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

GRS - 861

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

Abschlussbericht

Claudia Quester
Silvio Sperbeck
Philipp Terberger
Udo Weizel
Sandra Zoller

Juni 2026

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) unter dem Förderkennzeichen 4724R01600 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 BMUKN übereinstimmen.

GRS - 861
ISBN 978-3-911727-54-9

Deskriptoren

Anlagensicherung, Anpralllast, Cybersicherheit, Drohnen, Einwirkungen, IT-Bedrohungslage, nukleare Sicherungskultur, Sicherung der Beförderung, Sicherung, sicherungsrelevante Ereignisse, Sicherungstechnik

Inhaltverzeichnis

1 Einleitung, Aufgabenstellung und Zielsetzung

Gemäß dem Atomgesetz (AtG) ist für kerntechnische Anlagen sowie für die Beförderung von Kernbrennstoffen u. a. eine Genehmigungsvoraussetzung, dass der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) gewährleistet ist. Bei der Bewertung und Fortentwicklung von dafür benötigten Sicherungskonzepten soll stets der Stand von Wissenschaft, Technik und Erkenntnis im gebotenen Umfang berücksichtigt und bundeseinheitlich umgesetzt werden.

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 Organisationen für technische und wissenschaftliche Unterstützung (Technical and Scientific Support Organization - TSO), stellt ihre Fachkompetenz auf dem Gebiet der Sicherung einschließlich der Sicherheit der Informationstechnik (IT-Sicherheit, Cybersicherheit) insbesondere dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) 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. Fachkompetenz und Methoden können auch anderen Behörden und Sachverständigen unter Beachtung von Geheimhaltungsanforderungen für einzelne Aspekte zur Verfügung gestellt werden.

Als eine Zielsetzung dieses Eigenforschungsvorhabens sollte daher 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. Das erfasste Wissen sollte auch dazu genutzt werden, um neue Herausforderungen auf dem Gebiet der Sicherung einschließlich Cybersicherheit zu identifizieren, generische Lösungsansätze und Anforderungen zur Verbesserung 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 analysiert werden.

Dafür verfolgte dieses Eigenforschungsvorhaben verschiedene 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 sowie von Ereignissen mit Sicherungsrelevanz

AP 1.1: Verfolgen, Erfassen und Auswerten von Entwicklungen potenzieller Hilfsmittel für Täter und von Sicherungsmaßnahmen

- Entwicklungen von technischen Systemen, Werkzeugen, Fahrzeugen etc., die von Tätern genutzt werden können sowie von neuen Technologien, die ein Potenzial für eine Anwendung durch Täter besitzen
- Trends und Neuerungen in der Sicherungstechnik als eine Basis für die Bewertung und Fortentwicklung von Sicherungskonzepten sowie deren bundeseinheitliche Umsetzung auf einer generischen Ebene
- Entwicklungen der nukleare Sicherungskultur auf nationaler und internationaler Ebene mit Bezug zu anderen Branchen und interdisziplinäre Aspekte für deren Bewertung, Erhalt, Weiterentwicklung und Stärkung
- Recherchen, Teilnahme und Mitwirkung an Veranstaltungen

AP 1.2: Sichten, Auswählen und Bewerten von Ereignissen mit Sicherungsrelevanz

- zugängliche Quellen mit Informationen zu nationalen und internationalen Ereignissen mit Sicherungsrelevanz im Hinblick auf kerntechnische Anlagen und die Beförderung von Kernbrennstoffen
- Ersteinschätzung der Ereignisse, vertiefte Auswertung ausgewählter Ereignisse auf generischer Ebene bei Bedarf
- Pflege einer Access-Datenbank zur Dokumentation der Ereignisse

AP 2: Erfassung und Auswertung der IT-Bedrohungslage

AP 2.1: Erfassen der IT-Bedrohungslage

- indirekte Ermittlung der IT-Bedrohungslage auf Basis von Aspekten wie beobachtete Cyberangriffe und IT-Sicherheitsvorfälle, Bekanntwerden von Schadsoftwarekomponenten oder Schwachstellen in relevanten IT-Systemen, eingesetzte Angriffstechniken, Verfügbarkeit von Angriffswerkzeugen und Dienstleistungen, Aktivitäten von Angreifer-Gruppierungen
- Recherchen einschlägiger nationaler und internationaler Quellen

AP 2.2: Ersteinschätzung von Ereignissen

- Einschätzung der Bedeutung der als möglicherweise relevant erkannten Ereignisse für die aktuelle IT-Bedrohungslage
- Kategorisierung anhand von grundlegenden Merkmalen wie kerntechnischer Bezug, Betroffenheit industrieller Steuerungssysteme und Sicherungssysteme, Innentäter, Lieferkette, physische Schäden
- ungewöhnliche, abweichende oder neue Aspekte in Bezug auf die bisherige IT-Bedrohungslage

AP 3: Entwicklung von Technik mit Bezug zu unbemannten Flugsystemen

AP 3.1: Verfolgung und Auswertung des Standes der Entwicklung

- Entwicklung unbemannter Flugsysteme (Uncrewed Aerial Vehicles – UAV, umgangssprachlich auch Drohnen), Arten von UAV, Steuerungssysteme
- Entwicklung technischer Möglichkeiten zur Detektion und Abwehr
- Fortschreibung rechtlicher Rahmenbedingungen für UAV, Gegenmaßnahmen

AP 3.2: Nationaler und internationaler Austausch zur Entwicklung

- Entwicklung von UAV, damit verbundene Gefährdungen kerntechnischer Anlagen und Gegenmaßnahmen

- Mitwirkung in einer Arbeitsgruppe des Bundesministeriums des Innern und des Bundesministeriums für Digitales und Verkehr zur Detektion und Abwehr von Drohnen, Teilnahme an internationalen Veranstaltungen

AP 4: Social Engineering und unwissentlicher Innentäter

AP 4.1: Cyberangriffe unter Mitwirkung eines unwissentlichen Innentäters

- Erfassen von mindestens acht relevanten Ereignissen aus einer Auswahl von realen Cyberangriffen unter Mitwirkung eines unwissentlichen Innentäters
- Ergebnisse des Screenings der IT-Bedrohungslage und gezielte Recherchen
- vergleichende Betrachtung bezüglich Gemeinsamkeiten und Unterschiede

AP 4.2: Angriffstechniken in Verbindung mit unwissentlichen Innentätern

- Herausarbeiten unterschiedlicher Angriffsmöglichkeiten und Angriffstechniken in Verbindung mit unwissentlichen Innentätern
- Ableitung von Angriffstechniken, die auf die Mitwirkung eines unwissentlichen Innentäters abzielen bzw. auf deren Identifikation und Rekrutierung

AP 5: Weiterentwicklung von Sicherungsstandards im Rahmen der internationalen Zusammenarbeit

AP 5.1: Mitwirkung an internationalen Veranstaltungen

- internationale Konferenzen und Fachtagungen mit aktuellem Bezug zur Sicherung einschließlich Cybersicherheit
- internationale Gremien oder Veranstaltungen wie Trainingskurse zu ausgewählten Aspekten der Sicherung einschließlich Cybersicherheit

AP 5.2: Abstimmungen mit TSO anderer Länder

- bilateraler Austausch von aktuellen Erkenntnissen zu speziellen Aspekten der Sicherung mit TSO anderer Länder, insbesondere Frankreich

AP 6: Eignung von Methoden zur Abschätzung der Anpralllast für den Durchfahrschutz

AP 6.1: Recherche zu gängigen Methoden

- Methoden zur Abschätzung und Berechnung der Anpralllast von Fahrzeugen sowie dafür vorhandene Versuchsergebnisse
- Recherche von normativen Vorgaben, Regelwerken außerhalb der Europäischen Union (EU), detaillierteren Methoden, numerischen Simulationen, Publikationen zur Entwicklung und Anwendung von Methoden

AP 6.2: Ursachen für starke Abweichungen zwischen Methoden

- Vergleich verschiedener Methoden und deren Grundlagen
- Anwendung gängiger und zielführend erscheinender Methoden für repräsentative Beispiele

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

Gewonnene Erkenntnisse und konkrete Ergebnisse dienten u. a. im Rahmen des Auftragsforschungsvorhabens FKZ 4724R01610 als Grundlage für die Weiterentwicklung des nationalen Regelwerks der Sicherung (SEWD-Regelwerk) und zur fachlichen Beratung des BMUKN.

Zum Erkenntnisgewinn der Sachverständigen sowie zum Erkennen aktueller Trends und Schwerpunkte im Sinne des Standes von Wissenschaft, Technik und 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 Eigenforschungsvorhabens 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 und Konferenzen 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 Eigenforschungsvorhaben hatte eine Laufzeit vom 01.07.2024 bis zum 31.05.2026 nach kostenneutraler Verlängerung.

2 Stand von Wissenschaft, Technik und Erkenntnis

Systementwicklungen mit Bezug zur Sicherung und die am Markt verfügbaren technischen Möglichkeiten und Technologien für die Sicherung und für den Einsatz bei SEWD sollten verfolgt und ausgewertet werden, um Trends und Neuerungen in der Sicherungstechnik sowie geänderte Möglichkeiten für SEWD rechtzeitig erkennen zu können. Dabei sollten auch weitere Fragestellungen zu Sicherungsbelangen identifiziert werden.

Insbesondere die Entwicklung von UAV ist ein hochdynamischer Prozess. Aufgrund der stetig wachsenden Nutzung von UAV sollte deren Entwicklung in Bezug auf eine mögliche Nutzung als Hilfsmittel für SEWD kontinuierlich beobachtet werden.

Für die Etablierung und Aufrechterhaltung eines robusten Sicherungsregimes ist der Faktor Mensch von fundamentaler Bedeutung, wobei die Sicherungskultur den zentralen Kern darstellt. Erfahrungen, Wissen und guten Praktiken zur nuklearen Sicherungskultur, auch mit Bezug zu anderen Branchen und interdisziplinären Aspekten, sollten auf nationaler und internationaler Ebene ausgetauscht werden, um daraus Erkenntnisse für die Bewertung, den Erhalt, die Weiterentwicklung und die Stärkung der nuklearen Sicherungskultur zu gewinnen.

Aspekte im Zusammenhang mit der Cybersicherheit umfassen auch alle Bereiche, die den Faktor Mensch und dessen Interaktion mit IT-Systemen betreffen. Der wichtigste Angriffsvektor ist dabei das sogenannte Social Engineering, bei dem Menschen manipulieret und ausgenutzt werden, so dass sie freiwillig bzw. nicht wissentlich die Ziele der Angreifer durch eigene Handlungen unterstützen. Das Social Engineering als eines der erfolgreichsten und häufigsten Angriffsvektoren im Bereich der Cybersicherheit sollte weiterführend untersucht werden.

Für die Auslegung von Durchfahrschutzeinrichtungen existieren verschiedene gängige Möglichkeiten, die Anpralllast von Fahrzeugen zu errechnen, bei deren Anwendung starke Abweichungen der Ergebnisse festgestellt wurden. U. a. für Festlegungen im Rahmen der Lastannahmen Anlagen /BMU 23a/ und bei der Umsetzung weiterer Teile des SEWD-Regelwerks werden begründete und nachvollziehbare Aussagen zur Ermittlung der Anpralllast benötigt. Ursachen für Abweichungen sollten erkannt sowie eine begründete Auswahl von Berechnungsmethoden und von geeigneten Eingangswerten für die Berechnungen abgeleitet werden.

Während der Vorhabenlaufzeit wurden u. a. die Eignung möglicher Quellen und Medien für Recherchen geprüft und wichtige Konferenzen, Workshops, Fachforen etc. eruiert.

2.1 Nukleare Sicherungskultur

Für die nukleare Sicherung ist die Sicherungskultur gemäß Internationaler Atomenergie-Organisation (IAEO) das Zusammenspiel von Eigenschaften, inneren Einstellungen und Verhaltensweisen von Einzelpersonen, Organisationen und Einrichtungen, das 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.

Für den Erkenntnisgewinn wurden Literaturrecherchen durchgeführt und Veranstaltungen besucht.

Literaturrecherchen wurden durchgeführt zum Verständnis und zur Anwendung von kulturellen Aspekten in anderen Branchen mit einem vergleichbaren Sicherheitsbewusstsein wie der Luftfahrt und der Medizin. Mögliche Sensibilisierungsmaßnahmen für eine wirksame und robuste Sicherungskultur bzw. für ein sicherungsgerichtetes Handeln wurden weitergehend untersucht. Aufbauend darauf wurde eine potenzielle Anwendung im Bereich der nuklearen Sicherung analysiert, wobei erste Einschätzungen sowie Herausforderungen der praktischen Umsetzung im Rahmen der Vorbereitung einer explorativen Befragung berücksichtigt wurden.

Eine Recherche des Dokuments “European Regional Focus Group on Nuclear Security During Decommissioning Summary Report” /INS 24/, der Zusammenfassung eines Workshops zur nuklearen Sicherung während Stilllegung und Abbau (Nuclear Security during Decommissioning), erbrachte folgende Erkenntnisse:

- wichtige Statements zur nuklearen Sicherungskultur aus internationaler Sicht
  - die nukleare Sicherungskultur wurde als der wichtigste Faktor hervorgehoben, um eine effektive nukleare Sicherung bei unvorhersehbaren Situationen während Stilllegung und Abbau zu gewährleisten
  - die nukleare Sicherungskultur wird vor und während der Stilllegung und des Abbaus wichtiger als je zuvor
- weitere Punkte zur Bedeutung der nuklearen Sicherungskultur als Bestätigung aus internationaler Sicht
  - Sicherungskultur muss an nationaler Kultur und Organisationskultur ausgerichtet werden
  - für eine effektive Sicherungskultur müssen neue Beteiligte entsprechend gewonnen/begeistert werden, bzw. die Ausprägungen vorhandener Kulturen sollen für eine wirksame Sicherung genutzt werden
  - Sicherungskultur wird als übergreifend begriffen - also auch der Aspekt der Schnittstelle Sicherheit-Sicherung wird auf der Ebene der Kulturen verstärkt adressiert
  - Sicherungskultur wird sehr häufig mit Awareness genannt, also mit bewusster Wahrnehmung, Sensibilisierung und Aufklärung

Obwohl in der Sicherung in Deutschland bauliche und sonstige technische Sicherungsmaßnahmen grundsätzlich personellen und organisatorischen Sicherungsmaßnahmen vorgezogen werden, ist eine erfolgreiche Sicherung kerntechnischer Anlagen wesentlich vom eingesetzten Personal und dessen Handeln abhängig – dem sogenannten menschlichen Faktor. Ziel von Awareness-Maßnahmen ist die Sensibilisierung und gezielte Lenkung der Aufmerksamkeit der Beteiligten für ein spezielles Thema, die Schaffung von Akzeptanz und Verständnis für Sicherungsmaßnahmen und die methodische Beeinflussung hin zu einem bestimmten Verhalten.

Für den Erkenntnisgewinn wurden die nachfolgenden nationalen und internationalen Veranstaltungen genutzt:

- Vorbereitung und Teilnahme an der Veranstaltung Take Aware 2025 in Wuppertal vom 20. bis 22.05.2025
  Die Take Aware ist die größte Veranstaltung zum Thema „security awareness“ im

deutschsprachigen Raum D-A-CH. Schwerpunkte waren die Beeinflussung der Awareness durch künstliche Intelligenz (KI), Erfahrungsaustausch, Sammeln von Informationen aus der Praxis anderer sicherungs- und sicherheitssensibler Branchen und Knüpfen von Kontakten (Reisebericht /GRS 25b/).

