

**Internationales GVA-
Datenaustausch-
projekt ICDE
2017 bis 2020**

**Systematische Aufbereitung
der weltweiten
Betriebserfahrung mit
gemeinsam verursachten
Ausfällen im Rahmen
einer internationalen
Expertengruppe**

**Internationales GVA-
Datenaustausch-
projekt ICDE
2017 bis 2020**

**Systematische Aufbereitung
der weltweiten
Betriebserfahrung mit
gemeinsam verursachten
Ausfällen im Rahmen
einer internationalen
Expertengruppe**

Abschlussbericht

Benjamin Brück
Marc Foldenauer
Michael Homann
Christian Lambertus
Albert Kreuser

Dezember 2020

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Kennzeichen 4717R01337 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

Deskriptoren

Gemeinsam verursachte Ausfälle (GVA), Internationale Betriebserfahrungsauswertung, OECD/NEA International Common-Cause Failure Data Exchange (ICDE) Project

Kurzfassung

Ereignisse mit gemeinsam verursachten Ausfällen (GVA) können die Verfügbarkeit von Einrichtungen des Sicherheitssystems von Kernkraftwerken (KKW) signifikant beeinträchtigen. Deshalb werden Informationen und Daten zu GVA-Ereignissen in einer Reihe von Ländern systematisch gesammelt und analysiert. Aufgrund der geringen Eintrittswahrscheinlichkeit von GVA reicht die Betriebserfahrung allein aus deutschen Kernkraftwerken für eine umfassende Bewertung von GVA nicht aus. Daher ist es notwendig, auch die Betriebserfahrung anderer Länder, die vergleichbare Technik einsetzen, zu nutzen.

Um die Betriebserfahrung mit GVA aus anderen Ländern zur Weiterentwicklung der Beurteilungsgrundlagen für GVA nutzen zu können, hat die GRS die Etablierung eines internationalen GVA-Arbeitskreises maßgeblich mitinitiiert. Dieser Arbeitskreis entwickelte das Projekt „International Common Cause Failure Data Exchange“ (ICDE). Das Ziel dieses seit mehr als 20 Jahren laufenden Projektes ist es, einen breit angelegten Informationsaustausch über beobachtete Ereignisse mit GVA-Relevanz zu organisieren, GVA-Ereignisse auszuwerten und die dabei erzielten Ergebnisse zu veröffentlichen sowie den Stand von Wissenschaft und Technik bezüglich GVA fortzuschreiben.

Die Arbeiten der GRS im Rahmen des ICDE-Vorhabens zur Bereitstellung und Auswertung der Betriebserfahrung mit GVA dienen der Absicherung und Erweiterung der Erkenntnisse über GVA im Hinblick auf probabilistische Sicherheitsanalysen, der Förderung des Verständnisses der Ursachen und Mechanismen von GVA und zur Bewertung von vorbeugenden Maßnahmen gegen das Auftreten von GVA.

Durch den langfristig angelegten Austausch sollen:

- GVA-Ereignisse, ihre Ursachen und Verhinderungsmöglichkeiten besser verstanden werden,
- ein qualitativer Einblick in die grundlegenden Ursachen („root causes“) von GVA-Ereignissen gewonnen werden, der dann genutzt werden kann, um vorbeugende Maßnahmen gegen das Auftreten solcher Ereignisse oder zur Abmilderung der Auswirkungen abzuleiten,
- ein effizienter Erfahrungsrückfluss über beobachtete GVA-Phänomene etabliert werden, der z. B. zur Entwicklung von Indikatoren zur risikoinformierten Aufsicht genutzt werden kann,

- quantitative Informationen über GVA-Ereignisse gewonnen werden, um die Wirksamkeit von vorbeugenden Maßnahmen analysieren zu können und um belastbare Grundlagen für Zuverlässigkeitskennzahlen für GVA-Ereignisse im Rahmen von probabilistischen Sicherheitsanalysen zu erhalten.

Durch die Zusammenarbeit mit den am ICDE-Projekt beteiligten internationalen Partnerorganisationen wird der Umfang der vorliegenden Betriebserfahrung bezüglich GVA-Ereignissen gegenüber der rein nationalen Betriebserfahrung um mehr als den Faktor 10 erweitert. Hierdurch wird Folgendes erreicht:

- Die Informationsbasis bezüglich Ursachen, Fehlermechanismen und Auswirkungen von GVA wird erheblich verbreitert. Dies ermöglicht die Entwicklung von Vorsorgemaßnahmen auch gegen solche GVA-Phänomene, die in der deutschen Betriebserfahrung noch nicht beobachtet worden sind.
- Es werden Erkenntnisse hinsichtlich in ausländischen Kernkraftwerken getroffener Maßnahmen zur Vermeidung von GVA gewonnen.
- Es werden Informationen über die teilweise unterschiedlichen Methoden bei der Erfassung, Auswertung und Modellierung von GVA-Ereignissen in den verschiedenen Ländern ausgetauscht. Dieser Austausch dient der methodologischen Weiterentwicklung, auch im Hinblick auf Angleichung oder Vereinheitlichung der Auswertungs- und Analysemethodik.

Schwerpunkte der Arbeiten im ICDE-Lenungskreis sind die Erstellung einer einheitlichen Datenbasis mit detaillierten Ausfall- und Ursachenbeschreibungen sowie Bewertungen von GVA-Ereignissen aus Anlagen in den Herkunftsländern der Projektteilnehmer.

Ein systematischer Informationsaustausch zu GVA-Ereignissen fand bisher zu den Komponentenarten „Kreispumpen“, „Notstromdieselgeneratoren“, „Motorbetätigte Absperrrarmaturen“, „Sicherheits- und Entlastungsventile“, „Rückschlagarmaturen“, „Batterien“, „Leistungsschalter“, „Füllstandsmessungen“, „Steuerstäbe und Steuerstabantriebe“, „Wärmetauscher“, „Frischdampfisolationsventile“, „Lüfter“ und „Softwarebasierte Leittechnik“ statt. Zu der Komponentenart „Wechselrichter“ hat der Erstrundeninformationsaustausch begonnen, die deutschen Informationen sind hierzu bereits eingespeist. Im Berichtszeitraum wurde die Aktualisierung der deutschen GVA-Betriebserfahrung für alle

Komponentenarten bis zum Ende des Jahres 2010 abgeschlossen. Die im Vorläufervorhaben begonnene Aktualisierung für den Zeitraum bis 2015 wurde fortgesetzt. Für fünf von neun nach 2011 betriebenen Anlagen ist jetzt der Zeitraum von 2011 bis 2015 ausgewertet.

In der ICDE-Datenbank sind zurzeit insgesamt 1761¹ Ereignisse, davon 143 vollständige GVA, erfasst. Die Anzahl der zur Verfügung gestellten Ereignisberichte übertrifft die aus der deutschen Betriebserfahrung vorhandenen Ereignisberichte um ein Vielfaches (z. B. sind bei Steuerstäben und Steuerstabantrieben von insgesamt 173 Ereignissen in der ICDE-Datenbank nur vier Ereignisse aus deutschen Anlagen). Insbesondere aus den USA und Frankreich mit ihrer großen Anzahl von Anlagen liegt eine Vielzahl an Ereignissen vor. Umfang und Detaillierungsgrad der Ereignisberichte der Teilnehmer sind in der Regel aussagekräftig genug, um die aufgetretenen Schadensmechanismen nachvollziehen und hinsichtlich ihrer Übertragbarkeit auf deutsche KKW bewerten zu können.

Während der Laufzeit des jetzt abgeschlossenen Vorhabens 4717R01337 hat der ICDE-Lenkungskreis in sechs Workshops Ereignisse aus der ICDE-Datenbank im Hinblick auf verschiedenen Fragestellungen diskutiert. Dabei wurde Folgendes untersucht:

- Welche GVA-Ereignisse zeigen Abhängigkeiten zwischen sicherheitsrelevanten Systemen? Aus dieser Fragestellung lassen sich Erkenntnisse zur Ursache von systemübergreifenden GVA und deren Auswirkungen ableiten.
- Welche Rolle spielt menschliches Fehlverhalten für das Auftreten von GVA-Ereignissen? Hierbei wurde insbesondere untersucht, wie häufig menschliches Fehlverhalten ursächlich war oder einen Beitrag zum Ereignis lieferte.
- Welche Erkenntnisse lassen sich aus GVA-Ereignissen gewinnen, die bei den Anforderungen von redundanten Sicherheitssystemen auftraten?

Darüber hinaus hat die GRS 63 aus ausländischen Anlagen in die ICDE-Datenbank eingespeiste Ereignisberichte systematisch ausgewertet. In den Vorläufervorhaben SR 2545, 3608R01338, 3611R01335 und 3614R01301 wurden bereits die in der ICDE-Datenbank zum jeweiligen Zeitpunkt vorhandenen Ereignisberichte zu Kreiselpumpen,

¹ Die angegebenen Zahlen beziehen sich auf die Anzahl der Ereignisse, die bereits sämtliche Stufen des QS-Prozesses durchlaufen haben. Darüber hinaus gibt es zu jedem Zeitpunkt weitere Ereignisse in der Datenbank, die sich noch in unterschiedlichen Stadien des QS-Prozesses befinden.

Notstromdieseln und Füllstandsmessungen, sowie motorbetätigten Absperrarmaturen, Rückschlagarmaturen, Sicherheits- und Entlastungsventilen, Leistungsschaltern, Batterien, Steuerstabantrieben, Wärmetauschern sowie Frischdampfisolationsventile hinsichtlich der jeweils aufgetreten GVA-Phänomene ausgewertet und mit den aus deutschen Anlagen bekannten Phänomenen verglichen. Die Ergebnisse sind in den Berichten /GRS 08a/, /GRS 08b/, /GRS 11a/, /GRS 11b/ /GRS 14a/, /GRS 14b/ und /GRS 17/ beschrieben.

In diesem Vorhaben wurde darauf aufbauend die seit den im vorherigen Absatz beschriebenen Erstausswertungen neu angefallene ausländische Betriebserfahrung ausgewertet. In Kapitel 2 dieses Berichts werden die für deutsche Anlagen als relevant erachteten Ereignisse kurz beschrieben und Hinweise formuliert, wie die bei diesen Ereignissen aufgetretenen Phänomene bei deutschen KKW verhindert werden können.

Abstract

Common-cause-failure (CCF) events can significantly impact the availability of the safety system of nuclear power plants. In recognition of this, CCF data is systematically being collected and analysed in several countries. Due to the low probability of occurrence of such events, it is not possible to derive a comprehensive evaluation of all relevant CCF-phenomena only from the operating experience in German nuclear power plants. Therefore, it is necessary to make use of the operating experience of other countries using similar technology.

The usage of CCF operating experience from other countries requires a common understanding about such CCF and how to collect data about them. To develop such a common understanding GRS decisively co-initiated the setting up of an international common-cause failure working group. This working group has elaborated the project „International Common-Cause Failure Data Exchange” (ICDE). The project’s objective is to organise a broad exchange of information concerning observed events with relevance to common-cause failures.

