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

GRS - 773

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

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

Mark Pelzer
Claudia Quester
Philipp Terberger
Udo Weizel

Mai 2024

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4721R01611 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 BMUV übereinstimmen.

GRS - 773
ISBN 978-3-910548-65-7

Deskriptoren

Anlagensicherung, Drohnen, Einwirkungen, 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 sowie für die Beförderung von Kernbrennstoffen u. a. eine Genehmigungsvoraussetzung, dass der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) gewährleistet ist. Mit dem 17. Änderungsgesetz zum AtG wurden die Grundlagen der nuklearen Sicherung auf Gesetzesebene klargestellt, wie der Umfang des erforderlichen Schutzes gegen SEWD durch Sicherungsmaßnahmen des Genehmigungsinhabers, die mit Schutzmaßnahmen des Staates im Rahmen des integrierten Sicherungs- und Schutzkonzeptes abgestimmt werden, sowie u. a. die allgemeinen Schutzziele der Sicherung und die Bedeutung der Schnittstelle von Sicherung und Sicherheit.

Bei der Sicherung soll bei der Bewertung und Fortentwicklung von Sicherungskonzepten stets der Stand von Wissenschaft, Technik und Erkenntnis im gebotenen Umfang berücksichtigt und bundeseinheitlich umgesetzt werden. Der Stand von Wissenschaft, Technik und Erkenntnis für die Sicherung einschließlich der Sicherheit der Informationstechnik (IT-Sicherheit, Cybersicherheit) im nationalen und internationalen Rahmen umfasst u. a. technische 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 Einrichtungen 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 Cybersicherheit insbesondere dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) 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 Wissenschaft, Technik und Erkenntnis auf nationaler und internationaler Ebene und das Vorhalten fortschrittlicher Prüf- und Bewertungsmethoden erforderlich. Die 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 erhalten und kontinuierlich ausgebaut werden, um ihre Fähigkeit, Sachverhalte zu aktuellen Fragen der Sicherung einschließlich Cybersicherheit in kerntechnischen Anlagen und bei der Beförderung von Kernbrennstoffen stets auf der Basis des national und international verfügbaren Wissensstandes zu bearbeiten, zu gewährleisten und abzusichern. Dazu sollte der Stand von Wissenschaft, Technik und die Erkenntnis im Bereich der Sicherung und Cybersicherheit systematisch erfasst und ausgewertet werden. Das erfasste Wissen soll auch dazu genutzt werden, um neue Herausforderungen im Bereich der Sicherung und Cybersicherheit zu identifizieren, generische Lösungsansätze und Anforderungen zur Verbesserung der Sicherung und Cybersicherheit 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 die IT-Bedrohungslage sollten mit den grundsätzlichen Schritten Sichtung, Erstbewertung und vertiefte Auswertung auf generischer Ebene bei Bedarf 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 Sicherung und IT-Sicherheit sowie von Ereignissen mit Sicherungsrelevanz und der IT-Bedrohungslage
  - hinsichtlich der Entwicklung von technischen Hilfsmitteln zur Einwirkung und von Systemen zur Sicherung,
  - zur Erfassung der IT-Bedrohungslage wie IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten, Aktivitäten von fortgeschrittenen andauernden Bedrohungen (Advanced Persistent Threats - APTs),
  - zur Erfassung von Ereignissen mit Sicherungsrelevanz sowie deren Bewertung zur Identifizierung von Lücken bei der Sicherung und deren Einordnung bezüglich der Bedeutung für die Sicherung,

  - zur Etablierung und Verwendung von Definitionen,
  - zur Identifizierung von Themen der Sicherung und Cybersicherheit mit Forschungs- und Entwicklungsbedarf.
- AP 2: Analyse von Ereignissen mit IT-Sicherheitsrelevanz und Einbindung des MITRE ATT&CK Frameworks
  - zur Identifizierung und Bewertung von Lücken bei der Cybersicherheit,
  - mit der Auswertung der erfassten IT-Bedrohungslage und Ersteinschätzungen für ausgewählte Ereignisse,
  - auf Basis der Bewertung eines Analyse-Hilfsmittels und dessen Anpassung,
  - mit der Entwicklung von Lösungsansätzen.
- AP 3: Grundlagen für die Stärkung der nationalen nuklearen Sicherungskultur
  - mit weiterführenden Recherchen zur nuklearen Sicherungskultur bezüglich internationaler Empfehlungen und Erfahrungen und Konzepten anderer Staaten, Branchen und Wissenschaftsgebiete,
  - mit einer Ableitung von Bewertungskriterien.
- AP 4: Weiterentwicklung von Sicherungsstandards im Rahmen der internationalen Zusammenarbeit
  - bei Expertentreffen und -gremien der Internationalen Atomenergie-Organisation (IAEO),
  - durch bilateraler Expertenaustausch.

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 4721R01610 als Grundlage für die Weiterentwicklung des deutschen Regelwerks der Sicherung (SEWD-Regelwerk) und zur Fachberatung des BMUV.

Zum Erkenntnisgewinn der Sachverständigen sowie zum Erkennen aktueller Trends und Schwerpunkte im Sinne des Standes von Wissenschaft, Technik und zur Erkenntnis auf dem Gebiet der Sicherung und der Cybersicherheit 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 Wissenschaft, Technik und Erkenntnis im Bereich der Sicherung einschließlich Cybersicherheit 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 vom 02.11.2021 bis zum 30.06.2024.

2 Stand von Wissenschaft, Technik und Erkenntnis

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.

Während der Vorhabenlaufzeit wurden die Eignung möglicher Quellen und Medien für Recherchen geprüft und 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 identifizieren, generisch zu bewerten und ggf. Handlungsbedarf zu erkennen.

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

Das 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 werden regelmäßig ausgewertet, um Schlussfolgerungen für die Sicherung und die Fortschreibung des SEWD-Regelwerks, insbesondere der Lastannahmen, zu ziehen. In diesem Zusammenhang werden auch Neuentwicklungen mit Potenzial als Hilfsmittel für Einwirkungen identifiziert.

Die Recherche zu aktuellen Entwicklungen von Sicherungsmaßnahmen erfolgt vor allem in Fachmagazinen für Sicherungstechnik. Die Informationen und Erkenntnisse aus der Teilnahme bzw. Mitwirkung an nationalen Fachveranstaltungen, Fachmessen etc. zur Sicherung und Sicherungstechnik werden in Bezug auf relevante Neuheiten geprüft.

Ausgewählte Erkenntnisse mit Relevanz für die Sicherung sind nachfolgend zusammengestellt:

Bereich biometrische Identifikation

Handvenenscanner, unter anderem der Firma iCOGNIZE GmbH, werden bereits in deutschen kerntechnischen Einrichtungen eingesetzt. Das biometrische Merkmal „Handvenen“ ist laut Hersteller sicherer als Irisscan-Verfahren. Die Falschakzeptanzrate (FAR; englisch: false acceptance rate), die die Wahrscheinlichkeit angibt, dass bei einem Zutrittskontrollsystem Zugang gewährt wird, obwohl keine Zugangsberechtigung vorliegt, liegt bei $<8x10^{-5}$ %.

Die Möglichkeit, das System durch eine von einer berechtigen Person „abgetrennten“ Hand zu manipulieren, ist ohne größeren Aufwand nicht möglich. Eine abgetrennte Hand würde aufgrund des Druckverlustes innerhalb der Venen und der damit einhergehenden Verringerung des Durchmessers ein unterschiedliches Venenmuster ergeben im Vergleich zu einer „lebenden“ Hand. Das System erkennt sogar die Veränderung des Handvenenmusters, welches sich aufgrund unterschiedlicher Außentemperaturen ausbildet.

Das gespeicherte Handvenenmuster wird teilweise aufgrund der Datenschutz-Grundverordnung (DSVGO) auf einem Mitarbeiterausweis gespeichert, dann bei Zutrittsbegehren nur temporär zum Abgleich auf einer Auswerteeinheit gespeichert und nach erfolgtem Zutritt wieder verworfen. Zum Schutz gegen Missbrauch wird heutzutage die 2-Faktor-Authentifizierung umgesetzt, z. B. mit einem personalisierten Ausweis und dem Scan des Handvenenmusters.

Wichtig beim Einsatz von Handvenenscannern ist der Schutz der gespeicherten Handvenenmustern.

Bereich Kameratechnik

Die Multifocal-Sensortechnik (MFS-Technologie) am Perimeter, z. B. des Herstellers Dallmeier, arbeitet im Unterschied zu Single-Sensor-Kameras mit mehreren Sensoren mit jeweils unterschiedlichen Brennweiten. Damit kann von einem Standort aus, z. B. mit dem Panomera-System, ein großes Areal detailliert überblickt werden. Bewegungen von Objekten können über lange Strecken ohne Aufzeichnungslücken oder Kamerawechsel nachvollzogen werden. Vorteile liegen dabei u. a. in einer hohen Dynamik, einer

durchgängige Tiefenschärfe, einer optimalen Brennweite für jeden Bereich und einem gleichmäßigen Auflösungsraster über dem gesamten Bereich. Die Auflösung kann nahezu beliebig skaliert werden. (vgl. auch Ergebnisse des Eigenforschungsvorhabens 4721R01620 zur Erfassung und Verfolgung von technischen Entwicklungen zur Abschätzung von Einsatzmöglichkeiten von Videokameras mit KI-getriebener Videoanalyse im Bereich der Sicherung).

Bereich Barriere

Eine Recherche betraf die Barrierewirksamkeit von verschiedenen Tresoren für die Verwendung in kerntechnischen Anlagen, insbesondere zur anforderungsgerechten Verwahrung von sicherungsrelevanten Schlüsseln. Dabei wurden auch Einzelheiten zum Aufbau eines Tresores nach DIN EN 1143-1 /DIN 19/ in Erfahrung gebracht, um die Belastbarkeit im Sinne des SEWD-Regelwerks abschätzen zu können. Als Fazit dieser ersten Voruntersuchung ist festzuhalten, dass die Ableitung einer Korrelation zwischen den Widerstandsklassen nach DIN EN 1143-1 und den Widerstandsklassen gemäß dem SEWD-Regelwerk (bspw. Barriere B, C und D) im Rahmen dieses ersten Arbeitsumfanges nicht möglich war. Dafür bedarf es vertiefter Untersuchungen und ggf. auch ergänzender Versuche.