- Vorbereitung und Teilnahme am Swiss Security Awareness Day 2025 in Bern am 11.09.2025
  Schwerpunkte waren das Erfassung von neuen branchenübergreifenden, integrativen Ansätzen und der Austausch mit internationalen Partnern (Reisebericht /GRS 25d/).

- Vorbereitung und Teilnahme an der Veranstaltung Take Aware 2026 in Düsseldorf vom 20. bis 21.05.2026
  Schwerpunkte waren Security Awareness in der Praxis, KI und Cyber Security sowie Menschlicher Faktor und Psychologie (Reisebericht /GRS 26b/).

Auf der Take Aware 2025 in Wuppertal vom 20. bis 22.05.2025 konnten Erfahrungen auf dem Gebiet der Sicherungskultur zwischen internationalen Experten im deutschsprachigen Raum ausgetauscht und Informationen auf dem Stand von Wissenschaft, Technik und Erkenntnissen aus der Praxis anderer sicherungs- und sicherheitssensibler Branchen gesammelt werden. Die zunehmende Bedrohung insbesondere der Cybersicherheit, aber auch der peripheren (Sicherheits-)Bereiche wurde verdeutlicht. Die Bedeutung des Faktors Mensch für die Sicherheit wurde aufgezeigt und Hinweise, Erkenntnisse und Erfahrungen zur Stärkung der Fähigkeiten zum aktiven Beitragen geteilt. Die ausschließliche Durchführung von Belehrungen und E-Learnings wird als nicht sonderlich wirksam betrachtet – stattdessen sollten die Mitarbeiter emotional angesprochen werden. Eine Einbeziehung der Nutzung von Maßnahmen auch im Privaten, eine positive und offene Kommunikation und die Verfolgung spielerischer Ansätze führen zu mehr Sichtbarkeit und Akzeptanz sowie zu einer erhöhten Wirksamkeit von Maßnahmen. Der Einsatz von KI ist auch im Awareness-Umfeld zu beobachten. Es werden große Potenziale wie Arbeitserleichterung oder Produktivitätssteigerung, aber auch gewisse Unsicherheiten wie mangelnde Transparenz durch nicht nachvollziehbare KI-Entscheidungen oder der ggf. ungewollte Informationsabfluss gesehen. Ausgewählte Erkenntnisse dazu sind in /GRS 25b/ zusammengestellt und betreffen insbesondere:

- Der Zusammenhang zwischen den Aspekten Awareness, Behaviour und Culture (ABC) im Sinne einer Sicherungskultur wurde am Beispiel der Cybersicherheit dargestellt. Für den Aspekt Awareness wurden Ziele definiert, z. B. Cyberrisiken

kennen, Interessen und Motivation wecken, Verständnis für Maßnahmen schaffen. Hierbei wurde Awareness als Summe von Wissen und Einstellung definiert und als Fundament für die weiteren Tätigkeiten festgelegt. Für den Aspekt Behaviour wurden Ziele definiert, z. B. gelerntes Wissen anwenden, Verhaltensänderung fördern, Routinen und Gewohnheiten aufbauen, agieren statt reagieren. Für den Aspekt Culture wurden die Schwerpunkte gemeinsame Werte, Normen und Vorbilder, gelebte Verantwortung und Sicherheit als Selbstverständnis dargestellt. Die Grundsätze wie Umfragen, Evaluationen, Leitbilderstellung, Wertschätzung und Anerkennung, Umgang mit Fehlern (Fehlerkultur) oder die Einrichtung von anonymen Meldestellen wurden adressiert. Als Ergänzung wurde der Aspekt Governance (Organisationssteuerung) präsentiert mit Schwerpunkten wie Schaffung eines strategischen Rahmens für Awareness, Definition von klaren Verantwortlichkeiten für Behaviour und Culture, Schaffung und Ausbau von Prozessen und Zielvorgaben, Messen, Steuern und Verbessern sowie Integration in die Organisation.

- Am Beispiel einer Awareness-Kampagne wurde die Wirksamkeit von emotionalen Aspekten verdeutlicht, durch die Verwendung von Mitteln der Gamification zur Erhöhung der Awareness.

- Die Einsatzmöglichkeiten von KI für die Security Awareness, wie die Analyse des Nutzungsverhaltens der Mitarbeiter und darauf basierende maßgeschneiderte Schulungsinhalte oder realistische Simulationen, wurden vorgestellt. Dabei wurden auch Risiken wie Datenschutzbedenken (Überwachungskultur statt Sicherheitskultur) und technische Limitationen (Alarmmüdigkeit aufgrund vieler Falschmeldungen bei komplexen Szenarien; mangelnde Interpretierbarkeit/Nachvollziehbarkeit von KI-Entscheidungen) eingegangen.

- Die Bedeutung einer offenen Kommunikation von Vorfällen, deren Analyse sowie die Ableitung und wirksame Bekanntgabe von Folgemaßnahmen wurde im Zusammenhang mit der Stärkung der Informationssicherheit adressiert. Dabei sind die Zusammenarbeit und gegenseitige Unterstützung, das Einstehen für das Thema Cybersicherheit und die Bereitstellung von Ressourcen und das Bekenntnis durch das Management von besonderer Bedeutung - Awareness-Maßnahmen sollten durch das Management die entsprechende Bedeutung zugemessen bekommen. Wirksame Awareness ist ein langwieriger Prozess und kann nur durch regelmäßige und kontinuierliche Kommunikation erzielt werden.

- Zur Wirksamkeitsmessung von Cybersecurity Awareness Trainings wurden die sieben Stufen der Cybersecurity-Ausbildung (Bedrohungsbewusstsein, Bedrohungsmerkmale, Bedrohungskonsequenzen, Maßnahmenauswahl, Maßnahmenverständnis, Maßnahmenbeherrschung und Anschlussmaßnahmen) vorgestellt und auf die Herausforderung des Messens eingegangen. Standard-Testverfahren wie Leistungsüberprüfung messen kein Verhalten, aber durch Situational Judgment Tests, bei denen Verhaltensbeobachtungen getätigt werden, sind Aussagen über das zukünftige Verhalten möglich.

Der Swiss Security Awareness Day fand am 11.09.2025 in Bern statt und diente dem fachlichen Austausch zu aktuellen Ansätzen der Security Awareness. Im Mittelpunkt standen praxisnahe Vorträge, Workshops und Erfahrungsberichte zur Stärkung einer wirksamen Sicherungskultur in unterschiedlichen Branchen. Ausgewählte Erkenntnisse dazu sind in /GRS 25b/ zusammengestellt. Dazu gehören insbesondere:

- Der Mensch ist ein zentraler Faktor für Sicherung
  Technische Maßnahmen allein reichen nicht aus. Wirksame Sicherung hängt maßgeblich vom Verhalten, Bewusstsein und Verantwortungsgefühl der Mitarbeitenden ab.

- Security Awareness muss nutzerorientiert gestaltet werden
  Maßnahmen sollten die Perspektive der Nutzer berücksichtigen, sie im Alltag unterstützen und nicht behindern. Besonders wirksam sind interessante Schulungen, Storytelling und praxisnahe Ansätze.

- Führungskräfte haben eine Schlüsselrolle
  Eine respektvolle, verständnisvolle Führungskultur kann Innentäterrisiken verringern. Dominantes Führungsverhalten wirkt dagegen eher kontraproduktiv.

- Wissen allein führt nicht automatisch zu sicherem Verhalten
  Viele Awareness-Schulungen scheitern nicht am fehlenden Wissen, sondern an mangelnder Überzeugung und Motivation. Deshalb sollten Mitarbeitende auch emotional angesprochen werden.

- Gamification und praktische Übungen fördern die Wirksamkeit
  Die Veranstaltung zeigte, dass spielerische und interaktive Elemente helfen können, Sicherungskonzepte erlebbar zu machen und nachhaltiger zu vermitteln.

Der Austausch und das Networking waren fachlich wertvoll. Neben Vorträgen und Workshops lieferten Pausengespräche und der Apéro zusätzliche Erkenntnisse und ermöglichten den Ausbau nationaler Netzwerke im Bereich Security Awareness.

Die Teilnahme an der Take Aware 2026 ist vor dem Hintergrund einzuordnen, dass Veranstaltungen mit einem ausdrücklichen Schwerpunkt auf Sicherungskultur nur sehr begrenzt verfügbar sind. Die Take Aware bietet hierzu eine fachlich relevante Schnittstelle, da sie zentrale Aspekte der Security Awareness, Sicherheitskultur, Kommunikation, Führung und Verhaltensänderung behandelt, die auch für Fragestellungen der Sicherungskultur von Bedeutung sind. Bereits bei der Teilnahme an der Take Aware 2025 konnten hierzu wertvolle Gespräche geführt und thematische Querverbindungen zwischen Sicherheits- und Sicherungskultur herausgearbeitet werden.

Ziel der erneuten Teilnahme war es daher, aktuelle Entwicklungen im Bereich Security Awareness und Sicherheitskultur zu verfolgen, neue methodische Ansätze kennenzulernen und den fachlichen Austausch zu möglichen Übertragungen auf die Sicherungskultur fortzuführen. Eine ausführliche Zusammenfassung ist in /GRS 26b/ zu finden.

Inhaltlich bot die Veranstaltung einen praxisnahen Überblick über aktuelle Ansätze der Security Awareness, insbesondere zu wirksamer Kommunikation, emotionaler Ansprache, künstlicher Intelligenz und Social Engineering. Besonders hervorzuheben war der Beitrag von TreeSolution Security Awareness AG, der einen konkreten Zugang zur Messbarkeit von Sicherheitskultur und Awareness aufgezeigt hat.

Die TreeSolution Security Awareness AG ist ein spezialisiertes Schweizer Unternehmen für Informationssicherheit und Security Awareness, das seit 2005 Organisationen bei der Sensibilisierung von Mitarbeitenden für Cyber-Bedrohungen und beim Aufbau einer nachhaltigen Sicherheitskultur unterstützt. Dr. Thomas Schlienger stellte einen quantitativen Ansatz zur Messung von Sicherheitskultur und Awareness vor. Grundlage waren insgesamt 88 Erhebungen, die in den letzten 20 Jahren durchgeführt wurden mit über 100.000 Teilnehmenden und rund 4,5 Mio. Einzelantworten. Eine Erhebung bestand dabei jeweils aus dem Ausfüllen eines strukturierten Fragenkatalogs durch Mitarbeitende. Durch wiederholte Messungen mit gleichbleibenden Fragen lassen sich Entwicklungen über mehrere Jahre vergleichen, Schwachstellen erkennen und Maßnahmen gezielter steuern.

Die im Vortrag vorgestellten drei anonymisierten Fallstudien machten deutlich, dass Sicherheitskultur messbar ist, sich aber je nach Organisation unterschiedlich entwickelt. In den Fallstudien werden vor allem die gemessenen Verbesserungsbereiche beschrieben; konkrete interne Einzelmaßnahmen der Organisationen wurden nicht im Detail offengelegt. Daher sind die Ergebnisse als sichtbare Verbesserungsbereiche bzw. daraus ableitbare Maßnahmenfelder zu verstehen. Nachfolgende Fallbeispiele wurden vorgestellt:

- Organisation A, eine national tätige Organisation mit 1.000 bis 5.000 Mitarbeitenden, wurde über 13 Jahre viermal untersucht und zeigte insgesamt eine positive Entwicklung, vor allem bei Organisationsstruktur, Wissen, Vorbildfunktion, Kommunikation, Problemmanagement und Schulungen. Gleichzeitig ging jedoch die Einstellung der Mitarbeitenden zurück, was zeigt, dass formale Verbesserungen nicht automatisch zu einer dauerhaft positiven Haltung führen.
- Organisation B, eine multinationale Organisation mit 25.000 bis 50.000 Mitarbeitenden, zeigte über sieben Jahre den stärksten Reifezuwachs. Verbesserungen zeigten sich hier gleichzeitig bei Schulung, Wahrnehmung, Kommunikation, Problemmanagement, Arbeits- und Technologiegestaltung sowie Einstellung. Dies spricht dafür, dass Sicherheitskultur besonders wirksam wächst, wenn mehrere Handlungsfelder gleichzeitig adressiert werden.
- Organisation C, eine multinationale Organisation mit 5.000 bis 25.000 Mitarbeitenden, wurde über vier Jahre jährlich untersucht. Hier zeigte sich, dass Verbesserungen zwar kurzfristig erreicht werden können, insbesondere bei Arbeits- und Technologiegestaltung sowie Problemmanagement, dass Fortschritte bei Kommunikation und Führung jedoch weniger stabil sind und kontinuierlich gepflegt werden müssen.

Die Teilnahme an der Take Aware 2026 war fachlich wertvoll, da sie aktuelle Entwicklungen im Bereich Security Awareness und Sicherheitskultur praxisnah aufzeigte und wichtige Schnittstellen zur Sicherungskultur verdeutlichte. Es bestätigte sich erneut, dass wirksame Sicherheits- bzw. Sicherungskultur nicht allein durch technische Maßnahmen oder reine Wissensvermittlung entsteht, sondern durch verständliche Kommunikation, Führungsvorbild, Motivation, alltagstaugliche Prozesse und eine dauerhafte organisatorische Verankerung.

Für eine Anwendung der bisher gewonnen Erkenntnisse wurde eine Selbstbewertung in Bezug auf die Sicherungskultur in der GRS vorbereitet, basierend auf den Empfehlungen

des internationalen Regelwerk Nuclear Security Series (NSS) der IAEO, des Umsetzungsleitfadens NSS 7 /IAE 08/ und des technischen Leitfadens NSS 28-T /IAE 17/, sowie den Vorgaben der Leitlinie Sicherungskultur /BMU 23b/ des SEWD-Regelwerks. Die Umfrage dient als Startpunkt zur Standortbestimmung der Sicherungskultur in der GRS. Ziel des ersten Durchlaufs ist es, eine erste realistische Einschätzung zu erhalten, wobei diese Umfrage allein, als erster Schritt in einem kontinuierlichen Verbesserungsprozess, noch kein vollständiges Gesamtbild der Sicherungskultur in der GRS liefern kann. Als Grundlage wurden sieben Merkmale einer wirksamen Sicherungskultur ausgewählt. Die Fragen wurden auf Basis der jeweiligen Merkmalsbeschreibungen formuliert. Die Ergebnisse der Umfrage sollen transparent kommuniziert werden. Auf dieser Basis sollen Maßnahmen zur Weiterentwicklung der Sicherungskultur abgeleitet werden.

2.2 Entwicklungen mit Relevanz für SEWD

Das Ziel der Arbeiten bestand darin, relevante Trends technischer und methodischer Entwicklungen in Bezug auf deren Verwendung für mögliche SEWD und ggf. zur Sicherung gegen derartige Einwirkungen zu identifizieren, 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 für SEWD genutzt werden können. Das in den Vorläufervorhaben begonnene regelmäßige Verfolgen der technischen Entwicklung von typischen marktgängigen Werkzeugen, Geräten, Beförderungsmitteln 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 Fortschreibung 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 wurden auch Neuentwicklungen mit einem Potenzial als Hilfsmittel für Einwirkungen identifiziert.

Im Rahmen des Vorhabens wurden für den Erkenntnisgewinn auch nationale und internationale Veranstaltungen genutzt, insbesondere:

- Teilnahme an einer praktischen Anwendung eines Hilfsmittels der Lastannahmen Relevante Schwerpunkte waren die Wirksamkeit und die Rahmenbedingungen

beim Einsatz dieses Hilfsmittels. Die Erkenntnisse zum Hilfsmittel wurden zusammengestellt (Reisebericht /GRS 24b/).