The work of GRS within the framework of the ICDE project for the provision and evaluation of the operational experience with CCF serves to validate and broaden the knowledge about CCF with regard to probabilistic safety analyses, to promote the understanding of the causes and mechanisms of CCF and to evaluate the effectiveness of precautionary measures against CCF.

The objectives of the exchange on a long-term basis are to

- improve the comprehension of CCF events and their causes and their prevention,
- generate qualitative insights into the root causes of CCF events which can then be used to derive and assess preventive measures against the occurrence of such events or their consequences,
- establish an efficient feedback of experience gained in connection with observed common-cause failure phenomena which could be used e.g. for the development of indicators for risk-based inspections,
- provide quantitative information regarding the occurrence of common-cause failures to analyse the effectiveness of preventive measures and to obtain safe bases for common-cause failure reliability data in the frame of PSA.

Due to the co-operation with the partner organisations involved in the ICDE project, the extent of the feedback of experience with CCF events is substantially increased in comparison to the experience resulting from national operating experience. This will

- enlarge the information base for early identification of non or little known CCF phenomena including their causes and effects,
- provide experience with preventive measures taken in nuclear power plants of other countries,
- supply information regarding partly different methods in collecting, evaluating and modelling CCF events in different countries. Thus, knowledge is gained to promote further development of the methods in the aim of assimilation or standardisation.

The main focus of the work within the ICDE Steering Group is the creation of a uniform data basis with detailed breakdowns of failure and causes as well as evaluations of CCF events from plants in the countries of origin of the project participants.

Meanwhile, the information exchange in the frame of the ICDE project covers the operating experience for the component types "Centrifugal Pumps", "Emergency Diesel Generators", "Motor Operated Valves", "Safety- and Relief-Valves", "Check Valves", "Batteries", "Breakers", "Level Measurement", "Control Rods Drive Assemblies", "Heat Exchangers", "Main Steam Isolation Valves", "Fans" and "Digital I&C". For the component type "Inverters", the first-round information exchange has started, the German information has already been fed in. In the period under review, the updating of the German CCF operating experience for all component types for the period 2003 to 2015 was continued; currently, the evaluations for five of the nine plants operated after 2011 have been analysed.

In total, the ICDE database currently contains about 1761 events, 143 of these events were complete CCF were all redundant components failed. The number of event reports from foreign countries surpasses the own sources many times (e.g. control rod drive assemblies: 4 events from German plants, total: 173 events). Especially from the USA and France with their large number of power plants a large number of events originates. Extent and grade of details of the participants' event reports are sufficiently expressive to understand the observed failure mechanisms.

During the now finished project 4717R01337 several safety-relevant issues were discussed by the ICDE Steering Group in six workshops. It was analysed

- which CCF events show dependencies between safety-relevant systems? From this question, findings on the cause of cross-system CCF and its effects can be derived,
- what role does human error play in the occurrence of CCF events? In particular, it was investigated how often human error was the cause or a contribution to the event,
- what insights can be gained from CCF events that occurred during the demand of redundant safety systems?

Furthermore, GRS has systematically assessed the event reports which were provided by organisations from the other countries to the ICDE data exchange. In the previous projects SR 2545, 3608R01338, 3611R01335 and 3614R01301, the available event reports on centrifugal pumps, emergency diesel generators and level measurement equipment as well as on motor operated valves, check valves, safety/relief valves, switch gears, breakers, batteries, control rod drive assemblies and heat exchangers were analysed with regard to the observed CCF phenomena. These phenomena were compared to the phenomena already known in German plants in the reports /GRS 08a/, /GRS 08b/, /GRS 11a/, /GRS 11b/, /GRS 14a/, /GRS 14b/ and /GRS 17/.

In this project, the new foreign operating experience gained since the initial evaluations described in the previous paragraph was evaluated. In chapter 2 of this report those events which are regarded as relevant also for German plants are briefly described and ideas are presented how to prevent such events in German NPP.

Inhaltsverzeichnis

	Kurzfassung	I
	Abstract	V
	Inhaltsverzeichnis.....	IX
1	Einführung und Zielsetzung.....	1
2	Auswertung der ICDE-Ereignisse aus anderen Ländern.....	5
2.1	Datenbasis	6
2.2	Komponentenart Batterien.....	7
2.3	Komponentenart Kreiselpumpen.....	8
2.4	Komponentenart Steuerstäbe mit Antrieben.....	10
2.5	Komponentenart Notstromdieselaggregate	10
2.6	Komponentenart Lüfter	12
2.7	Komponentenart motorbetätigte Absperrarmaturen (MOVs).....	15
2.8	Zusammenfassung der Auswertungen	16
A	Anhang.....	19
A.1	Organisation des ICDE-Projekts	19
A.2	Abstimmung von Art und Umfang der für den ICDE-Datenaustausch vorgesehenen Informationen.....	22
A.3	Ergebnisse des ICDE-Projekts.....	36
A.4	Zusammenfassung und Ausblick zum ICDE-Projekt.....	46
	Literaturverzeichnis	49
	Tabellenverzeichnis	55

1 Einführung und Zielsetzung

Ereignisse mit gemeinsam verursachten Ausfällen (GVA) können die Verfügbarkeit von Einrichtungen des Sicherheitssystems in Kernkraftwerken signifikant beeinträchtigen. Deshalb werden Informationen und Daten zu GVA-Ereignissen in einer Reihe von Ländern systematisch gesammelt und analysiert. Aufgrund der geringen Eintrittswahrscheinlichkeit von GVA-Ereignissen reicht die Betriebserfahrung deutscher Kernkraftwerke nicht für eine umfassende Bewertung aus. Deshalb ist es notwendig, auch die Betriebserfahrung anderer Länder, in denen vergleichbare Technik eingesetzt wird, zu nutzen.

Eine direkte Nutzung der qualitativen und quantitativen GVA-Datensammlungen anderer Länder wird aber dadurch erschwert, dass die Kriterien, die bei der Sammlung von GVA-Ereignissen angewendet werden, und die Bewertung von GVA-Ereignissen in den einzelnen Ländern teilweise unterschiedlich sind. Außerdem kann es auch bei prinzipiell vergleichbarer Technik im Einzelfall wichtig sein, konstruktive Details zu kennen, um eine Übertragbarkeit beurteilen zu können. Eine weitere Schwierigkeit besteht darin, dass die Beschreibungen der gemeldeten Ereignisse, ihrer Ursachen und der Kopplungsfaktoren, die für die Bewertung der Ereignisse wichtig sind, gewöhnlich in den jeweiligen Landessprachen verfasst sind.

Um die Betriebserfahrung mit GVA aus anderen Ländern zur Weiterentwicklung der Beurteilungsgrundlagen für GVA nutzen zu können, hat die GRS die Etablierung eines internationalen GVA-Arbeitskreises maßgeblich mit initiiert. Dieser Arbeitskreis entwickelte das Projekt „International Common Cause Failure Data Exchange“ (ICDE), das seit 1996 unter der Schirmherrschaft der OECD/NEA betrieben wird. Das Ziel dieses Projektes ist es, einen breit angelegten Informationsaustausch über beobachtete Ereignisse mit GVA-Relevanz zu organisieren. Dabei soll die Betriebserfahrung mit GVA der wesentlichen Komponenten des Sicherheitssystems erfasst werden.

Der Lenkungskreis des ICDE-Projektes setzt sich zusammen aus GVA-Experten der teilnehmenden Organisationen. Beteiligt sind hierbei sowohl Aufsichtsbehörden als auch Gutachterorganisationen und Forschungseinrichtungen. Teilweise werden die teilnehmenden Organisationen durch die Betreiber unterstützt. Zusätzlich zur Koordination der Datensammlung definiert der Lenkungskreis den internationalen Stand von Wissenschaft und Technik bei der Erfassung und Bewertung von gemeinsam verursachten Ausfällen.

Die GRS arbeitet von Anfang an kontinuierlich im Lenkungskreis des ICDE-Projektes mit. Die Finanzierung der Mitarbeit der GRS im Lenkungskreis und der Aufbereitung von Informationen zu deutscher Betriebserfahrung mit GVA entsprechend den Anforderungen von ICDE erfolgte zunächst in den BMU-Vorhaben SR 2276, SR 2418, SR 2468, SR 2545, 3608R01338, 3611R01335 und 3614R01301 und wurde im Rahmen des am 30.06.2020 abgeschlossenen und mit diesem Bericht dokumentierten Vorhabens 4717R01337 fortgeführt. Die GRS beabsichtigt die Mitarbeit im ICDE-Projekt im Rahmen des Nachfolgevorhabens 4720R01350 fortzusetzen.

Die Arbeiten der GRS im Rahmen des ICDE-Vorhabens zur Bereitstellung und Auswertung der Betriebserfahrung mit GVA dienen der Absicherung und Erweiterung der Erkenntnisse über GVA im Hinblick auf probabilistische Sicherheitsanalysen, der Förderung des Verständnisses der Ursachen und Mechanismen von GVA und zur Bewertung von vorbeugenden Maßnahmen gegen das Auftreten von GVA.

Durch den langfristig angelegten Austausch sollen:

- GVA-Ereignisse, ihre Ursachen und Verhinderungsmöglichkeiten besser verstanden werden,
- qualitative Einblicke in die grundlegenden Ursachen („root causes“) von GVA-Ereignissen gewonnen werden, die dann genutzt werden können, um vorbeugende Maßnahmen gegen das Auftreten solcher Ereignisse oder zur Abmilderung der Auswirkungen abzuleiten,
- ein effizienter Erfahrungsrückfluss über beobachtete GVA-Phänomene etabliert werden, der z. B. zur Entwicklung von Indikatoren zur risikoinformierten Aufsicht genutzt werden kann,
- quantitative Informationen über GVA-Ereignisse gewonnen werden, um die Wirksamkeit von vorbeugenden Maßnahmen analysieren zu können und um belastbare Grundlagen für Zuverlässigkeitskennzahlen für GVA-Ereignisse im Rahmen von probabilistischen Sicherheitsanalysen zu erhalten.

Durch die Zusammenarbeit mit den am ICDE-Projekt beteiligten internationalen Partnerorganisationen wird der Umfang der vorliegenden Betriebserfahrung bezüglich GVA-Ereignisse gegenüber der rein nationalen Betriebserfahrung um mehr als den Faktor 10 erweitert. Hierdurch wird Folgendes erreicht:

- Die Informationsbasis bezüglich Ursachen, Fehlermechanismen und Auswirkungen von GVA wird erheblich verbreitet. Dies ermöglicht die Entwicklung von Vorsorgemaßnahmen auch gegen solche GVA-Phänomene, die in der deutschen Betriebserfahrung noch nicht beobachtet worden sind.
- Es werden Erkenntnisse hinsichtlich in ausländischen Kernkraftwerken getroffener Maßnahmen zur Vermeidung von GVA gewonnen.
- Es werden Informationen über die teilweise unterschiedlichen Methoden bei der Erfassung, Auswertung und Modellierung von GVA-Ereignissen in den verschiedenen Ländern ausgetauscht. Dieser Austausch dient der methodologischen Weiterentwicklung, auch im Hinblick auf Angleichung oder Vereinheitlichung der Auswertungs- und Analysemethodik.

