksamkeit für Belange der Sicherung von kerntechnischen Anlagen generisch bewertet. Daraus resultieren keine Erkenntnisse, die eine Neubewertung von Sicherungsmaßnahmen erfordern würden.

Die Ergebnisse der Recherche und der Bewertung wurden in der technischen Notiz „Hilfsmittel zum gewaltsamen Öffnen von Türen, Halligan-Tool“ /GRS 20a/ dargestellt. Die Details der Bewertung mit Bezug auf die Sicherung kerntechnischer Anlagen und damit die gesamte technische Notiz sind als VS-NfD eingestuft.

2.3 Sicherung von Endlagern für relevante Endlagerkonzepte

Mit dem Standortauswahlgesetz wurde die Suche nach einem Endlager für hochradioaktive Abfälle auf eine gesetzliche Grundlage gestellt, und die technische und planerische Kompetenz für die Endlagerung wurde mit der Schaffung der Bundesgesellschaft für Endlagerung (BGE) mbH gebündelt. Das Verfahren der Auswahl eines Standortes zur Endlagerung hochradioaktiver Abfälle hat begonnen.

Für die Sicherung von Endlagern gegen SEWD fehlen jedoch bisher mögliche, vom jeweiligen Endlagerkonzept abhängige, generische Sicherungskonzepte und deren Bewertung.

Für die Endlagerung von hochradioaktiven Abfällen und anderen radioaktiven Stoffen sollte deshalb der Sicherungsbedarf für relevante Endlagerkonzepte auf der Ebene von generischen, standortunabhängigen Anforderungen an die Sicherung und zugehörigen geeigneten Sicherungsmaßnahmen, auch unter Berücksichtigung internationaler Konzepte und Erfahrungen, ermittelt werden. Der Stand von W,T&E soll dafür im erforderlichen Umfang ausgewertet werden.

Informationen zur Sicherung von Endlagern wurden für relevante Endlagerkonzepte auf internationaler und nationaler Ebene recherchiert, insbesondere die Konzepte für die Endlagerung hochradioaktiver Abfälle, die Grundlagen für die Sicherung von Endlagern

auf internationaler Ebene gemäß internationalem Regelwerk und die bestehenden Sicherungskonzepte in Deutschland wie für die Schachtanlage Konrad. Eine Übertragbarkeit von Sicherungskonzepten in anderen Ländern auf die Gegebenheiten in Deutschland wurde geprüft und bewertet.

Im Zuge der Recherchen erfolgte eine Kontaktaufnahme zur BGE für zusätzliche Informationen zu Endlager-Sicherungskonzepten, die ebenfalls bewertet wurden. Bezüglich ausgewählter Kriterien erfolgte eine vertiefte Betrachtung von Sicherungsaspekten. Als ein Aspekt mit besonderer Bedeutung für die Endlagerkonzepte wurde dabei der Schnittstelle von Sicherheit und Sicherung die entsprechende Bedeutung beigemessen.

Zu den Arbeiten gehörten regelmäßige Abstimmungen mit BMU und BGE zu den laufenden Arbeiten, den Ergebnissen und den weiteren Zielstellungen.

Die Anforderungen an die Endlagerung radioaktiver Abfälle unterscheiden sich abhängig von der Halbwertszeit, der Radioaktivität und der damit verbundenen Zerfallswärme der Abfälle. Eine Unterscheidung zwischen schwach- und mittelradioaktiven sowie hochradioaktiven Abfällen oder eine zweiteilige Unterscheidung zwischen wärmeerzeugenden Abfällen und Abfällen mit vernachlässigbarer Wärmeerzeugung ist üblich. Die Endlagerung hochradioaktiver Abfälle stellt eine Herausforderung aufgrund des Gefahrenpotentials dar. Als Endlagerkonzept, welches die daraus resultierenden Anforderungen erfüllen kann, hat sich weltweit die geologische Tiefenlagerung durchgesetzt. Durch die Endlagerung in tiefen geologischen Formationen soll der sichere Einschluss der Abfälle zur Ver- und Behinderung von Radionuklidfreisetzungen gewährleistet werden. Im Sinne einer Synergie von Sicherheits- und Sicherungsmaßnahmen bietet ein solches Konzept gleichzeitig auch einen Schutz gegen SEWD. In den meisten Ländern ist die Rückholbarkeit der hochradioaktiven Abfälle eine weitere Kategorie, welche bei der Endlagerung beachtet werden muss.

Das Regelwerk der IAEO enthält zum jetzigen Zeitpunkt keine spezifischen Dokumente für die Sicherung von Endlagern, aber die generelle Handhabung von radioaktiven Abfällen wird in verschiedenen Dokumenten thematisiert. Im internationalen Regelwerk wird außerdem die Entsorgung von radioaktivem Abfall im Allgemeinen thematisiert. Radioaktive Abfälle im Betriebsbereich eines Endlagers sollten so wie radioaktive Stoffe an anderen Orten gesichert werden. Im Gegensatz dazu befinden sich radioaktive Abfälle im Bereich für die Endlagerung oft von Natur aus hinter physischen Barrieren mit stark begrenzter Anzahl an Zugangspunkten. Ein wichtiger Aspekt für die Endlagerung ist

daher ein integriertes Konzept von Sicherheits- und Sicherungsmaßnahmen, die sich nicht gegenseitig beeinträchtigen, sondern sich durch Synergieeffekt soweit wie möglich gegenseitig unterstützen und verstärken.

In Deutschland gibt es mit der Schachtanlage Asse II und dem Endlager Morsleben zwei Endlager, in denen bereits schwach- und mittelradioaktive Abfälle eingelagert wurden. Außerdem wird der Schacht Konrad nach der im Jahr 2007 abgeschlossenen Genehmigung zu einem Endlager für schwach- und mittelradioaktive Abfälle ausgebaut. Für hochradioaktive Abfälle wurde die Suche nach einem Endlagerstandort begonnen. Perspektivisch soll eine Richtlinie zur Sicherung von Endlagern gegen SEWD erstellt werden. Bei der Untersuchung der Lage in Deutschland war daher insbesondere der Umgang mit bestrahltem Kernbrennstoff, die Sicherung von Zwischenlagern gegen SEWD und bestehende Sicherungskonzepte für Endlager mit leicht- und mittelradioaktiven Abfällen relevant. Um eine Übertragbarkeit von bestehenden Sicherungskonzepten auf ein Endlager in Deutschland prüfen zu können, wurden die grundlegenden Rahmenbedingungen des Entsorgungskonzepts in Deutschland betrachtet, das zunächst auf einer Optimierung der Sicherheit basiert, aber starke Auswirkungen auf ein Sicherungskonzept hat. Die vier grundlegenden Prinzipien für hochradioaktive Abfälle sind Konzentration, Isolation, Nachsorgefreiheit und der Verschluss in großer Tiefe. Eine Isolation soll durch praktisch wasserundurchlässige Gesteinsschichten realisiert werden. Welche Behältertypen für die Endlagerung verwendet werden, steht bisher nicht fest, aber vor allem zwei Behältertypen mit einer jeweils danach angepassten Lagerungsmethode sind in der Diskussion: Kokillen, die in Bohrlöchern innerhalb des Stollens eingelagert werden, und die Streckenlagerung in POLLUX-Behältern. Bei Betrachtung der allgemeinen Schutzziele für die Sicherung von Zwischenlagern wird ersichtlich, dass diese für das Konzept der Endlagerung in tiefen geologischen Schichten andere Konsequenzen für die Sicherung ergeben.

Für schwach- und mittelradioaktive Abfälle sind in vielen Ländern bereits Endlager errichtet worden. Für hochradioaktive Abfälle aus der Kerntechnik ist weltweit noch kein Endlager in Betrieb. Im Jahr 2000 wurde der Standort Olkiluoto als finnisches Endlager für hochradioaktive Abfälle ausgewählt und seit Ende 2015 finden in 400-500 m Tiefe die Bauarbeiten zur Errichtung statt. Die Entsorgung des radioaktiven Abfalls in der Anlage soll in den 2020er Jahren starten. Damit wäre das Endlager Olkiluoto das erste Endlager für hochradioaktive Abfälle aus der Kerntechnik in tiefen geologischen

Formationen, so dass die Betrachtung des zugehörigen Sicherungskonzepts besonders relevant war.

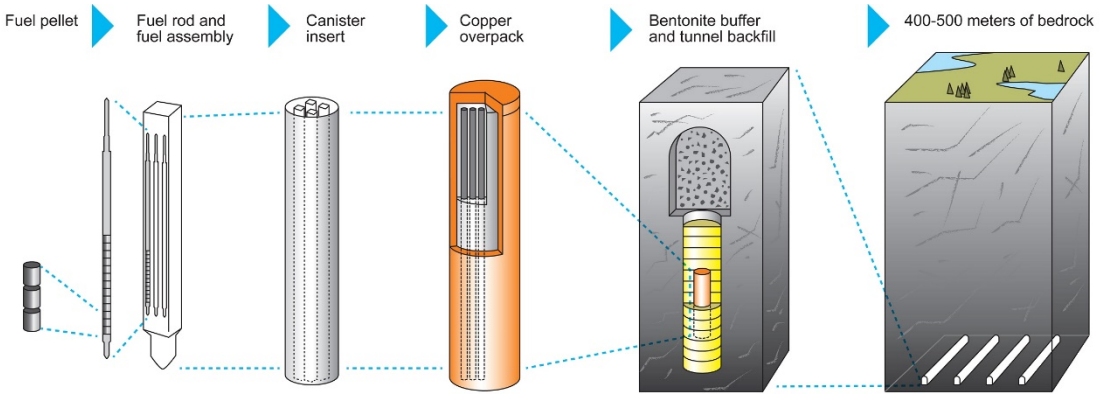

Abb. 2.2 KBS-3 Einlagerungskonzept der finnischen Firma Posiva zur Endlagerung[3]

Gegenwärtig besteht jedoch noch kein finales Sicherungskonzept. Deshalb hat die finnische atomrechtliche Behörde STUK ein nationales Forschungs- und Entwicklungsprogramm ins Leben gerufen mit dem Hauptziel der Fertigstellung des finnischen Sicherungskonzepts für die Endlagerung.