- Besuch der Fachmesse Enforce Tac vom 23. bis 25.02.2026 in Nürnberg
  Relevante Schwerpunkte waren u. a. die Sicherung von kritischer Infrastruktur (KRITIS), Erfahrungen aus dem Krieg in der Ukraine und Cybersicherheit (Reisebericht /GRS 26c/).

2.3 Technik mit Bezug zu UAV

In den Vorläufervorhaben wurden Recherchen zum Stand von Wissenschaft, Technik und Erkenntnis im Hinblick auf unbemannte Fahrzeuge, insbesondere UAV, durchgeführt. Aufgrund der hochdynamischen Entwicklung in diesem Bereich sollte dieser Stand in Bezug auf die sich aus der Weiterentwicklung von UAV potenziell ergebende Gefährdung sowie in Bezug auf den Entwicklungsprozess von Gegenmaßnahmen zur Detektion und Abwehr von UAV kontinuierlich verfolgt und ausgewertet werden.

Im Rahmen dieses Eigenforschungsvorhabens erfolgte die Verfolgung und Auswertung des Standes von Wissenschaft, Technik und Erkenntnis in Bezug auf die potenzielle Gefährdung von kerntechnischen Anlagen, die aus den sich dynamisch entwickelnden Möglichkeiten von UAV resultieren, sowie in Bezug auf die parallele Entwicklung von Möglichkeiten zur Detektion und Abwehr von UAV, zeitlich begrenzt bis zum Start des speziellen Forschungsvorhabens 4725E03411 „Fähigkeiten von Drohnen und damit verbundene Gefahren und Anwendungen" ab Mitte des Jahres 2025, in dessen Rahmen die Arbeiten kontinuierlich fortgeführt werden.

Ein weiterer Aspekt der Arbeiten betraf den nationalen und internationalen Austausch zu den Entwicklungen und relevanten Erkenntnissen.

Für den Erkenntnisgewinn im Zusammenhang mit der Entwicklung von UAV und Abwehrmaßnahmen wurden insbesondere nationale und internationale Veranstaltungen genutzt:

- Teilnahme an der „International Conference on Enhancing Nuclear Safety and Security Through Technical and Scientific Support Organizations (TSOs)“ (TSO-Konferenz) vom 02. bis 06.12.2024 in Wien
  Relevante Aspekte waren u. a. internationaler Austausch mit Experten anderer

TSO zu UAV und den damit verbundenen Gefährdungen sowie Anbahnung von Kontakten für den künftigen internationalen Austausch zu UAV (Reisebericht /GRS 25c/).

- Teilnahme am Symposium Anlagensicherung, TÜV Nord, in Hamburg am 04. und 05.02.2025 mit einem breiten Spektrum der Möglichkeit zum Erfahrungsaustausch zwischen Vertretern von Behörden, Gutachterorganisationen und Betreibern Informationen zum Thema Drohnen als Transportmittel eines bestimmten Hilfsmittels wurden gesammelt. Themen wie Cybersicherheit, KI in der Sicherung und Sprengstoff wurden erörtert.

- Teilnahme am Reallabor der AG DAD zur Drohnendetektion und -abwehr an Flughäfen am 19.03.2025 mit Fokus im ersten Schritt auf Detektion und Verifikation von unterschiedlichen Drohnen durch die Kombination verschiedener Systeme unter unterschiedlichen Bedingungen
  Der Besuchertag am Reallabor zeigte einen kleinen Einblick in den Aufbau und in Teilergebnisse einer dreiwöchigen Erprobungsphase an einem kleinen Flughafen.

- Teilnahme am jährlichen Kongress des Verbandes für Sicherheitstechnik (VfS) in Leipzig am 06. und 07.05.2025 unter dem Motto „Gemeinsam für eine sichere Welt“ mit Themen wie Drohnen, Video, Perimetersicherung, KRITIS, Zufahrtsschutz, KI
  Der Fokus der Teilnahme lag insbesondere auf Drohnen in Bezug zu KRITIS und rechtlichen Bedingungen für die Abwehr, auf Perimetersicherung mit Unterstützung durch Drohnen und durch KI sowie auf dem Sammeln von Informationen und Knüpfen von Kontakten (Reisebericht /GRS 25a/).

- Mitwirkung am Symposium Anlagensicherung, TÜV Nord, in Hamburg am 10. und 11.02.2026
  Das Symposium wurde mit der Präsentation „Die Rolle von Drohnen in der kerntechnischen Sicherheit und Sicherung“ unterstützt.

- Besuch der Fachmesse Enforce Tac in Nürnberg vom 23. bis 25.02.2026 mit einem Fokus auf Drohnendetektion und -abwehr sowie Schutz vor Drohnen (Reisebericht /GRS 26c/)

Auf dem VfS-Kongress in Leipzig am 06. und 07.05.2025 wurde zur rechtlichen Seite der Drohnendetektion und -abwehr u. a. festgestellt: In Deutschland gibt es derzeit keine Rechtsgrundlage für einen notwendigen KRITIS-Schutz vor Drohnen. Die aktuelle

Referentenfassung des KRITIS-Dachgesetzes bietet keinen Schutz vor Drohnen, sondern es werden nur Risiken und Pflichten adressiert. Die EU-Drohnenverordnung von 2021 bietet keine Antworten hinsichtlich der Abwehrregelungen zu Drohnen. Eine einfache Detektion von Drohnen durch Radar oder Richtfunk kann im schlimmsten Fall zum Verstoß gegen das Telekommunikationsgesetz, Datenschutz und Strafgesetz führen. Bei der Abwehr von Drohnen orientieren sich die Juristen an einer Rechtsprechung, bei dem eine Privatperson eine Drohne mit dem Luftgewehr abgeschossen hat und mit Bezug auf eine Störung der Privatsphäre freigesprochen wurde (AZ.9CS926 Amtsgericht Riesa). Bei Unternehmen ist eine solche Privatsphäre nur schwierig zu begründen und daher gibt es aktuell keine Möglichkeiten bei der Drohnenabwehr. Staatliche Einrichtungen haben ein Abwehrrecht, aber müssen die Verhältnismäßigkeit beachten.

Zum Einsatz von Drohnen in der Perimetersicherung wurden verschiedene Möglichkeiten vorgestellt:

- Drohne auf Platz im Werksgelände, startet im Bedarfsfall
- Drohne fliegt Patrouille am Perimeter
- Drohne an zentraler Stelle, startet leitstandbasiert
- Unterstützung der Werksfeuerwehr
- Begutachtung schwer erreichbarer Orte

Entsprechende Flüge bedürfen einer Betriebsgenehmigung. Bei der Vorführung eines Drohnenflugs ohne Sichtkontakt mit on-board-Kamerasystemen und GPS-Tracking auf der Digitalen Plattform Unbemannte Luftfahrt (DIPUL), mit kilometerweit entferntem Drohnenstandort, wurde die Navigation durch vorgegebene Routen oder manuellen Flug gewährleistet. Die hochauflösenden Kameras konnten Fahrzeugkennzeichen auf 120 m Entfernung wiedergeben. Eine zugeschaltete Wärmebildkamera ermöglichte die Identifizierung von Wärmesignaturen.

Auf der TSO-Konferenz vom 02. bis 06.12.2024 in Wien, in Kooperation von IAEO und der European Technical Safety Organizations Network (ETSON), erfolgte u. a. ein internationaler Austausch zur Entwicklung von UAV und den damit verbunden Gefährdungen kerntechnischer Anlagen und möglichen Gegenmaßnahmen. Als Beispiel für den Einsatz von UAV in kerntechnischen Anlagen wurde die Möglichkeit einer Ferninspektionstechnologie zur Untersuchung von Behältern für radioaktive Abfälle vorgestellt (TÜV

Nord), in Verbindung mit einer automatischen Auswertung von Befunden durch den Einsatz von KI. Für derartige Inspektion ist neben der Lösung technischer Herausforderungen vor allem noch eine Klärung rechtlicher Aspekte erforderlich.

Die Fachmesse Enforce Tac vom 23. bis 25.02.2026 in Nürnberg bot Standpräsentationen von Ausstellern, Fachvorträge und Produktdemonstrationen. Ein Schwerpunkt war der Austausch mit Ausstellern zur Drohnenabwehr, insbesondere zum Einsatz von Netzen als Neutralisationsmittel. Die Unternehmen Securiton und Argus Interception präsentierten integrierte Systeme, die Detektion, Identifikation und anschließende Ausschaltung von Drohnen in einem Gesamtansatz vereinen. Die Besonderheit beider Hersteller liegt in der gezielten Bekämpfung von Drohnen mit einer Netztechnologie, sodass die Fluggeräte funktionsunfähig gemacht werden, ohne sie zu zerstören. Vorteilhaft ist u. a., dass die Systeme auch autonom arbeiten können, diversitäre Detektionsmethoden nutzen und Systemupdates über physische Speichermedien erfolgen (erhöhte Cybersicherheit). Bei mehreren Produktdemonstrationen wurden die Einsatzfähigkeit und praktische Wirkung der Systeme in realitätsnahen Szenarien vorgestellt. Diese Vorführungen ermöglichten einen unmittelbaren Einblick in die operative Leistungsfähigkeit der Produkte.

2.4 Social Engineering und unwissentlicher Innentäter

Das Social Engineering ist einer der wichtigsten Angriffsvektoren im Zusammenhang mit der Cybersicherheit sowie dem Faktor Mensch und dessen Interaktion mit IT-Systemen, bei dem Angreifer Menschen derartig manipulieren und ausnutzen, dass sie freiwillig bzw. nicht wissentlich die Ziele der Angreifer durch eigene Handlungen unterstützen. Hierbei zielen Angreifer direkt auf die Unwissenheit, Arglosigkeit oder Nachlässigkeit des Opfers ab. Allgemein besteht das Ziel der Angreifer dabei im Wesentlichen darin, das Opfer zur Installation von Schadsoftware, zur Preisgabe sensibler Informationen oder zur Durchführung bestimmter Handlungen zu bewegen. Der erfolgreiche und häufig angewandte Angriffsvektor des Social Engineering im Bereich der Cybersicherheit kann in verschiedenen Formen im Rahmen von einzelnen Cyberangriffen oder Angriffskampagnen realisiert werden. Die Opfer von Social Engineering werden hierbei zu unwissentlichen Innentätern.

Im Rahmen des Vorhabens wurde mit grundlegenden Arbeiten zum Themenfeld von Cyberangriffen unter Mitwirkung unwissentlicher Innentäter begonnen. Eine erste und im

Hinblick auf relevante Angriffsmöglichkeiten bzw. Angriffstechniken vorbereitende Bearbeitung dieser Thematik erfolgte durch die Recherche nach realen Cyberangriffen unter Mitwirkung unwissentlicher Innentäter. Eine Auswahl dieser Cyberangriffe wurde ausgewertet und beschrieben. Auf Basis dieser ausgewerteten Cyberangriffe erfolgte die Herausarbeitung unterschiedlicher Angriffsmöglichkeiten bzw. Angriffstechniken, die auf die Mitwirkung unwissentlicher Innentäter abzielen. Es wurden acht Angriffsmöglichkeiten bzw. Angriffstechniken identifiziert, die im Rahmen des Vorhabens betrachtet wurden. Diese sind:

- Spear-Phishing
- Watering-Hole-Angriffe
- Zertifizierung von maliziösen Komponenten
- Unterlassung
- Unter-Druck-Setzen von Personen
- Unvorsichtigkeit im Umgang mit sensiblen Informationen
- Nichteinhaltung von Prozeduren
- Nutzung schwacher Passwörter

Jede dieser acht Angriffsmöglichkeiten bzw. Angriffstechniken wurde beschrieben und diskutiert. Zudem wurde zu jeder dieser acht Angriffsmöglichkeiten bzw. Angriffstechniken ein ausgesuchter Cyberangriff ausführlich beschrieben, bei dem die jeweilige Angriffsmöglichkeit bzw. Angriffstechnik angewendet wurde. Dabei wurde insbesondere auf die Art und Weise der Ausnutzung unwissentlicher Innentäter eingegangen, sofern der GRS hierzu Informationen vorlagen. Außerdem erfolgte eine kurze Beschreibung weiterer Cyberangriffe, bei denen die jeweilige Angriffsmöglichkeit bzw. Angriffstechnik eingesetzt wurde.

Des Weiteren erfolgte eine vergleichende Betrachtung der ausgewerteten Cyberangriffe unter Mitwirkung unwissentlicher Innentäter bzw. der diskutierten Angriffsmöglichkeiten und Angriffstechniken. Dabei wurden für die zu jeder der acht diskutierten Angriffsmöglichkeiten bzw. Angriffstechniken beschriebenen realen Cyberangriffe die Merkmale dieser Angriffe gesucht und zusammengefasst. Anschließend erfolgte ein Vergleich dieser Merkmale, um Gemeinsamkeiten und Unterschiede bezüglich der betrachteten Angriffsmöglichkeiten bzw. Angriffstechniken herauszuarbeiten. Es wurden Merkmale wie die

Sammlung von Informationen über mögliche Opfer im Vorfeld des Angriffs, der Zugriff der Angreifer auf das Netzwerk der Opfer, die Ausnutzung von Schwachstellen, die spezifische Ausführung des Angriffs auf einen ausgesuchten Personenkreis oder bestimmte Organisationen, der Versuch des Vertrauensaufbaus durch die Angreifer, die Installation von Schadsoftware, die Unvorsichtigkeit von Mitarbeitern, die Nutzung eines Angriffs auf die Lieferkette, ein fehlendes Sicherheitsbewusstsein oder der Aufbau einer Drohkulisse und die Manipulation der Opfer identifiziert, die Gemeinsamkeiten in mehreren der betrachteten Angriffsmöglichkeiten und Angriffstechniken aufweisen. Generell lässt sich durch die vergleichende Betrachtung der ausgewerteten Cyberangriffe unter Mitwirkung unwissentlicher Innentäter sagen, dass viele der identifizierten Merkmale Gemeinsamkeiten für mehrere der betrachteten Angriffsmöglichkeiten und Angriffstechniken aufweisen.

Da Social Engineering sowohl einen der am häufigsten angewandten als auch erfolgreichsten Angriffsvektoren im Bereich der Cybersicherheit darstellt, aber aufgrund der Vielzahl bekannter Techniken des Social Engineering nicht alle diese Techniken im Rahmen des Vorhabens umfassend betrachtet werden konnten, wurden 26 Social Engineering Techniken kurz dargestellt. Bei diesen Techniken handelt es sich z. B. um DNS-Spoofing, Baiting, Media Dropping, CEO Fraud, Tailgating, MFA Bombing oder SEO-Poisoning. Ein Teil dieser 26 Techniken wurde im Rahmen der acht detailliert betrachteten Angriffsmöglichkeiten bzw. Angriffstechniken bereits beschrieben, für die meisten der kurz dargestellten Techniken des Social Engineering erfolgte im Rahmen dieses Vorhabens allerdings keine ausführliche Betrachtung. Diese könnte im Rahmen eines Nachfolgevorhabens erfolgen.