Da im Lenkungskreis des ICDE-Projektes GVA-Experten aus allen beteiligten Organisationen vertreten sind, wird durch die eigene Mitarbeit im Lenkungskreis die Mitwirkung am aktuellen internationalen Diskussionsstand zu GVA sichergestellt. Schwerpunkte der Arbeiten im ICDE-Projekt sind die Erstellung einer einheitlichen Datenbasis mit detaillierten Ausfall- und Ursachenbeschreibungen sowie Bewertungen von GVA-Ereignissen aus Anlagen in den Herkunftsländern der Projektteilnehmer.

Mit den Berichten /GRS 08a/, /GRS 08b/, /GRS 11a/, /GRS 11b/, /GRS 14a/, /GRS 14b/ sowie /GRS 17/ hat die GRS basierend auf der zum Zeitpunkt der Berichtserstellung verfügbaren Datenlage die aus den ausländischen Anlagen in die ICDE-Datenbank eingespeisten Ereignisbeschreibungen dahingehend ausgewertet, ob die identifizierten Fehlermechanismen auch auf deutsche KKW übertragbar sind. In diesem Vorhaben wurde darauf aufbauend die seit diesen Erstausswertungen neu angefallene ausländische Betriebserfahrung ausgewertet. In Kapitel 2 dieses Berichts werden die für deutsche Anlagen als relevant erachteten Ereignisse kurz beschrieben und Hinweise formuliert, wie die bei diesen Ereignissen aufgetretenen Phänomene bei deutschen KKW verhindert werden können.

2 Auswertung der ICDE-Ereignisse aus anderen Ländern

Durch den Datenaustausch im Rahmen des ICDE-Projekts wird die Informationsbasis zu GVA-Ereignissen gegenüber der aus deutschen Kernkraftwerken für den gleichen verfügbaren Zeitraum um mehr als das Zehnfache erweitert. Dadurch wird die Grundlage für die Bewertung von GVA substantiell verbreitert und abgesichert. Um diese Erweiterung der Datenbasis zur generischen Unterstützung von aufsichtlichen Fragestellungen nutzbar zu machen, wurden Ereignisberichte, die im Rahmen des ICDE-Datenaustauschs von den Teilnehmerorganisationen aus den anderen Ländern erhalten wurden, systematisch ausgewertet.

Im Vorhaben SR 2545 wurde dazu mit einer Auswertung der Ereignisse zu Kreiselpumpen, Notstromdieselaggregaten und Füllstandsmessungen begonnen (vgl. /GRS 08a/ und /GRS 08b/). Dabei wurde die Übertragbarkeit der Ereignisse auf deutsche Anlagen bewertet, indem die in ausländischen Anlagen beobachteten Phänomene mit den aus deutschen Anlagen bekannten Phänomenen verglichen wurden. Diese Auswertung wurde im Vorhaben 3608R01338 für die Komponentenarten motorbetätigte Absperrarmaturen, Rückschlagarmaturen, Sicherheits- und Entlastungsventile, Batterien und Leistungsschalter fortgeführt (vgl. /GRS 11a/, /GRS 11b/).

Mit den Komponentenarten Steuerstäbe, Steuerstabantriebe und Wärmetauscher wurde diese Auswertung im Vorhaben 3611R01335 fortgesetzt. Mit Abschluss des Vorhabens 3611R01335 (/GRS 14a/ sowie /GRS 14b/) waren somit alle ICDE-Komponentenarten mit Ausnahme von Lüftern, Frischdampfisolationsventilen und Softwarebasierter Leittechnik erfasst, es bestanden jedoch erhebliche Unterschiede in der verwendeten Datenbasis. Für Kreiselpumpen und Diesel wurde der Auswertung ein Stand der Datenbank vom 06.09.2005 zugrunde gelegt /GRS 08a/, die Auswertung für Steuerstäbe und Wärmetauscher basierte auf einer Datenbasis mit Stand vom 20.06.2011 /GRS 14b/.

Im Vorgängervorhaben 3614R01301 wurden erstmals auch die Komponentenarten Lüfter, Frischdampfisolationsventile und Softwarebasierte Leittechnik erfasst. Hinzu kamen jetzt die Komponentenart Wechselrichter und die Unterkategorie komponentenübergreifender GVA.

2.1 Datenbasis

Seit der letzten Auswertung der ICDE-Ereignisse im Jahr 2017 hat sich die Zahl der ausländischen Ereignisse in der ICDE-Datenbank um 63 erhöht. Eine Übersicht über die im Rahmen von /GRS 08a/, /GRS 11b/, /GRS 14b/ und /GRS 17/ ausgewertete sowie die in der ICDE-Datenbank seitdem zusätzlich verfügbare Betriebserfahrung mit GVA ist in Tab. 2.1 dargestellt. Die neuen Ereignisse beschränken sich auf die sechs Komponentenarten Batterien, Kreiselpumpen, Steuerstäbe mit Antrieben, Notstromdiesel, Lüfter und Motorbetätigte Armaturen. Der höchste Anstieg ist in der Komponentenart Lüfter zu verzeichnen.

Tab. 2.1 Vergleich vorhandene und neue, bisher nicht ausgewertete GVA-Ereignisse

Komponentenart	Ausländische ICDE-Ereignisse	
	Gesamtanzahl	Anzahl neuer Ereignisse
Batterien	67	1
Leistungsschalter	98	-
Kreiselpumpen	344	14
Rückschlagarmaturen	98	-
Steuerstäbe mit Antrieben	167	1
Komponentenübergreifender GVA	0	-
Notstromdiesel	210	16
Digitale Leittechnik	0	-
Lüfter	30	30
Wärmetauscher	41	-
Wechselrichter	0	-
Füllstandsmessungen	146	-
Frischdampfisolationsventile	2	-
Motorbetätigte Armaturen	151	2
Sicherheits- & Entlastungsventile	225	-
Summe	1.579	63

Für die Auswertung wurden zunächst die von Deutschland in die ICDE-Datenbank eingespeisten Ereignisse von der Bewertung ausgeschlossen, da deren systematische Fehlermechanismen und Ursachen bereits durch die nationale Vorkommnisauswertung erfasst worden sind. Für die übrigen Ereignisse wurde das beobachtete GVA-Ereignis

kurz charakterisiert. Dabei wurde jeweils nur der Fehlermechanismus betrachtet, unabhängig davon, wie viele Komponenten auf Grund dieses Fehlermechanismus ausgefallen waren. Wenn sich dabei zeigte, dass ein Fehlermechanismus spezifisch für eine Bauart einer Komponente ist, die in Deutschland nicht eingesetzt wird, wurde auch dieses Ereignis nicht weiter betrachtet. Die verbleibenden identifizierten Fehlermechanismen wurden gruppiert, die Gruppierung erfolgte hierbei hinsichtlich der aufgetretenen Ursachen, betroffene Einrichtungen und Bauteile oder anderer Gemeinsamkeiten.

Anschließend wurde im Rahmen einer Expertenrunde zunächst diskutiert, ob die identifizierten Fehlermechanismen auch für deutsche Anlagen relevant sind. Ein Fehlermechanismus wurde dabei als relevant bewertet, wenn er auf deutsche Anlagen übertragbar, dort aber noch nicht beobachtet worden ist oder wenn er grundsätzlich aus der deutschen Betriebserfahrung bekannt ist, jedoch noch neue, sicherheitstechnisch relevante Aspekte beobachtet wurden. Bei den für deutsche KKW relevanten Fehlermechanismen wurde anschließend in der Expertenrunde diskutiert, ob der beobachtete Fehlermechanismus eine Weiterleitungsnachricht rechtfertigt oder ob er lediglich in Form eines sicherheitstechnischen Hinweises im Rahmen dieses Berichtes aufgegriffen wird.

In den folgenden Abschnitten werden für die in diesem Vorhaben ausgewerteten Komponentenarten zunächst jeweils die in der ausländischen Betriebserfahrung identifizierten Gruppen von Fehlermechanismen vorgestellt und kurz charakterisiert.

2.2 Komponentenart Batterien

In der ICDE-Datenbank sind 77 Ereignisbeschreibungen für die Komponentenart Batterien vorhanden. Zehn der Ereignisse beziehen sich auf deutsche Anlagen. Für die Auswertung wurde ein neuer ausländischer Eintrag bewertet.

Bei dem Ereignis fielen Batterien bei einem Kapazitätstest durch. Grund hierfür war eine vorzeitige Alterung wegen zu hoher Umgebungstemperaturen. Hinzu kam, dass die Erhaltungsladespannung nicht an die verwendeten Batterien und die verwendeten Gleichrichter angepasst waren. In Deutschland beschreibt die KTA-Regel 3703 wiederkehrende Prüfungen für Batterien. Hierin wird die Kontrolle der Temperatur und der Lüftungsanlage im Batterieraum, sowie die Kontrolle der Erhaltungsladespannung am Gleichrichter mindestens monatlich gefordert. Eine Übertragbarkeit ist damit nicht gegeben.

2.3 Komponentenart Kreiselpumpen

Die Komponentenart Kreiselpumpen enthält Pumpen in den redundant ausgelegten Sicherheitsteilsystemen. Dieses umfasst z. B. Sicherheitseinspeisepumpen, Not- und Nachkühlpumpen, Zwischenkühlpumpen und Nebenkühlwasserpumpen. Den Pumpen sind die jeweiligen elektro- und leittechnischen Einrichtungen zugeordnet, die alleinig dem Betrieb der jeweiligen Komponenten dienen, wie z. B. die Antriebssteuerung und der Leistungsschalter der jeweiligen Pumpe.

Von den insgesamt 376 GVA-Ereignissen in der ICDE-Datenbank für diese Komponentenart stammen 32 aus deutschen Anlagen. 14 neue ausländische Ereignisse wurden seit der letzten Auswertung in die Datenbank eingetragen. Für diese Ereignisse wurden die beobachteten GVA-Phänomene zusammengefasst und durch eine Expertengruppe auf ihre Relevanz für deutsche Anlagen bewertet. In Tab. 2.2 sind die gebildeten Gruppen von Fehlerkategorien mit der jeweiligen Ereignisanzahl dargestellt.

Tab. 2.2 Gruppierung der identifizierten Fehlermechanismen an Kreiselpumpen

Fehlerkategorie	Ereignisanzahl
Mechanische Schäden an Welle, Lager oder Laufrad	4
Fehler der Leittechnik und elektrischer Versorgung	3
Montage- und Wartungsmängel (Dichtungsschäden, Korrosion, Alterungsmanagement)	3
Vibrationen	3
Auslegungs- bzw. Konstruktionsfehler	1

Mechanische Schäden traten in vier Fällen auf. Diese betrafen zwei Mal einen Wellenanriss, einmal einen Lagerschaden und einmal Schäden an einer Laufradmutter.