Auf Basis der Erkenntnisse aus Recherchen und deren Auswertung wurden Regelungsgrundlagen für ein Sicherungskonzept diskutiert, und Konsequenzen für Regelungen zur Endlagersicherung wurden abgeleitet. Die Informationen zu konkreten Sicherungskonzepten und die Bewertungen mit Bezug auf die Sicherung wurden als VS-NfD eingestuft.

Die Ergebnisse sind im technischen Bericht „Sicherung in der Endlagerung“ /GRS 21b/ dargestellt mit

- einem Überblick über Konzepte für die Endlagerung hochradioaktiver Abfälle,
- den Ergebnissen der Recherchen im internationalen Regelwerk zu den Grundlagen für die Sicherung von Endlagern,
- einer Übersicht zu bestehenden und ehemaligen Sicherungskonzepten von Endlagern in Deutschland,

[3] Quelle: Homepage Posiva, http://www.posiva.fi/en/final_disposal/basics_of_the_final_disposal, Abgerufen 14.12.2020

- Informationen zu einem vorgesehenen allgemeinen Sicherungskonzept für ein finnisches Endlager für hochradioaktive Abfälle in Planung und Bau sowie einer Untersuchung zu Aspekten, die sich auf Endlagerkonzepte in Deutschland übertragen lassen
- einer Bewertung der für die Sicherung von Endlagern relevanten Aspekten mit einer ergänzenden Einschätzung, wie auf Grundlage dieser Erkenntnisse das weitere Vorgehen bei der Entwicklung eines Regelwerks zur Endlagerung aussehen könnte beziehungsweise welche Aspekte hierbei beachtet werden sollten.

Die Ergebnisse bilden eine Grundlage für die Fortschreibung des SEWD-Regelwerks im Rahmen der Auftragsforschung.

Die wesentlichen Ergebnisse, ohne die entsprechend dem Handbuch für den Geheimschutz in der Wirtschaft als Verschlusssache einzustufenden Aspekte, sind im technischen Bericht „Sicherung in der Endlagerung“ /GRS 21h/ enthalten.

2.4 Schnittstelle Sicherheit und Sicherung

Im internationalen Rahmen wurden Empfehlungs-Dokumente getrennt für die Sicherheit und die Sicherung erarbeitet. Aber die internationale Diskussion dazu führt zunehmend zu der Erkenntnis, dass es zwischen beiden Gebieten nutzbare Synergien gibt. Bisher wurde diese Diskussion national nicht systematisch verfolgt und hinsichtlich der nationalen Umsetzbarkeit einschließlich erforderlicher Anpassungen von Regelungen ausgewertet. Deshalb sollten für die Schnittstelle Sicherheit-Sicherung bei kerntechnischen Anlagen Synergien und Möglichkeiten für eine verbesserte Berücksichtigung der Schnittstelle abgeleitet werden. Dazu sollte in einem ersten Schritt der Stand von W,T&E bezüglich der Schnittstelle im erforderlichen Umfang recherchiert und ausgewertet werden, ergänzt durch erste generische Auswertungen zur Verbesserung von Sicherungsstandards.

Der Stand von W,T&E für die Schnittstelle von Sicherheit und Sicherung wurde hinsichtlich möglicher Synergien zusammengestellt. Dazu wurden ausgewählte internationale Dokumente ausgewertet und Erkenntnisse aus internationalen Fachtagungen abgeleitet mit dem Fokus auf den Dokumenten, die der internationalen Diskussion im Zusammenhang mit der Schnittstelle zugrunde liegen. Auf generischer Ebene wurden Synergien an der Schnittstelle Sicherheit und Sicherung für den nationalen Bereich abgeleitet und es

wurden Vorschläge zur Verbesserung der Nutzung dieser Synergien im deutschen Sicherungsregime erarbeitet.

Für die Recherche wurden relevante internationale Dokumente zur Schnittstelle Sicherheit und Sicherung ausgewählt sowie der Ergebnisse von internationalen Konferenzen mit einem Schwerpunkt auf diesem Thema:

- Dokumente des internationalen Regelwerks der IAEO zur Sicherheit
- Dokumente des internationalen Regelwerks Nuclear Security Series (NSS) der IAEO zur Sicherung
- Beratertreffen “Technical Meeting on the Safety and Security Interface - Approaches and National Experiences” der IAEA am 29.10. - 01.11.2018 in Wien mit dem Ziel, die technischen Elemente an der Schnittstelle zwischen Sicherheit und Sicherung zu identifizieren
- internationale Konferenz zur nuklearen Sicherung (Sustaining and Strengthening Efforts) (ICONS 2020) vom 10. Bis 14.02.2020 bei der IAEA in Wien, die viele Aspekte der Sicherung abdeckt, u. a. die Schnittstelle zwischen Sicherung und Sicherheit

im Zuge der Auswertung der Rechercheergebnisse erfolgte eine Systematisierung von relevanten Aspekten bezüglich Konfliktpotential, Lösungsansätze und insbesondere Synergien aus internationaler Sicht.

Wesentliche Aspekte für eine Definition der Schnittstelle sind demnach aus internationaler Sicht auf Basis verschiedener Ansätze:

- Schnittstelle erwächst aus dem gemeinsamen Ziel des Schutzes von Personen (Leben und Gesundheit), Gütern, Gesellschaft und Umwelt - gegen die schädliche Wirkung ionisierender Strahlung
- Schnittstelle ist ein gemeinsamer Bereich, der die Auslegung und Umsetzung von Sicherheits- und Sicherungsmaßnahmen in einer ausgewogenen Weise ermöglicht
- Schnittstelle umfasst Aspekte von Sicherheits- und Sicherungsanforderungen und -maßnahmen, die sich gegenseitig ergänzen oder einander entgegenwirken können

- Vorgehen für die Schnittstelle: Sicherheits- und Sicherungsmaßnahmen in einem umfassenden Ansatz auslegen und umsetzen; Synergien zwischen Sicherheit und Sicherung entwickeln bzw. erreichen; sicherstellen, dass Sicherheitsmaßnahmen nicht die Sicherung behindern und dass Sicherungsmaßnahmen nicht die Sicherheit behindern; entwickeln und umsetzen von Sicherheitsanforderungen sowie Sicherungsempfehlungen und -maßnahmen bezüglich der Sicherheit und Sicherung von Kernmaterial, sonstigen radioaktiven Stoffen, zugehörigen Anlagen und Einrichtungen

Auf generischer Ebene wurden für den nationalen Bereich Synergien und Vorschlägen zu deren verbesserter Nutzung abgeleitet. Diese wurden an den internationalen Empfehlungen und an den bisherigen Vorgaben im nationalen SEWD-Regelwerk gespiegelt.

Dazu wurde wesentliche (repräsentative) Vorgaben des SEWD-Regelwerks im Zusammenhang mit der Schnittstelle Sicherheit und Sicherung bzw. mit dem Umgang mit dieser Schnittstelle recherchiert, systematisiert und zusammengestellt. Auf dieser Basis wurde die mögliche Bedeutung internationaler Erkenntnisse für das nationale SEWD-Regelwerk ausgewertet. Dafür wurden Vorschläge für mögliche Anpassungen und für eine mögliche künftige Berücksichtigung der Schnittstelle bei der Auslegung der Sicherung und im SEWD-Regelwerk abgeleitet. Die Vorgaben des SEWD-Regelwerks und die generische Auswertung mit Bezug zum SEWD-Regelwerk wurden als VS-NfD eingestuft.

Die Ergebnisse sind im technischen Bericht „Schnittstelle Sicherheit-Sicherung für kerntechnische Anlagen, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis“ /GRS 21c/ dargestellt mit

- der Definition der Schnittstelle Sicherheit – Sicherung auf Basis von Vorgaben und Empfehlungen im internationalen Regelwerk,
- einer systematischen Zusammenstellung von relevanten Schnittstellen in ausgewählten Teilen des Regelwerks der IAEO zur Sicherheit einerseits und in ausgewählten Teilen des Regelwerks der IAEO zur Sicherung andererseits,
- einer systematischen Zusammenstellung der Erkenntnisse aktueller Diskussionen zur Schnittstelle auf ausgewählten internationalen Konferenzen,
- einer generischen Auswertung für den nationalen Bereich.

Die Ergebnisse bilden eine Grundlage für die Fortschreibung des SEWD-Regelwerks im Rahmen der Auftragsforschung.