Die Bearbeitung weiterer Aspekte, die auf den in diesem Vorhaben betrachteten Aspekten aufbauen, sowie eine weitere Vertiefung der im Rahmen dieses Vorhabens durchgeführten grundlegenden Arbeiten zum Themenfeld von Cyberangriffen unter Mitwirkung eines unwissentlichen Innentäters könnte ebenfalls im Rahmen eines Nachfolgevorhabens erfolgen. Weitere zu bearbeitende Aspekte sind beispielsweise die Recherche, Beschreibung und Diskussion von Detektionsmöglichkeiten in Bezug auf derartige Cyberangriffe oder die Recherche, Beschreibung und Diskussion von vorbeugenden Sicherungsmaßnahmen in Bezug auf unwissentliche Innentäter.

Zu den zum Themenfeld Social Engineering sowie Cyberangriffen unter Mitwirkung unwissentlicher Innentäter erzielten Arbeitsergebnissen wurde der separate Bericht

„Einsatz von Social Engineering und Handlungen unwissentlicher Innentäter im Rahmen von Cyberangriffen“ /GRS 26d/ erstellt.

2.5 Methoden zur Abschätzung der Anpralllast

Für die Berechnung der Anpralllast von Fahrzeugen, u. a. zur Auslegung von Durchfahrschutzeinrichtungen, existieren verschiedene gängige Möglichkeiten. Bereits die Norm DIN EN 1991-1-7:2010-12 (Eurocode 1) /DIN 10a/ für außergewöhnliche Einwirkungen bietet mehrere Möglichkeiten. Der neue Nationale Anhang zum Eurocode 1 (DIN EN 1991-1-7/NA:2019-09) /DIN 19/ wurde in erster Linie bezüglich der verschiedenen Anpralllasten (Schiffs-, Zug-, Straßenfahrzeuganprall) überarbeitet. Für die nachfolgend herangezogenen Berechnungsmethoden für Straßenfahrzeuge ergab die Prüfung der Nationalen Anhänge DIN EN 1991-1-7/NA:2010-12 /DIN 10b/ und DIN EN 1991-1-7/NA:2019-09 /DIN 19/ keine Änderungen, da der informative Anhang C von /DIN 10a/ für Straßenfahrzeuge, auf den sich DIN EN 1991-1-7/NA /DIN 10b/ und DIN EN 1991-1-7/NA /DIN 19/ weiterhin beziehen, bislang unverändert geblieben ist. Allerdings befindet sich derzeit der gesamte Eurocode 1 /DIN 10a/ in Überarbeitung. Daher sollte dieses Thema in den nächsten Jahren weiter beobachtet werden.

Der in der EU aktuell gültige Eurocode 1 /DIN 10a/ bietet im informativen Anhang C bislang hauptsächlich zwei Varianten zur dynamischen Anprallberechnung. Die eine Variante bezieht sich auf Anhang C.2.1 zur Berechnung des harten Stoßes, deren Ergebnisse i. d. R. auf der sicheren Seite liegen, und die andere gemäß Anhang C.2.2 zur Berechnung des weichen Stoßes. Auch wenn beide Varianten in Deutschland nach Ansicht der nationalen Anhänge /DIN 10b/ und /DIN 19/ im gewöhnlichen Bauwesen in der Regel nur für eine Vorbemessung geeignet sind, so stellen die Berechnungsmöglichkeiten des Anhangs C dennoch wichtige Berechnungsmethoden der Anpralllast dar, die für die Festlungen von Lastannahmen oder zur Bewertung von Durchfahrschutzeinrichtungen für die Anlagensicherung als sehr hilfreich erachtet werden. Abschnitt 4.3.1 wurde fachlich überarbeitet.

Weitere Berechnungsmöglichkeiten von Anpralllasten außerhalb des Eurocodes betreffen u. a. alte Genehmigungsunterlagen, deren Gültigkeit bzw. Richtigkeit einzuschätzen ist, verschiedene Regelwerke außerhalb der EU und detailliertere Methoden wie das Modell PM320 der PollerMax GmbH oder numerische Simulationen. In der älteren Norm DIN 1072 von 1985 /DIN 85/ sind z. B. keine Formeln zur Berechnung der Anprallast

angegeben, sondern nur Werte. Bei der Anwendung verschiedener Methoden wurden starke Abweichungen der Ergebnisse festgestellt, wobei deren Ursachen nicht sofort offensichtlich sind.

Auf Basis von Erkenntnissen zu den Ursachen für stark abweichende Ergebnisse bei der Anwendung verschiedener Methoden zur Berechnung der Anpralllast von Fahrzeugen sollte eine begründete Auswahl von solchen Methoden getroffen werden, die die Realität am besten abbilden, und möglichst auch eine begründete Auswahl von geeigneten Eingangswerten für die Anwendung dieser Methoden abgeleitet werden.

2.5.1 Erkenntnisse aus Veranstaltungen

Für den Erkenntnisgewinn im Zusammenhang mit Durchfahrschutzeinrichtungen und Anpralllasten wurde u. a. die Teilnahme an nationalen und internationalen Veranstaltungen genutzt, insbesondere:

- Seminar des VfS zu Durchfahrschutzeinrichtungen in Berlin am 22. und 23.10.2024: Informationen u. a. zur Auslegung, zu verschiedenen Methoden zur Umrechnung der kinetischen Energie eines Fahrzeugs auf den Durchfahrschutz, zu Versuchsergebnissen
- jährlicher VfS-Kongress in Leipzig am 06. und 07.05.2025 unter dem Motto „Gemeinsam für eine sichere Welt“: Themen u. a. Erkenntnisse aus Anschlägen und Nutzung von Fahrzeugen als Waffe, Sammeln von Informationen, Knüpfen von Kontakten (Reisebericht /GRS 25a/)

Auf dem o. g. Seminar des VfS wurde eine Reihe von Erkenntnissen im Zusammenhang mit Fahrzeuganschlägen und zur Auslegung von Durchfahrschutzeinrichtungen gewonnen. Auf dem VfS-Kongress wurden u. a. spezifische Erkenntnisse zur Nutzung von Fahrzeugen als Waffe gewonnen. Diese Erkenntnisse sind nachfolgend zusammengestellt.

Bedrohung durch Fahrzeuganschläge

Die Anzahl von Straftaten mit Fahrzeugen, sogenannte Überfahrtaten, bei denen Fahrzeuge als Waffe genutzt werden, ist in den letzten Jahren international deutlich gestiegen (siehe Vortrag Yan St-Pierre, Experte aus Kanada zur internationalen Bedrohungslage in Abb. 2.1).

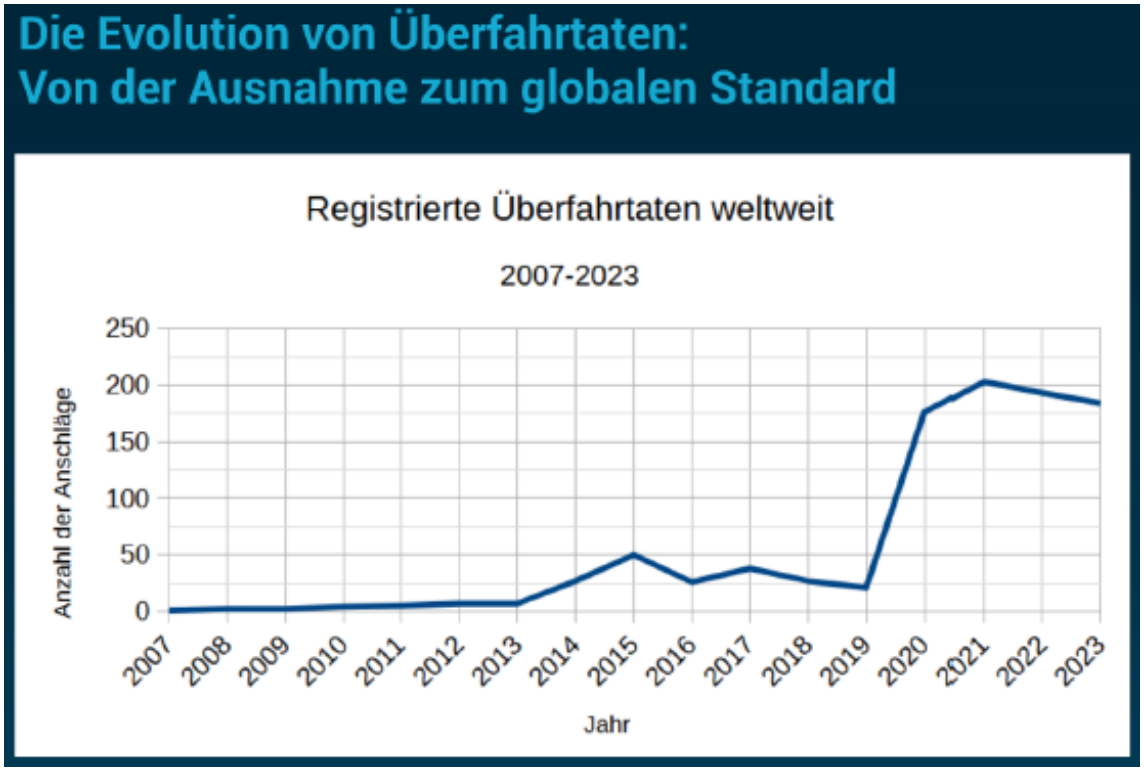

Abb. 2.1 Entwicklung von Überfahrtaten mit Fahrzeugen als Waffe /VFS 24/

Demnach wurde u. a. eine Diversifizierung von Akteuren und Motiven beobachtet: In den Jahren von 2007 – 2016 wurden Fahrzeuganschläge fast ausschließlich von muslimischen Extremisten oder im Zusammenhang mit dem Israel-Palästina-Konflikt verübt. In den Jahren 2017 – 2018 nahm die Nutzung durch rechtsextreme Akteure zu. Ab dem Jahr 2019 wurden Fahrzeuganschläge zum Standard für politische Gewalt, versuchte Massenmorde oder absichtliche Tötungsversuche.

Weiterhin wandelte sich die Zielauswahl von statischen zu mobilen Zielen und von spezifischen Orten mit willkürlichen Opfern zu beweglichen Zielgruppen. Die meisten Fahrzeuganschläge richteten sich auf Gebäude, meist für Raubüberfälle, aber auch gegen symbolische Werte.

Aktuell werden bei Anschlägen auch zwei Fahrzeuge gleichzeitig eingesetzt.

Relevante Fahrzeugmassen

International wird derzeit als maßgebender Fall der Anprall eines monolithischen Lastkraftwagens (Lkw) mit 30 t Gesamtgewicht (z. B. Muldenkipper) mit einer Geschwindigkeit von 80 km/h betrachtet, was zu einer bemerkenswert hohen kinetischen Energie von

> 7400 kJ führt. Gemäß Referent C. Schneider (als Deutschlands einziger, Stand 2024, international zugelassener Sachverständiger und Fachplaner für Zufahrtsschutz des Register of Security Engineers and Specialists (RSES)[1] für Hostile Vehicle Mitigation (HVM), der u. a. für den Durchfahrschutz am Breitscheidplatz in Berlin zuständig war) war im Jahr 2024 weltweit nur ca. zehn bis zwölf Durchfahrschutzeinrichtungen in Betrieb, die solche Lasten abtragen können. Derartige Durchfahrschutzeinrichtungen wurden erst vor wenigen Jahren entwickelt und zertifiziert.

Lkw mit einer höheren Fahrzeugmasse als beim o. g. maßgebenden Fall existieren demnach nur als Sattelzüge. Das Sattelgelenk führt beim praktischen Aufprall zum Ausknicken des Sattelzuges am Sattelgelenk. Dadurch verhält sich der Sattelzug wie zwei Fahrzeuge (Sattelzugmaschine und Sattelauflieger) und muss anders betrachtet werden als ein monolithischer Lkw. Beim Anprall eines Sattelzugs geht ein großer Teil der kinetischen Energie seitlich weg. Auf der sicheren Seite liegend kann jedoch angenommen werden, dass es nicht zu einem signifikanten Ausknicken kommt.

Modus operandi für Fahrzeuganschläge

Lkw sind sehr einfach zu stehlen. Entsprechende In-situ-Versuche ergaben einen zeitlichen Aufwand von wenigen Minuten.

Lkw können sehr einfach, z. B. mit einem Stein und Kabelbindern, als unbemannte Fahrzeuge eingesetzt werden, um Verluste unter den Tätern zu vermeiden. Eine Suizidbereitschaft von Tätern ist damit nicht erforderlich.

Das automatische Bremssystem der modernen Lkw kann sehr einfach durch Aufkleben von Pflastern o. ä. außer Betrieb gesetzt werden.

Auslegung von Durchfahrschutzeinrichtungen

Viele Durchfahrschutzeinrichtungen, die durch statische Berechnungen mit Ersatzlasten nachgewiesen wurden, hielten im Versuch nicht stand.

---

[1] Das RSES ist global anerkannt, länderübergreifend und herstellerunabhängig. Es wird staatlich von der Britischen National Protective Security Authority (NPSA) gefördert und von der Institution of Civil Engineers (ICE) verwaltet. Das RSES gilt weltweit als sehr hoher Standard für die Zulassung von nachweisbar qualifizierten Ingenieuren und Spezialisten zur Planung und Durchführung von Maßnahmen der technischen Gefahrenabwehr.

Der dynamische Widerstand ist manchmal kleiner als der statische Widerstand (z. B. beim sogenannten Cavalese-Effekt[2]).

Bei der Nutzung von Gräben als Durchfahrschutz muss die erforderliche Breite in Abhängigkeit der Geschwindigkeit mit der Parabelformel geprüft werden, denn bei unzureichender Grabenbreite ist sonst das Überspringen möglich. Derartige Berechnungen können bei nicht horizontal verlaufendem Gelände z. B. auf Basis der Gleichung für den sogenannten schiefen Wurf durchgeführt werden, siehe Abb. 2.2. Die Geländesteigung wird mit dem Winkels α beschrieben, die Wurfweite mit x_w und die Erdbeschleunigung mit g.

$$x_w = \frac{v_0^2}{g} sin2\alpha$$

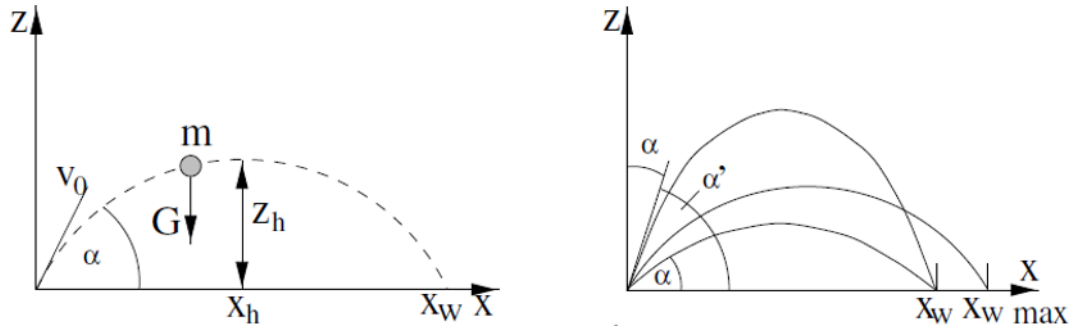

Abb. 2.2 Schiefer Wurf und Wurfparabel für verschiedene Wurfwinkel

Experimentelle Versuche haben gezeigt, dass es ein schneller SUV schafft, bei ebenem Gelände einen 4 m breiten Graben zu überspringen.