Bei einem Fall führte der Mindestmengenbetrieb der betroffenen Nachkühlpumpe zum Ermüdungsbruch der Pumpenwelle. Die ungleichmäßige Umströmung der Laufradschaufeln führte zu Fretting. In einem anderen Fall wurde Fretting in einer Nachkühlpumpe durch eine gelöste Laufradmutter ausgelöst. Diese hatte sich in Folge hoher Temperaturschwankungen gelöst. Die Ursache für beide Fälle lag in spezifischen Bauteilfehlern, die durch gezielte Nachrüstmaßnahmen korrigiert wurden. In deutschen Anlagen sind Schäden an Pumpenwellen und gelösten Laufradmuttern bekannt und werden in der Weiterleitungsnachricht 2016-11 beschrieben.

In einem Fall der Fehlerkategorie „Fehler der Leittechnik und elektrischer Versorgung“ löste der Überspannungsschutz eines Schaltschranks das Abschalten einer Hauptkühlwasserpumpe aus. Nach thermografischen Untersuchungen am offenen Schaltschrank wurden die Schaltschranktüren zu stark geschlossen, was den in der Tür verbauten Überspannungsschutz auslöste. Ein anderer Fall war auf Fehler in den Leistungsschaltern der Pumpen zurückzuführen, in einem weiteren führte ein Phasenkurzschluss in einer von drei Hauptkühlwasserpumpen zu deren Versagen. Ähnliche Fehlerphänomene sind bereits in Deutschland bekannt und in der Auslegung bzw. den Prozessanweisungen berücksichtigt.

Drei Fälle konnten der Fehlerkategorie *Montage- und Wartungsmängel* zugeordnet werden. Diese zeigten sich in Form von Leckagen an Wellendichtungen, einem korrodierten Gewinde an Entwässerungsgewindestopfen und mangelhaftem Alterungsmanagement von Sicherheitseinrichtungen. Im Vergleich zur deutschen Betriebserfahrung ergeben sich hieraus aber keine neuen Erkenntnisse.

Ein Ereigniseintrag, der der Fehlerkategorie „Vibrationen“ zugeordnet wurde, teilt sich in drei Einzelereignisse auf, die in der Anlage an der gleichen Komponentengruppe in kurzem Abstand hintereinander auftraten. Einmal führte ein Fehler an der Statorwicklung zur Schwingungsanregung, das andere Mal war ein Schaden des Motoraxiallagers aufgrund von Kriechströmen für die Vibrationen verantwortlich. Die Erdung der Motorströme war hier nicht ausreichend. Beim letzten der drei Fälle lagen Kurzschlüsse in der Motorwicklung (1x Phasenschluss, 1x Erdschluss) vor. Die Ursache dieser Einzelereignisse wurde zu mangelhaftem Alterungsmanagement zusammengefasst und daher in einem Ereignis gemeldet. Weiterhin sind bei einem Ereignis Vibrationen aufgrund einer verdrehten Pumpenwelle aufgetreten. Schwingungen und Vibrationen sind aus der deutschen Betriebserfahrung hinreichend bekannt und liefern keine neuen Erkenntnisse.

Der Fehlerkategorie „Auslegungs- und Konstruktionsfehler“ wurde ein Ereignis zugeordnet. Hier kam es zum Startversagen einer Hilfsspeisewasserpumpe infolge des Ansprechens des Überstromschutzes der 6kV-Schiene. Zuvor waren neue Schütze in der betroffenen Redundanz eingebaut worden, bei denen jedoch das Zeitglied im Gegensatz zur vorherigen Version fehlte. Man nahm an, dass der eingebaute Filter den Gleichstromanteil filtert und das Zeitglied unnötig machte. Der Anlaufstrom innerhalb der ersten Millisekunden reichte zur Auslösung des Schützes jedoch aus. Schütze dieser Bauart werden in Deutschland nicht in sicherheitstechnisch wichtigen Systemen eingesetzt.

2.4 Komponentenart Steuerstäbe mit Antrieben

Für die Komponentenart Steuerstäbe mit Antrieben sind in der ICDE-Datenbank insgesamt 173 Einträge vorhanden, wobei sechs aus deutschen Anlagen stammen. In der zum Auswertungszeitraum verfügbaren Datenbasis war ein nicht ausgewerteter ausländischer Eintrag vorhanden.

Bei diesem Fall wurden 4 von 26 Steuerstäben beim Probetrieb der automatischen Leistungsregelung nicht in ihre Endposition verfahren. Dies war auf die systemspezifische Auslegung der Antriebssteuerung zurückzuführen. Je nach Art der Anlage unterscheiden sich die Konstruktionen der Steuerstabantriebe. Bestimmte Merkmale sind dabei nicht auf andere Konstruktionen übertragbar. So ist dieser Fall auf deutsche Stabantriebe nicht übertragbar.

2.5 Komponentenart Notstromdieselaggregate

Die Komponentenart Notstromdiesel umfasst das Notstromaggregat mit dem zugehörigen Notstromgenerator und Generatorschalter, zudem wird die Leittechnik zur Steuerung der Komponente mitefasst. Von den insgesamt 241 Ereignissen in der ICDE-Datenbank stammen 31 aus deutschen Anlagen. Es wurden seit der letzten Auswertung 16 neue ausländische GVA-Ereignisse zu der Datenbank hinzugefügt. Die Fehlermechanismen wurden im Rahmen des Vorhabens ausgewertet und nach der unten dargestellten Tabelle in Kategorien nach Gemeinsamkeiten, wie Ursache und betroffene Bauteile, gruppiert.

Tab. 2.3 Gruppierung der identifizierten Fehlermechanismen an Notstromdieselaggregaten

Fehlerkategorie	Ereignisanzahl
Konstruktions- und Bauteilfehler	4
Instandhaltungsfehler	5
Schäden an Halterungen	3
Leckage	2
Fehlsignale Messgeräte	2

Eine überwiegende Anzahl der beobachteten Ereignisse wurde durch bekannte Fehlermechanismen ausgelöst. Fünf Ereignisse wurden der Fehlerkategorie „Instandhaltungsfehler“ zugeordnet. Bei den Fehlern handelte es sich um Verdrahtungsfehler im Zusammenhang mit Prüfversäumnissen, Schwächen im Instandhaltung- und Alterungsmanagement, sowie Instandhaltungsarbeiten, die zu Rissen an einer Kraftstoffleitung führten.

In vier Fällen kam es zu bekannten „Konstruktions- und Bauteilfehlern“ der Notstromdiesel, wie etwa mangelndem Spiel einer Armatur im Kühlkreislauf oder Schäden an Pleuellagern wozu die GRS Empfehlungen in der Weiterleitungsnachricht 2010-02 geschrieben hat.

Bei drei Ereignissen traten Schäden an verschiedenen Halterungen auf. Darunter zwei Ereignisse bei denen erhöhte Abnutzungen an neuen Treibstoffleitungen im Bereich der Halterungen zu Korrosion führten und in einem fortgeschrittenen Stadium zur Leckage der Treibstoffleitungen geführt hätten. In einem weiteren Fall mit fehlerhaften Halterungen löste sich die Spindel-Antriebsverbindung am 3-Wege-Ventil im Motorkühlsystem. Im Anforderungsfall wären die Notstromdiesel zwar angelaufen, die fehlende Kühlung hätte aber zu einem Betriebsversagen geführt. In Deutschland sind Fälle mit fehlerhaften Halterungen bzw. deren Montage bekannt.

Leckagen traten bei zwei Ereignissen auf. Bei einem Ereignis führte eine geringe Wasserleckage an Zylinderköpfen und die sich daraus bildenden Tropfen zu Schäden am elektrischen Anschluss des Überdrehzahlschutzes und löste diesen aus, sodass ein Starten des Diesels im Anforderungsfall verhindert worden wäre. Gleichzeitig waren die

elektrischen Anschlüsse unzureichend isoliert. Bei einem zweiten Fall wurden Ablagerungen im Bereich der metallischen Dichtung der Dieseleinspritzpumpe an beiden Notstromdieseln vorgefunden. Dies war auf die Wirkung von Frostschutzmittel, dass im Bereich der Pumpenfeder aus einer Leckstelle trat, zurückzuführen. Schäden im Zusammenhang mit Frostschutzmitteln, insbesondere aufgrund deren Zusätze, sind in der deutschen Betriebserfahrung bekannt.

Fehlsignale von Messgeräten führten in zwei Fällen zu Ausfällen der Notstromdiesel. In beiden Fällen lieferten an zwei Notstromdieseln Temperaturmessgeräte Fehlsignale zur Regelung des 3-Wege-Ventils im Motokühlsystem, was einen potentiellen Ausfall während des Betriebs durch mangelnde Kühlung hervorgerufen hätte. Diese Fehlermechanismen sind in Deutschland bekannt.

2.6 Komponentenart Lüfter

Die Komponentenart Lüfter enthält sicherheitstechnisch wichtige Lüfter, die sich nicht bereits innerhalb der Komponentenabgrenzung einer anderen Komponentenart befinden (z. B. bei den Notstromdieselaggregaten oder Kreiselpumpen). Betrachtet werden sowohl radiale als auch axiale Lüfter, die weiter durch ihre Leistung (unter 10 kW und über 10 kW) unterteilt werden. Als Ausfallarten werden „startet nicht“ und „Betriebsversagen“ betrachtet. Von den insgesamt 32 Ereignissen in der ICDE-Datenbank stammen 2 aus deutschen Anlagen. Da sich zum Zeitpunkt der letzten Auswertung ausländischer Ereignisse noch keine Ereignisse mit Lüftern in der Datenbank befanden, werden hier erstmals ausländische Ereignisse mit Lüftern ausgewertet. Zunächst wurden die Fehlermechanismen ausgewertet und nach der unten dargestellten Tabelle in Kategorien nach Gemeinsamkeiten, wie Ursache und betroffene Bauteile, gruppiert.

Tab. 2.4 Gruppierung der identifizierten Fehlermechanismen an Lüftern

Fehlerkategorie	Ereignisanzahl
Schäden am Antriebsriemen	12
Bauteilfehler	9
Instandhaltungsfehler	4
Lagerschäden	3
Fehler in der Leittechnik	2

Bei der Komponentenart Lüfter traten die meisten Fehler in der Kategorie *Schäden am Antriebsriemen* auf. Die Ursache lag sehr häufig an einem mangelhaften Alterungsmanagement. Nicht getauschte Riemen versprödeten und rissen. Weiterhin traten im Zusammenhang mit Antriebsriemen fehlerhafte Instandhaltungsmaßnahmen auf. Fehlpositionierte Gehäuse führten zu erhöhter Reibung an den Antriebsriemen. Antriebsrollen auf Motor und Lüfterseite wurden falsch positioniert, wodurch sich die Antriebsriemen verdrehten. Für die deutsche Betriebserfahrung ergeben sich hieraus keine neuen Erkenntnisse.