Die wesentlichen Ergebnisse, ohne die entsprechend dem Handbuch für den Geheimschutz in der Wirtschaft als Verschlusssache einzustufenden Aspekte, sind im technischen Bericht „Schnittstelle Sicherheit-Sicherung für kerntechnische Anlagen, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis“ /GRS 21g/ enthalten.

2.5 Nukleare Sicherungskultur

Für die nukleare Sicherung ist die Sicherungskultur gemäß IAEO das Zusammenspiel von Eigenschaften, inneren Einstellungen und Verhaltensweisen von Einzelpersonen, Organisationen und Einrichtungen, das dazu dient, die Sicherung zu unterstützen und zu steigern.

Der Sicherungskultur als wichtiger Bestandteil der Sicherung kerntechnischer Anlagen und der Beförderung von Kernbrennstoffen und sonstigen radioaktiven Stoffen wird im internationalen Maßstab eine zunehmend hohe Bedeutung zugemessen. Mit dem Positionspapier von Bund und Ländern zur „Sicherheitskultur in atomrechtlichen Genehmigungs- und Aufsichtsbehörden" liegt eine nationale Vorgabe zur Etablierung einer Sicherungskultur auf der Ebene der Behörden vor. Dennoch soll die nukleare Sicherungskultur, auch im Sinne des Action Plan des BMU /GRS 20c/ zur IPPAS-Mission Deutschland 2017 (internationaler Beratungsservice der IAEO zum physischen Schutz - International Physical Protection Advisory Service), auf allen Ebenen weiter gefördert werden. Zusätzliche Anforderungen bezüglich der Aufrechterhaltung des hohen Niveaus der Sicherungskultur erwachsen aus dem geänderten Rahmen für den Betrieb von Kernkraftwerken (KKW) infolge des Atomausstiegs und den damit verbundenen Möglichkeiten, für die Aufgaben bei der Stilllegung entsprechend qualifiziertes und vor allem motiviertes Personal zu beschäftigen. Für einen Erhalt bzw. eine Verbesserung der Sicherungskultur in allen involvierten Organisationen sollen deshalb geeignete Kriterien für deren Bewertung abgeleitet werden, die eine Grundlage für die Erarbeitung eines Leitfadens zur Sicherungskultur im Rahmen eines anderen Vorhabens darstellen können. Da Untersuchungen im Zusammenhang mit der Sicherungskultur ursprünglich nicht vorgesehen waren, wurden zusätzliche Mittel für eine erste Recherche und deren Auswertung zum Stand von W,T&E bereitgestellt.

Auf Basis internationaler Empfehlungen für Kriterien zur Bewertung der Sicherungskultur sollten geeignete Indizien für eine robuste Sicherungskultur ausgewählt und auf einer generischen Ebene an die nationalen Gegebenheiten angepasst werden. Dazu sollten internationale Dokumente ausgewertet werden.

Der internationale Stand von Empfehlungen bezüglich der nuklearen Sicherungskultur und aktuelle internationale Entwicklungen und Zielsetzungen sowie der nationale Stand und bisherige nationale Aktivitäten wurden recherchiert und ausgewertet. Dabei wurde auf die Integration der Sicherungskultur in die Sicherheitskultur eingegangen sowie der perspektivische Erhalt, Ausbau und Entwicklung der Kompetenz für die nukleare Sicherung thematisiert. Die Rechercheergebnisse wurden bewertet, und Empfehlungen für künftige Aktivitäten im nationalen Rahmen und im internationalen Umfeld wurden abgeleitet.

Als eine Erkenntnis lässt sich festhalten, dass die nukleare Sicherungskultur z. B. aufgrund der steigenden Zahl an internationalen Empfehlungen, durch Schwerpunktbildung auf europäischer Ebene und durch die Veröffentlichung von Anwendungsfällen an Bedeutung gewinnt.

Die Ergebnisse sind im technischen Bericht „Sicherungskultur, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis“ /GRS 21d/ dargestellt mit

- den Rechercheergebnissen zum internationalen und zum nationalen Stand von Empfehlungen zur nuklearen Sicherungskultur
- aktuellen Entwicklungen und Zielsetzungen zur nuklearen Sicherungskultur auf internationaler Ebene,
- Empfehlungen zum Kompetenzerhalt und gemeinnützigen Wissensaufbau, zur Fortschreibung des SEWD-Regelwerks mit Blick auf die Sicherungskultur und zu weiterführenden Potentialen.

Die Ergebnisse bilden eine Grundlage für die Fortschreibung des SEWD-Regelwerks im Rahmen der Auftragsforschung.

2.6 Verfolgen der Entwicklungen und Ereignisse mit Relevanz für die IT-Sicherheit

In der Sicherung soll stets der Stand von W,T&E bei der Bewertung und Fortentwicklung von Sicherungskonzepten im gebotenen Umfang berücksichtigt und bundeseinheitlich umgesetzt werden. Das betrifft in besonderem Maße den von einer dynamischen Entwicklung geprägten Bereich der IT-Systeme. Die regulatorische Basis für die IT-Sicherheit geht nicht über die Ebene der Anforderungen hinaus, so dass die Ebene der Maßnahmen durch solche gemäß dem Stand von W,T&E abgedeckt wird.

Geeignete Recherchequellen mit Informationen zu nationalen und internationalen Ereignissen mit IT-Sicherheitsrelevanz im Hinblick auf kerntechnische Anlagen wurden gesucht, identifiziert und ausgewählt.

Die Voraussetzungen für die Dokumentation von Erkenntnissen zum Stand von W,T&E wurden geschaffen. Dafür wurden zunächst die konzeptionellen Voraussetzungen geschaffen durch den Entwurf einer Tabelle zur Darstellung von Recherche-Ergebnissen.

Es erfolgte eine kontinuierliche Recherche bzgl. der IT-Sicherheit insbesondere auf fachspezifischen Webseiten:

- Sichtung bereits bekannter und genutzter Quellen mit Informationen zu nationalen und internationalen IT-Sicherheitsvorfällen
- Screening von potenziellen Hilfsmitteln, Schwachstellen, IT-Sicherheitsvorfällen, IT-Angriffen, Aktivitäten bekannter Angreifer-Gruppierungen mit Schwerpunkt industrielle Steuerungssysteme und kritische Infrastrukturen (KRITIS)
- Screening von Meldungen des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Besondere Randbedingungen für die Recherchen bzgl. der IT-Sicherheit ergaben sich aufgrund der Pandemiesituation:

- Begrenzung auf die vertrauenswürdigen Quellen BSI und United States Computer Emergency Readiness Team (US-CERT)

Die erkannten Ereignisse wurden einer Erstbewertung hinsichtlich ihrer Relevanz für nationale kerntechnische Anlagen unterzogen. Die Auswertung von Rechercheergebnissen bzgl. der IT-Sicherheit umfasste u. a. die Entwicklung von Hilfsmitteln, die von Tätern genutzt werden können.

Die Dokumentation der Rechercheergebnisse erfolgt auf Basis einer dafür entwickelten Struktur. Diese berücksichtigt einerseits die Art der Ereignisse mit Relevanz für die IT-Sicherheit, wie Schwachstellen, IT-Angriffswerkzeuge, IT-Sicherheitsvorfälle und IT-Angriffe, und andererseits die Chronologie. Außerdem besteht die Möglichkeit, Bezüge zwischen zusammenhängenden oder aufeinander aufbauenden Ereignissen deutlich zu machen (siehe auch Kap. 3.3).

Die Anforderungen an die IT-Sicherheit wurden unter Berücksichtigung aktueller Dokumente der International Electrotechnical Commission (IEC) und der IAEO generisch weiterentwickelt.

2.7 Definitionen für die IT-Sicherheit

Ein Katalog mit Definitionen für die IT-Sicherheit wurde unter Berücksichtigung von Vorgaben in aktuellen nationalen und internationalen Regelwerken und Dokumenten zur IT-Sicherheit entwickelt. Er dient u. a. zur Unterstützung bei der Systematisierung von Rechercheergebnisse und der vereinheitlichten Darstellung von Erkenntnissen.

Die Ergebnisse wurden bei der Mitwirkung in der ENSRA-WENRA Working Group on Cyber Security im Rahmen eines anderen Vorhabens vorgestellt und diskutiert. Der Katalog soll im Nachfolgevorhaben bedarfsgerecht weiterentwickelt und kontinuierlich gepflegt werden.

3 Ereignisse mit Sicherungsrelevanz und relevante IT-Sicherheitsvorfälle

Arbeiten im Rahmen des AP 2: Analyse von Ereignissen mit Sicherungsrelevanz und IT-Sicherheitsrelevanz

Nationale und internationale IT-Sicherheitsvorfälle und weitere Ereignisse mit Sicherungsrelevanz sollten regelmäßig gesichtet werden. Dabei ist auch eine Erstbewertung der Ereignisse erforderlich, um die Relevanz für die Sicherung und die IT-Sicherheit einschätzen zu können. Die als relevant erkannten Ereignisse sollten umfassend ausgewertet werden. Die Analysen von Ereignissen und IT-Sicherheitsvorfällen erfolgen grundsätzlich auf generischer Ebene und haben Modellcharakter für konkrete Anlagen. Eine weitergehende Auswertung bei möglicher Rückwirkung auf das SEWD-Regelwerk auf dieser Basis kann im Rahmen eines anderen Vorhabens auf Anforderung des BMU erfolgen.