2.2 Drohnen

In den Vorläufervorhaben wurden Recherchen zum Stand von Wissenschaft, Technik und Erkenntnis im Hinblick auf unbemannte Fahrzeuge, insbesondere auf Luftfahrzeuge (unmanned aerial vehicle, uncrewed aerial vehicle – UAV, umgangssprachlich Drohnen) durchgeführt. Die fortschreitende Entwicklung und Verfügbarkeit stetig leistungsfähigerer Fahrzeuge führen dazu, dass sich die Attraktivität für Nutzer ständig erhöht. Ein zusätzlicher Aspekt sind die geringen Anschaffungskosten. Das führt dazu, dass insbesondere Drohnen auch verstärkt im Zusammenhang mit Anforderungen an die Sicherung betrachtet werden müssen.

Die zunehmende Bedeutung und Weiterentwicklung unbemannter Systeme (insbesondere durch den Ukrainekrieg, der als weltweit einzigartiges Testfeld für UAV gilt) und deren stetig steigende Verbreitung machen es erforderlich, bei der Erfassung des Standes von Wissenschaft, Technik und Erkenntnis für die Sicherung auch solche unbemannten Systeme zu berücksichtigen. Dazu wurde im Rahmen des Vorhabens insbesondere die Mitwirkung an internationalen Veranstaltungen genutzt (siehe Kap. 4).

Eine Präsentation bei der Webkonferenz „Safe & Secure Transport of radioactive Materials“ /GRS 22a/ (siehe Kap. 4) setzte sich mit den Herausforderungen auseinander, die im Zusammenhang mit einer möglichen Verwendung von Drohnen durch Angreifer bei der Beförderung von radioaktivem Material oder Kernbrennstoffen auftreten können, z. B. für Sabotage- oder Störaktionen. Aber auch Gegenmaßnahmen bei Erkennen einer anfliegenden Drohne wurden dargestellt. Als Fazit wurde die Entwicklung von Regelungen für den Einsatz von Drohnen vorgeschlagen einschließlich deren Fortschreibung zur Berücksichtigung der Fortschritte der Drohnentechnologie sowie zur Berücksichtigung der Schnittstelle Sicherheit-Sicherung.

Fragen der Drohnendetektion und -abwehr wurden verstärkt im Rahmen des VfS-Kongresses im Mai 2022 in Kassel vorgetragen und diskutiert. Das Potenzial der Drohnendetektion liegt demnach vor allem in einer genaueren Lokalisierung der Drohne, ihrer Geschwindigkeit, Größe und Richtung sowie der Position des Steuerers, da mit diesen Informationen Maßnahmen zur Aufrechterhaltung der Sicherheit effektiver gestaltet werden können. Geeignete Technologien dafür sind insbesondere Radar, Radiofrequenz (RF), Elektro-optische Überwachung mit Kameras (EO) und Infrarotüberwachung (IR). Mit einem Drohnendetektionssystem müssen diese Daten der verschiedenen Sensoren kombiniert und gemeinsam ausgewertet werden (Multidatensensorfusion).

Die bei der Mitwirkung am Technical Meeting (TM) der IAEO zu UAV in Albuquerque /GRS 23b/ (siehe Kap. 4) gesammelten Informationen und Erfahrungen tragen dazu bei, die eigenen Kenntnisse über den Stand von Wissenschaft, Technik und Erkenntnis hinsichtlich der Abwehr von Drohnen als Aspekt der Sicherung weiter auszubauen, da auf internationaler Ebene wertvolle Erfahrungen und Erkenntnisse zu Drohnen vorliegen. Der Erfahrungsaustausch und die Diskussion waren sehr zielführend hinsichtlich der Herausforderungen und Lösungsansätze sowohl bei der Verwendung von Drohnen zur Unterstützung der Sicherungsmaßnahmen bei Nuklearanlagen als auch zur Detektion von Drohnen und zu Gegenmaßnahmen zur Abwehr von Drohnen. Hervorzuheben sind auch die vergleichbaren Herausforderungen und Herangehensweisen in der Luftfahrt (Flughäfen) und anderen kritischen Infrastrukturen, die eine Grundlage für eine zielführende und effiziente Zusammenarbeit und Weiterentwicklung darstellen kann.

Auf dem Consultancy Meeting (CM) der IAEO zu UAV in Wien /GRS 24a/ (siehe Kap. 4) wurde ein internationales Forschungsprojekt (Coordinated Research Project, CRP) generiert, welches gewährleistet, auch kommende Entwicklungen im Bereich unbemannter Systeme zu berücksichtigen. Die Mitwirkung daran, u. a. mit dem Vortrag „Detection of

UAV“, erbrachten neue Erkenntnisse über den Stand von Wissenschaft, Technik und Erkenntnis hinsichtlich des Themenbereichs unbemannter Systeme, da auf internationaler Ebene wertvolle Erfahrungen und Erkenntnisse in diesem Bereich vorliegen. In Präsentationen wurden aktuelle Informationen zu den technischen Möglichkeiten von Drohnen, aber auch von unbemannten Bodenfahrzeugen und maritimen Fahrzeugen bereitgestellt. Der Erfahrungsaustausch und die Diskussion betrafen insbesondere die Herausforderungen und Lösungsansätze sowohl bei der Verwendung zur Unterstützung der Sicherungsmaßnahmen als auch zur Detektion und zur Abwehr. Daraus ergeben sich Erkenntnisse zur Verbesserung der nationalen nuklearen Sicherung bezüglich Drohnen.

Resümierend können folgende UAV-Typen (und deren Eigenschaften) genannt werden:

Multicopter:

- weit verbreitet mit unterschiedlicher Anzahl von Rotoren, auch als Bausatz erhältlich,
- langsamer oder schwebender Flug möglich,
- Senkrechtstart möglich,
- begrenzte Reichweite und Flugdauer (abhängig von Nutzlast und Größe),
- Einsatz: privat, kommerzieller Einsatz stark steigend,
- Einsatz von Drohnen zur Übersicht der Situation,
- Assistenzsysteme verfügbar.

Starrflügelflugzeug:

- hohe Geschwindigkeit und Manövrierfähigkeit,
- große Reichweite,
- Startmöglichkeit muss vorhanden sein,
- kein Schwebeflug.

Zur Detektion, Identifizierung, Verifikation und Nachverfolgung von UAV stehen folgende wesentliche technischen Möglichkeiten zur Verfügung:

- Akustik,
- Radar,
- Radiofrequenzanalyse,
- Optisch.

Im Folgenden wird kurz auf die Technologie der Detektionssysteme und deren Eigenschaften eingegangen:

Akustik:

Akustische Sensoren empfangen die akustischen Profile der Drohnen und können so Informationen über deren Art und Standort gewinnen. In der folgenden Tabelle (Tab. 2.1) sind die grundlegenden Eigenschaften dargestellt.

Tab. 2.1 Eigenschaften der akustischen Detektion von UAV

Erfassungsmodus	Mikrofonanordnungen zur Erfassung von UAV-Schallwellen
Sensorsichtfeld	90 - 360°
Wetter	anfällig (Wind, Niederschlag)
Bereich (2.5kg UAV)	gering
Ortungsgenauigkeit	niedrig, nur in Richtung der Peilung
Nachverfolgungsgenauigkeit	medium
Nachtbetrieb	ja
autonome UAV-Erfassung	ja
Schwächen	begrenzte Reichweite, anfällig für Witterungsverhältnisse und Hintergrundgeräusche
Stärken	Sichtverbindung nicht erforderlich, Rundumsicht, Nachtbetrieb

Radar:

Ein Radargerät basiert auf der Verwendung von elektromagnetischen Wellen. Die elektromagnetischen Wellen werden in kurzen Impulsen ausgestrahlt, die von Objekten in ihrem Weg reflektiert werden. Anhand dieser Informationen kann ein Radarsystem feststellen, wie groß ein Objekt ist und wie schnell es sich bewegt. In der folgenden Tabelle (Tab. 2.2) sind die grundlegenden Eigenschaften dargestellt.

Tab. 2.2 Eigenschaften der Radar Detektion von UAV

Erfassungsmodus	aktive Erfassung reflektierter Funksignale
Sensorsichtfeld	90-360° (horizontal), 3-90° (vertikal)
Wetter	anfällig, Feuchtigkeit/Regen
Bereich (2.5kg UAV)	variabel, typischerweise mittel bis hoch
Ortungsgenauigkeit	hoch, 3D Lokalisierung
Nachverfolgungsgenauigkeit	sehr hoch
Nachtbetrieb	ja
autonome UAV-Erfassung	ja
Schwächen	begrenzter Erfassungsbereich, anfällig für Witterungsverhältnisse
Stärken	große/mittlere Reichweite, multidirektional, sehr hohe Nachverfolgungsgenauigkeit, Nachtbetrieb

Radiofrequenzanalyse:

Ein Radiofrequenz (RF)-Detektor ist ein Gerät, mit dem das Vorhandensein von RF-Wellen in physikalischen Übertragungsmedien festgestellt werden kann. In der folgenden Tabelle (Tab. 2.3) sind die grundlegenden Eigenschaften dargestellt.

Tab. 2.3 Eigenschaften der RF-Detektion von UAV

Erfassungsmodus	Empfang und Analyse von RF-Übertragungen (Video, Steuerung, Telemetrie, Wi-Fi)
Sensorsichtfeld	360°
Wetter	geringe Wirkung (Dämpfung der Signale)
Bereich (2.5kg UAV)	sehr hoch
Ortungsgenauigkeit	medium, nur in Richtung der Peilung zu 2D Ortung
Nachverfolgungsgenauigkeit	hoch
Nachtbetrieb	ja
autonome UAV-Erfassung	ja
Schwächen	dark mode UAV, RF-Hintergrundrauschen
Stärken	Große Reichweite, omnidirektional, hohe Nachverfolgungsgenauigkeit, Nachtbetrieb

Optisch:

In der folgenden Tabelle (Tab. 2.4) sind die grundlegenden Eigenschaften von Kamerasystemen dargestellt.