Am zweithäufigsten traten *Bauteilfehler* auf. Es kam zu bekannten Fehlermechanismen wie Schäden an einem Kabel wegen häufigem An- und Abklemmen, Motorüberhitzung aufgrund fehlerhafter Wicklungen und fehlerhaften Fixierungsstiften am Gehäuse. In einem Fall führte ein nachträglicher Tausch des Magnetkerns in einem Relais zu dessen Versagen, was in der Folge zum Ausfall der Wartenlüftung führte. Diese Phänomene und Ausfallmechanismen sind in der deutschen Betriebserfahrung bekannt. In weiteren Fällen waren fehlerhafte Sicherungen ereignisauslösend. Hier kam es zur Fehlauslösung, die durch eine Kombination aus hohen Anlaufströmen und schnellen Sicherungen verursacht wurde. Der hohe und langandauernde Anlaufstrom hatte die Charakteristik der Sicherung mit der Zeit verändert. Die Betreiber starteten im Nachgang ein Austauschprogramm zum Einsatz von langsamen Sicherungen. Die Priorität lag dabei auf Systemen mit Komponenten, die Betriebsarten mit hohen Anlaufströmen mit einem Nennstrom > 4 A durchlaufen und mit schnellen 10 A-Sicherungen abgesichert waren. Für die deutsche Betriebserfahrung leitet sich hieraus ein Hinweis ab.

Weiterhin traten vier *Instandhaltungsfehler* auf. Es wurden Instandhaltungsarbeiten an redundanten Lüftern gleichzeitig durchgeführt und ein vergessener Schweißdraht blockierte die Zuluftklappen des Hilfsanlagengebäudes. Weiterhin wurde in einem Fall

Schmiermittel verwendet, das nicht den Herstellervorgaben entsprach, in einem anderen Fall führte eine übermäßige Schmierung der Motorwicklung zur Überhitzung der Motorlager. Da das letztgenannte Phänomen aus der deutschen Betriebserfahrung bislang nicht bekannt war, ergibt sich hieraus ein Hinweis.

Lagerschäden traten bei einem Ereignis aufgrund von gelösten Lagerteilen auf. In den beiden anderen Ereignissen mit Lagerschäden ist die Ereignisursache unbekannt.

Zwei Ereignisse wurden wegen Fehlern in der Leittechnik ausgelöst. Bei einem Ereignis erlitt ein Durchflussmessgerät einen Schaden und lieferte falsche Messwerte, bei einem weiteren Ereignis führte ein Fehler in der Steuerelektronik mit gleichzeitiger Anforderung von Start und Stopp auf Grund einer Fehlstellung/-positionierung eines Luftregisters zum Verschleiß des Riemens und erhöhter Temperatur und letztlich zum Ausfall zweier Lüfter. Ähnliche Ereignisse mit Leittechnikfehlern sind aus der deutschen Betriebserfahrung bekannt.

Zusammenfassend lässt sich feststellen, dass in der hier ausgewerteten internationalen Betriebserfahrung mit Lüftern zwei systematische Fehlermechanismen beobachtet wurden, die auf deutsche Anlagen übertragbar, aber aus der deutschen Betriebserfahrung mit GVA noch nicht bekannt sind. Diese aus der deutschen Betriebserfahrung bisher unbekannt systematischen Fehlermechanismen und ihre Ursachen sind in Tabelle 2.5 dargestellt.

Tab. 2.5 Für deutsche KKW relevante systematische Fehlermechanismen bei Lüftern

Fehlerkategorie	Fehlermechanismus
Bauteilfehler	Veränderung der Auslösecharakteristik von schnellauslösenden Sicherungen der Lüftermotoren nach häufigen Starts mit hohen Anlaufströmen
Instandhaltungsfehler	Übermäßige Schmierung der Motorwicklung führt zur Überhitzung der Motorlager

Hieraus leitet die GRS folgende sicherheitstechnische Hinweise ab:

- Im Alterungsmanagement von Lüftern sollte auch eine mögliche Kennliniendrift von Sicherungen berücksichtigt werden.
- Bei der Instandhaltung von Lüftermotoren sollten die verwendeten Schmiermittelmengen angemessen sein.

2.7 Komponentenart motorbetätigte Absperrarmaturen (MOVs)

Im Rahmen des ICDE-Projekts werden Ereignisse an motorbetätigten Absperrarmaturen in sicherheitstechnisch wichtigen Systemen gesammelt, dies umfasst unter anderem folgende Systeme:

- Notspeisesystem
- Not- und Nachkühlsystem
- Zwischenkühlwassersystem
- Nebenkühlwassersystem
- Absperrventile vor den Druckhalterabblaseventilen.

Von 168 Einträgen in der ICDE-Datenbank stammen 17 aus deutschen Anlagen. Es wurden seit der letzten Auswertung zwei neue ausländische GVA-Ereignisse zu der Datenbank hinzugefügt.

Bei einem Ereignis kam es zum fehlerhaften Schließen von zwei Ventilen im Nachwärmeabfuhrsystem aufgrund starken Verschleißes an den Innengewinden der Gewindemuttern. Für die deutsche Betriebserfahrung ergeben sich hieraus keine neuen Erkenntnisse.

Beim zweiten Ereignis ließen sich zwei Ventile des Nachkühlsystems nach der Reparatur eines Entlüftungsventils nicht mehr öffnen. Unterschiedliche thermische Expansion des Ventilgehäuses im Sitz führte zu erhöhten Reibkräften und zum Ausfall von zwei redundanten Ventilen. Derartige Fälle mit motorbetätigten Armaturen sind in Deutschland bislang nicht bekannt, jedoch trat ein ähnlicher Fall bereits 1992 bei Druckhalterarmaturen auf. Ein Sicherheitsventil öffnete während einer WKP nicht, da u. a. der Sitz und Kegel aus Materialien mit unterschiedlichem Ausdehnungskoeffizienten hergestellt waren. Bei Abkühlungsprozessen zieht sich der Sitz stärker zusammen als der Kegel und umklammert diesen. Letztlich führten Änderungen an der Einbaugeometrie zur Abhilfe. Der Fehlermechanismus ist somit aus der deutschen Betriebserfahrung bekannt.

2.8 Zusammenfassung der Auswertungen

Im Rahmen von AP 2 des Vorhabens wurde für alle innerhalb des ICDE-Projekts erfassten Komponentenarten die mit Stand vom 06.05.2020 in der Datenbank enthaltene internationale Betriebserfahrung mit GVA ausgewertet. Insgesamt wurden bis jetzt 1.536 ausländische GVA-Ereignisse ausgewertet, 63 GVA-Ereignisse wurden im Rahmen dieses Vorhabens analysiert. Durch diese Auswertungen konnte der Erfahrungsumfang bezüglich GVA-Ereignisse und somit auch bezüglich der zugrundeliegenden Fehlermechanismen im Vergleich zur rein deutschen GVA-Betriebserfahrung ausgeweitet werden.

Im Zuge der Auswertungen konnten auch ein neuer Fehlermechanismus identifiziert und Häufungen bestimmter Fehlermechanismen in der ausländischen Betriebserfahrung beobachtet werden, die in der deutschen Betriebserfahrung alleine nicht zu beobachten sind. Sofern die beobachteten Fehlermechanismen auch für deutsche Anlagen relevant waren, wurden sicherheitstechnische Hinweise formuliert.

Die GRS beabsichtigt, im Rahmen des geplanten Nachfolgevorhabens zu 4717R01337 eine kontinuierliche, jährliche Auswertung der in die ICDE-Datenbank eingespeisten GVA-Ereignisse aus ausländischen KKW durchzuführen, um daraus sicherheitstechni-

sche Hinweise oder Weiterleitungsnachrichten ableiten zu können. Diese Vorgehensweise würde einen Beitrag dazu leisten, den durch die kontinuierliche Abschaltung deutscher Anlagen verursachten Verlust an nationaler Betriebserfahrung auszugleichen.

A Anhang

A.1 Organisation des ICDE-Projekts

A.1.1 Aufgabenverteilung innerhalb des Projekts

Im Rahmen des ICDE-Vorhabens müssen erhebliche Mengen sensibler Informationen – sowohl bezüglich der Anlagentechnik wie auch der beobachteten Ereignisse – sicher und effizient gehandhabt werden. Um dies zu gewährleisten, ist das ICDE-Projekt, dessen vorbereitende Aktivitäten Ende 1994 anliefen, in eine etablierte internationale Organisation eingebunden. Seit Ende 1996 hat das „Committee on the Safety of Nuclear Installations“ (CSNI) der OECD/NEA die formale Verwaltung des ICDE-Projekts übernommen.

Die Steuerung des Projekts erfolgt durch den ICDE-Lenkungskreis („Steering Group“). Dieser wird dabei vom NEA-Sekretariat und dem so genannten „Operating Agent“ unterstützt. Das NEA-Sekretariat ist verantwortlich für die finanzielle Verwaltung und technische Unterstützung des Projekts seitens der OECD/NEA. Der Operating Agent ist für die Datenbank und die Konsistenz der Daten verantwortlich. Der Lenkungsreis tagt durchschnittlich zweimal pro Jahr. Die im ICDE-Lenkungskreis zusammengeschlossenen Partnerorganisationen verpflichten sich in einer jeweils über drei oder vier Jahre laufenden Vereinbarung, fachlich zu dem Projekt beizutragen und die anteiligen Kosten für den Operating Agent zu übernehmen. Die aktuelle Vereinbarung („Phase 8“) läuft noch bis Dezember 2022.

A.1.1.1 ICDE-Lenkungskreis

Der ICDE-Lenkungskreis wird von den Projektkoordinatoren aller Teilnehmerorganisationen gebildet. Zum Verantwortungsbereich des ICDE-Lenkungskreises gehört es u. a., dass Entscheidungen getroffen werden zur

- Vorbereitung der rechtlich verbindlichen Vereinbarung zur Projektdurchführung,
- Sicherstellung der finanziellen Mittel zur Durchführung des Projekts durch Genehmigung des Budgets und der Kontrolle der Verwendung der Mittel,
- Sicherstellung der technischen Mittel, die zur Projektdurchführung notwendig sind,

- Benennung des Vorsitzenden des ICDE-Projekts,
- Aufnahme neuer Mitglieder,
- Abstimmung über Art und Umfang der auszutauschenden Informationen,
- Entwicklung von detaillierten Anforderungen an die Informationstiefe zu den GVA-Ereignissen und den zugehörigen Beobachtungseinheiten (Komponentengruppen), die in die ICDE-Datenbank aufgenommen werden sollen, und von Vorgaben zur Klassifizierung und Bewertung von ICDE-Ereignissen,
- Benennung von Federführenden für einzelne Projektaufgaben,
- Festlegung von Prioritäten für einzelne Aufgaben,
- Überwachung des Fortschritts der einzelnen Projektaufgaben,
- Überwachung der Arbeiten des Operating Agents,
- Bestimmung des Informationsflusses (öffentliche Information und Vertraulichkeit),
- Aufbau und Inhalt der Projektberichte,
- Qualitätssicherung.

Gegenwärtig sind folgende Partnerorganisationen im Lenkungskreis des ICDE-Projekts vertreten und bringen dort die Betriebserfahrung mit GVA-Ereignissen aus ihren jeweiligen Heimatländern ein: NRC (USA), CNSC (Kanada), IRSN (Frankreich), GRS (Deutschland), ENSI (Schweiz), SSM (Schweden), STUK (Finnland), NRA (Japan), UJV (Tschechische Republik) und ANVS (Niederlande). In den Heimatländern der beteiligten Organisationen werden mehr als 58 % (256 von 441) der weltweit existierenden Kernkraftwerksblöcke betrieben.