3.1 Ereignisse mit Sicherungsrelevanz

Geeignete Recherchequellen mit Informationen zu nationalen und internationalen Ereignissen mit Sicherungsrelevanz im Hinblick auf kerntechnische Anlagen einschließlich der Beförderung von Kernbrennstoffen wie Pressemeldungen, Literatur, spezielle Datenbanken wurden gesucht, identifiziert, ausgewählt und gesichtet. Als eine Recherchequelle wurde auch die Datenbank Incident and Trafficing Database (ITDB) der IAEO über das BMU in Form von Ereignis-Digests herangezogen.

Die Voraussetzungen für die Dokumentation der Ergebnisse wurden durch die Erstellung einer ACCESS-Datenbank geschaffen. Es wurden verschiedene Kategorien in der Datenbank vordefiniert, zu denen für jedes Ereignis Angaben gemacht werden können. Basierend auf den Angaben können die Daten in der Datenbank sortiert, extrahiert und weiterverwendet werden.

Die folgenden Kategorien sind in der Datenbank definiert:

1. Laufende Nummer
2. Datum
3. Anlage/Ort
4. Land
5. Durchgeführt?
   Die Kategorie wird markiert, wenn SEWD gegen die kerntechnische Anlage durchgeführt wurden. Dazu zählt auch ein Versuch von SEWD, die nicht erfolgreich abgeschlossen werden konnten. Eine Markierung wird nicht gesetzt, wenn nur Planung und eventuelle Vorbereitungshandlungen erfolgt sind.
6. Art des Ereignisses
   Mehrfachnennungen sind möglich. Es stehen folgende Ereignisarten zur Auswahl:
   - Bewaffnete Angriffe und Bombenexplosionen,
   - Böswilliger Einsatz von radioaktiven Stoffen,
   - Diebstahl Kernbrennstoffe,
   - Diebstahl sonstige radioaktiver Stoffe,
   - Einbringen unerlaubter Gegenstände,
   - Eindringen mit Fahrzeugen,
   - Eindringen ohne Fahrzeuge,
   - Einsatz unbemannter Fahrzeuge,
   - Einwirkungen durch Innentäter,
   - Einwirkungen durch Störer,
   - Flugzeugabsturz,
   - IT-Sicherheit,
   - Menschliches oder institutionelles Versagen,
   - Nötigung/Geiselnahme/Erpressung,
   - Sabotage,
   - Transport radioaktiver Stoffe.
7. Kurzbeschreibung
8. Beschreibung
9. Freisetzung? Entwendung? Freisetzung nach Entwendung?
10. Quellen

Die ausgewählten Quellen zu sicherungsrelevanten Ereignissen wurden gesichtet, relevante Ereignisse mit Bezug zu Kernmaterial, radioaktiven Stoffen, kerntechnischen Anlagen und der Beförderung radioaktiver Stoffe wurden ausgewählt und einer Erstbewertung unterzogen. Diese ist gleichzeitig die Voraussetzung für die Auswahl von Ereignissen, die einer vertieften Auswertung auf generischer Ebene bei Bedarf unterzogen werden.

Die Bewertung der Ereignisse erfolgte hinsichtlich ihrer Bedeutung für die Sicherung radioaktiver Stoffe in Deutschland und deren Abdeckung durch das SEWD-Regelwerk mit dem Ziel, Lücken in der Sicherung und in der Abdeckung durch das SEWD-Regelwerk zu erkennen. Daher wurde insbesondere nach Ereignissen gesucht, bei denen kerntechnische Anlagen oder Beförderungsvorgänge unmittelbares Ziel von SEWD waren. Darüber hinaus wurden Ereignisse in die Datenbank aufgenommen, die nicht unmittelbar im Zusammenhang mit SEWD auf kerntechnische Anlagen oder Beförderungsvorgängen standen, aber möglicherweise relevante Informationen hinsichtlich Täterverhalten oder Lücken in Sicherungskonzepten bzw. -einrichtungen beinhalten. Dabei sind z. B. Einwirkungen von Störern, Ereignisse im Zusammenhang mit Kernwaffen oder Schiffen mit Kernenergieantrieb, illegaler Handel mit Kernbrennstoffen oder sonstigen radioaktiven Stoffen sowie Ereignisse mit IT-Sicherheitsrelevanz zu nennen.

Als Beispiel für einen bewaffneten Angriff sind die Ereignisse des 08.11.2007 im Kernforschungszentrum Pelindaba in Südafrika zu nennen. Vier Angreifer deaktivierten einen Elektrozaun und drangen in die Anlage ein. Sie wurden von einem Mitarbeiter überrascht und schossen ihn nieder. Die Angreifer entwendeten zwei Laptops und verließen das Gelände wieder. Sie waren auf Bildern der Videoanlage zu sehen, diese wurden jedoch nicht überwacht. Die Angreifer entkamen unerkannt. Es wird spekuliert, dass sie Informationen von einem Innentäter erhalten hatten, da sie sich anscheinend mit den örtlichen Begebenheiten und den technischen Einrichtungen auskannten.

Im Kernkraftwerk Ignalina, Litauen, wurde im Jahr 1992 ein ganzes Brennelement entwendet, indem es unter einem Bus befestigt wurde. Dabei kam es zu Absprachen zwischen Anlagenmitarbeitern und Wachpersonal.

Bei den erfassten Ereignissen mit Einwirkungen durch Innentäter handelt es sich meistens um Sabotage. So wurde im Jahr 2006 ein Loch, das jemand in ein Rohr im Kernkraftwerk Turkey Point, USA, gebohrt hatte, entdeckt. Das Loch hatte einen Durchmesser von ca. 3 mm, das Rohr war Teil des unter Druck stehenden Kühlkreislaufs. Im Jahr

2014 wurde im Kernkraftwerk Doel, Belgien, ein Ventil geöffnet, so dass Schmieröl auslief, das eigentlich zum Schmieren der Turbine benötigt wurde. Es kam zur automatischen Abschaltung des Kraftwerks. Der Täter konnte nicht identifiziert werden.

Die Erkenntnisse aus der Erstbewertung dieser Ereignisse lassen keine Rückschüsse auf mögliche Lücken im deutschen SEWD-Regelwerk bzw. bei dessen Umsetzung in den Sicherungskonzepten für deutsche kerntechnische Anlagen zu. Es bestand daher bislang kein Bedarf für eine vertiefte Auswertung dieser Ereignisse.

Die Dokumentation der ausgewählten sicherungsrelevanten Ereignisse, der Ergebnisse der Erstbewertung und der Erkenntnisse aus einer vertieften Auswertung auf generischer Ebene bei Bedarf erfolgt in der ACCESS-Datenbank. Dabei wurde versucht, bei jedem dokumentierten Ereignis Angaben in allen vordefinierten Kategorien in der Datenbank zu machen. Anhand dieser Kategorien können Informationen aus der Datenbank extrahiert und graphisch dargestellt werden. Dies wird im Folgenden anhand von Beispielen illustriert.

In Abb. 3.1 ist die zeitliche Verteilung der Ereignisse auf die sechs in der Datenbank berücksichtigten Dekaden seit dem Jahr 1961 dargestellt. Dabei wird im linken Diagramm zwischen durchgeführten und nicht durchgeführten (d. h. nur geplanten) Ereignissen unterschieden. Im rechten Diagramm wird wiederum zwischen Ereignissen mit und ohne Entwendung/Freisetzung unterschieden.

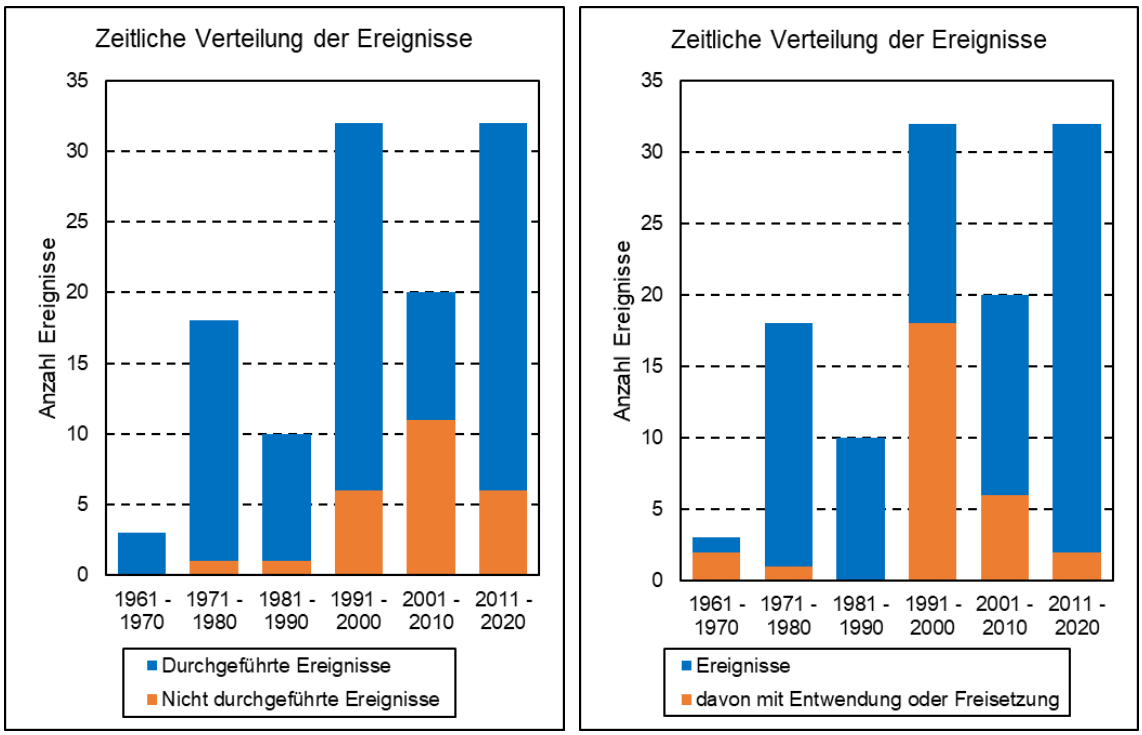

Abb. 3.1 Graphische Darstellungen der Datenbankeinträge als zeitliche Verteilungen