Tab. 2.4 Eigenschaften der optischen Detektion von UAV

Erfassungsmodus	Reflexionen oder Emissionen von sichtbaren bis infraroten (IR) Lichtwellenlängen
Sensorsichtfeld	variabel, sehr klein bis 360°, abhängig von der Bildverarbeitung
Wetter	anfällig (abhängig von der Wellenlänge; IR ist viel weniger anfällig)
Bereich (2.5kg UAV)	gering bis hoch
Ortungsgenauigkeit	nur in Richtung der Peilung (keine Distanzinformationen)
Nachverfolgungsgenauigkeit	hoch
Nachtbetrieb	Keine Beeinträchtigung für Systeme mit IR-Wellenlänge
autonome UAV-Erfassung	ja
Schwächen	UAV Lokalisierung ist schwer für ein stand alone System
Stärken	variable Reichweite, multidirektional, hohe Verfolgungsgenauigkeit

Zusammenfassend stehen viele technische Möglichkeiten zur Verfügung. Das vorhandene Umfeld spielt eine Rolle (Interferenzen, störende Bodenbeschaffenheiten und Gebäude, etc.). Es ist anhand der Detektion schwer festzustellen, um das Gefährdungspotenzial richtig einzustufen. Es gibt keine eine Einzellösung. Eine kombinierte Lösung aus Radar, RF und Optik scheint die beste Option zu sein.

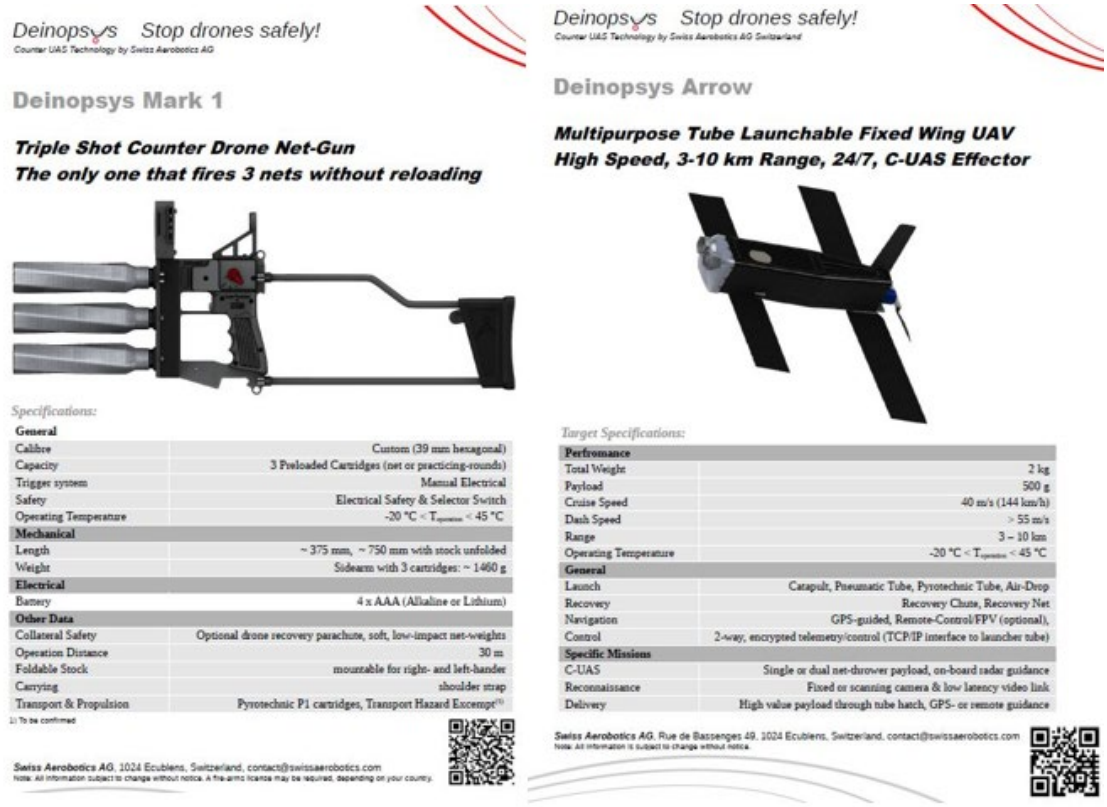
Bei der Abwehr von Drohnen (Counter-UAV) gibt es folgende Systeme:

- Jammen
  - Stören der Funkverbindung,
  - nicht wirksam bei autonomen Drohnen und Drohnen in Eigenbau,
  - Übernahme und kontrollierte Landung mit Zusatzgerät möglich.
- Spoofing
  - Überlagern des GPS-Signals mit starkem Sender,
  - Vortäuschen falscher Koordinaten bzw. Orientierungslosigkeit.
- Geo-Fencing
  - Flugverbotszone mittels GPS-Koordinaten einrichten,
  - virtuelle Grenze,
  - „legale“ Drohnen mit GPS ausgestattet.
- Elektromagnetischer (Im-)Puls (EMP)
  - kurzzeitige breitbandige elektromagnetische Strahlung, die bei einem einmaligen, hochenergetischen Ausgleichsvorgang abgegeben wird,
  - Drohne stürzt unkontrolliert ab (abhängig von der Stärke des EMP),
  - stark abhängig von der Distanz.
- Abschuss und/oder Zerstörung anfliegender Drohnen
  - Netzschuss-Geräte (mobil und stationär),
  - Drohne-Hunter, Jägerdrohne mit Netzschuss-Gerät,
  - Schusswaffen.

Die Verwendung von Abwehrmaßnahmen ist nicht unproblematisch. Zum einen Existieren juristische Hürden und zum andern bürgen die aufgelisteten Technologien ein

immenses Risiko bzgl. Kollateralschäden. Sowohl unbeteiligte Dritte als auch das zu schützende Objekt können in Mitleidenschaft gezogen werden. Auch hier gilt, wie bei der Detektion, dass es keine ideale Einzellösung gibt. Die optimale Abwehr von UAV greift auf ein Arsenal von Möglichkeiten zurück. Letztlich hängt es auch vom zu schützenden Objekt ab, was und wie die Technologien eingesetzt werden können.

Auch die Perimeter Protection im Januar 2023 in Nürnberg befasste sich schwerpunktmäßig mit der Thematik Drohnen, wobei wiederum die Drohnendetektion, aber auch die neueste Rechtslage bei der Drohnenabwehr und die Möglichkeiten der Drohnenabwehr im Vordergrund standen. Bei der Drohnenabwehr gibt es demnach unter anderem die Möglichkeit des Einsatzes einer Netzpistole oder das Abfangen mit einer weiteren Drohne. U. a. wurde dazu von der Schweizer Firma Swiss Aaerobotics AG für Drohnen- und Drohnenabwehr-Technologien eine Netzpistole Deinopsys Mark 1 mit einer Reichweite bis 30 m vorgestellt. Es besteht die Möglichkeit für den Abschuss mehrere Netze und grundsätzlich auch der Montage an Drohnen. Zwischenzeitlich ist mit dem Deinopsys Arrow ein Hilfsmittel für die Drohnenabwehr für Entfernungen bis ca. 3 km verfügbar.



Deinopsys Stop drones safely!
Counter UAS Technology by Swiss Aerobotics AG

Deinopsys Mark 1

Triple Shot Counter Drone Net-Gun
The only one that fires 3 nets without reloading

Specifications:

General	
Calibre	Custom (39 mm hexagonal)
Capacity	3 Preloaded Cartridges (net or practicing-rounds)
Trigger system	Manual Electrical
Safety	Electrical Safety & Selector Switch
Operating Temperature	-20 °C < $T_{operation}$ < 45 °C
Mechanical	
Length	~ 375 mm, ~ 750 mm with stock unfolded
Weight	Sidearm with 3 cartridges: ~ 1460 g
Electrical	
Battery	4 x AAA (Alkaline or Lithium)
Other Data	
Collateral Safety	Optional drone recovery parachute, soft, low-impact net-weights
Operation Distance	30 m
Foldable Stock	mountable for right- and left-hander
Carrying	shoulder strap
Transport & Propulsion	Pyrotechnic P1 cartridges, Transport Hazard Exempt[1]

[1] To be confirmed

Swiss Aerobotics AG, 1024 Ecublens, Switzerland, contact@swissaerobotics.com
Note: All information subject to change without notice. A fire-arms licence may be required, depending on your country.

Deinopsys Stop drones safely!
Counter UAS Technology by Swiss Aerobotics AG Switzerland

Deinopsys Arrow

Multipurpose Tube Launchable Fixed Wing UAV
High Speed, 3-10 km Range, 24/7, C-UAS Effector

Target Specifications:

Perfromance	
Total Weight	2 kg
Payload	500 g
Cruise Speed	40 m/s (144 km/h)
Dash Speed	> 55 m/s
Range	3 – 10 km
Operating Temperature	-20 °C < $T_{operation}$ < 45 °C
General	
Launch	Catapult, Pneumatic Tube, Pyrotechnic Tube, Air-Drop
Recovery	Recovery Chute, Recovery Net
Navigation	GPS-guided, Remote-Control/FPV (optional),
Control	2-way, encrypted telemetry/control (TCP/IP interface to launcher tube)
Specific Missions	
C-UAS	Single or dual net-thrower payload, on-board radar guidance
Reconnaissance	Fixed or scanning camera & low latency video link
Delivery	High value payload through tube hatch, GPS- or remote guidance

Swiss Aerobotics AG, Rue de Bassenges 49, 1024 Ecublens, Switzerland, contact@swissaerobotics.com
Note: All information is subject to change without notice.

Abb. 2.1 Technische Datenblätter zu Drohnenabwehr-Systemen der Firma Swiss Aaerobotics AG

Quellen: https://swissaerobotics.com/wp-content/uploads/2024/02/Deinopsys_Mark1_Factsheet.pdf/

https://swissaerobotics.com/wp-content/uploads/2023/01/A4_Arrow_v3.pdf

2.3 Nukleare Sicherungskultur

Für die nukleare Sicherung ist die Sicherungskultur gemäß IAEO das Zusammenspiel von Eigenschaften, inneren Einstellungen und Verhaltensweisen von Einzelpersonen, Organisationen und Einrichtungen, welches dazu dient, die Sicherung zu unterstützen und zu steigern. Eine wirksame Sicherungskultur trägt dazu bei, den Schutz des Menschen und der Umwelt vor der schädlichen Wirkung ionisierender Strahlung in Bezug auf SEWD zu unterstützen und zu verbessern. Sie wird bestimmt durch eine sicherungsgerichtete Grundhaltung und das Bewusstsein für potenzielle Bedrohungen durch SEWD sowie die persönliche Verantwortung für den Schutz vor diesen Bedrohungen.