Die Einspeisung von Daten erfolgt über die Projektkoordinatoren der einzelnen Teilnehmerorganisationen. Die ICDE-Datenbank ist nur für diejenigen Organisationen zugänglich, die die rechtlich verbindliche Vereinbarung zur Projektdurchführung unterschrieben und selbst auch eigene Daten eingespeist haben.

A.1.1.2 NEA-Sekretariat

Die OECD/NEA ist verantwortlich für die Verwaltung des Projekts entsprechend der Regeln der OECD. Dies beinhaltet Sekretariats- und Verwaltungsarbeiten im Zusammenhang mit der Finanzierung des Projekts wie Einforderung der Umlage der Mitgliedsorganisationen, Bezahlung des Operating Agents und Führung des Projekthaushalts. Die NEA bestimmt das Projektsekretariat, hat jedoch keinen Einfluss auf die inhaltliche Arbeit des Lenkungsausschusses.

A.1.1.3 Operating Agent

Der Operating Agent betreibt die ICDE-Datenbank und übernimmt die zentrale Führung der Projektdokumentation. Der Operating Agent führt die von den Projektteilnehmern gelieferten Informationen in der ICDE-Datenbank zusammen. Dabei kontrolliert er, ob die von den Projektkoordinatoren der teilnehmenden Organisationen zur Verfügung gestellten Informationen mit den Anforderungen der ICDE-Kodieranleitungen übereinstimmen. Zusammen mit den Projektkoordinatoren der teilnehmenden Organisationen stellt der Operating Agent sicher, dass die für den Austausch zur Verfügung gestellten Informationen korrekt in die ICDE-Datenbank aufgenommen werden. Die detaillierte Aufgabenverteilung zur Qualitätssicherung ist in einem Arbeitspapier des Projekts festgelegt („ICDE Quality Assurance Programme“).

A.1.2 Vertraulichkeit der ICDE-Daten

Für den detaillierten Informationsaustausch zu GVA-Ereignissen innerhalb des ICDE ist eine besondere Vertraulichkeit vereinbart worden, die dadurch gewahrt wird, dass die Ereignisberichte und die darin enthaltenen Detailinformationen als Geschäftsgeheimnisse zu behandeln sind (*proprietary information*) und als Arbeitsmaterial nur für die Teilnehmer des ICDE-Lenkungskreises, die aktiv zu dem Datenaustausch beitragen, zugänglich sind. Vertrauliche Informationen, die nur für den ICDE-Lenkungskreis freigegeben worden sind, werden nicht an die OECD/NEA weitergegeben.

A.1.3 Zustimmung der deutschen Betreiber

Für eine aktive Teilnahme am internationalen GVA-Datenaustausch und für eine Mitarbeit im ICDE-Lenkungskreis ist die Weitergabe von Informationen aus dem eigenen Herkunftsland erforderlich. Hierbei handelt es sich zum einen um Informationen bezüglich des Aufbaus der Anlagen, zum anderen um Berichte bezüglich der beobachteten Ereignisse mit GVA-Potenzial. Die entsprechenden Informationen liegen der GRS vor und werden von dieser entsprechend den Vorgaben des ICDE-Projekts aufbereitet.

Um solche Informationen an andere Teilnehmerorganisationen weitergeben zu können, ist die Zustimmung der deutschen Betreiber erforderlich. Diese Zustimmung ist der GRS von der Technischen Vereinigung der Großkraftwerksbetreiber e.V. (VGB) Ende 1997 formell erteilt worden. Zwischen GRS und VGB ist vereinbart worden, dass die Datenweitergabe an den ICDE-Lenkungskreis in gleicher Weise wie bei der Weitergabe von Meldungen an das „Incident Reporting System“ (IRS) der OECD/NEA bzw. der IAEA erfolgt. Dabei erstellt die GRS zunächst die Informationen zu den GVA-Ereignissen entsprechend den ICDE-Anforderungen in englischer Sprache und versendet sie dann vor der Weitergabe an den ICDE-Lenkungskreis an die Betreiber der jeweiligen Kernkraftwerke zur Abstimmung. Die im Rahmen der Zusammenarbeit von den ausländischen Teilnehmern dem ICDE-Lenkungskreis zur Verfügung gestellten Informationen werden dann von der GRS der VGB zur Verfügung gestellt. Diese verteilt die Informationen an alle Betreiber der deutschen Kernkraftwerke. Auch dieser Informationsaustausch unterliegt in beiden Richtungen wegen seiner Sensitivität der besonderen Vertraulichkeit (siehe hierzu Abschnitt A 1.2).

A.2 Abstimmung von Art und Umfang der für den ICDE-Datenaustausch vorgesehenen Informationen

Im Rahmen der Arbeiten, an denen die GRS im Rahmen der Vorläufervorhaben zum aktuellen Vorhaben 4717R01337 teilgenommen hat, ist zur Sicherstellung einer einheitlichen Qualität der ausgetauschten Informationen vom ICDE-Lenkungskreis eine grundsätzliche Abstimmung über Art und Umfang der auszutauschenden Informationen vorgenommen und ein entsprechendes allgemeines Datenaustauschformat erarbeitet worden. Auf Basis dieses Formats ist die ICDE-Datenbank entwickelt worden.

Das allgemeine Datenaustauschformat beinhaltet detaillierte Anforderungen an die Informationstiefe zu den GVA-Ereignissen, die in die ICDE-Datenbank aufgenommen werden sollen. Außerdem werden Erläuterungen zur Klassifizierung und Bewertung von ICDE-Ereignissen gegeben. Die entsprechenden Erläuterungen, Anleitungen und Hinweise werden in einer „Kodieranleitung“, dem *General Coding Guide* zusammengefasst. Der General Coding Guide beschreibt zum einen das für sämtliche Komponentenarten gültige Datenaustauschformat und zum anderen für jede einzelne Komponententart die entsprechenden Besonderheiten. Zusätzlich sind Hinweise und Erläuterungen zur Analyse von GVA-Ereignissen enthalten.

Im Berichtszeitraum wurde zusätzlich zu den schon vorhandenen komponentenartsspezifischen Kodieranleitungen (Kreiselpumpen, Notstromdieselmotoren, motorbetriebene Absperrarmaturen, Rückschlagarmaturen, Sicherheits- und Entlastungsventile, Batterien, Füllstandsmessungen, Leistungsschalter, Steuerstäbe und Steuerstabantriebe, Wärmetauscher, Frischdampfisolationsventile, Lüfter, Softwarebasierte Leittechnik und Umformer (Wechselrichter)) an einer Kodieranleitung für komponentengruppenübergreifende GVA gearbeitet. Diese liegt als Entwurf vor.

Die aktuelle Fassung des General Coding Guide ist diesem Bericht in Anhang A beigelegt. In dieser Fassung sind sowohl die allgemeinen Kodieranleitungen, die bis jetzt fertiggestellten komponentenspezifischen Kodieranleitungen, die „Failure Analysis Coding Guidelines“ und die neuentwickelte „CCF Root Cause Analysis“ enthalten. In den Failure Analysis Coding Guidelines werden Kriterien und Definitionen für die vertiefte qualitative Analyse der ICDE-Ereignisse definiert. In der CCF Root Cause Analysis wird beschrieben, wie die Ereignisursache anhand der kodierten Ereignismerkmale bestimmt wird. Unter A 2.5.2 wird dieses Vorgehen genauer beschrieben. Der General Coding Guide wird stetig fortgeschrieben.

Ausgehend von der als CSNI Tech Note Publication NEA/CSNI/R(2004)4 im Jahr 2004 veröffentlichten Fassung wurden bis 2020 insgesamt neun innerhalb der ICDE-Projektdokumentation verfügbare Revisionen und drei Veröffentlichungen des Dokuments erarbeitet.

In den nachfolgenden Abschnitten wird ein kurzer Überblick über den Inhalt der Kodieranleitungen gegeben. Anschließend wird die Struktur der ICDE-Datenbank vorgestellt.

A.2.1 Allgemeine ICDE-Kodieranleitung

Die allgemeine ICDE-Kodieranleitung /ICDE 19/ beschreibt den Umfang des im Rahmen des ICDE-Projekts angelegten Datenaustauschs hinsichtlich der zu erfassenden Komponentenarten und definiert:

- Ereignisse, die für den Datenaustausch in Frage kommen, als ICDE-Ereignisse, die sowohl GVA-Ereignisse als auch potentielle GVA-Ereignisse sein können (durch die Ausweitung des GVA-Datenaustauschs auf potentielle GVA-Ereignisse soll die Sammlung von GVA-Phänomenen auf eine möglichst breite Basis gestellt werden),
- wie die Beobachtungseinheiten (Komponentengruppen), für die ICDE-Ereignisse gesammelt bzw. gebildet werden, kodiert werden,
- welche Informationen zur Identifizierung und Beschreibung einer Beobachtungseinheit erforderlich sind,
- welche statistischen Informationen zur Bestimmung der Beobachtungszeit bzw. entsprechender Bezugsgrößen für jede Beobachtungseinheit erforderlich sind,
- welche Informationen zur Beschreibung und Klassifizierung eines beobachteten ICDE-Ereignisses erforderlich sind.

Die einzelnen Informationen werden in entsprechenden Feldern der ICDE-Datenbank abgelegt. Zu jedem Datenfeld gibt es Vorgaben aus den allgemeinen Kodieranleitungen. Dies sind z. B. Merkpostenlisten, um eine umfassende und damit auswertbare Beschreibung der ICDE-Ereignisse sicherzustellen, oder Erläuterungen zur Klassifizierung und Bewertung der Ereignisse.

A.2.2 Komponentenartspezifische Kodieranleitungen

Die komponentenartspezifischen Kodieranleitungen umfassen

- eine allgemeine Beschreibung der zu erfassenden Komponenten einschließlich ihrer Aufgaben und Funktionsweise,
- eine Liste der Systeme, aus denen ICDE-Ereignisse mit diesen Komponenten erfasst werden sollen,
- eine Liste der Typen von Komponenten, die zu der betrachteten Komponentenart erfasst werden sollen (mit Typen sind hier nicht die Typbezeichnungen einzelner Hersteller gemeint, sondern Klassen von Komponenten einer Komponentenart, die sich nach physikalischer Funktionsweise oder prinzipiellem mechanischem Aufbau unterscheiden; bei Rückschlagarmaturen wird beispielsweise nach Rückschlagklappen und Rückschlagventilen unterschieden, bei Druckmessumformern unter anderem nach Messumformern mit Membranmesswerk oder mit Rohrfedermesswerk),
- eine Festlegung der Komponentengrenzen,
- eine Definition eines (Ausfall-)Ereignisses bei den betrachteten Komponenten,
- eine Festlegung, welche Komponenten zu einer Beobachtungseinheit/Komponentengruppe für die Erfassung von ICDE-Ereignissen zusammengefasst werden,
- eine Festlegung des minimalen Zeitraums, für den eine Auswertung der Betriebserfahrung durchgeführt werden soll,
- eine Liste von allgemeinen Regeln zur Kodierung von ICDE-Ereignissen,
- eine Definition der relevanten Ausfallarten und Beispiele zur Bewertung von geschädigten Komponenten, die zum Zeitpunkt der Entdeckung des Schadens im Hinblick auf die bewertete Ausfallart (z. B. Pumpe fördert nicht) nicht vollständig funktionsunfähig waren,
- eine Liste von Ausfallarten, für die die Auswertung der Betriebserfahrung obligatorisch ist, und eine Liste von Ausfallarten, für die die Betriebserfahrung optional eingespeist werden kann.