Die geringe Anzahl an Ereignissen in den 1960er Jahren ist wahrscheinlich auf die damals noch geringe Anzahl an KKW zurückzuführen. In den 1970er Jahren kam es zu zahlreichen SEWD gegen im Bau befindliche KKW, die teilweise noch nicht über fertiggestellte Sicherungseinrichtungen verfügten. Dies ist in den 1980er Jahren in geringerem Ausmaß noch zu beobachten. Der starke Anstieg der Ereignisse in den 1990er Jahren ist u. a. auf den Zerfall der Sowjetunion zurückzuführen. Diese Ereignisse stehen oft im Zusammenhang mit der Entwendung von Kernbrennstoffen. Einer der Gründe für den Anstieg der Ereignisse in den 2010er Jahren geht möglicherweise darauf zurück, dass Informationen über diese Ereignisse deutlich leichter verfügbar sind, da z. B. Pressemeldungen in größerem Ausmaß im Internet verfügbar sind. Es ist darüber hinaus in den letzten 30 Jahren zu beobachten, dass der Anteil an Ereignissen, die in einem Zusammenhang mit Entwendung oder Freisetzung stehen, kontinuierlich zurückgeht.

In Abb. 3.2 sind die Häufigkeiten der in der Datenbank definierten Arten der Ereignisse graphisch dargestellt. Dabei wird zwischen Ereignissen mit und ohne Entwendung/Freisetzung unterschieden. In dieser Kategorie sind in der Datenbank Mehrfachnennungen möglich.

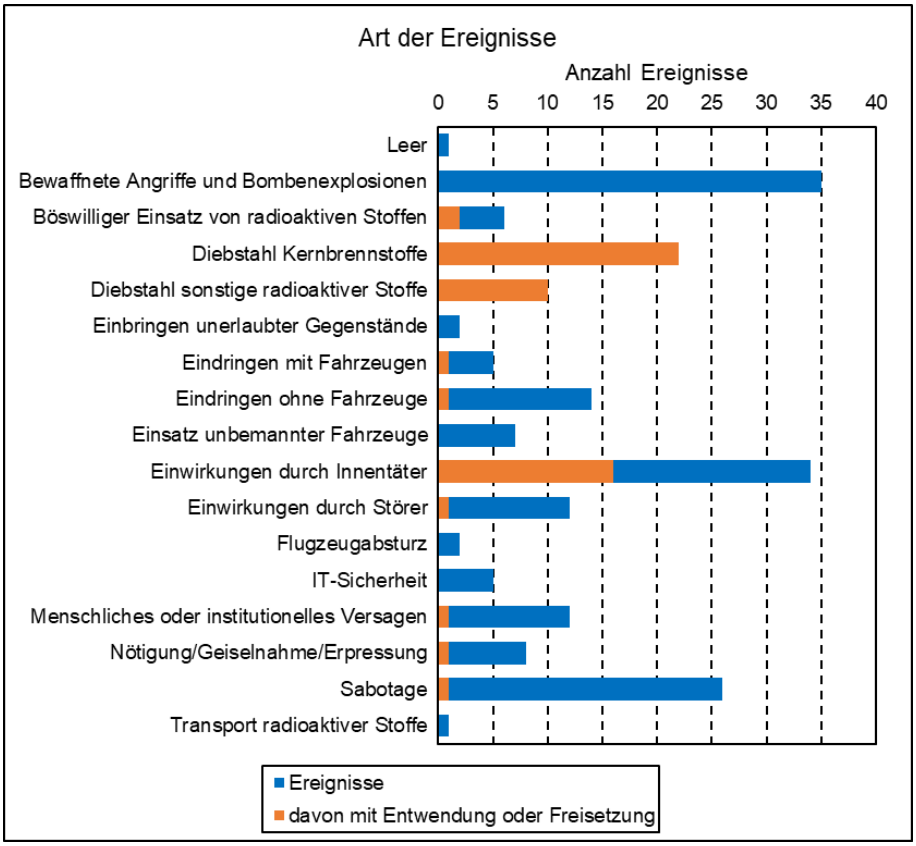

Abb. 3.2 Graphische Darstellung der Datenbankeinträge hinsichtlich der Arten der Ereignisse

Als häufigste Ereignisarten können anhand dieser Auswertung bewaffnete Angriffe und Bombenexplosionen, Einwirkungen durch Innentäter, Sabotage sowie Diebstahl von Kernbrennstoffen identifiziert werden. Dass die Ereignisarten Diebstahl Kernbrennstoffe und Diebstahl sonstige radioaktive Stoffe in einem Zusammenhang zu Entwendung/Freisetzung stehen, ist offensichtlich. Bemerkenswert ist dagegen, dass Versuche von Entwendung bzw. Freisetzung oft in einem Zusammenhang mit Einwirkungen durch Innentäter stehen. Auf der anderen Seite wurden insbesondere keine Versuche von Entwendung bzw. Freisetzung dokumentiert, die in einem Zusammenhang mit bewaffneten Angriffen und Bombenexplosionen stehen.

Diese exemplarischen Auswertungen der in der Datenbank enthaltenen Informationen sollen den praktischen Nutzen der Datenbank illustrieren. Es wurde der Stand der Datenbank im Mai 2021 verwendet. Die Datenbank wird kontinuierlich gepflegt und weiterentwickelt. Dafür werden regelmäßig Quellen gesichtet, bestehende Einträge in der Datenbank aktualisiert und neue Einträge ergänzt.

3.2 Generische Bewertung ausgewählter Ereignisse

Ein sicherungsrelevantes Vorkommnis am Standort KKW Grafenrheinfeld (KKG) wurde recherchiert und generisch bewertet. Auf dem Anlagengelände des seit 2015 stillgelegten KKG wird seit 2006 auch ein standortnahes Zwischenlager für abgebrannte Kernbrennstoffe betrieben, das innerhalb des äußeren Sicherungsbereichs am Standort liegt. Das Werksgelände wird durch eine Sicherungszaunanlage eingefasst.

Schwerpunkte der Bewertung waren die mögliche Einordnung als meldepflichtiges Ereignis und eine mögliche Relevanz für die Sicherungsmaßnahmen an kerntechnischen Anlagen.

Aus Presseberichten lässt sich der Sachverhalt zum Vorkommnis wie folgt zusammenfassen: Am 05. Juni 2020 erhielt die Polizei um 04 Uhr eine Meldung zu einem gewaltsamen Zutritt zum Werksgelände des KKG. Ferner erhielt auch der Objektsicherungsdienst (OSD) eine Meldung und veranlasst die Überprüfung. Beim Eintreffen des OSD flüchteten die Tatverdächtigen zu Fuß bzw. mit ihrem Fahrzeug (Lastkraftwagen). Im weiteren Verlauf verunfallten die Tatverdächtigen auf der nahegelegenen Staatsstraße und flüchteten ohne Beute. Die Polizei konnte nach erfolgreicher Fahndung sechs Männer im Alter von 20 bis 37 festnehmen.

Die vorliegenden, begrenzten Informationen zum Vorkommnis wurde auf Basis relevanter Anforderungen des SEWD-Regelwerks und der atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung (AtSMV) bewertet. Als Fazit erscheint eine Meldepflicht nach AtSMV als nicht erforderlich, wohingegen das zu unterstellende Vorgehen als meldepflichtig bezüglich der Vorgaben gemäß „Meldepflichtige sicherungsrelevante Vorkommnisse in kerntechnischen Einrichtungen und beim Transport von Kernbrennstoffen“ angesehen wird. Weitere Informationen zum Vorgehen und zu den Reaktionsmaßnahmen sowie deren Auswertung könnten eine Grundlage für den kontinuierlichen Verbesserungsprozess der Sicherung darstellen sowie Hinweise für eine robuste Sicherungskultur liefern.

Die Ergebnisse der Recherche und der Bewertung wurden in der technischen Notiz „Bewertung Buntmetalldiebstahl KKW Grafenrheinfeld (KKG) 06/2020 als meldepflichtiges Ereignis im Rahmen der Sicherung“ /GRS 20b/ dargestellt. Die Bewertung mit Bezug auf die Sicherung kerntechnischer Anlagen wird als VS-NfD eingestuft.