Als wichtige neue internationale Norm wurde die ISO 22343 von 2023 identifiziert, die in deutsche Übersetzung seit April 2025 verbindlich existiert, und sich in die beiden Teile 1 /DIN 25a/ und 2 /DIN 25b/ aufgliedert. Sie stellt eine anerkannte Regel der Technik dar. Das sogenannte Performance Rating von Durchfahrschutzprodukten enthält gemäß ISO 22343 auch den Trümmerflug. Der wurde gemäß eines älteren International Workshop Agreements (IWA), IWA14-1:2013 /ISO 13a/ und IWA14-2:2013 /ISO 13b/, noch nicht berücksichtigt.

[2] Militärjets haben dreimal Seilbahnseile – zuletzt 1998 in Cavalese – gekappt, ohne selbst abzustürzen. Das ist statisch gesehen unmöglich bei der Dicke und Festigkeit der Seile.

Derzeit sind international ca. 700 Durchfahrschutzprodukte auf dem Markt verfügbar, die gemäß der britischen Behörde für zivile Terrorvorkehr NPSA zertifiziert sind. Nach Aussage von Referent C. Schneider können Vorgaben der NPSA, die dem Stand von Wissenschaft und Technik entsprechen, von Behörden als Amtshilfe genutzt werden. Zertifikate einzelner Durchfahrschutzprodukte können dort ggf. bezogen werden. Die Registrierung der Durchfahrschutzprodukte ist für den Hersteller kostenlos.

Ermittlungsmöglichkeiten der Anpralllast:

Gemäß Nachfrage bei Experte C. Schneider sind derzeit mindestens drei gängige Methoden zur Umrechnung der kinetischen Energie eines Fahrzeugs beim Anprall auf Durchfahrschutzeinrichtungen zu beachten:

- Formel nach Popp (z. B. vom ursprünglichen Statiker für Durchfahrschutzeinrichtungen für die Nebenzufahrt in Gorleben genutzt)
- Eurocode 1 Teil 7 (DIN EN 1991-1-7/NA) /DIN 19/ zu hartem und weichem Stoß (Eingangswerte streuen stark, weitere Untersuchungen erforderlich)
- numerische Methoden

Täterprofil und -motivation für Überfahrtaten

Die Anzahl von Vorfällen mit Fahrzeugen als Waffe hat über die Zeit enorm zugenommen. Seit Beginn 2021 konnten ca. 700 Vorfälle weltweit verzeichnet werden, von denen etwa 40% aus Gründen persönlicher Verwirrung durchgeführt wurden und ca. 13% auf Terror zurückzuführen waren. Hauptziele waren hierbei die Polizei (18%) und Demonstranten (14%).

Deutschland ist weltweit unter den TOP-5-Ländern für Angriffe mit Fahrzeugen mit folgender Anzahl von Vorfällen: 10 x 2021, 21 x 2022, 23 x 2023, 13 x 2024, 2 x 2025. Hauptgründe für die Nutzung von Fahrzeugen als Waffe in Deutschland sind Straßenblockaden (45%), persönlicher Verwirrung (25%), häusliche Gewalt (13%) und Terror (4%). Dies zeigt, dass meist persönliche Gründe und Affekt Ursache für solche Vorfälle sind. Hauptziele in Deutschland waren demnach Demonstranten (48%), Zivilisten (15%), Partner (12%), Fußgänger (8%) und Polizei (2%).

Erkenntnisse für den Durchfahrschutz

Nach den ersten Aufrufen zu Überfahrtaten mit Fahrzeugen im Jahr 2010 durch den Islamischen Staat stieg ab 2013 die Anzahl derartiger Vorfälle exponentiell an. Nutzfahrzeuge sind effektive Terrorwaffen, da eine hohe Opferzahl mit einem geringen Aufwand erreicht werden kann. Eine Erkenntnis aus den Anschlägen in Magdeburg und München ist, dass diese hätten verhindert werden können. Allerdings verhindern Durchfahrschutzmaßnahmen wie Poller oder andere Fahrzeuge allein nicht das Durchdringen eines Nutzfahrzeugs. Zufahrtschutz unterliegt der Bauordnung, sodass in erster Linie bauliche Maßnahmen bereits bei der Ausgestaltung der Bereiche getroffen werden müssen, und erst in zweiter Linie sollen technische Hindernisse hinzugezogen werden.

2.5.2 Erkenntnisse aus Recherchen

Nachfolgend sind Informationen und Instrumente (Rechentools) von einer Plattform des Joint Research Centre (JRC) /JRC 25/ systematisch zusammenzustellt, die i. A. in Bezug auf den Durchfahrschutz hilfreich sein können. Die wissenschaftliche Kernkompetenz von JRC liegt historisch gesehen auf der Beurteilung von schnellen dynamischen Phänomenen. Die Forschungstätigkeiten des JRC unterstützen den politischen Rahmen der EU (Strategie der Union (2020), die EU-Agenda zur Terrorismusbekämpfung (2020) und den Aktionsplan zur Unterstützung des Schutzes des öffentlichen Raums (2017)) mit besonderem Schwerpunkt auf dem Schutz des öffentlichen Raums vor Terroranschlägen. Sie befasst sich auch mit Aspekten des Schutzes von KRITIS im Einklang mit der EU-Richtlinie über die Resilienz kritischer Einrichtungen. Die Bedrohungslage in der heutigen Zeit ist sehr dynamisch und die terroristischen Angriffstaktiken werden ständig weiterentwickelt und optimiert, was angepasste Schutzmaßnahmen auf der Grundlage der zugrundeliegenden wissenschaftlichen Forschung erforderlich macht. Daher hat sich das JRC neben den schnellen dynamischen Phänomenen auch weiteren zugehörigen Themen gewidmet wie Fahrzeuge als Waffe, Unbemannte Fahrzeugsysteme, Schwachstellen und Risikobewertung sowie terrorismus- und extremismusbezogene Datenerhebung.

Das JRC bietet auf seiner Plattform /JRC 25/ verschiedene sicherungstechnische Instrumente an. Die Registrierung auf der Seite ist erforderlich, um Zugang zu den Instrumenten zu erhalten. Bei der Registrierung empfiehlt sich die Zwei-Faktoren-Authentifizierung über die Authentifizierungsapp „mobiler EU-Login“. Einige Instrumente wie **V**erhicle **SPE**ed **E**valuation and **D**ynamics Assessment (V-SPEED) müssen vorher angefragt und

freigeschaltet werden. Diese Instrumente sind kleine Rechentools, die ihre Benutzeroberfläche direkt auf der Webseite haben. Zu den auf /JRC 25/ aufgeführten Instrumenten gehören:

- BLADE
- V-SPEED
- EUROPLEXUS
- Urban Blast Simulation
- Sec Data (Terrorismus, Extremismus und Vorfälle mit unbemannten Luftfahrtsystemen)
- Veröffentlichungen und Informationen
- Generische Fahrzeugmodelle
- Numerische Simulationen im Bereich HVM

Im Folgenden werden Informationen zu den einzelnen Instrumenten aufgeführt, die einen Bezug zum Durchfahrschutz haben.

- V-SPEED
  - Bewertung der Höchstgeschwindigkeit von Bedrohungsfahrzeugen anhand der städtischen Straßengeometrie (OpenStreetMap)
  - manuelle Eingabe der Angriffsstrecke möglich, falls Strecke in OpenStreetMap nicht eingezeichnet
  - Eingrenzung bedrohender feindlicher Fahrzeuge anhand von Geschwindigkeit und Masse
  - Anwendung folgt der Logik einer Fahrzeugdynamikbewertung (Vehicle Dynamics Assessment, VDA)
  - je nach Menge der zu berechnenden Angriffswege ist der zeitliche Rechenaufwand größer, sodass einzelne Abfragen sinnvoller sind

- EUROPLEXUS
  - Bewertung der Leistung von Strukturmodellen unter Explosions- und Aufprallbelastungen
  - Simulationssoftware zur Analyse von schnellen transienten Phänomenen
    - Aufprall
    - Explosion
    - Fluid-Struktur-Wechselwirkung
  - Berücksichtigung von
    - geometrischer Nichtlinearität (große Verschiebung bzw. Dehnung)
    - Nichtlinearität von Materialien (Plastizität, Viskoplastizität)
  - Programm verwendet expliziten Algorithmus (Zentraldifferenz)
  - verschiedene Methoden möglich oder in Entwicklung
    - Finite Elemente Methode (FEM)
    - Smoothed Particle Hydrodynamics (SPH)
    - Spektral Elemente
    - Diffuse Elemente
  - Umfangreiche Bibliothek von Materialtypen für
    - Festkörper
    - Flüssigkeiten
    - spezielle Medien
  - verschiedene Beschreibungen im Code möglich
    - Lagrangsche Beschreibung (Strukturbereich)
    - Eulersche Beschreibung (Fluidprobleme)
    - Arbitrary Lagrangsche-Eulersche Beschreibung (Fluid-Struktur-Interaktion)
  - auf /JRC 25/ lediglich Weiterleitung zur offiziellen Seite

    - Programm zum Downloaden unter: http://www-epx.cea.fr/index.php
        - eine abgespeckte Variante für Lehre und Wissenschaft ist erhältlich
        - eine Vollversion für Lehre und Wissenschaft bedarf eines Lizenzvertrags für Bildung und Forschung
        - eine kommerzielle Nutzung bedarf einer Extraanfrage (kostenpflichtig)
- Generische Fahrzeugmodelle
    - erstellt für numerische Aufprallsimulationen gegen Fahrzeugsicherheitsbarrieren
    - entspricht den Normen CEN/TR 16303 und ISO 22343
    - validiert gegen Crash-Experimente
    - einstellbare Parameter: Abmessungen, Masse, Crash-bedingte Steifigkeit
        - N1 Fahrzeugmodell
        - N2A/N3D Fahrzeugmodell
        - N3G Fahrzeugmodell
    - frei zugänglich
- Numerische Simulationen HVM
    - kein separates Instrument auf /JRC 25/, sondern Kompetenz von JRC
    - Nutzung von LS-Dyna
    - Simulation der Interaktion zwischen Fahrzeugbarrieren und der Bodenbeschaffenheit im Fall eines Aufpralls mit Fahrzeugen
    - Variation der Fahrzeugparameter wie Raddurchmesser, Fahrzeuglänge, Bodenfreiheit oder Ladung
    - Bewertung unterschiedlicher Aufprallgeschwindigkeiten, Aufprallwinkel und Standortbedingungen

Zusammenfassend kann festgehalten werden, dass JRC im Bereich dieses Themas ein sehr umfassendes Wissen hat, auf der Plattform /JRC 25/ jedoch nur ein geringer Teil preisgegeben wird. Zu den verschiedenen Instrumenten gibt es Factsheets und teilweise

Tutorials, die eine Bedienung deutlich erleichtern. Das Instrument V-SPEED ist für eine erste Abschätzung hilfreich, das nach Freigabe zugänglich ist. Beim kommerziell erhältlichen Programm EUROPLEXUS ist eine vertiefte Bewertung durch die Simulationsabteilung der GRS sinnvoll, was vollumfänglich erst nach Erhalt einer Lizenz möglich ist, da die Funktionen in der Basisvariante eingeschränkt sind. Eine Einschätzung der Kompetenz von JRC hinsichtlich der Simulation im Bereich HVM ist nicht möglich, da diese Instrumente nicht auf /JRC 25/ zugänglich sind. Es wird erwähnt, dass auf der Plattform /JRC 25/ auch Instrumente aufgeführt werden, die aktuell in der Entwicklung sind. Möglich ist, dass diese Instrumente nach erfolgreicher Erprobungsphase auf der Plattform zugänglich sein werden.

Zur Klärung von Ursachen für die teils starken Abweichungen von Berechnungsergebnissen bei der bisherigen Anwendung verschiedener Methoden Ansätze zur Abschätzung der Anpralllast wurden diese und deren Grundlagen im Rahmen dieses Vorhabens miteinander verglichen, und erste Gründe wurden erarbeitet, die aber in einem Nachfolgevorhaben vertieft und abgesichert werden sollten.

Während manche Methoden auf Basis der Annahme starrer Köper oft mit konservativen Ersatzkräften arbeiten, nutzen andere Methoden wie die ISO 22343 /DIN 25a/ und /DIN 25b/ reale Energiebetrachtungen und physische Crash-Testergebnisse, was die starken Abweichungen in den Lasten erklären kann. Während die physikalische Energie dieselbe bleibt, führt die Frage, wie diese kinetische Energie in den verschiedenen Normen/Methoden abstrahiert wird (insbesondere statische Kraft vs. dynamische Verformung), ggf. zu stark abweichenden Bemessungswerten. Einige Normen rechnen mit starren Lkw-Fronten, andere berücksichtigen die Elastizität moderner Knautschzonen, was die resultierende Stoßkraft massiv reduziert.

Darüber hinaus sind Ursachen für die Unterschiede der berechneten Werte von Anpralllasten in den unterschiedlichen Sicherheitskonzepten und Modellvereinfachungen zu suchen. So nimmt der Eurocode für Standardstraßen andere Fahrzeuggewichte und Anprallgeschwindigkeiten an als beispielsweise amerikanische Richtlinien wie die des American Association of State Highway and Transportation Officials (AASHTO).

Die o. g. Ursachen sollten in einem Folgevorhaben näher untersucht und abgesichert werden, damit in einem weiteren Schritt Empfehlungen für anzuwendende Normen/Methoden gegeben werden können.

2.5.3 Abgeschlossene Arbeiten

Folgende Arbeiten konnten im Rahmen dieses Vorhabens abgeschlossen werden:

- Recherche zu gängigen Methoden, Identifizieren der neuen internationalen Norm IWA14-1:2013 /ISO 13a/ und IWA14-2:2013 /ISO 13b/, ISO 22343 Teile 1 /ISO 23a/ und 2 /ISO 23b/ von 2023 bzw. von 2025 als deutsche Fassung /DIN 25a/ und /DIN 25b/ sowie Durcharbeitung und Zusammenstellung von Erkenntnissen
- Recherche zu Experimenten in GRS-Datenbanken bzw. in Ergebnisberichten zu Experimenten, bei der keine hilfreichen Erkenntnisse bzgl. detaillierter Lasten bzw. deren Berechnung abgeleitet werden konnten

Gegenstand der Recherche zu gängigen Methoden zur Abschätzung und Berechnung der Anpralllast von Fahrzeugen sowie zu dafür vorhandenen Versuchsergebnissen waren insbesondere normative Vorgaben, detailliertere Methoden, numerische Simulationen und Publikationen zur Entwicklung und Anwendung von entsprechenden Methoden sowie einer begrenzten Anzahl von Versuchen. Weitere internationale Regelwerke wie die des AASHTO könnten ergänzend in einem Nachfolgevorhaben näher untersucht werden.

Arbeiten zur Klärung von Ursachen für starke Abweichungen zwischen Methoden konnten im Rahmen dieses Vorhabens zum Teil abgeschlossen werden.

Kontakte zu Experten für Methoden zur Berechnung der Anpralllast und der Auslegung von Durchfahrschutzeinrichtungen wurden für eine Fortsetzung der Arbeiten angebahnt.

3 Ereignisse

Die Sicherstellung des erforderlichen Schutzes gegen SEWD basiert unter anderem auf einer aktuellen und detaillierten Kenntnis der Bedrohungslage. Diese wird auch durch Ereignisse mit Relevanz für Sicherung und Cybersicherheit sichtbar. Daher ist es notwendig, entsprechende Ereignisse auf nationaler und internationaler Ebene regelmäßig zu sichten und auch einer Erstbewertung zu unterziehen, um die Relevanz für die Sicherung und die Cybersicherheit einschätzen zu können. Die als relevant erkannten Ereignisse sollten umfassend ausgewertet werden. Die Analysen von derartigen Ereignissen 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 BMUKN erfolgen.