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. Mit der neu erstellten Leitlinie Sicherungskultur /BMU 23/, die im Jahr 2023 in Kraft gesetzt wurde, liegen Handlungs- und Umsetzungsvorschläge vor, an denen sich insbesondere der Genehmigungsinhaber, aber auch andere Organisationen orientieren können. Dennoch soll die nukleare Sicherungskultur auf allen Ebenen erfasst und weiter gefördert werden.

Zusätzliche Anforderungen bezüglich der Aufrechterhaltung des hohen Niveaus der nuklearen Sicherungskultur erwachsen insbesondere aus dem geänderten Rahmen für Stilllegung und Abbau von Kernkraftwerken (KKW) nach dem Ausstieg Deutschlands aus der Nutzung der Kernenergie zur Stromerzeugung. Damit einhergehend wird auf den Werksgeländen der Genehmigungsinhaber zunehmend Personal anderer Branchen tätig sein. Neben den regulatorischen Anforderungen an das Personal, wie die atomrechtliche Zuverlässigkeit, sind auch eine wirksame standortweite Sicherungskultur und ein sicherungsgerichtetes Handeln bedeutsam. Eine niederschwellige und zielgerichtete Einflussnahme auf das Handeln kann dabei zum gewünschten Verhalten führen.

Die bisherigen begrenzten Recherchen zur nuklearen Sicherungskultur sollten fortgesetzt und vertieft werden mit einem möglichen Fokus auf: Konzepte und Erfahrungen anderer Staaten und Institutionen, andere Branchen mit vergleichbarem Sicherheits- und Sicherungsbewusstsein, Fehlerkultur, interdisziplinäre Aspekte, psychologische Schwerpunkte etc. Für die Bewertung von nur mittelbar feststellbaren Einstellungen und Haltungen von Personen und Organisationen sollten geeignete Kriterien abgeleitet werden.

Die Teilnahme am “International Workshop on Nuclear Security in Practice” /GRS 22b/ (siehe Kap. 4) erbrachte insbesondere durch den Erfahrungsaustausch und die Diskussionen auf internationaler Ebene neue fachliche Erkenntnisse zu internationalen Aspekten der nuklearen Sicherungskultur und zu deren Grundlagen sowie zu deren Bewertung und Stärkung. Die Informationen auf dem Stand von Wissenschaft, Technik und Erkenntnis erweitern die Kenntnisse zur nuklearen Sicherungskultur im Hinblick auf Konzepte und Erfahrungen anderer Staaten. Erste internationale Kontakte konnten angebahnt werden.

Die Mitwirkung am „Workshop on Nuclear Security Culture in Practice“ /GRS 23a/ (siehe Kap. 4) zur Unterstützung der IAEO mit vertieften Diskussionen zur nuklearen

Sicherungskultur brachte umfangreiche fachliche Erkenntnisse zu Herausforderungen und internationalen Lösungsansätze bei der Umsetzung von sicherungskulturellen Themen. Wertvolle Hinweise wurden u. a. hinsichtlich der indirekten Erfassung des Engagements der Organisationsführungen der Genehmigungsinhaber oder der Erhöhung der Aufmerksamkeit auf dieser Ebene gegeben. Eine Übertragbarkeit auf nationale Rahmenbedingungen ist gegeben und wird geprüft. Die Anbahnung von internationalen Kontakten wurde fortgesetzt, und der internationale fachliche Austausch wurde intensiviert.

Die Teilnahme an der Veranstaltung „Security Awareness Expert“ /GRS 22c/ (siehe Kap. 4), deren Ziel die Wissensvermittlung und der Erfahrungsaustausch zu Themen wie psychologische Grundlagen, Ansätze zur dauerhaften Integration der Sicherheit bzw. Sicherung in den Arbeitsalltag und Entwicklung von Security-Awareness-Konzepten ist, brachte neue Erkenntnisse auf dem Stand von Wissenschaft, Technik und Erkenntnis insbesondere auf Basis von Erfahrungen anderer Branchen mit ähnlichem Sicherheitsbedürfnis und vergleichbarem Sicherheits- und Sicherungsbewusstsein. Spezielle Aspekte betrafen dabei u. a. den Trend, dass besonders nicht unmittelbar mit Sicherheit/Sicherung betrauten Personen eine zunehmend entscheidendere Rolle für die Sicherheit/Sicherung zukommt, weiterhin den für bestimmte Mitarbeitertypen ggf. zielführenden Einsatz von spielerischen Elementen zur Aufmerksamkeitserlangung und -steigerung (sog. Gamification) für die Sicherheit/Sicherung in Konkurrenz zu anderen Themen sowie erneut die Bedeutung der Überprüfung der Wirksamkeit von Maßnahmen. Dafür muss bei der Auswertung zwischen Instrumenten zur Erfassung der Steigerung der Sicherheit/Sicherung und zur Erfassung des Ressourceneinsatzes für Bewusstseinssteigerungsmaßnahmen differenziert werden.

Beim Treffen mit Experten der TH Wildau, Fachgebiet Luftfahrttechnik/ Luftfahrtmanagement /GRS 22d/ (siehe Kap. 4) und dem Austausch zu Aspekten der Sicherungskultur wurde das stark ausgeprägte Sicherheits-/Sicherungsverständnis beider Branchen erkenntlich. Es wurden einige Parallelitäten, wie Regelwerk, klare Verantwortungsteilung und Rolle der Sicherheitsbehörden identifiziert, aber Unterschiede wie die Interpretation von Ansätzen zur Stärkung des sicherheitsgerichteten Handelns wurden sichtbar. Die neuen Erkenntnisse umfassen auch Ansätze für weitere Untersuchungen zur Identifikation von Sicherheits-/Sicherungsmaßnahmen, um zur kontinuierlichen Verbesserung beizutragen und um branchenübergreifend gewonnene Erkenntnisse zielgerichtet einzusetzen.

Die branchenübergreifende Zusammenarbeit auf dem Gebiet der Sicherung und insbesondere der Sicherungskultur wurde mit dem Aufbau eines regelmäßigen Informationsaustausches mit der TH Wildau zur Identifikation und Analyse von sicherungsrelevanten Erfahrungswerten aus der Luftfahrt und möglichen Erkenntnissen für die nukleare Sicherung/Sicherungskultur fortgeführt und ausgebaut. Einzelne Verstöße unterhalb der Meldeschwelle wurden thematisiert und mögliche Ursachen ergründet. Auch aufgrund der erkannten Übereinstimmungen sowie der Vulnerabilität der kritischen Infrastruktur ist eine übergreifende Forschungskooperation denkbar und vorgesehen.

Es wurden Recherchen zur Auswertung von Praktiken für die Stärkung eines sicherungsgerichteten Handelns durchgeführt, und es wurden Erkenntnisse zu Sensibilisierungsmethoden (Awareness) für die Stärkung eines sicherungsgerichteten Handelns und zur Bewertung von deren Anwendbarkeit im nuklearen Umfeld gesammelt.

Der internationale Stand von Empfehlungen bezüglich der nuklearen Sicherungskultur, aktuelle internationale Entwicklungen und Zielsetzungen sowie Ergebnisse aus internationalen Kampagnen zur Stärkung des sicherungsgerichteten Handelns wurden erfasst, bewertet und diskutiert. Auch der nationale Stand und bisherige nationale Aktivitäten wurden recherchiert und ausgewertet.

Die Herausforderungen bei der Umsetzung der neuen Leitlinie Sicherungskultur /BMU 23/ wurden untersucht. Dabei wurden auch die übergeordneten Aspekte einer lernenden Organisation sowie der ganzheitliche Kulturbegriff berücksichtigt. Die Bewertung der Ergebnisse ist bisher noch nicht abgeschlossen. Es ist jedoch bereits absehbar, dass künftige Aktivitäten im nationalen Rahmen und im internationalen Umfeld intensiviert werden sollten, um eine wirksame Sicherungskultur in einem sich wandelnden Umfeld effizient erfassen und beeinflussen zu können.

Als eine Erkenntnis lässt sich festhalten, dass die nukleare Sicherungskultur z. B. aufgrund der steigenden Zahl an internationalen Empfehlungen und auch durch die Veröffentlichung von Anwendungsfällen an Bedeutung gewinnt. Durch die Fokussierung auf das Handeln der agierenden Organisationen und Personen werden die Awarenessmaßnahmen zur Stärkung eines sicherungsgerichteten Handelns weiter an Bedeutung gewinnen. Insbesondere der Wettstreit um die Aufmerksamkeit der Mitarbeiter wird für die Wirksamkeit der Sicherung entscheidend sein. Eine ganzheitliche Betrachtung, unter Berücksichtigung der Organisationsspezifika und vor allem der Sicherheitskultur und IT-Sicherungskultur, ist einer singulären Betrachtung vorzuziehen.

Die Ergebnisse können wie folgt zusammengefasst werden zu:

- Begriffsdefinition sowie Abgrenzung zu und Gemeinsamkeiten mit anderen Kulturbegriffen,
- Ergebnisse der fortgeführten Recherchen zum internationalen und zum nationalen Stand von Empfehlungen zur nuklearen Sicherungskultur,
- aktuelle Entwicklungen, Zielsetzungen, Umsetzungen und Herausforderungen zur nuklearen Sicherungskultur auf internationaler Ebene,
- aktuelle branchenübergreifende Entwicklungen zur Awarenessmaßnahmen zur Beeinflussung der Mitarbeiter zu sicherungsgerichtetem Handeln,
- Intensivierung der Zusammenarbeit mit der sicherungsaffinen Luftfahrtbranche,
- Beginn des Aufbaus eines internationalen Netzwerkes (JAP, US, HUN) für den Erfahrungsaustausch zu empirischen Erkenntnissen zur nuklearen Sicherungskultur,
- Empfehlungen zum Kompetenzerhalt und gemeinnützigen Wissensaufbau sowie zur Entwicklung von weiterführenden Potentialen.

Erkenntnisse dieses Forschungsvorhabens sind z. B. bei der Erstellung der Leitlinie Sicherungskultur /BMU 23/ in die Dokumentation von Kriterien für eine wirksame Sicherungskultur eingeflossen.

Die Ergebnisse bilden eine Grundlage für die Unterstützung des BMUV bei der Umsetzung der Leitlinie Sicherungskultur und deren Evaluation im Rahmen der Auftragsforschung.