3.3 Relevante IT-Sicherheitsvorfälle

Die IT-Bedrohungslage entwickelt sich sehr dynamisch, beispielsweise durch das Bekanntwerden oder sogar die Ausnutzung neu erkannter oder bisher nicht geschlossener Schwachstellen in industriellen Steuerungssystemen bzw. in für kritische Infrastrukturen relevanten IT-Systemen, durch zunehmende, gezielte, technisch versierte und andauernde Angriffe mit fortgeschrittenen Methoden, Schadsoftwarekomponenten und IT--Angriffswerkzeugen sowie die sich kontinuierlich weiterentwickelnden Techniken, Taktiken und Vorgehensweisen der IT-Angreifer und insbesondere sogenannter APT-Gruppierungen (APT - Advanced Persistent Threats). Auf nationaler und internationaler Ebene sind regelmäßig IT-Sicherheitsvorfälle mit sicherungstechnischer Bedeutung und potenziell auf kerntechnische Anlagen und Einrichtungen übertragbaren Aspekten zu verzeichnen, woraus sich Veränderungen der IT-Bedrohungslage ergeben. Für die IT-Sicherheit kommt damit der regelmäßigen Analyse der Bedrohungslage, aber auch der Bewertung des Standes von W,T&E zu Prävention und Detektion von IT-Angriffen sowie zur Reaktion auf IT-Angriffe eine besondere Bedeutung zu.

Bereits in den Vorläufervorhaben wurden ausgewählte geeignete Recherchequellen mit Informationen zu nationalen und internationalen IT-Sicherheitsvorfällen kontinuierlich gesichtet. Daran anknüpfend wurde über die Laufzeit dieses Vorhabens hinweg die Entwicklung der IT-Bedrohungslage (für industrielle Steuerungssysteme und kritische Infrastrukturen relevante IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten, APTs) kontinuierlich verfolgt und ausgewertet. Hierzu wurden einschlägige, zugängliche nationale und internationale Quellen zur Informationssicherheit wie Literatur, fachspezifische Webseiten, Fachveranstaltungen, Veröffentlichungen von IT-Sicherheitsfirmen und Herstellern von industriellen Steuerungssystemen gesucht, identifiziert, ausgewählt und genutzt. Dazu zählen insbesondere auch BSI-Cybersicherheits-Warnmeldungen und internationalen CERT-Meldungen.

Die Voraussetzung für die Dokumentation von IT-Sicherheitsvorfällen und den Erkenntnissen aus deren Erstbewertung wurde durch die Konzeption einer geeigneten Struktur und der Erstellung eines daran ausgerichteten lebenden Dokuments geschaffen.

Auf Basis der gewählten Recherchequellen erfolgte ein regelmäßiges Screening der IT-Bedrohungslage. Relevante Schwachstellen, IT-Sicherheitsvorfälle, IT-Angriffe sowie Informationen zu IT-Angriffswerkzeugen, Schadsoftwarekomponenten und APTs wurden ausgewählt und einer Erstbewertung u. a. im Hinblick auf die IT-Sicherheit in kriti-

schen Infrastrukturen und insbesondere in kerntechnischen Anlagen unterzogen. Zusätzlich zu den jeweils aktuell bekannt werdenden IT-Sicherheitsvorfällen, IT-Angriffskampagnen und Schwachstellen in industriellen Steuerungssystemen wurden auch frühere, herausragende Vorfälle, Angriffe und Schwachstellen ausgewertet, um ein möglichst vollständiges Bild der für die kerntechnischen Anlagen relevanten IT-Bedrohungslage zu erhalten. Hierbei hat sich gezeigt, dass aufgrund der sich ebenfalls kontinuierlich ändernden Informationslage zu Vorfällen, Angriffen und Schwachstellen auch die Ersteinschätzungen immer wieder auf ihre Aktualität geprüft und ggf. angepasst werden müssen.

Die Dokumentation der ausgewählten IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten und APTs sowie die jeweiligen Ersteinschätzungen erfolgt in einem lebenden Dokument zur IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen. Der Stand Mai 2021 dieses lebenden Dokuments ist in den technischen Bericht „IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen“ /GRS 21f/ eingeflossen. Es umfasst zahlreiche IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten und APTs, darunter:

- Schwachstellen und IT-Angriffswerkzeuge
  - Brutal Kangaroo
  - Meltdown und Spectre
  - Schwachstellen in Siemens SPPA-T3000, Profinet sowie S7 und PCS7
  - Schwachstellen in ABB 800xA
  - Zerologon
  - Amnesia:33
  - Microsoft Exchange
  - NAME:WRECK

- IT-Sicherheitsvorfälle und IT-Angriffe
  - BlackEnergy 1, 2 und 3 sowie GreyEnergy
  - Stuxnet
  - Duqu und Flame/sKyWIper
  - Shamoon
  - Havex, Karagany und Heriplor
  - Crashoverride/Industroyer
  - Mirai
  - WannaCry
  - NotPetya
  - Emotet
  - Snake/Evans
  - SolarWinds
- APT-Gruppierungen
  - APT29/Cozy Bear
  - APT32/OceanLotus
  - APT38/Lazarus Group
  - Avivore
  - Dragonfly/Energetic Bear
  - Electrum
  - Kimsuky
  - Sandworm
  - Tonto Team
  - Turla
  - Xenotime

In dem lebenden und kontinuierlich gepflegten Dokument werden sowohl die Schwachstellen und IT-Angriffswerkzeuge einerseits als auch die IT-Sicherheitsvorfälle und IT-Angriffe andererseits zusätzlich noch chronologisch erfasst. Bezüge zwischen zusammenhängenden oder aufeinander aufbauenden Angriffen und Angriffswerkzeugen werden deutlich gemacht. Dies gilt insbesondere auch für die Bezüge zwischen den beschriebenen APT-Gruppierungen und den von ihnen eingesetzten IT-Angriffswerkzeugen und durch sie erfolgenden IT-Angriffen.

Im Verlauf des Vorhabens erfolgte in Bezug auf diejenigen IT-Angriffe oder Schwachstellen, bei denen im Rahmen der Erstbewertung eine besondere Relevanz für deutsche kerntechnische Anlagen ausgemacht wurde, eine Abstimmung mit dem BMU und ggf. im Rahmen der Auftragsforschung eine vertiefte Auswertung der Sachverhalte.

3.4 Bewertung von IT-Sicherheitsvorfällen bei Lieferketten

Während der Vorhabenslaufzeit haben sich Lieferketten (Supply Chains) verstärkt als Schwachstellen für die Sicherung von Kernbrennstoffen und zugehöriger Anlagen und Einrichtungen herausgestellt. Insbesondere Lieferketten von IT-Systemen stehen mit der Digitalisierung und Internationalisierung der Lieferketten in den letzten zehn Jahren vermehrt im Fokus, wenn es um die Ausnutzung von Schwachstellen in und Angriffspfade auf IT-Systeme geht. Zunehmend werden IT-Sicherheitsvorfälle bekannt, bei denen bereits mit Schadsoftware infizierte IT-Systeme geliefert und eingebaut wurden oder denen eine Verletzung der Informationssicherheit bei einem Zulieferer zugrunde liegt. Global kam es in den letzten Jahren zu diversen IT-Sicherheitsvorfällen im Zusammenhang mit der Lieferkette, die u. a. kritische Infrastrukturen betrafen und teilweise einen Bezug zu kerntechnischen Anlagen und Einrichtungen aufwiesen. Auch in einem deutschen KKW wurde bereits ein Vorkommnis im Zusammenhang mit der Lieferkette eines schutzbedürftigen IT-Systems festgestellt. Aktuell werden auf internationalen Tagungen zur IT-Sicherheit von industriellen Steuerungssystemen, wie dem IAEO Technical Meeting on Computer Security Approaches and Applications in Nuclear Security (Berlin, 23.-27.9.2019) oder der IET Cyber Security for Industrial Control Systems (London, 5.-6.3.2020), die besonderen Herausforderungen der IT-Sicherheit in Bezug auf die Lieferketten diskutiert. Auch beim Jahresgespräch zwischen BMU und GRS am 12.03.2020 herrschte Einigkeit über die Bedeutung der Lieferketten für die IT-Sicherheit. Daher wurde es als erforderlich angesehen, die Thematik als weiteren Schwerpunkt aufzugreifen.

Dazu sollte eine gezielte Recherche zu bisherigen IT-Sicherheitsvorfällen mit Bezug zur Lieferkette durchgeführt und dieser Aspekt anschließend kontinuierlich weiterverfolgt werden. Da dieser Schwerpunkt im Rahmen der ursprünglich geplanten Arbeiten jedoch nicht im erforderlichen Umfang abgedeckt werden kann, und eine Erweiterung des Spektrums der kontinuierlich verfolgten IT-Sicherheitsvorfälle auch auf den Bereich außerhalb kritischer Infrastrukturen erforderlich ist, wurden zusätzliche Mittel für die Recherchen und deren Auswertung zum Stand von W,T&E bereitgestellt.

Die Arbeiten an den IT-Sicherheitsvorfällen in Bezug auf die Lieferkette umfassten Überlegungen und die Festlegung zum Vorgehen, die Recherche und die Auswahl von Ereignissen, die Ordnung der Ereignisse nach Relevanz, die Auswertung der Rechercheergebnisse zu ausgewählten IT-Angriffen über die Lieferkette und zu IT-Sicherheitsvorfällen in Zusammenhang mit der Lieferkette, die Erstellung einer Übersicht über die Zunahme von Lieferkettenereignissen und den Bedeutungszuwachs von IT-Sicherheit in diesem Gebiet sowie die Dokumentation der Erkenntnisse in einem Bericht. Dabei wurden neben Lieferkettenangriffen mit Bezug zu kerntechnischen Anlagen auch solche Lieferkettenangriffe betrachtet, welche keinen direkten Bezug zu kerntechnischen Anlagen haben, jedoch Erkenntnisse für Lieferkettenangriffe auf kerntechnische Anlagen und Einrichtungen ermöglichen.