Aus den Erfahrungen der in den letzten Jahren im Rahmen des Lenkungskreises durchgeführten themen- und komponentenspezifischen Workshops zeigte sich, dass es zahlreiche offensichtliche oder versteckte Abhängigkeiten zwischen den einzelnen in den

komponentenartspezifischen Kodieranleitungen definierten Beobachtungseinheiten / Komponentengruppen gibt, wie z. B. gemeinsame Instandhaltungsteams und -verfahren, Einzelteile, die in mehreren Komponentengruppen verwendet werden, gemeinsames Kühlwasser, übergeordnete Leittechnik oder interne und externe Faktoren, die mehrere Komponentengruppen gleichzeitig betreffen können. Da systematische Fehler in diesen Bereichen zu schweren Beeinträchtigungen der Sicherheitssysteme führen können, sollen diese in Zukunft in Form von komponentengruppenübergreifenden GVA erfasst und analysiert werden.

Im Berichtszeitraum wurde deshalb eine Kodieranleitung für komponentengruppenübergreifende GVA erstellt, die sich derzeit im Entwurfsstadium befindet. Die Erfassung solcher komponentengruppenübergreifenden GVA erforderte spezielle Anpassungen in der Datenbanksoftware durch den Operating Agent. Mit dieser Anpassung ist es jetzt möglich ein beobachtetes Ereignis mehreren Komponentengruppen zuzuordnen. Derzeit werden erste Erfahrungen mit den neuen Möglichkeiten zur Kodierung gesammelt.

A.2.3 Kodieranleitung zur Ereignisanalyse

Die mit dem bisher durchgeführten Datenaustausch gewonnene Erfahrung nutzt der ICDE-Lenkungskreis, um bei Bedarf die Kodieranleitungen zu überarbeiten bzw. zu ergänzen. Folgende Aspekte werden im Rahmen der vom ICDE-Lenkungskreis durchgeführten Analysen erfasst und in der ICDE-Datenbank als Teil der "Common Cause Event Records" zu den Ereignissen zusätzlich kodiert:

- Eine Liste von Codes zur Markierung von „wichtigen“ Ereignissen, die neben dem GVA-Aspekt aus anderen Gründen von Interesse sind, z. B. Ereignisse,
 - bei denen mehrere unterschiedliche GVA aufgetreten sind,
 - die nicht mit dem normalen Prüfprogramm erkannt wurden,
 - bei denen nicht bekannte Abhängigkeiten erkannt wurden,
 - bei denen mehrere Blöcke betroffen waren,
 - bei denen es zu komponentengruppenübergreifenden Ausfällen gekommen ist,
 - bei denen mehrere Qualitätssicherungsmaßnahmen zur Verhinderung von GVA versagt hatten.

- Eine Liste von Schweregradklassen zur Bewertung von GVA mitsamt entsprechender Filter für die Datenbankoberfläche, um Analysen von Ereignissen mit ähnlichen Auswirkungen auf die jeweilige Komponentengruppe zu ermöglichen, z. B:
 - vollständiger Ausfall aller Komponenten einer Komponentengruppe,
 - mehrere, aber nicht alle Komponenten einer Komponentengruppe ausgefallen,
 - eine Komponente ausgefallen und mindestens eine weitere Komponente beeinträchtigt,
 - alle Komponenten der Komponentengruppe ausgefallen oder beeinträchtigt,
 - alle Komponenten der Komponentengruppe beeinträchtigt, aber keine ausgefallen,
 - mehrere, aber nicht alle Komponenten einer Komponentengruppe beeinträchtigt, aber keine Komponente ausgefallen.

Darüber enthält die Kodieranleitung zur Ereignisanalyse die verschiedenen zusätzlichen Klassifizierungen der Ereignisse, die in der Vergangenheit in den Auswerteberichten des ICDE-Projekts (siehe Abschnitt A.3.2) verwendet wurden.

Hierbei handelt es sich vor allem um zusätzliche Bewertungskategorien zur Klassifizierung von Fehlermechanismen und Ausfallursachen (*Failure Cause Categories*) für statistische Aufbereitungen der Ereignisse in den Auswerteberichten. Es wurden zwei Gruppen von Ausfallursachen definiert:

- Mängel in der Betriebsführung:
 - Unzulängliche Instandhaltungs- oder Testprozeduren
 - Alterungsmanagement unzureichend
 - Fehler der Betriebsmannschaft bei Instandhaltung/Test
- Design, Konstruktions- oder Herstellungsfehler:
 - Ungeeignetes Design einer Komponente oder eines Systems
 - Unzureichende Konstruktion oder Herstellung
 - Ungeeignete Design-Modifikation

Des Weiteren enthält die Kodieranleitung zur Ereignisanalyse systematisierte, komponentenartsspezifische Codes zur Beschreibung von GVA-Fehlermechanismen (*Failure mechanism category* bzw. *Failure mechanism sub-category*). Die entsprechenden Codes wurden sukzessive im Rahmen der Workshops entwickelt und liegen jetzt für alle Komponententypen mit Ausnahme von Lüftern, Frischdampfisolationsventilen sowie Softwarebasierter Leittechnik vor. Für die noch ausstehenden Komponententypen ist die Zahl der in der Datenbank hinterlegten Ereignisse noch nicht groß genug, um im Rahmen eines Komponentenworkshops entsprechende Kategorien zu entwickeln. Sobald ein entsprechender Umfang an Betriebserfahrung vorliegt, werden die entsprechenden Codes für die noch ausstehenden Komponententypen (einschließlich der jüngsten Komponententyp „Wechselrichter“) entwickelt und ausformuliert.

A.2.4 Root Cause Analysis

Bei den in den letzten Jahren durchgeführten Workshops zeigte sich bei einigen Ereignissen, dass die in der Datenbank kodierten Ereignisursachen (alte Root causes) nicht eindeutig aus den Ereignisbeschreibungen ableitbar waren. Bei mehreren Ereignissen war es möglich, mehrere Root causes zu identifizieren, von denen aber nur eine in der Datenbank kodiert war. Ausgehend von dieser Schwierigkeit, eine Ereignisursache unter Berücksichtigung verschiedener beitragender Aspekte zu bestimmen, wurde die Kodierung des Datenbankfeldes Root cause erweitert und das Konzept der „Root Cause Analysis“ entwickelt. In den Workshops fiel auf, dass die Begründung der Root causes nicht immer nachvollziehbar war. Dem Konzept wurde folgende Definition /IAEA 14/ der Ereignisursache vorangestellt:

The root cause is the most fundamental reason for an event or adverse condition, which if corrected will effectively prevent or minimize recurrence of the event or condition.

Die Ereignisursache ist der grundlegendste Grund für ein Ereignis oder einen ungünstigen Zustand, der, wenn er korrigiert wird, das Wiederauftreten des Ereignisses oder Zustands wirksam verhindert oder minimiert.

Zur Umsetzung des neuen Konzepts wurde das bisherige in der ICDE-Datenbank verwendete Datenfeld Root cause in Event Cause umbenannt und ein zusätzliches Feld Root cause eingefügt.

Um eine Ereignisursache (neue Root cause) zu bestimmen, werden nun Teile der bereits in der Datenbank vorzufindenden Kodierungen nach einem bestimmten Schema kombiniert. Dieses Vorgehen wird automatisch durch die Datenbanksoftware umgesetzt und ist in der neuesten Version enthalten (siehe Abschnitt A.2.5.2). Im Anhang 3 der allgemeinen Kodieranleitung /ICDE 19/ wird das Vorgehen genauer beschrieben.

A.2.5 ICDE-Datenbank

Die Oberfläche der ICDE-Datenbank basiert auf der .NET Software der Firma Microsoft. Für jede im Rahmen des ICDE-Datenaustauschs erfasste Komponentenart gibt es eine eigene Datenbankansicht. Diese Ansichten sind unter einer Oberfläche integriert. Die Zugangsmöglichkeiten zu den einzelnen Ansichten und damit zu den für jede Komponentenart erfassten Informationen sind durch ein umfangreiches Berechtigungssystem reglementiert.

Für den ersten Datenaustausch zu einer neuen Komponentenart ergänzt der Operating Agent die Definitionstabellen der ICDE-Datenbank nach der Abstimmung der komponentenartspezifischen Kodieranleitung im ICDE-Lenkungskreis mit den entsprechenden Wertelisten und erzeugt so eine „leere“ Datenbank als neue Ansicht für die neue Komponentenart. Nach einer ersten Erprobung der „leeren“ Datenbank durch die für die jeweilige Komponentenart federführende Organisation sendet der Operating Agent je eine Kopie der ergänzten Datenbank an die Projektkoordinatoren derjenigen Organisationen, die am Datenaustausch teilnehmen wollen. Diese Projektkoordinatoren sorgen dann dafür, dass die Betriebserfahrung aus den eigenen Herkunftsländern entsprechend den Vorgaben und Mindestanforderungen aus den Kodierungsanleitungen erfasst und in ihre Datenbankkopie eingespeist wird. Diese senden sie dann an den Operating Agent, der eine Qualitätssicherung durchführt (siehe Abschnitt A 1.1), gegebenenfalls Klarstellungen oder Ergänzungen seitens des Projektkoordinators der federführenden Organisation einfordert und danach die Daten in die Stamm-Datenbank überspielt.

Wenn die Daten aller Teilnehmer am ersten Datenaustausch zu einer neuen Komponentenart eingegangen sind, erhält jede Organisation, die eigene Daten geliefert hat, die Stammdatenbank mit allen Daten aus dem ersten Datenaustausch dieser Teilnehmer zugesandt.

Bei späteren Datenupdates, bei denen für eine Komponentenart zusätzliche Beobachtungszeiträume ausgewertet werden, erhält jede Organisation, die eigene Daten geliefert

hat, die Stammdatenbank mit allen Daten zugesandt, auf die die Organisation zugriffsberechtigt ist. Da nicht alle Organisationen bei jeder Komponentenart am Datenaustausch teilnehmen und bei den einzelnen Komponentenarten nicht in gleichem Umfang Daten in die ICDE-Datenbank einspeisen, wird auf diese Weise sichergestellt, dass jede Organisation nur Daten für solche Komponentenarten und Auswertzeiträume erhält, für die sie auch eigene Beiträge geliefert hat.