2.4 Verfolgen der Entwicklungen und von Ereignissen mit Relevanz für die IT-Sicherheit

In der Sicherung soll stets der Stand von Wissenschaft, Technik und Erkenntnis 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 Wissenschaft, Technik und Erkenntnis abgedeckt wird.

Die bislang genutzten Recherchequellen mit Informationen zu nationalen und internationalen Ereignissen mit IT-Sicherheitsrelevanz im Hinblick auf kerntechnische Anlagen wurden weiter genutzt. Zusätzlich wurden weitere Recherchequellen identifiziert und bei Bedarf genutzt.

Die Rechercheergebnisse wurden in der im Vorläufervorhaben entworfenen Tabelle erfasst (siehe hierzu auch Abschnitt 3.2).

Über die Vorhabenlaufzeit hinweg erfolgte eine kontinuierliche Recherche bzgl. der IT-Sicherheit insbesondere auf fachspezifischen Webseiten:

- Screening von Meldungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie von entsprechenden Meldungen der US-amerikanischen CISA,
- Sichtung bereits bekannter und genutzter, sowie neu identifizierter 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).

Die erkannten Ereignisse wurden parallel zur Kategorisierung und Zuordnung zu Themenschwerpunkten einer Erstbewertung hinsichtlich ihrer Übertragbarkeit auf, sowie sonstigen Relevanz für nationale kerntechnische Anlagen, Einrichtungen und Tätigkeiten unterzogen. Die Ergebnisse dieser Arbeitsschritte fanden Eingang in die Priorisierung der Ereignisse.

Die Dokumentation der Rechercheergebnisse und die Organisation der zugehörigen weiterführenden Informationen 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.

2.5 Definitionen für die IT-Sicherheit

Der im Vorläufervorhaben entwickelte Katalog mit Definitionen wurde über die Vorhabenlaufzeit gepflegt. Hierbei wurden im Verlauf der Vorhabenlaufzeit insbesondere

Definitionen ergänzt, die im Zusammenhang mit den beim Screening identifizierten IT-Sicherheitsvorfälle und Schwachstellen (siehe 2.4) und der Erstbewertung dieser Screeningergebnisse (siehe 3.2) relevant waren.

3 Ereignisse mit Sicherungsrelevanz und relevante IT-Sicherheitsvorfälle

Die Sicherstellung des erforderlichen Schutzes gegen SEWD basiert unter anderem auf einer aktuellen und detaillierten Kenntnis der Bedrohungslage. Daher ist es notwendig, nationale und internationale IT-Sicherheitsvorfälle und weitere Ereignisse mit Sicherungsrelevanz regelmäßig zu sichten. 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 BMUV erfolgen.

3.1 Ereignisse mit Sicherungsrelevanz

Arbeiten im Rahmen von AP 1:

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

Die Dokumentation der Ergebnisse erfolgt in der dafür erstellten ACCESS-Datenbank „DESi – Datenbank zu Ereignissen mit Sicherungsrelevanz“. In der DESi sind verschiedene Kategorien vordefiniert, zu denen für jedes Ereignis Angaben gemacht werden können. Basierend auf den Angaben können die Daten in DESi sortiert, extrahiert und weiterverwendet werden.

Die in DESi definierten Kategorien wurden im Abschlussbericht des Vorläufervorhabens FKZ 4718R01611 /GRS 21/ aufgeführt und beschrieben. In der aktuellen Version der DESi wurde die Kategorie „Tätermotiv“ (Auswahlmöglichkeiten: andere, Anti-Atomkraft-Aktivismus, Ethnonationalismus, geistig verwirrt, Habgier, Islamismus, Kriegshandlung, Linksradikalismus, organisierte Kriminalität, Rechtsradikalismus und unbekannt)

ergänzt. Für die Kategorie „Art des Ereignisses“ wurde als Ereignisart der „unerlaubte Besitz von radioaktiven Stoffen“ ergänzt.

Weitere relevante Ereignisse mit Bezug zu Kernmaterial, radioaktiven Stoffen, kerntechnischen Anlagen und der Beförderung radioaktiver Stoffe wurden recherchiert, ausgewählt und in DESi aufgenommen und einer Erstbewertung unterzogen. Diese Erstbewertung ist gleichzeitig die Voraussetzung für die Auswahl von Ereignissen, die für eine vertiefte Auswertung auf generischer Ebene in Betracht gezogen werden können.

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 DESi 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.

Beispiele für sicherungsrelevante Ereignisse in den letzten Jahren betreffen wiederholt den Einsatz von Drohnen. So wurden z. B. im Zeitraum 14. – 20.01.2022 Drohnen über allen schwedischen Kernkraftwerken gesichtet. Der Ursprung dieser Drohnen ist unbekannt. Angaben zum Flugverhalten deuten darauf hin, dass es sich um professionelle Drohnen gehandelt haben könnte. Auch in den USA wurden in vielen Fällen Drohnen über kerntechnischen Anlagen gesichtet. Besonders hervorzuheben sind Ereignisse am 29. und 30.09.2019, als jeweils vier bis sechs Drohnen über dem Kraftwerk Palo Verde gesichtet wurden. Laut Schätzungen des Sicherungspersonals vor Ort, hatten die Drohnen einen Durchmesser von mehr als 2 Fuß (ca. 60 cm). Für den ersten Tag wird berichtet, dass sie sich mehr als 1,5 Stunden über der Anlage befanden.

In Hinblick auf Drohnen ist das folgende Ereignis ohne direkten Bezug zu kerntechnischen Anlagen relevant. Im Juni 2020 versuchten Unbekannte mutmaßlich, mit einer Drohne ein Umspannwerk im Bundesstaat Pennsylvania in den USA zu sabotieren. An der Drohne (Typ DJI Mavic 2) war ein dicker Kupferdraht mit Nylonschnüren befestigt.

Die Kamera und die Speicherkarte waren entfernt worden. Mutmaßlich sollte mit dem Kupferdraht ein Transformator oder eine Versorgungsleitung kurzgeschlossen werden, was z. B. zu einem Stromausfall oder einem Feuer hätte führen können. Stattdessen stürzte die Drohne aber auf einem benachbarten Gebäudedach ab. Es entstand kein Schaden am Umspannwerk.

Im Nordosten Frankreichs wurde am 26.08.2021 ein 26-jähriger Mann festgenommen, der in einem Ausbildungszentrum damit angegeben hatte, dass er eine schmutzige Bombe gebaut hätte und diese gegen öffentliche Einrichtungen einsetzen wollte. Es stellte sich heraus, dass er vier selbstgebaute Bomben besaß, von denen drei laut der französischen Nationalpolizei funktionstüchtig gewesen seien. Außerdem besaß er Uranoxid in Pulverform. Der Mann erklärte, dass er alles auf der Internetseite Ebay gekauft habe. Angeblich wies der Mann erhebliche psychische Probleme auf und wurde im Krankenhaus betreut.

Die Erkenntnisse aus der Erstbewertung der in DESi aufgenommenen 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 DESi. Dabei wurde versucht, bei jedem dokumentierten Ereignis Angaben in allen vordefinierten Kategorien in DESi zu machen. Anhand dieser Kategorien können Informationen aus DESi extrahiert und graphisch dargestellt werden, was bereits in /GRS 21/ anhand von Beispielen illustriert wurde. Da in DESi seitdem weitere Ereignisse aufgenommen wurden, werden im Folgenden die aktualisierten Beispiele dargestellt. Bezüglich der weiterhin gültigen Interpretation wird auf /GRS 21/ verwiesen.

In folgender Abbildung (Abb. 3.1) ist die zeitliche Verteilung der Ereignisse auf die sechs in DESi berücksichtigten Dekaden seit dem Jahr 1961 sowie die „angebrochene“ Dekade 2021 – 2024 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.

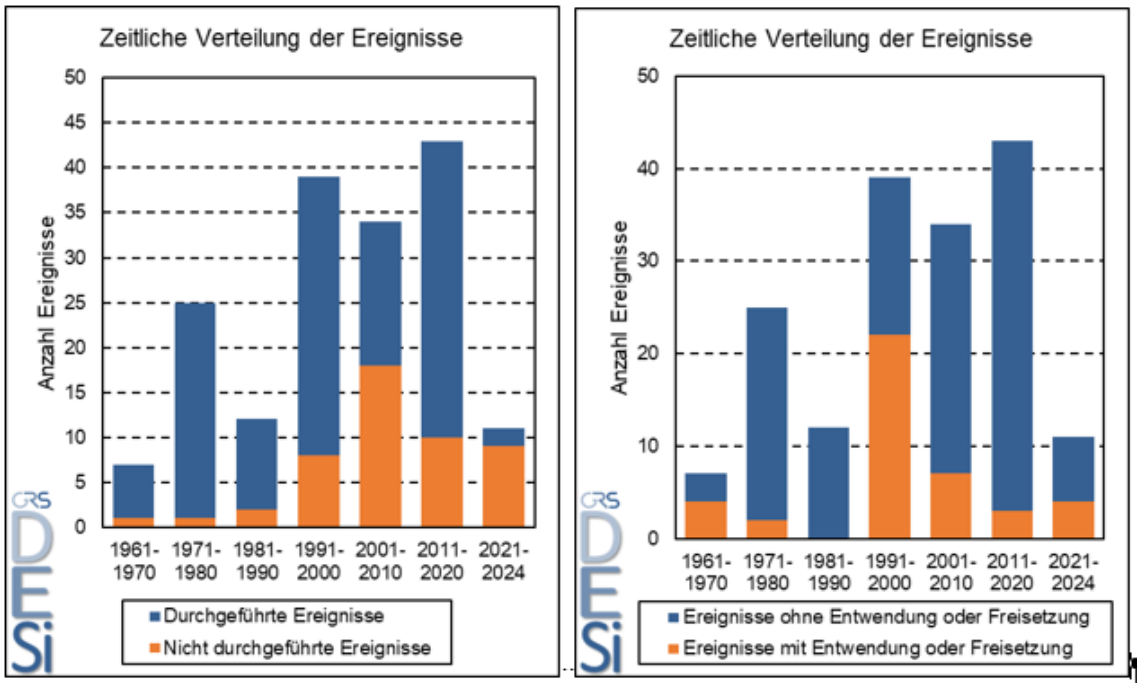


Abb. 3.1 Graphische Darstellungen der DESi-Einträge als zeitliche Verteilungen

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.