Die beschriebenen durchgeführten IT-Angriffe über die Lieferkette zeigen, dass sowohl Datendiebstahl als auch Manipulationen innerhalb und außerhalb der angegriffenen Zielsysteme eine ernstzunehmende Bedrohung für kerntechnische Anlagen und Einrichtungen darstellen. Dies sollte weiter beobachtet werden und tiefergehende Untersuchungen zu notwendigen, möglichen Vorkehrungen im Rahmen der Vorbeugung und Abwehr von IT-Angriffen über die Lieferkette nach sich ziehen.

Die Ergebnisse sind im technischen Bericht „IT-Sicherheit in der Lieferkette, Initiale Untersuchung des aktuellen Standes der Wissenschaft und Technik“ /GRS 21e/ dargestellt mit

- einer Beschreibung bekannter IT-Angriffe und IT-Sicherheitsvorfälle über die Lieferkette mit kerntechnischen Bezügen,
- einer Beschreibung bekannter herausragender IT-Angriffe über die Lieferkette ohne derzeit bekannte kerntechnische Bezüge,
- einer Kurzbeschreibung weiterer IT-Angriffe über die Lieferkette ohne derzeit bekannte kerntechnische Bezüge,

- einer Darlegung der Bedeutungsänderung von IT-Angriffen über die Lieferkette in der IT-Sicherheit.

Zu den beschriebenen Supply-Chain-Angriffen zählen

- Angriffe mit Bezug zu kerntechnischen Anlagen
  - Virenfund in einem deutschen Kernkraftwerk
  - NotPetya
  - Dragonfly
  - Ingérop Datenverlust
  - Schadsoftwarefund in einem japanischen Kernkraftwerk
- Angriffe ohne bekannt gewordenen Bezug zu kerntechnischen Anlagen
  - ShadowHammer
  - Target Datendiebstahl
  - Magecart
  - Ccleaner Hack
  - Kingslayer
  - Operation Red Signature
  - MediaGet

Eines der bekanntesten Beispiele für einen Supply-Chain-Angriff ist die massive Angriffswelle mit der Schadsoftware NotPetya aus dem Jahr 2017. Damals waren weltweit Unternehmen und weitere Organisationen von einem massiven Ausfall ihrer IT-Infrastruktur betroffen. Im Frühling 2017 erlangten unbekannte Angreifer Zugriff auf die Server des Unternehmens Linkos Group und übernahmen unbemerkt die Kontrolle über die Updateserver des Unternehmens. Von hier aus verteilten die Angreifer auf IT-Systeme, welche das Programm M.E.Doc der Linkos Group installiert hatten, über die Updateroutinen des Programms eine Backdoor. Die Angreifer luden auf allen betroffenen Systemen die Schadsoftware NotPetya mit der installierten Backdoor hoch und aktivierten diese zeitgleich am 27.06.2017. Die Schadsoftware NotPetya breitete sich in den betroffenen IT-Netzwerken aus, vernichtete sämtliche gespeicherte Daten der betroffenen Systeme und

versuchte, weitere IT-Systeme zu infizieren. Innerhalb weniger Tage entstand ein geschätzter wirtschaftlicher Schaden von ca. 10 Mrd. Dollar für weltweit agierende Unternehmen /WIR 17/. Betroffen war unter anderem auch das Kernkraftwerk Tschernobyl. Dort fiel z. B. die automatisierte Strahlungsmessung aus /PRV 17/.

4 Fachlicher Austausch auf nationaler und internationaler Ebene

Eine Grundlage zur Erfassung und Weiterentwicklung des Standes von W,T&E bei der Sicherung ist der fachliche Austausch zwischen Experten auf dem Gebiet der Sicherung. Auch die Fachkompetenz auf dem Gebiet der Sicherung und der IT-Sicherheit kann im Rahmen der internationalen wissenschaftlichen Zusammenarbeit gefestigt und erweitert werden.

Ausgesuchte internationale Fachveranstaltungen zur Verbesserung der nuklearen Sicherung sollten durch eine Mitwirkung und die Bereitstellung technisch-wissenschaftlichen Sachverstands unterstützt werden. Über den bilateralen Austausch zwischen der GRS und wissenschaftlich-technischen Unterstützungsorganisationen (Technical and Scientific Support Organizations - TSO) anderer Länder sollte ein Know-how-Transfer auf dem Gebiet der Sicherung von kerntechnischen Anlagen und von Beförderungen sowie der IT-Sicherheit gefördert werden.

Arbeiten im Rahmen des AP 1: Erfassung und Auswertung des Standes von Wissenschaft, Technik und Erkenntnis bei der Sicherung

Im Rahmen des AP 1 erfolgte mit der Zustimmung des BMU eine Mitwirkung an folgenden Fachveranstaltungen:

- Symposium Anlagensicherung 2019 der TÜV NORD Akademie, Vorbereitung und Vortrag von zwei Präsentationen zu den Scherpunkten IAEA-Regelwerk zur Sicherung und Härtung der Zwischenlager, Austausch mit Fachkollegen zum Stand von W,T&E hinsichtlich Trends und Neuerungen der Sicherungstechnik, zu Möglichkeiten für Einwirkungen und zur Bewertung und Fortentwicklung von Sicherungskonzepten
- Fachforum Unbemannte Systeme der Deutschen Gesellschaft für Wehrtechnik (DWT) am 22.05.2019 in Bonn, Austausch mit Fachexperten zum Stand von Wissenschaft und Technik bezüglich unbemannter Luftfahrzeuge (unmanned aircraft system - UAS) und Abwehrmöglichkeiten (Trends und Neuerungen, Möglichkeiten für SEWD), Austausch zu Regelwerken für die Nutzung von UAS und Abwehrmaßnahmen, u. a. Einschränkungen von Abwehrtechniken (Eingriff in die Luftsicherheit, Genehmigung der Bundesnetzagentur), Reisebericht

- “Training Course on Preventive and Protective Measures against Insider Threats” der IAEA bei den Sandia National Laboratories, Albuquerque am 15. - 19. Juli 2019; erstmalige Trainingsveranstaltung für Fortgeschrittene zur Innentäterproblematik; Vorgehen zur Erstellung, Umsetzung und Bewertung umfassender Konzepte zur Minimierung der Gefährdung kerntechnischer Anlagen durch Handlungen von Innentätern mit den Schwerpunkten: Erkennen potenzieller Innentäter und Entwicklung/Evaluation von Maßnahmen gegen Innentäter (Prävention, Reaktion); hoher Praxisbezug durch die Teilnehmer; Reisebericht
- KELI „Konferenz zur Elektro-, Leit- und Informationstechnik“ des VGB, 24./25. November 2020, als online-Tagung aufgrund der Pandemiesituation, eine der führenden Fachkonferenzen zur Elektro-, Leit- und Informationstechnik in der Energieversorgung im Zweijahresrhythmus, neue Herausforderungen durch Industrie 4.0, Digitalisierung und IT-Sicherheit, Technische Entwicklungen und neue regulatorische Rahmenbedingungen

Arbeiten im Rahmen des AP 3: Weiterentwicklung von Sicherungsstandards im Rahmen der internationalen Zusammenarbeit

Durch die internationale Zusammenarbeit und Wissenschaftskooperation im Rahmen ausgewählter internationaler Fachveranstaltungen zur Verbesserung der nuklearen Sicherung wurde ein Beitrag zur Festigung und Erweiterung der Fachkompetenz der GRS auf dem Gebiet der Sicherung und der IT-Sicherheit geleistet. Gleichzeitig wurden die Fachveranstaltungen durch die Bereitstellung technisch-wissenschaftlichen Sachverstands unterstützt.

Im Rahmen des AP 3 erfolgte mit der Zustimmung des BMU eine Mitwirkung an folgenden internationalen Konferenzen und Trainingskursen:

- “Technical Meeting on Computer Security Approaches and Applications in Nuclear Security” der IAEA in Berlin am 23. - 27.09.2019, Veranstaltung für einen umfassenden Überblick über den aktuellen Stand der IT-Sicherheit im nuklearen Umfeld und den aktuellen Stand von Wissenschaft und Technik; Erfassung und Auswertung des Standes von Wissenschaft, Technik und Erkenntnis in Ergänzung zu den Arbeiten unter AP 1, fachliche Perspektiven unterschiedlicher Nationen, Einblick in den Wissensstand der teilnehmenden Nationen

- Bilaterales Treffen mit einem Experten des Japan's Independent Institute am 22.01.2021 in der GRS Köln, Erfahrungsaustausch zum international Stand der Sicherung von KKW
- virtuelle Internationale Konferenz zur IT-Sicherheit „7th Annual Control Systems CyberSec USA" vom 29. - 31.03.2021

Darüber hinaus wurde die geplante Teilnahme am EUROSAFE Forum 2020, Paris, geplant November 2020, vorbereitet durch die Erstellung eines Abstrakt für eine Präsentation „Anpassung der Anlagensicherung bei der Stilllegung von KKW“. Aufgrund der Pandemiesituation wurde das Forum verschoben, so dass eine Teilnahme voraussichtlich erst im Rahmen eines Nachfolgevorhabens möglich ist. Schwerpunkte des Forums sind u. a. nukleare Sicherung, IT-Sicherheit, Schnittstelle von Sicherheit und Sicherung, Erfahrungen und künftige Entwicklungen.