3.1 Ereignisse mit Sicherungsrelevanz

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, spezielle Datenbanken etc. wurden regelmäßig gesichtet. Als eine Recherchequelle wurde dabei die Incident and Trafficking Database (ITDB) der IAEO über das BMUKN 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 der DESi sortiert, extrahiert und weiterverwendet werden.

Die in der DESi definierten Kategorien wurden in den Abschlussberichten der Vorläufervorhaben FKZ 4718R01611 /GRS 21/ und FKZ 4721R01611 /GRS 24a/ aufgeführt und beschrieben. Strukturelle Änderungen oder Änderungen an den verschiedenen Kategorien wurden im vergangenen Vorhaben nicht durchgeführt. Teilweise wurden bestehende Einträge auf der Basis von neuen Informationen angepasst.

Weitere relevante Ereignisse mit Bezug zu Kernmaterial, radioaktiven Stoffen, kerntechnischen Anlagen und der Beförderung radioaktiver Stoffe wurden recherchiert, ausgewählt, in die 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 die 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 Relevanz für die Cybersicherheit zu nennen.

Beispiele für sicherungsrelevante Ereignisse in den letzten Jahren lassen sich vor allem im Rahmen der Kriege zwischen der Ukraine und Russland sowie zwischen Israel oder den USA und dem Iran finden. Sicherungsrelevante Ereignisse in der Ukraine oder in Russland stehen oft in Zusammenhang mit Drohnen. So kommt es sehr häufig zu Sichtungen von Drohnen in der Nähe von ukrainischen Kernkraftwerken. Am 14.02.2025 schlug eine russische Drohne iranischer Bauart (Geran-2) in dem New Safe Confinement von Reaktor 4 des Kernkraftwerks Tschernobyl ein, wobei ein Loch von ca. 15 m² entstand. Die Wand des Turbinengebäudes von Block 6 des Kernkraftwerks Saporischschja wurde bei einem Drohneneinschlag am 30.05.2026 beschädigt. Sicherungsrelevante Ereignisse im Iran sind meistens militärische Angriffe von Israel und/oder den USA mit Fliegerbomben oder Marschflugkörpern. Ziele waren im Juni 2025 die Atomanlagen Natanz und Fordo, das Nuklearforschungszentrum Isfahan sowie der Schwerwasserreaktor IR-40 bei Arak.

Auch außerhalb von offenen Kriegen kommt es oft zu Drohnenüberflügen über kerntechnischen Anlagen. Im August 2024 wurden an mehreren Tagen schnell fliegende Drohnen über dem ChemCoast Park in Brunsbüttel, in dem sich auch das Kernkraftwerk befindet, gesichtet. Es wird spekuliert, dass es sich um russische Drohnen des Typs Orlan-

10 handelt. Aus den USA wird berichtet, dass am 08.01.2025 vier bis fünf Drohnen das Kernkraftwerk Prairie Island überflogen. Am 09.11.2025 wurden mindestens drei Drohnen über dem Kernkraftwerk Doel in Belgien gesichtet.

Bereits am 04.11.2023 fuhr ein 66-jähriger Mann mit seinem Auto (Toyota Camry) durch das Tor des Anlagengeländes des Kernkraftwerks Oconee (USA), versuchte Mitarbeitende des Objektsicherungsdienstes zu rammen und verließ das Gelände, indem er durch einen Zaun fuhr. Der Fahrer wurde am nächsten Tag in einem leerstehenden Gebäude gefunden und festgenommen. Bei der Festnahme führte er 1,36 g Methamphetamin mit sich.

Die Erkenntnisse aus der Erstbewertung der in die 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 auf generischer Basis.

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 DESi. Dabei wurde versucht, bei jedem dokumentierten Ereignis Angaben in allen vordefinierten Kategorien in der DESi zu machen. Anhand dieser Kategorien können Informationen aus der DESi extrahiert und graphisch dargestellt werden, was bereits in /GRS 21/ und /GRS 24a/ illustriert wurde. Da in die DESi seitdem weitere Ereignisse aufgenommen wurden, werden im Folgenden die aktualisierten Beispiele dargestellt.

In folgender Abbildung (Abb. 3.1) ist die zeitliche Verteilung der Ereignisse auf die sechs in der DESi berücksichtigten Dekaden seit dem Jahr 1961 sowie aktuelle laufende Dekade 2021 – 2026 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.

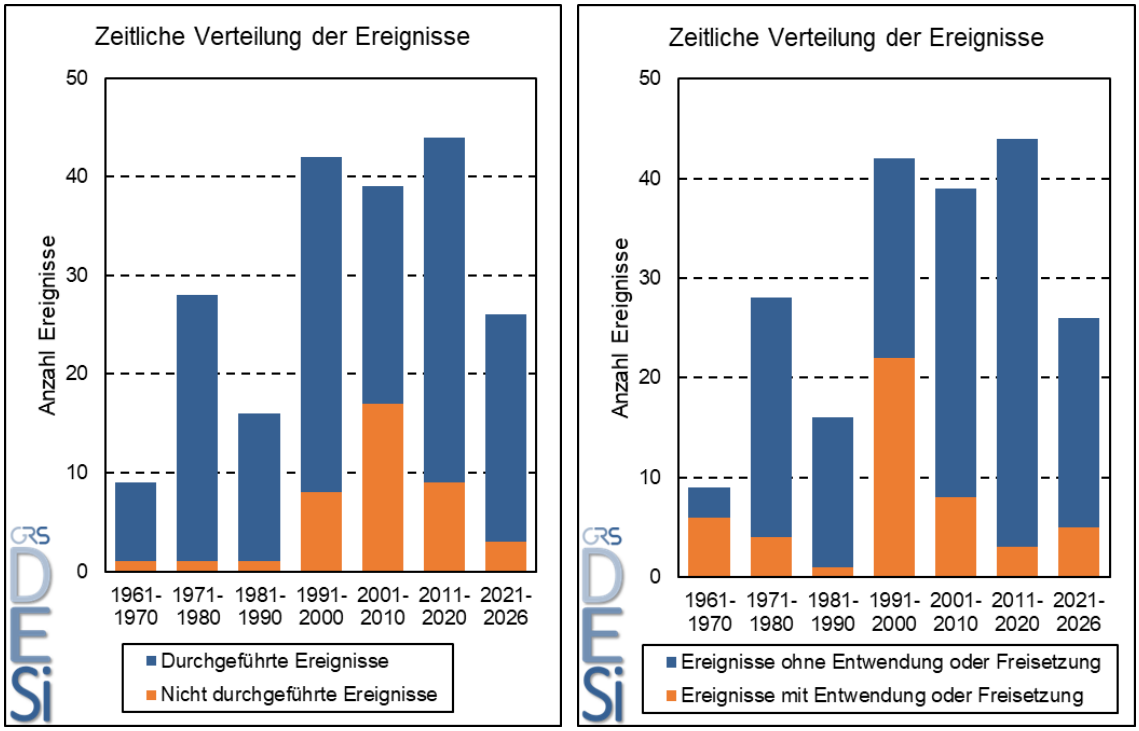

Abb. 3.1 Graphische Darstellungen der DESi-Einträge als zeitliche Verteilungen

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.

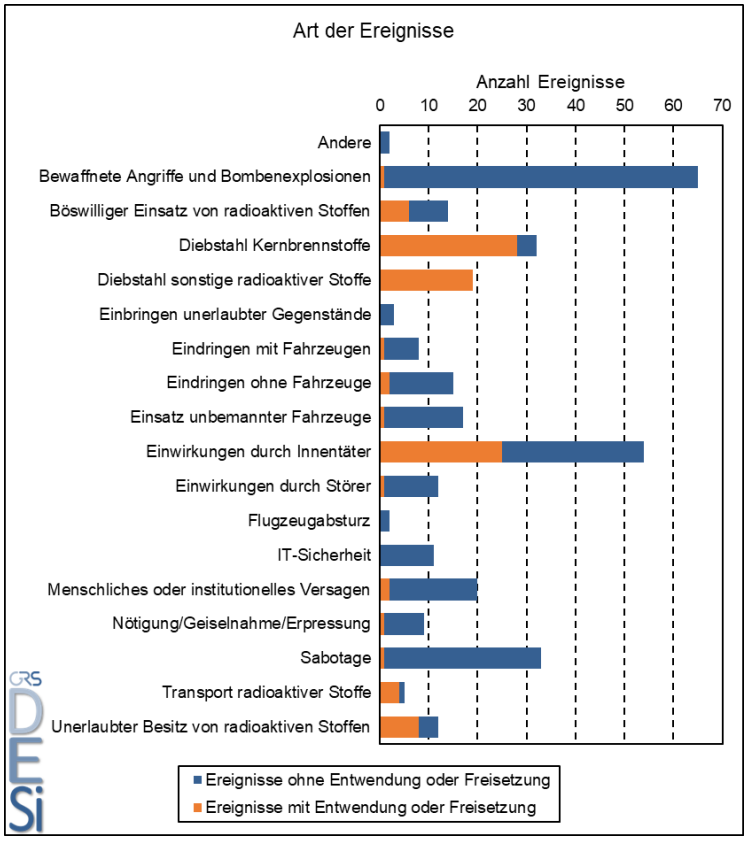

Abb. 3.2 Graphische Darstellung der DESi-Einträge hinsichtlich der Arten der Ereignisse

In Abb. 3.3 sind die Häufigkeiten der in der DESi genannten Tätermotive graphisch dargestellt. Dabei wird zwischen durchgeführten und nicht durchgeführten Ereignissen unterschieden. In dieser Kategorie sind in der DESi Mehrfachnennungen möglich. Für eine tiefere (insbesondere statistische) Analyse sind diese Ergebnisse nicht geeignet. Abb. 3.3 dient aber als Eindruck zu den in der DESi aufgenommenen Ereignissen.

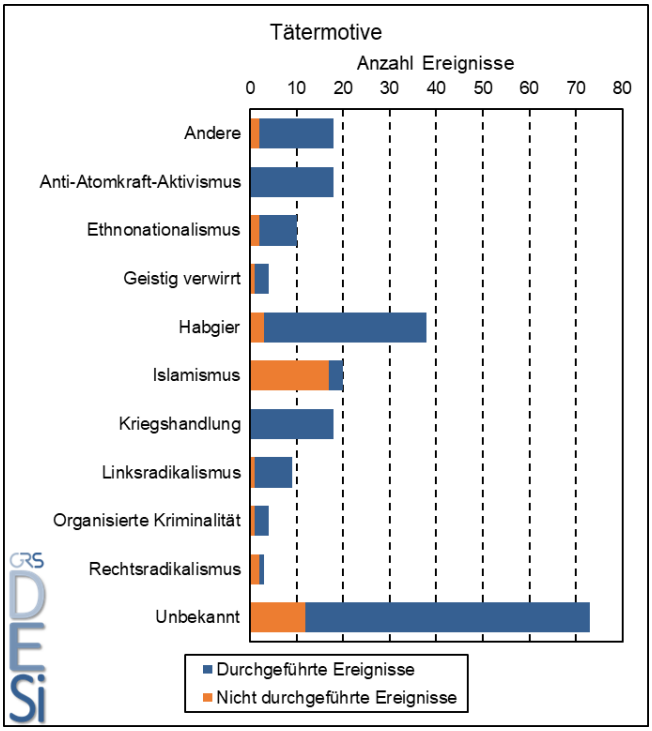

Abb. 3.3 Graphische Darstellung der DESi-Einträge hinsichtlich der Tätermotive

Diese exemplarischen Auswertungen der in der DESi enthaltenen Informationen sollen den praktischen Nutzen der DESi illustrieren. Es wurde der Stand der DESi im Mai 2026 verwendet. Die DESi wird kontinuierlich gepflegt und weiterentwickelt. Dafür werden regelmäßig Quellen gesichtet, bestehende Einträge in der DESi aktualisiert und neue Einträge ergänzt.

3.2 IT-Bedrohungslage

Für alle kerntechnischen Anlagen, Einrichtungen, Umgänge und Tätigkeiten ist der Schutz gegen SEWD essenziell. Dies schließt physische Angriffe und Cyberangriffe ebenso ein wie kombinierte Angriffe. Zur Gewährleistung des erforderlichen Schutzes sind Maßnahmen der Sicherung und auch der Cybersicherheit notwendig, für deren Auswahl und Auslegung sowohl die aktuelle Bedrohungslage als auch die tatsächliche Angriffsoberfläche zu berücksichtigen sind.

Als Summe aller potenziellen Angriffsvektoren fasst die Angriffsoberfläche alle Punkte und Faktoren zusammen, an denen ein Angreifer ansetzen könnte, um Angriffsschritte durchzuführen (z. B. in das interne Netzwerk einzudringen, Manipulationen vorzunehmen, Auswirkungen hervorzurufen oder Inhalte zu exfiltrieren). Hierzu zählen z. B.:

- Grad der Digitalisierung in allen Bereichen
- Einsatz programmierbarer und rechnerbasierter industrieller Steuerungssysteme sowie anderer IT-Systeme
- Einsatz von Remote-Verbindungen für z. B. Bedienung, Wartung, Inspektion
- Ausgliederung sensibler Dienstleistungen
- beteiligte Lieferketten
- softwarebedingte Alterungseffekte
- Einsatz von Cloudlösungen, rechnergestützten Überwachungswerkzeugen und KI-basierten Anwendungen

Hieraus wird deutlich, dass die Angriffsoberfläche sich für alle konkreten Anlagen, Einrichtungen, Umgänge und Tätigkeiten unterscheidet und sich individuell mit der Zeit verändert. Aufgrund einer Vielzahl von Faktoren wie der fortschreitenden Digitalisierung und der stetigen Erweiterung von Funktionalitäten, der zunehmenden Vernetzung unter den einzelnen IT-Systemen und auch nach außen, der zunehmenden Auslagerung sensibler Informationen und Dienstleistungen sowie der wachsenden Verzweigung der beteiligten Lieferketten von IT-Systemen, IT-Dienstleistungen und relevanten Hardware und ihrer Abhängigkeiten untereinander haben in den vergangenen Monaten und Jahren dazu geführt, dass Angriffsoberflächen auch im nuklearen Bereich typischerweise deutlich größer, aber auch diffuser geworden sind.