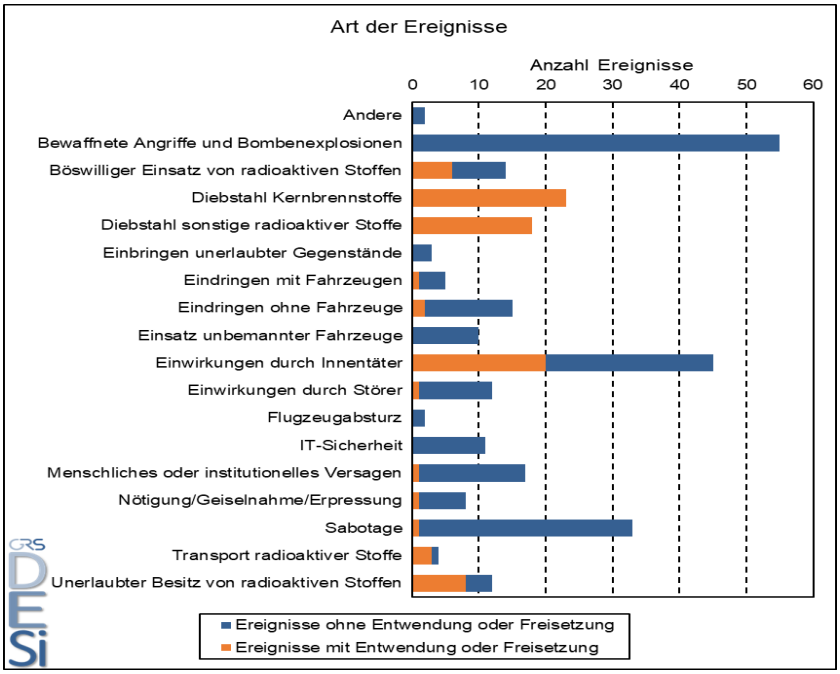


Abb. 3.2 Graphische Darstellung der DESi-Einträge hinsichtlich der Arten der Ereignisse

In Abb. 3.3 sind die Häufigkeiten der in DESi genannten Tätermotive graphisch dargestellt. Dabei wird zwischen durchgeführten und nicht durchgeführten Ereignissen unterschieden. In dieser Kategorie sind in DESi Mehrfachnennungen möglich. Wie zu erkennen ist, ist bei vielen Ereignissen das Tätermotiv nicht bekannt (ca. 37 % der DESi-Einträge). Bei vielen weiteren Ereignissen kann zwar ein Tätermotiv zugeordnet werden, allerdings ist diese Zuordnung mit starken Unsicherheiten behaftet. Für eine tiefere (insbesondere statistische) Analyse sind diese Ergebnisse nicht geeignet. Abb. 3.3 dient aber als Eindruck zu den in DESi aufgenommenen Ereignissen.

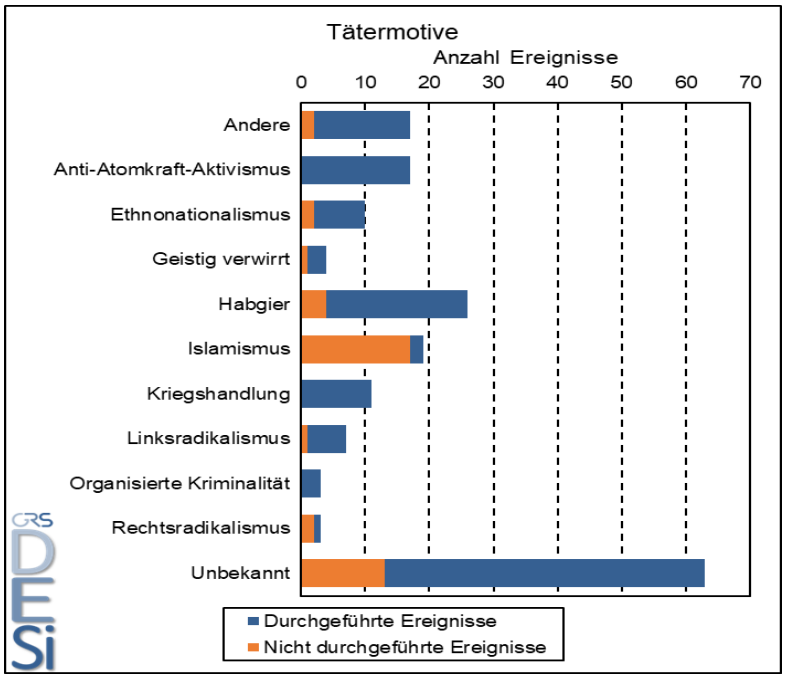


Abb. 3.3 Graphische Darstellung der DESi-Einträge hinsichtlich der Tätermotive

Diese exemplarischen Auswertungen der in DESi enthaltenen Informationen sollen den praktischen Nutzen von DESi illustrieren. Es wurde der Stand der DESi im Mai 2024 verwendet. DESi wird kontinuierlich gepflegt und weiterentwickelt. Dafür werden regelmäßig Quellen gesichtet, bestehende Einträge in DESi aktualisiert und neue Einträge ergänzt.

3.2 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,
- zunehmende, gezielte, technisch versierte und über einen langen Zeitraum ausgeführte bzw. 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.

Auf nationaler und internationaler Ebene sind regelmäßig IT-Sicherheitsvorfälle mit sicherungstechnischer Bedeutung und potenziell auf kerntechnische Anlagen und Einrichtungen übertragbarer Aspekte zu verzeichnen, woraus sich Veränderungen der IT-Bedrohungslage ergeben können. Für die IT-Sicherheit kommt damit der regelmäßigen Analyse der IT-Bedrohungslage, aber auch der Bewertung des Standes von Wissenschaft, Technik und Erkenntnis zu Prävention und Detektion von IT-Angriffen sowie zur Reaktion auf IT-Angriffe eine besondere Bedeutung zu. Ebenfalls relevant sind hierbei Angriffe, die nicht als reine IT-Angriffe sondern als kombinierte Angriffe ausgeführt werden.

Bereits in den Vorläufervorhaben wurden ausgewählte geeignete Recherchequellen mit Informationen zu nationalen und internationalen IT-Sicherheitsvorfällen kontinuierlich gesichtet. Daran anknüpfend wurde die Entwicklung der IT-Bedrohungslage (für industrielle Steuerungssysteme und kritische Infrastrukturen relevante IT-Sicherheitsvorfälle, IT-Angriffe einschließlich IT-Angriffswerkzeuge, Schwachstellen, Schadsoftwarekomponenten, Aktivitäten bekannter Angreifer-Gruppierungen - 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 Tabelle für die Erfassung der Screeningergebnisse und der Dokumentation der Erstbetrachtung,
- einer geeigneten Struktur zur Ablage und Organisation der weiterführenden Informationen zu den Ereignissen sowie
- eines daran ausgerichteten, kontinuierlich weitergeführten Dokuments für die übersichtliche Dokumentation der entsprechend hoch priorisierten Schwachstellen, Angriffswerkzeuge, IT-Sicherheitsvorfälle und Schadsoftwarekomponenten geschaffen.

Die genannte Tabelle sowie die Struktur zur Ablage und Organisation weiterführender Informationen wurden zunächst im Rahmen des Screenings (siehe Abschnitt 2.4) mit Informationen befüllt. Die Tabelle sowie die Struktur zur Organisation wurden anschließend im Rahmen dieses Arbeitspunktes weiter befüllt. Neben den eigentlichen Screeningergebnissen werden für die einzelnen IT-Sicherheitsvorfälle grundlegende informative Eckpunkte sowie die Arbeitsergebnisse in Bezug auf die Kategorisierung und Priorisierung der IT-Sicherheitsvorfälle erfasst. Zusätzlich wurden ab 2023 die in der Tabelle enthaltenen Informationen um eine Zuordnung zu verschiedenen Themenschwerpunkten ergänzt, um für relevante Themen eine schnelle Identifikation von Ereignissen zu ermöglichen. Die in der Tabelle enthaltenen Informationen dienen als Grundlage für die regelmäßig stattfindende Auswahl von besonders relevanten IT-Sicherheitsvorfällen und Schwachstellen. In diese Auswahl fließen Aspekte wie Kategorisierung, Priorisierung und Zuordnung der Ereignisse ein. Für die ausgewählten IT-Sicherheitsvorfälle werden die Erkenntnisse aus der Erstbewertung in das kontinuierlich weitergeführte Dokument für die übersichtliche Dokumentation überführt. Das Dokument dient als Basis für die vertiefte Analyse dieser Ereignisse im Rahmen der Auftragsforschung.

Arbeiten im Rahmen von AP 1:

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 APT´s wurden ausgewählt und einer Erstbewertung u. a. im Hinblick auf die IT-Sicherheit in kritischen Infrastrukturen und insbesondere in kerntechnischen Anlagen unterzogen. Zusätzlich zu den jeweils aktuell bekanntwerdenden IT-Sicherheitsvorfällen, IT-Angriffs-

kampagnen 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 Kategorisierung, Priorisierung und Zuordnung von herausragenden Ereignissen immer wieder überprüft und ggf. angepasst werden müssen.