Über einen regelmäßigen bilateralen Austausch zwischen der GRS und der französischen TSO, dem Institut für Strahlenschutz und nukleare Sicherheit (Institut de radioprotection et de sûreté nucléaire - IRSN). soll ein bidirektionaler internationaler Know-how-Transfer auf dem Gebiet der Sicherung von kerntechnischen Anlagen und von Beförderungen sowie der IT-Sicherheit gefördert werden. Aufgrund der Pandemiesituation waren die Möglichkeiten für einen solchen Austausch sehr eingeschränkt. Deshalb beschränkten sich die Arbeiten auf die fachliche und organisatorische Vorbereitung der Fortführung des im Vorläufervorhaben begonnenen bilateralen Austauschs mit IRSN zu aktuellen Fragen der Sicherung kerntechnischer Anlagen und Transporte.

5 Projektabwicklung

Arbeiten im Rahmen des AP 1: Erfassung und Auswertung des Standes von Wissenschaft, Technik und Erkenntnis bei der Sicherung

Im Rahmen der Projektabwicklung wurden Aufgaben der Projektleitung, insbesondere die übergreifende fachliche Koordination bei der Auftragsabarbeitung, des Projektcontrollings und der Ergebnisdokumentation gemäß § 12 Abs. 1 ABFE-BMU einschließlich Korrekturen des Projektplanes bei erkanntem Erfordernis durchgeführt.

Dazu gehört auch die Anpassung von ursprünglich geplanten Kapazitäten, um die Arbeiten im Rahmen des Vorhabens zielgenau und umfassend durchführen zu können. Ein Erfordernis zur Aufnahme zusätzlicher Aspekte betraf Vorarbeiten zu einem geplanten Eigenforschungsvorhaben zur IT-Sicherheit mit Bezug auf die Lieferkette im Rahmen des AP 2, um zeitliche Verzögerungen bei der Analyse des erkannten Problems zu minimieren. Ein Erfordernis zur vertieften Bearbeitung ausgewählter Aspekte betraf die Endlager-Sicherung und die Schnittstelle Sicherheit-Sicherung im Rahmen des AP 1, um die jeweilige Zielstellung zu erreichen. Mit ergänzenden Arbeiten zur Sicherungskultur im Rahmen des AP 1sollte die Grundlage für die Unterstützung des BMU auf diesem Gebiet erweitert werden.

Zur Projektleitung gehörte auch die Vorbereitung und Durchführung von Projektgesprächen sowie sonstiger Abstimmungen mit dem BMU, z. B. hinsichtlich der Mitwirkung an ausgewählten internationalen Veranstaltungen.

Für eine quartalsweise Abstimmung mit dem BMU zum Stand des Vorhabens und zum Besprechen möglicher Herausforderungen für die weitere Bearbeitung wurde eine Übersicht zu den laufenden Arbeiten, zum Stand der Bearbeitung und zu den weiteren Schritten erstellt und gepflegt.

Es wurden vorbereitende Arbeiten für ein Nachfolgevorhaben mit Bezug auf relevante Zielstellungen auf Grundlage der Erkenntnisse des laufenden Vorhabens durchgeführt.

Literaturverzeichnis

/GRS 20a/ GRS, Hilfsmittel zum gewaltsamen Öffnen von Türen, Halligan-Tool, Technische Notiz, Stand November 2020, VS-NfD

/GRS 20b/ GRS, Bewertung Buntmetalldiebstahl KKW Grafenrheinfeld (KKG) 06/2020 als meldepflichtiges Ereignis im Rahmen der Sicherung, technische Notiz, Stand Juli 2020, VS-NfD

/GRS 20c/ GRS, Action Plan des BMU zur Umsetzung der Empfehlungen und Vorschläge der IPPAS-Experten, Vorschlag, Stand Mai 2020, VS-NfD

/GRS 21a/ GRS, Möglichkeiten zum Einsatz von Drohnen bei SEWD, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis, Entwurf, Stand Januar 2021, VS-NfD

/GRS 21b/ GRS, Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen, Sicherung in der Endlagerung, Entwurf, Stand Februar 2021, VS-NfD

/GRS 21c/ GRS, Schnittstelle Sicherheit-Sicherung für kerntechnische Anlagen, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis, Entwurf, Stand Januar 2021, VS-NfD

/GRS 21d/ GRS, Sicherungskultur, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis, Entwurf, Stand Januar 2021,

/GRS 21e/ GRS, IT-Sicherheit in der Lieferkette, Initiale Untersuchung des aktuellen Standes der Wissenschaft und Technik, Stand Mai 2021

/GRS 21f/ GRS, IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen, Stand Mai 2021, Erscheinungsdatum voraussichtlich Juni 2021 (noch nicht erschienen)

/GRS 21g/ GRS, Schnittstelle Sicherheit-Sicherung für kerntechnische Anlagen, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis, Entwurf, Stand Mai 2021

/GRS 21h/ GRS, Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen, Sicherung in der Endlagerung, Entwurf, Stand Juni 2021

/GRS 21i/ GRS, Möglichkeiten zum Einsatz von Drohnen für Belange der Sicherung, Recherche zum internationalen Stand von Wissenschaft, Technik und Erkenntnis, Entwurf, Stand Juni 2021

/LAB 21/ Fachportal Laborpraxis, Vogel Communications Group GmbH & Co. KG, Homepage von Laborpraxis Vogel, Specials, Wissenschaft und Forschung, Stahlharte Schäume als Sprengschutz, Adresse: https://www.laborpraxis.vogel.de/stahlharte-schaeume-als-sprengschutz-a-810633/, Abgerufen 16.06.2021

/PRO 19a/ Fachzeitschrift PROTECTOR Sicherheitstechnik und Wirtschaftsschutz, Ausgabe 11/2019, 47. Jahrgang, Schlütersche Verlagsgesellschaft mbH & Co. KG

/PRO 19b/ Fachzeitschrift PROTECTOR Sicherheitstechnik und Wirtschaftsschutz, Ausgabe 9/2019, 47. Jahrgang, Schlütersche Verlagsgesellschaft mbH & Co. KG

/PRO 19c/ Fachzeitschrift PROTECTOR Sicherheitstechnik und Wirtschaftsschutz, Ausgabe 4/2019, 47. Jahrgang, Schlütersche Verlagsgesellschaft mbH & Co. KG

/PRV 17/ Pravda: Der Virusangriff betraf das Kernkraftwerk Tschernobyl, Kiev 2017

/THW 21/ Bundesanstalt Technisches Hilfswerk, Homepage des THW, Einheiten und Technik, Ausstattung, Geräte, Betonkettensäge, Adresse: https://www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/betonkettensaege.html, Abgerufen 16.06.2021

/WIR 17/ Wired, Andy Greenberg: The untold Story of NotPetya, the Most Dev-astating Cyberattack in History, 2017

Abbildungsverzeichnis

Abkürzungsverzeichnis

AP	Arbeitspaket
APT	Advanced Persistent Threats
AtG	Atomgesetz
AtSMV	atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung
BGE	Bundesgesellschaft für Endlagerung
BMU	Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit
BSI	Bundesamts für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team des BSI
DWT	Deutsche Gesellschaft für Wehrtechnik
ENSRA	European Nuclear Security Regulators Association
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
IAEO	internationale Atomenergiebehörde
IEC	International Electrotechnical Commission
IPPAS	International Physical Protection Advisory Service (internationaler Beratungsservice der IAEO zum physischen Schutz)
IRSN	Institut de radioprotection et de sûreté nucléaire (Institut für Strahlenschutz und nukleare Sicherheit)
IT	Informationstechnik

ITDB	Incident and Trafficing Database
KKW	Kernraftwerk
KRITIS	kritische Infrastrukturen
NGA	Nuklearen Gefahrenabwehr
NSS	Nuclear Security Series (Regelwerk der IAEO zur Sicherung)
OSD	Objektsicherungsdienst
PTZ	Pan, Tilt and Zoom
SEWD	Störmaßnahmen oder sonstige Einwirkungen Dritter
THW	Technisches Hilfswerk
TSO	Technical and Scientific Support Organization (wissenschaftlich-technische Unterstützungsorganisation)
TÜV	Technischer Überwachungsverein
UAV	Unmanned Aerial Vehicle (unbemanntes, ggf. autonomes Fluggerät)
UGV	Unmanned Ground Vehicle (unbemanntes, ggf. autonomes Landfahrzeug)
USV	Unmanned Surface Vehicle (unbemanntes, ggf. autonomes Überwasser-Fahrzeug)
US-CERT	United States Computer Emergency Readiness Team
UUV	Unmanned Underwater Vehicle (unbemanntes, ggf. autonomes Unterwasser-Fahrzeug)
W,T&E	Wissenschaft, Technik und Erkenntnis

WENRA Western European Nuclear Regulators' Association

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-949088-35-3