Die aktuelle IT-Bedrohungslage spiegelt wider, wozu potenzielle Angreifer derzeit in der Lage sind und was sie antreibt. Zentrale Punkte sind dabei die Fähigkeiten, Kenntnisse und Ressourcen potenzieller Angreifer sowie ihre Motivation. Im Gegensatz zur Angriffsoberfläche kann die IT-Bedrohungslage daher nicht direkt, sondern nur indirekt ermittelt werden. Relevante Aspekte beinhalten u. a.:

- beobachtete Cyberangriffe und IT-Sicherheitsvorfälle
- Bekanntwerden von Schadsoftwarekomponenten
- Bekanntwerden oder sogar Ausnutzung neu erkannter oder bisher nicht geschlossener Schwachstellen in industriellen Steuerungssystemen bzw. in für KRITIS relevanten IT-Systemen
- eingesetzte Angriffstechniken

- Verfügbarkeit von Angriffswerkzeugen und entsprechenden Dienstleistungen
- Aktivitäten von Angreifer-Gruppierungen

Sekundäre Aspekte betreffen die Rückschlüsse, die sich hieraus ergeben, vor allem in Bezug auf:

- Motivation der Angreifer
- Zweck der Angriffe
- Fähigkeiten, Kenntnisse und Ressourcen der Angreifer
- Kreis der potenziellen Angreifer

Die IT-Bedrohungslage entwickelt sich sehr dynamisch. Der kontinuierlichen Verfolgung und Auswertung der IT-Bedrohungslage, einerseits als Abbild von Fähigkeiten und Motivation potenzieller Angreifer und andererseits als Überblick über die von IT-Angreifern eingesetzten Taktiken, Techniken und Vorgehensweisen, kommt eine besondere Bedeutung zu. In diesem Vorhaben wurde daher die Entwicklung der IT-Bedrohungslage für industrielle Steuerungssysteme und KRITIS kontinuierlich verfolgt. Für dieses kontinuierliche Screening der IT-Bedrohungslage wurden einschlägige nationale und internationale Quellen herangezogen und Informationen insbesondere in Bezug auf die oben genannten Aspekte zusammengetragen. Dabei standen Insbesondere Schwachstellen mit Bezug zu industriellen Steuerungssystemen und KRITIS sowie bekannt gewordene IT-Sicherheitsvorfälle, IT-Angriffe einschließlich dabei verwendeter IT-Angriffswerkzeuge und Schadsoftwarekomponenten sowie Aktivitäten bekannter Angreifer-Gruppierungen (APTs) im Vordergrund. Im Rahmen dieses Screening wurden die für eine Bewertung der IT-Bedrohungslage einschlägigen oder repräsentativen Rechercheergebnisse identifiziert und mit Hilfe einer dafür entwickelten Struktur in einem lebenden Dokument zur IT-Bedrohungslage dokumentiert. Anschließend wurden die Ereignisse sowohl einzeln als auch vor dem Hintergrund der aktuellen IT-Bedrohungslage betrachtet. Das Ziel dabei war es, zu einer ersten Einschätzung der Bedeutung der jeweiligen Ereignisse für die aktuelle IT-Bedrohungslage zu gelangen. Hierzu wurde zunächst eine Kategorisierung der Ereignisse anhand von grundlegenden Merkmalen vorgenommen, wie:

- kerntechnischer Bezug
- Betroffenheit industrieller Steuerungssysteme

- Betroffenheit von Sicherungssystemen
- Beteiligung von Innentätern
- Angriffsschritte auf die Lieferkette
- physische Schäden

Um einerseits ein breites Gesamtbild der aktuellen IT-Bedrohungslage und andererseits einen Überblick über Änderungen der IT-Bedrohungslage und Hinweise auf Trends bei Cyberangriffen zu erhalten, wurden insbesondere in Bezug auf die bisherige IT-Bedrohungslage ungewöhnliche, abweichende oder neue Aspekte berücksichtigt. Auf dieser Basis erfolgte auch eine Priorisierung der Ereignisse in Bezug auf ihre Relevanz für die Bewertung der aktuellen IT-Bedrohungslage.

Diese Arbeitsweise stellt zum einen eine breite initiale Erfassung von möglicherweise relevanten Vorfällen und zum anderen eine schrittweise Verfeinerung und Herausarbeitung von relevanten Inhalten sicher. Beispielsweise waren im Jahr 2025 mehrere Tausend Angriffe, Schwachstellen und IT-Sicherheitsvorfälle Gegenstand des Screenings. Hiervon wurden mehrere Hundert Fälle einschließlich der zu ihrer Auswertung relevanten Hintergrundinformationen in die Dokumentation aufgenommen. Im Rahmen regelmäßiger Diskussionen dieser dokumentierten Ereignisse wurden hiervon 130 aufgrund ihrer Relevanz ausgewählt, kategorisiert und priorisiert.

Im Jahr 2024 wurden auf Basis der Ergebnisse des Screenings zahlreiche Ereignisse zu unterschiedlichen Aspekten der IT-Bedrohungslage analysiert wie:

- Supply-Chain-Angriffe im Zusammenhang mit IT-Dienstleistern und Netzwerküberwachungssystemen
  Bei Supply-Chain-Angriffen wird das eigentliche Angriffsziel nicht direkt angegriffen, sondern zunächst ein – oftmals weniger gut geschütztes – Zwischenziel in der Lieferkette in den Fokus genommen. Eine besondere Bedeutung kommt dabei Angriffen auf IT-Dienstleister zu, da die Lieferkette als Multiplikator bei der Verbreitung des Angriffs dient und dadurch eine Vielzahl potenzieller Opfer erreicht werden können. Angriffe auf ein Netzwerküberwachungssystem, welches eingesetzt wird, um Angriffe zu erkennen, kann Angreifern die unbemerkte Ausführung weiterer Angriffsschritte sowie weitreichende Zugriffsmöglichkeiten auf das Zielsystem ermöglichen.

- Angreifbarkeit in der Softwareentwicklung
  Angriffe in der Entwicklungsphase eines Softwareproduktes können eine erhebliche Gefahr darstellen. Bereits in dieser frühen Phase des Softwarelebenszyklus vorgenommene Manipulationen sind für den eigentlichen Endanwender eines Produktes nur sehr schwer zu erkennen, insbesondere wenn das manipulierte Softwareprodukt vom Hersteller offiziell freigegeben wird. Ein solcher Angriff kann viele Sicherheitsmaßnahmen zur Detektion der Manipulationen umgehen.

- Cyberangriffe auf kryptografische Verfahren
  Cyberangriffe auf kryptografische Verfahren sind zumeist auch Angriffe auf die mit diesen Verfahren geschützten Informationen. Für Angreifer sind sie daher hochinteressant, da sie durch solche Angriffe an sensible Informationen gelangen können, die eigentlich mit diesen Verfahren vor unbefugten Zugriffen geschützt werden sollen.

- Cyberangriffe auf Fahrzeuge
  Moderne Fahrzeuge enthalten eine Vielzahl von IT-Systemen, die miteinander vernetzt sind und sowohl untereinander als auch mit IT-Systemen beim Hersteller kommunizieren können. IT-Systeme zur drahtlosen Kommunikation und Standortbestimmung erhöhen dabei die Angriffsoberfläche für Angriffe aus der Ferne zusätzlich. Im Kontext dieses Vorhabens sind Cyberangriffe auf Fahrzeuge und die dabei eingesetzten Angriffstechniken insbesondere mit Blick auf die Beförderung von kerntechnischem Material oder radioaktiven Stoffen relevant.

Auch im Jahr 2025 ergab sich aus den Ergebnissen des Screenings ein breites Spektrum an relevanten Aspekten für die IT-Bedrohungslage wie:

- Künstliche Intelligenz
  KI wird inzwischen vielfach und auf breiten Anwendungsfeldern eingesetzt. Aus Sicht der Cybersicherheit rücken dabei insbesondere zwei Aspekte in den Vordergrund. Zum einen stellt sich die Frage, inwiefern KI-basierte Systeme oder andere Systeme, die auf KI zurückgreifen durch Angreifer manipuliert werden könnten. Zum anderen wird KI immer häufiger auch von Angreifern als Unterstützung bei der Vorbereitung und Durchführung von Cyberangriffen eingesetzt.

- Geopolitische Spannungsfelder
  Cyberangriffe kommen heute in praktisch allen politischen Spannungsfeldern zum Einsatz. Bereits vor dem Hintergrund der wachsenden Spannungen zwischen

Russland und der Ukraine und noch einmal seit Kriegsausbruch ist es zu einem starken Anstieg der politisch und strategisch motivierten Cyberangriffe nicht nur in der Ukraine, sondern auch darüber hinaus, gekommen. Weitere Spannungsfelder, in denen es regelmäßig zu Cyberangriffen gekommen ist und die beispielhaft beleuchtet werden, sind der Krieg in Gaza, die Konflikte zwischen China und westlichen Staaten, Nordkorea und Südkorea sowie Iran und Israel.

- Industrielle Steuerungssysteme
  Schwachstellen in und Angriffe auf industrielle Steuerungssysteme kommen immer häufiger vor und bilden seit Jahren feste Schwerpunkte im Rahmen der IT-Bedrohungslage. Hierbei geht es zumeist um Disruption oder Destruktion der Systeme. Auch Ausspähung zur Gewinnung von Informationen beispielsweise für zukünftige Angriffsschritte ist eine häufige Motivation. Darüber hinaus kommt es auch zur Manipulation von industriellen Steuerungssystemen durch Cyberangriffe. Gerade bei industriellen Steuerungssystemen, die ja dazu dienen, verfahrenstechnischen Prozesse zu steuern, kommt es hierbei regelmäßig auch zu physischen Auswirkungen der Angriffe.

Die gesamten Ergebnisse des Screenings, von den dokumentierten Ereignissen bis hin zu den für die IT-Bedrohungslage als relevant identifizierten Fällen, einschließlich der Kategorisierung und Priorisierung, wurden fortlaufend und gemeinsam mit für eine weitere Auswertung relevanten Hintergrundinformationen und Rechercheergebnissen in geeigneter Weise dokumentiert und flossen in zahlreiche weiterführende Arbeiten im Bereich der Eigen- und Auftragsforschung ein, wie:

- Arbeiten zu Social Engineering und zum unwissentlichen Innentäter
- Arbeiten zum wissentlichen Innentäter
- Arbeiten zur Cybersicherheit in der Lieferkette
- Arbeiten im Hinblick auf Angriffstechniken und Vorgehensweisen
- eine detaillierte Auswertung der IT-Bedrohungslage zu industriellen Steuerungssystemen und KRITIS
- die Überarbeitung des SEWD-Regelwerks IT

4 Fachlicher Austausch auf internationaler Ebene

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.

4.1 Besuch bzw. Mitwirkung an internationalen Veranstaltungen

Ausgesuchte internationale Fachveranstaltungen zur Verbesserung der nuklearen Sicherung sollten durch eine Mitwirkung und die Bereitstellung technisch-wissenschaftlichen Sachverstands unterstützt werden. Mit der Zustimmung des BMUKN erfolgte eine Mitwirkung an folgenden internationalen Fachveranstaltungen zur Sicherung und Cybersicherheit:

- Teilnahme an der „International Conference on Enhancing Nuclear Safety and Security Through Technical and Scientific Support Organizations (TSOs)“ (TSO-Konferenz) vom 02. bis 06.12.2024 in Wien (Österreich)
  Relevante Aspekte waren u. a. ein bilateraler Austausch zu Aspekten der Sicherung mit TSO anderer Länder sowie Pflege, Erweiterung und Vertiefung der Kontakte zu Experten anderer TSO (siehe auch Abschnitt 4.2, Reisebericht /GRS 25c/).

- virtuelle Teilnahme am Kongress 38c3 (Chaos Communication Congress), Dezember 2024, Hamburg
  Relevante Aspekte waren u. a. der Stand der Cybersicherheit 2024, ein Überblick über die Entwicklung von kommerzieller Spyware auf iOS, Sabotage von IT-Systemen (z. B. Live-Demonstration von Angriffen), ein Update zur Aufdeckung der Sabotage-Software von NEWAG-Zügen, das Knacken des von US-Militär und NATO genutzten Verschlüsselungsalgorithmus „HALFLOOP-24“, Remote code execution durch das Ausnutzen einer Schwachstelle sowie Angriffe auf Energieübertragungsnetze (Teilnahmebericht /GRS 25e/).

- Teilnahme am Technical Meeting on the Application of Artificial Intelligence for Nuclear Security vom 20. bis 24.10.2025 in Wien (Österreich)
  Relevante Aspekte waren u. a. der Einsatz von KI und Maschinellem Lernen (ML) in der Kerntechnik sowie die Unterstützung der Integration von KI/ML und beim Kapazitätsaufbau (Reisebericht /GRS 26a/).

Auf der TSO-Konferenz vom 02. bis 06.12.2024 in Wien, in Kooperation von IAEO und ETSON, sollten u. a. bestehende Kontakte ausgebaut und neue Kontakte zu unterschiedlichen Interessengruppen geknüpft werden. TSO spielen weltweit sowohl im Bereich der nuklearen Sicherheit als auch der Sicherung eine Schlüsselrolle – insbesondere durch ihre fachliche Expertise und starke internationale Vernetzung. Die zunehmende Komplexität der Fragestellungen erfordert dabei immer häufiger eine ganzheitliche Betrachtung. In diesem Zusammenhang empfiehlt und fördert die IAEO, die Schnittstelle zwischen nuklearer Sicherheit und nuklearer Sicherung stärker miteinander zu verknüpfen. Am internationalen Austausch von aktuellen Erkenntnissen zu speziellen Aspekten der Sicherung im Rahmen der TSO-Konferenz waren Experten von TSOs aus Bangladesch, Belgien, China, Deutschland, Frankreich, Ghana, Jamaica, Japan, Kanada, Kenia, Nigeria, Norwegen, Oman, Pakistan, Polen, Rumänien, Russland, Saudi-Arabien, Simbabwe, Slowenien, Ukraine, USA und Ägypten beteiligt. Fachliche Beiträge kamen u. a. von der japanischen TSO Japan Atomic Energy Agency (JAEA) für die Regulierungsbehörde zu Forschungsschwerpunkten hinsichtlich Risikobewertung, Optimierung Notfallschutz, Umweltschutz und Langzeitbetrieb mit technischen Herausforderungen und Lösungsansätzen für die geplanten Laufzeitverlängerungen. Weiterhin u. a. von der belgischen TSO Bel V zu Planungen hinsichtlich Stilllegung und Abbau sowie Laufzeitverlängerung mit einer umfassenden Re-Evaluation des Anlagendesigns und Identifikation von Ertüchtigungsmaßnahmen sowie zu den russischen TSO, den Organisationen FSUE SEC NRS und JSC VO Safety, und deren Aufgaben wie Überprüfungen, Bewertung meldepflichtiger Ereignisse einschließlich abgeleiteter Sanktionen und fachliche Zuarbeit bei der Erarbeitung und Fortschreibung von Regelwerken.

Der Kongress 38c3 (Chaos Communication Congress) im Dezember 2024 in Hamburg stand unter dem Motto „Illegal Instructions“, was die inhaltliche Fokussierung der Veranstaltung auf die Sabotage von Geräten der operativen Technologie und Informationstechnologie verdeutlicht. In einer Vielzahl von Vorträgen wurde auf verschiedene Schwachstellen und Angriffsmöglichkeiten eingegangen, unter anderem wurden hierbei NATO-Verschlüsselungscode, Mobiltelefone, Straßenlaternen, Solarkraftwerke, Gefängnis-Software, die elektronische Patientenakte und der Windows Bitlocker thematisiert. Zwei der behandelten Themen waren im Hinblick auf dieses Vorhaben besonders interessant. Zum einen wurde ein bereits im Vorjahr bekannt gewordenen Vorfall im Zusammenhang mit in die Software eingebauten „Kill Switches“ in Zügen der polnischen Hersteller- und Instandhaltungsfirma Newag S.A. und der daraus resultierenden automatischen Fernabschaltung der Züge weiter thematisiert. In dem 2024 vorgestellten

Update-Vortrag wurde über die Entwicklungen seit dem Bekanntwerden der Manipulation durch Newag S.A. berichtet. Zusätzlich wurden weitere Erkenntnisse und der aktuelle Stand berichtet. Zum anderen erregte ein Vortrag über ein Datenleck bei Volkswagen (VW) starke Aufmerksamkeit. Für diesen Vortrag wurden Standortdaten von über 800.000 Elektroautos, welche VW mit einer Genauigkeit von ± 10 cm in einer unverschlüsselten Datenbank speicherte, ausgewertet. Die Bewegungsprofile der Autos lassen Rückschlüsse auf einzelne Personen und eine Vielzahl von persönlichen Daten zu. Diese Daten lassen sich potenziell für Erpressungen oder die Planung krimineller Handlungen nutzen. So ließen sich den einzelnen Personen beispielsweise ihre Freizeitgestaltung (z. B. Hobbies, Bordellbesuche, häufig besuchte Wohnhäuser) und weitere sensible Daten (z. B. Besuche bei Scheidungsanwälten, Schule und Freizeitaktivitäten der Kinder, Religionszugehörigkeit) zuordnen. Zudem konnte den Personen, inklusive potenzieller Berufsgeheimnisträger, ihre Arbeitsstätte zugeordnet werden (z. B. Bundesnachrichtendienst, Militärischer Abschirmdienst). Ähnliche Probleme wurde auch in einem weiteren Vortrag in Bezug auf das Sammlern von Handy-Standortdaten von mindestens Zehntausenden (mutmaßlich von Millionen) von Menschen, durch Databroker erläutert. Durch die Teilnahme ergab sich sowohl ein inhaltlicher Überblick über die momentan im Fokus stehenden Themen der Cybersicherheitsforschung als auch vertieftes Wissen über die vorgestellten Schwachstellen und Angriffsmöglichkeiten. Zudem konnten für die Arbeiten zur IT-Bedrohungslage im Rahmen dieses Vorhabens wertvolle Erkenntnisse gesammelt werden.