Die Dokumentation der ausgewählten IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten und APT´s sowie die jeweiligen Ersteinschätzungen erfolgt in einem kontinuierlich weitergeführten Dokument zur IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen. Der Stand November 2022 bzw. Oktober 2023 dieses Dokuments ist in den technischen Bericht „IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen 2022“ /GRS 22e/ bzw. „IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen 2023“ /GRS 23d/ eingeflossen. Es umfasst zahlreiche IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten und APT´s, während der Vorhabenlaufzeit sind u. a. folgende mit entsprechend hoher Priorisierung hinzugekommen:

- Schwachstellen und IT-Angriffswerkzeuge
  - Profinet – Schwachstellen in einem Kommunikationsstandard
  - Ramsay – Angriffswerkzeug für Cyberspionage
  - Schwachstelle in Hirschmann Switchen
  - Schwachstellen in Bachmann Controllern
  - INFRA:HALT – Schwachstellen in Netzwerkstacks
  - Nucleus:13 – Schwachstellen in Netzwerkstacks
  - Schwachstellen im DDS Protocol
  - BadAlloc – Schwachstellen in echtzeitfähigen OT und IoT Geräten
  - Schwachstellen in Siemens SIPROTEC 4
  - Schwachstellen in Kameras des Herstellers Geutebrück
  - DIAEnergie
  - Schwachstelle in Johnson Controls Videoüberwachungs und Zugangskontrollsystem
  - Log4Shell: Kritische Zero Day Schwachstelle in der Java Bibliothek log4j

- Incontroller/Pipedream – Set aus ICS spezifischen Angriffswerkzeugen
- ICEFALL
- Retbleed – Schwachstellen in CPUs
- SpringShell – Schwachstelle in der Java Bibliothek Spring
- Schwachstelle in Schneider Electric Easergy P3 und P5
- TL Storm 2.0, Schwachstelle in Aruba und Avaya Switches
- SATAn
- Schwachstellen in GPS Trackern
- Schwachstellen in Videoüberwachungssystemen und Network Attached Storage von QNAP
- TLStorm-Schwachstellen in UPS-Notstromgeräten von APC betreffen kritische Infrastrukturen
- Schwerwiegende Sicherheitslücken in einem Software Development Kit (SDK)
- Sicherheitslücken in Open Automation Software (OAS) gefährden kritische Infrastrukturen
- Jaguar Tooth
- Sicherheitslücken in Moxa MXsecurity Series betreffen kritische Infrastrukturen
- Netscaler/Citrix
- Schwachstelle in der APSystems Altenergy Power Control Software
- Kritische Schwachstellen in Siemens SIMATIC S7 1200 und S7 1500CPU Systemen
- Kritische Schwachstelle in BeyondTrust PRA und RS

- IT-Sicherheitsvorfälle und IT-Angriffe
  - DarkSide – Cyberangriff auf brasilianischen Energiesektor
  - Codecov – Cyberangriff über Bash Uploader Dev Tool
  - Kaseya – Globaler Cyberangriff
  - DarkSide – Cyberangriff auf Colonial Pipeline
  - Cyberangriff auf Kisters AG
  - Black Matter – Cyberangriffe auf kritische Infrastrukturen
  - APT28 – Cyberangriff auf Google
  - APT28 – Cyberangriffe im Rahmen einer Brute Force Kampagne
  - REvil – Cyberangriff auf US Fleischkonzern JBS
  - Conti – Cyberangriff auf den irischen Gesundheitsdienst

- Cyberangriffe mit SparrowDoor
- Cyberangriff auf WestRock
- Cuba –IT Angriffe auf kritische Infrastruktur
- Conti – Cyberangriff auf ONTEC
- Tiny Turla Globale Cyberangriffe
- Cyberangriff auf Vestas
- Cyberangriffe auf die Vereinten Nationen
- Ransomware – Cyberangriff auf Sogin
- SquirrelWaffle Loader
- WhisperGate – Cyberangriffe auf ukrainische Einrichtungen
- AcidRain – Cyberangriff auf die Satellitenkommunikation via KA Sat
- Killnet – Cyberangriffe auf Webseiten von Regierungseinrichtungen
- Cyberangriff auf Rosneft
- Industroyer 2 – Cyberangriff auf die ukrainische Energieversorgung
- Khouzestan Steel Co. – Cyberangriff auf iranisches Stahlwerk
- LockBit – Cyberangriff auf Top Aces
- Conti – Cyberangriff auf Regierungsstellen Costa Ricas
- Cyberangriff auf israelische Regierungswebseiten
- Cyberangriffe mit Bumblebee
- Cyberangriff auf Dienstleister von Okta
- Cyberangriffe im Jahr 2021 und 2022 auf den VPN Client Pulse Connect Secure
- Cyberangriff auf T Mobile US und folgende SIM Swaps
- Cyberangriffe mit DeadBolt
- Cyberangriff über USB Sticks
- Cyberangriff auf Oiltanking
- Cyberangriff auf Nordex
- Cyberangriff mit Black Basta Ransomware
- Cyberangriff mit BlackCat Ransomware
- Cyberangriffe mit Quietexit
- Cyberangriffe mit Hyperbro
- Cyberangriff auf WatchGuard Firewalls
- Physischer Angriff auf IT Infrastruktur in Frankreich

- Cyberangriff auf ein Unterseekabel
- Strahlenschutz Spanien
- ZuoRAT
- Cyberangriff auf Nexeya
- Cyberangriff auf Friedrich Vorwerk Gruppe
- Cyberangriff auf Gasnetzbetreiber Desfa (Griechenland)
- Zeppelin-Ransomware
- Hive-Ransomware
- Cuba-Ransomware
- Diebstahl von FBI-Daten hochrangiger Verantwortlicher für kritische Infrastrukturen
- Informationsdiebstahl im DIB-Sektor
- Spionageangriffe durch ATP Lazarus unter Nutzung von Log4Shell
- Social-Engineering Angriffe durch iranische APT-Gruppierungen
- Cyberangriff auf ABB
- Cyberangriff auf Rheinmetall
- Cyberangriff auf Cloud Nordic
- Physische Auswirkungen von Angriffen (meist Ransomware)
- Cyberangriff auf Sicherungs-Zaun (UK)
- BianLian-Ransomware
- Cyberangriff auf Albert Ziegler GmbH
- Angriff auf die polnische Bahn
- Cyberangriff auf das Bundesfinanzministerium (DDoSia-Projekt)
- Cyberangriffe auf osteuropäische Regierungen
- Cyberangriff auf Eurocontrol
- Cyberangriff auf Webseiten von Krankenhäusern
- Cyberangriffe auf die deutsche Behörde und deutsche Unternehmen
- Veröffentlichung von Daten im Bezug zur NATO
- Cyberangriff auf World Congress Webseite
- Cyberangriff auf Mailserver der Ukraine
- Cyberangriff auf russischen Radiosender
- Cyberangriff auf russische Webseiten

- Cyberangriff auf Infotel
- Cyberangriff auf Dozor-Teleport
- WinRaR
- Suncor
- Angriff auf E-Mail Security Gateway (ESG)-Geräte des Herstellers Barracuda
- Cyberangriff mittels Social Engineering unter Verwendung von Videomaterial
- Cyberangriffe auf japanische Verteidigungsnetzwerke und auf die japanische Cybersicherheitsbehörde
- Volt Typhoon – Cyberangriffe auf kritische Infrastrukturen in den USA
- Swift Slicer – Cyberangriffe auf Ziele in der Ukraine
- CaddyWiper – Cyberangriff auf Ukrinform
- Infamous Chisel – Cyberangriff auf Ziele in der Ukraine
- Cyberangriff auf Adesso
- CosmicBeetle
- Cyberangriff der Hackergruppierung Anonymous auf Websites der japanischen Regierung
- Cyberangriffe durch Kimsuky im Zusammenhang mit südkoreanischer Militärübung
- COSMIC Energy
- MOVEit Transfer Zero Day Schwachstelle und zugehöriger Cyberangriff durch die Cl0P Ransomware Gang
- Cyberangriff der APT Sandworm auf Energieunternehmen in der Ukraine im Oktober 2022
- Cyberangriff auf das Helmholtz-Zentrum Berlin

In dem kontinuierlich weitergeführten Dokument werden sowohl die Schwachstellen und IT-Angriffswerkzeuge einerseits als auch die IT-Sicherheitsvorfälle und IT-Angriffe andererseits 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 erfolgten 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 BMUV und ggf.

im Rahmen der Auftragsforschung eine vertiefte bzw. detaillierte Auswertung der Sachverhalte im Rahmen von Ersteinschätzungen oder Stellungnahmen.

Arbeiten im Rahmen von AP 2:

Die Analyse der in MITRE ATT&CK enthaltenen Taktiken, Techniken und Vorgehensweisen von Angreifern im Hinblick auf ihre Relevanz für kerntechnische Anlagen wurde weitergeführt. Hierbei erfolgte insbesondere eine Identifikation des Anpassungs- bzw. Ergänzungsbedarfs hinsichtlich der in MITRE ATT&CK enthaltenen Angriffstechniken mit Blick auf kerntechnische Anlagen. Ein entsprechender Anpassungs- bzw. Änderungsbedarf wurde in zahlreichen Taktiken und Techniken des MITRE ATT&CK Frameworks identifiziert, allerdings wurde deutlich, dass die Schwerpunkte bei den Themen Innentäter sowie Supply Chain zu finden waren. Auf Basis des identifizierten Anpassungs- bzw. Änderungsbedarfs wurden im Rahmen dieses Arbeitspunktes verschiedenen Arbeiten durchgeführt:

- Erweiterung von in MITRE ATT&CK bereits enthaltenen Angriffstechniken im kerntechnischen Kontext relevante Aspekte,
- Erarbeitung von zusätzlichen Angriffstechniken vor dem Hintergrund der Herausforderungen und Rahmenbedingungen im nuklearen Bereich.

Zu diesen Arbeiten wurde für die IAEA Konferenz CyberCon 23 ein Paper mit dem Titel „Keeping track of the threat landscape - Adapting the MITRE ATT&CK framework for nuclear facilities” verfasst, welches im Rahmen eines Fachvortrags auf der CyberCon 23 einem internationalen Fachpublikum vorgestellt wurde.

Die Erkenntnisse aus diesen Arbeiten werden in einem separaten technischen Bericht dargestellt, der bisher als Entwurf vorliegt /GRS 24b/ und im Rahmen des Nachfolgevorhabens finalisiert werden soll.

4 Fachlicher Austausch auf nationaler und internationaler Ebene

Arbeiten im Rahmen von AP 4:

Eine Grundlage zur Erfassung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis bei der Sicherung einschließlich der Cybersicherheit ist der fachliche Austausch zwischen Experten. Auch die Fachkompetenz 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.

Im Rahmen der internationalen Zusammenarbeit wurden folgende Arbeiten zur Weiterentwicklung von internationalen Sicherungsstandards sowie zum Erkennen neuer Aspekte bei weiterentwickelten Sicherungsstandards durchgeführt:

- Durchsicht und Kommentierung des Entwurfs zur IEC 63415 “Nuclear Power plants - Instrumentation and control systems - Use of formal security models for I&C security architecture design and assessment”,
- Prüfung des neuen IAEA Standards NSS 17-T (Rev. 1) „Computer Security Techniques for Nuclear Facilities“, September 2021, hinsichtlich der Veränderungen im Vergleich zum Vorläufer-Dokument NSS 17,
- Kommentierung des Community Draft des BSI „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung inklusive Formulare für den Nachweis zu § 8a (1a) BSIG und § 11 (1d) ENWG“.