Auf dem Technical Meeting on the Application of Artificial Intelligence for Nuclear Security vom 20. bis 24.10.2025 in Wien wurde deutlich, dass u. a. in den Bereichen Safeguards und Cybersicherheit zunehmend KI-Technologien zur Effizienzsteigerung eingesetzt werden, u. a. KI-gestützte Videoanalyse. Im Bereich Cyberabwehr werden ML-Modelle zur Erkennung von Anomalien in industriellen Steuerungssystemen (OT/ICS) eingesetzt, die Angriffe frühzeitig identifizieren können, zum Erkennen von Insider-Bedrohungen verstärkt KI, basierend auf Zutritts-, Verhaltens- und Videoüberwachungs-Daten. Risiken betreffen u. a. die Lieferkette von KI-Modellen, insbesondere vortrainierter externer Modelle, die manipuliert oder unzureichend dokumentiert sein können, weshalb Bedarf an Modell-Provenienz (Nachvollziehbarkeit und Vertrauenswürdigkeit der Herkunft eines KI-Modells), kryptografischer Integritätsprüfung und standardisierten Freigabeprozessen besteht. Für die Entwicklung von KI stellt es außerdem eine große Herausforderung dar, zu verhindern, dass eine KI „gefährliche“ Antworten zum Themengebiet der Kerntechnik ausgibt. Auch eine mit sensiblen kerntechnischen

Informationen trainierte KI würde eine potenzielle Gefahr darstellen, falls Innentäter sich Zugang verschaffen sollten. Die Möglichkeit zur Nutzung verschiedener KI könnte zu einer Aggregation von Wissen bei Tätern führen, die in Bezug auf die kerntechnische Sicherheit problematisch sein könnte. Ein weiteres Problem ist die internationale KI-Regulierung auf unterschiedlichem Niveau, für den Nuklearbereich besteht dringender Bedarf für internationale Standards und regulatorische Leitlinien. Letztlich bietet der Einsatz von KI ein erhebliches Potenzial bezüglich innovativer Neuerungen im Bereich von technischen, personellen oder auch organisatorischen Maßnahmen zur Sicherung, erfordert aber klare Regeln und Zuständigkeiten sowie Transparenz und abgestimmte regulatorische Rahmenbedingungen, um Vertrauen und Kontrollfähigkeit sicherzustellen.

Insbesondere in Verbindung mit Arbeiten in anderen AP erfolgte eine Mitwirkung an weiteren internationalen Fachveranstaltungen zur Sicherung und Cybersicherheit:

- Teilnahme an der Veranstaltung Take Aware 2025 in Wuppertal vom 20. bis 22.05.2025 (vorwiegend deutschsprachige Region D-A-CH), AP 1 Sicherungskultur
- Vorbereitung und Teilnahme am Swiss Security Awareness Day 2025 in Bern (Schweiz), dabei Erfassung von neuen branchenübergreifenden, integrativen Ansätzen und Austausch mit internationalen Partnern (D-A-CH-Region), AP 1 Sicherungskultur
- Teilnahme an der Veranstaltung Take Aware 2026 in Düsseldorf vom 20. bis 21.05.2026 (D-A-CH-Region), AP 1 Sicherungskultur
- Besuch der Fachmesse Enforce Tac in Nürnberg vom 23. bis 25.02.2026, relevante Schwerpunkte u. a. Drohnendetektion und -abwehr, Schutz vor Drohnen, AP 3 UAV

Die gewonnenen fachlichen Erkenntnisse wurden mit Bezug zu den Arbeiten in den jeweiligen AP dargestellt.

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 Cybersicherheit geleistet. Gleichzeitig wurden die Fachveranstaltungen durch die Bereitstellung technisch-wissenschaftlichen Sachverstands unterstützt.

4.2 Zusammenwirken mit TSO

Über den bilateralen Austausch zwischen der GRS und TSO anderer Länder sollte ein Know-how-Transfer auf dem Gebiet der Sicherung von kerntechnischen Anlagen und von Beförderungen sowie der Cybersicherheit gefördert werden. Die TSO spielen eine Schlüsselrolle im Bereich der nuklearen Sicherheit und Sicherung. Sie stellen den nationalen Aufsichtsbehörden wichtiges wissenschaftliches Fachwissen zur Verfügung, um eine optimale Entscheidungsfindung im Hinblick auf die Verbesserung der nuklearen Sicherheit, des Strahlenschutzes sowie der Sicherung von Anlagen und Tätigkeiten zu ermöglichen.

Im Rahmen eines bilateralen Austauschs zwischen TSO wurden folgende Aktivitäten durchgeführt:

- Organisation und Vorbereitung eines Treffens mit einer der Nachfolgeorganisationen der aufgelösten französischen TSO („Institut de radioprotection et de sûreté nucléaire“ - IRSN), dem Bureau Modélisation des effets des Armes et des eXplosifs
- Treffen und Austausch mit Vertretern des „Bureau Modélisation des effets des Armes et des eXplosifs“ am 09./10.10.2025 in Köln (Nachfolgeorganisation der IRSN) zum Themenbereich Einwirkungen und Freisetzung, Nachbereitung des Treffens

Über den bilateralen Austausch zwischen Experten der GRS für Sicherung und den Vertretern des französischen „Bureau Modélisation des effets des Armes et des eXplosifs“ wurde der bidirektionale internationale Know-how-Transfer auf dem Gebiet der Sicherung von kerntechnischen Anlagen und von Beförderungen wieder aufgenommen.

5 Projektabwicklung

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. Der Entwurf Ergebnisbericht § 13 ABFE-BMU des Vorläufervorhabens wurde finalisiert.

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

Für Abstimmungen mit dem BMUKN 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 23a/ Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, Lastannahmen zur Auslegung kerntechnischer Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (Lastannahmen Anlagen), Rev. 5.0 vom 30. Juni 2023, VS – VERTRAULICH, einschließlich
Erläuterungen und Hinweise zu den Lastannahmen Anlagen, Rev. 5.0 vom 30. Juni 2023, VS – VERTRAULICH

/BMU 23b/ 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 85/ Deutsches Institut für Normung e.V. (DIN): DIN 1072: Straßen- und Wegbrücken; Lastannahmen, Berlin, Dezember 1985

/DIN 10a/ Deutsches Institut für Normung e.V. (DIN): DIN EN 1991-1-7, Eurocode 1: Einwirkungen auf Tragwerke – Teil 1-7: Allgemeine Einwirkungen – Außergewöhnliche Einwirkungen; Deutsche Fassung EN 1991-1-7:2006 + AC:2010, Berlin, Dezember 2010

/DIN 10b/ Deutsches Institut für Normung e.V. (DIN): DIN EN 1991-1-7/NA:2010-12, Nationaler Anhang – National festgelegte Parameter – Eurocode 1: Einwirkungen auf Tragwerke – Teil 1-7: Allgemeine Einwirkungen – Außergewöhnliche Einwirkungen, Berlin, Dezember 2010

/DIN 19/ Deutsches Institut für Normung e.V. (DIN): DIN EN 1991-1-7/NA: Nationaler Anhang – National festgelegte Parameter – Eurocode 1: Einwirkungen auf Tragwerke – Teil 1-7: Allgemeine Einwirkungen – Außergewöhnliche Einwirkungen, Berlin, September 2019

/DIN 25a/ Deutsches Institut für Normung e.V. (DIN): Sicherheit und Resilienz – Fahrzeugsicherheitsbarrieren – Teil 1: Leistungsanforderung, Fahrzeuganprallprüfverfahren und Leistungsbewertung (ISO 22343-1:2023), DIN ISO 22343-1, Berlin, April 2025

/DIN 25b/ Deutsches Institut für Normung e.V. (DIN): Sicherheit und Resilienz – Fahrzeugsicherheitsbarrieren – Teil 2: Anwendung (ISO 22343-2:2023), DIN ISO 22343-2, Berlin, April 2025

/GRS 21/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, 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 24a/ 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, Vorhaben FKZ 4721R01611, Mai 2024, GRS – 773, ISBN 978-3-910548-65-7

/GRS 24b/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: Munitionsüberwachung Panzerfaust 3-T (Tandemhohlladung), Eimke, 31.07.-01.08.2024, Stand 02.08.2024, VS-NfD

/GRS 25a/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: VfS-Kongress in Leipzig: Gemeinsam für eine sichere Welt, Leipzig, 06.-07. Mai 2025, Stand 19.05.2025

/GRS 25b/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: Teilnahme an der Take Aware 2025, Wuppertal, 20.-22.Mai 2025, Stand 18.06.2025

/GRS 25c/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: Teilnahme an der International Conference on Enhancing Nuclear Safety and Security Through Technical and Scientific Support Organizations (TSOs): Challenges and Opportunities in a Rapidly Changing World”, Wien (Österreich) IAEO Hauptsitz, 02.-06.12.2024, Stand 25.01.2025

/GRS 25d/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: Teilnahme am Swiss Security Awareness Day 2025, Bern (Schweiz), 11.09.2025, Stand 11.12.2025

/GRS 25e/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Teilnahmebericht zum Vorhaben 4724R01600, Thema: Teilnahme an der Konferenz “38c3”, Hamburg, 27. bis 30.12.2024, ccc, Teilnahme online, Stand 03.02.2025

/GRS 26a/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht (Kurzform) zu den Vorhaben 4724R01600 und 4724R01610, Thema: IAEA Technical Meeting on the Application of Artificial Intelligence for Nuclear Security, 20.-24.10.2025, Wien (Österreich), Stand 06.01.2026

/GRS 26b/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: Teilnahme an der Take Aware 2026, Düsseldorf, 20.-21.05.2026, Stand 01.06.2026

/GRS 26c/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Reisebericht zum Vorhaben 4724R01600, Thema: Teilnahme an der Enforce Tac, Nürnberg, 23.-25.02.2026, Stand 24.06.2026

/GRS 26d/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Einsatz von Social Engineering und Handlungen unwissentlicher Innentäter im Rahmen von Cyberangriffen, GRS-862, ISBN 978-3-911727-55-6

/IAE 08/ International Atomic Energy Agency, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No. 7, Vienna, September 2008

/IAE 17/ International Atomic Energy Agency, Self-assessment of Nuclear Security Culture in Facilities and Activities, Technical Guidance, IAEA Nuclear Security Series No. 28-T, Vienna, November 2017

/INS 24/ INS Office of International Security, European Regional Focus Group on Nuclear Security During Decommissioning Summary Report, September 3–5, 2024 Cologne, Germany, Stand Oktober 2024

/ISO 13a/ ISO Internationale Organisation für Normung, International Workshop Agreement, Vehicle security barriers - Part 1: Performance requirement, vehicle impact test method and performance rating, Referenznummer IWA 14-1:2013(E), Schweiz, 2013

/ISO 13b/ ISO Internationale Organisation für Normung, International Workshop Agreement, Vehicle security barriers - Part 2: Application, Referenznummer IWA 14-2:2013(E), Schweiz, 2013

/ISO 23a/ ISO Internationale Organisation für Normung, Security and resilience - Vehicle security barriers - Part 1: Performance requirement, vehicle impact test method and performance rating, ISO 22343-1:2023(E), Schweiz, 2023

/ISO 23b/ ISO Internationale Organisation für Normung, Security and resilience - Vehicle security barriers - Part 1: Performance requirement, vehicle impact test method and performance rating, ISO 22343-2:2023(E), Schweiz, 2023

/JRC 25/ Joint Research Centre [HTML], Stand vom 2024, erreichbar unter: https://counterterrorism.ec.europa.eu/, zitiert am 13.05.2025

/VFS 24/ Verband für Sicherheitstechnik e.V. (VfS), Seminarunterlagen des VfS Seminars Zufahrtsschutz am 22. und 23.10.2024 in Berlin

Abbildungsverzeichnis

Abkürzungsverzeichnis

AASHTO	American Association of State Highway and Transportation Officials
ABFE	Allgemeine Bedingungen für Forschungs- und Entwicklungsverträge
AG DAD	gemeinsame Arbeitsgruppe „Detektion von Drohnen und Abwehr von unkooperativen Drohnen beginnend an den Verkehrsflughäfen“
AP	Arbeitspaket
APT	Advanced Persistent Threats
AtG	Atomgesetz
BMUKN	Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit
CEO	Chief Executive Officer
D-A-CH	Region Deutschland, Österreich, Schweiz
DESi	Datenbank zu Ereignissen mit Sicherungsrelevanz
DIN	Deutsches Institut für Normung
DIPUL	Digitalen Plattform Unbemannte Luftfahrt
DNS	Domain Name System
ETSON	European Technical Safety Organizations Network
EU	Europäischen Union
FEM	Finite Elemente Methode
GPS	Global Positioning System

GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
HVM	Hostile Vehicle Mitigation
IAEO	Internationale Atomenergiebehörde
ICE	Institution of Civil Engineers
IRSN	Institut de radioprotection et de sûreté nucléaire
IT	Informationstechnik
ITDB	Incident and Trafficking Database
JAEA	Japan Atomic Energy Agency
JRC	Joint Research Centre
KI	Künstliche Intelligenz
KRITIS	kritische Infrastrukturen
Lkw	Lastkraftwagen
MFA	Multi-Faktor-Authentifizierung
ML	Maschinelles Lernen
NATO	North Atlantic Treaty Organization
NPSA	(British) National Protective Security Authority
NSS	Nuclear Security Series (Regelwerk der IAEO zur Sicherung)
RSES	Register of Security Engineers and Specialists
SEO	Search Engine Optimization

SEWD	Störmaßnahmen oder sonstige Einwirkungen Dritter
SPH	Smoothed Particle Hydrodynamics
TSO	Technical and Scientific Support Organization
TÜV	Technischer Überwachungsverein
UAV	Unmanned Aerial Vehicle (unbemanntes und ggf. autonomes Fluggerät, umgangssprachlich auch Drohne)
VDA	Vehicle Dynamics Assessment
VfS	Verband für Sicherheitstechnik e.V.
VW	Volkswagen AG

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 978-3-911727-54-9