Die Erkenntnisse aus diesen Arbeiten wurden intern diskutiert und finden Eingang in die weiteren Arbeiten zum Thema Cybersicherheit. Im Fall der Kommentierung des Community Draft des BSI zur Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung wurden die Kommentare dem BSI zur Verfügung gestellt.

Zum fachlichen Austausch auf nationaler und internationaler Ebene wurden folgende Arbeiten durchgeführt:

- Bilateraler fachlicher Austausch mit einem Experten des Japan's Independent Institute (TSO) in einem Online-Meeting am 21.01.2022 zu aktuellen Fragen der Sicherung, u. a. Sicherungskultur,
- Bilaterales Treffen zum fachlichen Austausch mit einem Vertreter des Japanischen „National Institute of Maritime, Port and Aviation Technology, National Maritime Research Institute“ zu Fragen der Sicherung bei der Beförderung radioaktiver Stoffe in beiden Ländern, Auswertung,
- Vorbereitung eines weiteren bilateralen Treffens mit Vorschlägen zu Schwerpunkten für die Agenda, insbesondere zu den Aspekten Freisetzung, Übungen, Schnittstelle Sicherheit-Sicherung und IT-Sicherheit,
- Treffen mit Experten der Technischen Hochschule (TH) Wildau, Fachgebiet Luftfahrttechnik/Luftfahrtmanagement am 07.07.2022; Schnittstelle Sicherungs- und Sicherheitskultur, Parallelen und Unterschiede im sicherheits- und sicherungsgerichteten Handeln der Branchen Luftfahrt und Kerntechnik; Austausch zu Ansätzen zum sicheren Betrieb und zu „lessons learned“; Notiz /GRS 22d/.

In Verbindung mit Arbeiten in AP 1, AP 2 und AP 3 erfolgte mit der Zustimmung des BMUV eine Mitwirkung an folgenden internationalen Fachveranstaltungen zur Sicherung und Cybersicherheit:

- Teilnahme an der virtuellen Veranstaltung der IAEO „Safe & Secure Transport of radioactive Materials“ am 14.12.2021, online, Informationen auf dem Stand von Wissenschaft, Technik und Erkenntnis auf Basis von Erfahrungen anderer Nationen bei der Beförderung von Kernbrennstoffen und sonstigen radioaktiven Stoffen, internationaler Austausch zu Herausforderungen, Möglichkeiten und Gefahren der technischen Entwicklung, u. a. durch Drohnen, Reisebericht /GRS 22a/,
- Teilnahme an der Veranstaltung der IAEO “International Workshop on Nuclear Security in Practice” vom 19. - 22.09.2022 in Bahadurgarh, Indien, Vermittlung internationaler Empfehlungen der IAEO, zur Steigerung des Bewusstseins über die Bedeutung der nuklearen Sicherungskultur, zu deren Bewertung und Stärkung; Erfahrungsaustausch und Diskussion zur Nuklearen Sicherungskultur sowie deren Grundlagen, Informationen auf dem Stand von Wissenschaft, Technik und Erkenntnis auf Basis von Erfahrungen anderer Nationen; Forum auch für übergeordnete

Sicherungsthemen und zum Knüpfen von internationalen Kontakten, Reisebericht /GRS 22b/,

- Mitwirkung an der Veranstaltung der IAEO „Regional Workshop on Nuclear Security Culture in Practice“ vom 27.02. - 02.03.2022 in Tokai Ibaraki, Japan; Unterstützung der IAEO, internationaler Austausch von Erfahrungen zur nuklearen Sicherungskultur und weiteren Sicherungsthemen aus der Praxis anderer Nationen auf dem Stand von Wissenschaft, Technik und Erkenntnissen, vertieften Diskussionen zur nuklearen Sicherungskultur, Pflege und Erweiterung von Kontakten für die Fortsetzung der internationalen Zusammenarbeit, Reisebericht /GRS 23a/,

- Mitwirkung bei der „CyberCon 23“ im Juni 2023, Austausch zu internationalen Fragen der Informationssicherheit mit Experten der IAEO sowie der Mitgliedsstaaten der IAEO, Vortrag „Keeping Track of the Threat Landscape – Adapting the MITRE ATT&CK framework for nuclear facilities” vor einem internationalen Fachpublikum,

- Mitwirkung am Beratertreffen TM der IAEO zur Abwehr von unbemannten Flugobjekten (Uncrewed Aerial Vehicles - UAV) in Albuquerque, USA, Unterstützung der IAEO, internationaler Austausch zur Abwehr von UAV als Aspekt der Sicherung, Erkenntnisse zum Stand von Wissenschaft, Technik und Erkenntnis aus der Praxis anderer Nationen zur Verbesserung der nationalen nuklearen Sicherung bezüglich UAV, Pflege und Erweiterung von Kontakten für die Fortsetzung der internationalen Zusammenarbeit, Reisebericht /GRS 23b/,

- Mitwirkung am Expertentreffen CM der IAEO zu UAV und anderen unbemannten Systemen in Wien, Österreich, Unterstützung der IAEO, vertiefter internationaler Austausch zur Abwehr von UAV und anderer unbemannter Systeme als Aspekt der Sicherung, Erkenntnisse zum Stand von Wissenschaft, Technik und Erkenntnis aus der Praxis anderer Nationen, internationaler Austausch zur Verwendung von UAV für die Sicherung, Pflege und Erweiterung von Kontakten für Fortsetzung der internationalen Zusammenarbeit, Reisebericht /GRS 24a/,

Insbesondere in Verbindung mit Arbeiten in AP 1, AP 2 und AP 3 erfolgte weiterhin eine Mitwirkung an folgenden nationalen Fachveranstaltungen zur Sicherung und Cybersicherheit:

- Teilnahme am „9. Symposium Anlagensicherung“ am 11. - 12.10.2022 in Hamburg, Deutschland; Austausch über den Stand der Sicherung in der Kerntechnik in

Deutschland, Pflege und Erweiterung von Kontakten zu nationalen Experten der Sicherung,

- Teilnahme an der Veranstaltung „Security Awareness Expert“ der Simedia Akademie vom 25. - 28.10.2022 in Neu-Isenburg, Deutschland; Wissensvermittlung und Erfahrungsaustausch zu psychologischen Grundlagen, zu Ansätzen zur dauerhaften Integration der Sicherheit/Sicherung in den Arbeitsalltag und zur Entwicklung von Security Awareness Konzepten, Knüpfen von Kontakten zu Experten unterschiedlicher Interessengruppen und Branchen, Reisebericht /GRS 22c/,
- Teilnahme an der Veranstaltung „PROTECT 2023 - Fachkonferenz für den Schutz kritischer Infrastrukturen“ vom 08. - 09.11.2023 in Leipzig, Austausch zur Sicherung, Erkenntnisse u. a. zum Entwicklungsstand physischer Sicherungstechnik und zur allgemeinen Bedrohungslage, Pflege und Erweiterung von Kontakten zu nationalen Experten der Sicherung, Reisebericht /GRS 23c/.

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.

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. Während der Vorhabenlaufzeit konnten die Kontakte noch nicht aktiviert werden.

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.

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

Für Abstimmungen mit dem BMUV 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

/BMU 23/ Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, Leitlinie Sicherungskultur, Teil 1, Stand 06/23, RS-Handbuch 3-355, S I 6; AZ: 1341/003-2021.0003

/DIN 19/ Deutsches Institut für Normung e.V. (DIN): DIN EN 1143-1: Wertbehältnisse – Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl – Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume; Deutsche Fassung EN 1143-1:2019; Juli 2019.

/GRS 21/ GRS, Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen, Abschlussbericht, Vorhaben FKZ 4718R01611, Juni 2021, GRS – 646, ISBN 978-3-949088-35-3

/GRS 22a/ GRS, Reisebericht vom 25.01.2022, Thema: Teilnahme an der Webkonferenz „Safe & Secure Transport of radioactive Materials“ der IAEA im Dezember 2021, Online, 14.12.2021

/GRS 22b/ GRS, Reisebericht vom 27.09.2022, Thema: Besuch der IAEA-Veranstaltung International Workshop on Nuclear Security in Practice, Bahadurgarh, Indien, 19.-22.09.2022

/GRS 22c/ GRS, Reisebericht vom 02.12.2022, Thema: Besuch der Veranstaltung Security Awareness Expert der Simedia Akademie, Neu-Isenburg, Deutschland, 25.-28.10.2022

/GRS 22d/ GRS, Notiz vom 08.07.2022, Besuch TH Wildau, Fachgebiet Luftfahrttechnik/Luftfahrtmanagement, 07.07.2022, Anhänge

/GRS22e/ GRS, IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen – Stand November 2022, GRS-718, 2023, ISBN 978-3-910548-09-1

/GRS 23a/ GRS, Reisebericht vom 29.03.2023, Thema: Beiträge zum und Teilnahme am IAEA Regional Workshop on Nuclear Security Culture in Practice, Tokai Ibaraki, Japan, 27.02.–03.03.2023

/GRS 23b/ GRS, Reisebericht vom 30.11.2023, Thema: Technical Meeting on Nuclear Security Countermeasures for Uncrewed Aerial Vehicles (UAV), Albuquerque NM, USA, 30.10.–03.11.2023

/GRS 23c/ GRS, Reisebericht vom Dezember 2023, Thema: PROTEKT 2023 – Fachkonferenz für den Schutz kritischer Infrastrukturen“, Leipzig, Deutschland, 08.11.-09.11.2023

/GRS 23d/ GRS, IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen- Stand Oktober 2023, GRS-757, Februar 2024, ISBN 978-3-910548-48-0

/GRS 24a/ GRS, Reisebericht vom 07.03.2024, Thema: Consultancy Meeting on the Nuclear Security Implications of Uncrewed Aerial, Ground, and Maritime Systems, IAEA Hauptsitz Wien, Österreich, 05.–08.02.2024

/GRS 24b/ GRS, Anpassung und Ergänzung des MITRE ATT&CK Frameworks für Anwendung auf kerntechnische Anlagen und Einrichtungen, Entwurf, Stand 27.06.2024

Abbildungsverzeichnis

Tabellenverzeichnis

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	Kernkraftwerk
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)
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

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 978-3-910548-65-7