A.2.5.1 Struktur der ICDE-Datenbank

Die ICDE-Datenbank besteht aus zwei Teilen:

In den „**Observed Population Records (OP-Records)**“ werden die einzelnen Beobachtungseinheiten/Komponentengruppen beschrieben, die zum ausgewerteten Beobachtungsumfang gehören. Bei diesen Beobachtungseinheiten bzw. Komponentengruppen handelt es sich i. d. R. um Gruppen aus gleichartigen, redundanten Komponenten (wie z. B. die vier D1-Notstromdiesel in einem deutschen DWR), die eine identische oder sehr ähnliche Aufgabe im Sicherheitssystem haben. Erfasst werden u. a. folgende Informationen:

- Anlage
- Komponentenart
- Zugehöriges System
- Zahl der Einzelkomponenten
- Testmethode und Testintervall
- Hersteller

Darüber hinaus werden im OP-Record auch die zugehörigen statistischen Informationen wie z. B. der Beobachtungszeitraum sowie die Zahl der im ausgewerteten Beobachtungszeitraum aufgetretenen Einzelfehler für alle ausgewerteten Ausfallarten erfasst. Die „Observed Population Records“ bilden die Grundstruktur der Datensammlung und werden unabhängig von den erfassten GVA-Ereignissen zur Beschreibung der Grundgesamtheiten für jede ausgewertete Komponentenart angelegt, d. h. die OP-Records werden im Rahmen des Erstrundendatenaustauschs für alle vom Datenaustausch erfassten Komponenten angelegt, unabhängig davon, ob tatsächlich GVA-Ereignisse in der entsprechenden Komponentengruppe aufgetreten sind². Für die deutschen KKW existieren aktuell 1.468 OP-Records, die eine Betriebserfahrung von 29.819 Komponentengruppenjahren sowie 236.301 Komponentenjahren abdecken.

² Eine diesbezügliche Ausnahme stellt die Komponentenart „Softwarebasierte Leittechnik“ dar. Hier werden die Komponentengruppen erst angelegt, wenn ein GVA in der entsprechenden Komponentengruppe aufgetreten ist.

In den „**Common Cause Event Records**“ werden die beobachteten GVA-Ereignisse beschrieben und bewertet. Jedes Ereignis ist mit demjenigen Observed Population Record verknüpft, der die Beobachtungseinheit/Komponentengruppe beschreibt, in der das Ereignis aufgetreten ist. Die Common Cause Event Records umfassen Textfelder, numerische Felder sowie Schlüsselfelder. Mit Hilfe der Textfelder wird der Ereignisablauf, die Ereignisursache sowie die Bewertung des Ereignisses unter GVA-Gesichtspunkten beschrieben

Die zusätzlich vorhandenen Schlüsselfelder ermöglichen Recherchen unter bestimmten Gesichtspunkten wie z. B.

- Ausfallart,
- Ursachenklassifizierung (Event Cause und CCF Root Cause),
- getroffene Abhilfemaßnahmen (Klassifizierung),
- Art der Fehlerentdeckung (z. B. Test oder Anforderung).

Weitere Schlüsselfelder erlauben eine klassifizierende Bewertung der Gleichartigkeit der beobachteten Ausfall- bzw. Schadensursachen (*Shared Cause factor*), der Gleichzeitigkeit der beobachteten Ausfälle bzw. Schäden (*Time factor*) und des Schädigungsgrads der betroffenen Komponenten (*Component degradation value*). Der Schädigungsgrad der Komponenten wird mittels eines „Schädigungsvektors“ (*Impairment vector*) beschrieben, der den Grad der Schädigung der einzelnen Komponenten beschreibt. Hierbei wird folgendes Schema verwendet:

- Ausgefallen (**C**omplete Failure). Die Komponente war nicht in der Lage ihre sicherheitstechnische Funktion zu erfüllen.
- Geschädigt (**D**egraded). Die Komponente war im Wesentlichen in der Lage ihre spezifizierte sicherheitstechnische Funktion zu erfüllen, wies jedoch funktionsrelevante Schädigungen auf.
- Schwach geschädigt (**I**ncipient failure). Die Komponente war in der Lage ihre spezifizierte sicherheitstechnische Funktion zu erfüllen und wies keine funktionsrelevanten Schädigungen auf, war jedoch von einem GVA-Fehlermechanismus betroffen, der sich zu einem Funktionsausfall hätte entwickeln können.
- Funktionsfähig. (**W**orking). Die Komponente war von dem GVA-Fehlermechanismus nicht betroffen.

Weitere Details zum verwendeten Kodierungsschema sind im General Coding Guide, /ICDE 19/ enthalten.

A.2.5.2 Weiterentwicklung der ICDE-Datenbank

Im Berichtszeitraum wurde die Datenbanksoftware auf Anforderung des ICDE-Lenkungskreises laufend weiterentwickelt, so wurden z. B. Suchfunktionen und Navigiermöglichkeiten weiter optimiert. Zu den beiden wesentlichen Aspekten zählen die Implementierung der „Correlated events“ und der „Root Cause Analysis“. Beide Funktionen sind dazu geeignet, die Analyse der Datenbank so zu erweitern, dass bisher nicht erkannte oder auch nur vermutete Effekte untersucht werden können. Im Folgenden werden die beiden Funktionen kurz beschrieben.

Im Rahmen der Workshops hatte sich gezeigt, dass sich eine ganze Reihe von Erkenntnissen erst aus der vergleichenden Betrachtung mehrerer Ereignisse ergibt. Zu diesem Zweck wurde nun die Möglichkeit in der Datenbank integriert, mehrere Ereignisse thematisch zu kategorisieren und untereinander in Verbindung zu setzen. Diese Datenbankeinträge werden genutzt, um Informationen zu hinterlegen, die mehr als ein ICDE-Ereignis betreffen. Unter dem Reiter „Correlations“ können nun sogenannte „Event-event correlations“ und „Topical correlations“ erstellt werden. Im Falle von „Event-event correlations“ können verschiedene Systeme und Anlagen bzw. Blöcke betroffen sein. Hierbei gilt:

- Eine „event-event“-Korrelation kann nur angewendet werden, wenn es sich um dieselbe Komponentenart handelt.
- Es werden bestehende ICDE-Ereignisse und Komponentengruppen verwendet.
- Die Korrelationen werden als Verbindung in den jeweiligen Datenbankeinträgen der ICDE-Ereignisse hinterlegt.

Ein „Topical correlation“-Datensatz wird in der thematischen Analyse als Teilmenge der ICDE-Ereignisse definiert und folgendermaßen charakterisiert:

- Es werden bestehende ICDE-Ereignisse und Komponentengruppen verwendet.
- Gespeichert werden die gefundenen Korrelationen für ein Ereignis als Themenaspekt (correlation factors), sowie Korrelationen zu anderen Ereignissen.
- Es ist möglich, verschiedene Komponentenarten miteinander in Verbindung zu setzen.

Bisher sind in der Datenbank folgende Themenaspekte angelegt:

- Ereignisse durch externe Einwirkungen (External factors)
- Ereignisse infolge von Modifikationen an der Anlage (Modifications)
- Ereignisse, die mehrere Blöcke betroffen haben (Multi-unit)
- Ereignisse, die infolge einer verbesserten Testmethode hätten vermieden werden können (Improved testing)
- Ereignisse, bei denen mehrere Systeme betroffen waren (Multiple systems affected)
- Ereignisse, die die Sicherheitskultur betreffen (Safety culture)
- Ereignisse, die gleichzeitig Initiator sind und zum Verlust eines benötigten Sicherheitssystems führten (Common cause initiator)

Weiterhin wurde die „Root Cause Analysis“ als Prinzip und Funktion in die Datenbank eingeführt. Um nun den neudefinierten „Root Cause“ zu bestimmen, werden die in der ICDE-Datenbank bereits definierten Einträge zur Ursache (event cause – ehemals root cause), dem Kopplungsfaktor (coupling factor) und den Korrekturmaßnahmen (corrective actions) kombiniert. Dabei wird ausgenutzt, dass auch in den verwendeten Codes für „Coupling factor“ und „Corrective action“ implizit Hinweise auf die Ereignisursache enthalten sind. Beispielsweise deutet der Code „Hardware“ bei „Coupling factor“ darauf hin, dass das Design der betroffenen Komponenten zur Ausfallursache beigetragen hat. Im Rahmen der neuen „root cause analysis“ werden deshalb drei fundamentale Root-Cause-Aspekte definiert. Dies sind die Aspekte Design (D, „Design“), Prozeduren (P, „Procedures“), menschliches Handeln (H, „Human Actions“). Jedem dieser drei Datenbankeinträge event cause, coupling factor und corrective action wird einer dieser drei fundamentalen Root-Cause-Aspekte zugeordnet. Das Ergebnis der Root Cause Analysis wird dann in dem neuen Datenbankeintrag „Root Cause“ als Tripelkombination dieser drei fundamentalen Aspekte angegeben. Aufgrund der Komplexität von GVA-Ereignissen sind diese drei Aspekte eines Ereignisses nicht immer identisch, so dass Ereignisse eine ausschließliche Ursache, eine vorherrschende und eine beitragende Ursache oder gar keine vorherrschende Ursache haben können. Zusätzlich zu den drei oben aufgeführten Aspekten werden die Aspekte Umwelt (E, „Environment“) und Unbekannt (U, „Unkonwn“) verwendet. „Umwelt“ wird angewendet, wenn ein Umweltfaktor (z. B. extremes Wetter, Überschwemmungen usw.) zu dem Ereignis beigetragen hat. Da Umwelteinflüsse nicht als Ursache verstanden werden, wird eine der Tripelbestandteile

in diesem Fall nur als Auslöser bzw. Trigger des Ereignisses verstanden und als Umwelt (E, „Environment“) angegeben. Das genaue Vorgehen ist in Anhang 3 der allgemeinen Kodieranleitung /ICDE 19/ beschrieben.

A.3 Ergebnisse des ICDE-Projekts

A.3.1 Stand des ICDE-Datenaustauschs

Während des Berichtszeitraums erfolgten zu den Komponentenarten Batterien, Leistungsschalter, Kreiselpumpen, Rückschlagarmaturen, Steuerstäbe und Steuerstabantriebe, Notstromdieselgeneratoren, Lüfter, Wärmetauscher, Füllstandsmessungen, Frischdampfisolationsventile, motorbetätigten Absperrarmaturen, Sicherheits- und Entlastungsventile, Softwarebasierte Leittechnik sowie Umformer Updates für neue Beobachtungszeiträume. Weiterhin wurden fünf Ereignisse als komponentengruppenübergreifende GVA kodiert.

Insgesamt sind in der ICDE-Datenbank mit Stand vom 02.06.2020 1761 ICDE-Ereignisse (Event Records) für Deutschland, entsprechend der eigenen Auswertezwischenräume, zugänglich und 9630 Komponentengruppen in Datensätzen (OP-Records) erfasst. In Tab. 2.6 ist ein Überblick über die Verteilung dieser Datensätze auf die einzelnen Komponentenarten gegeben.

Tab. 2.6 Umfang ICDE-Datenbank

Komponentenart	Anzahl der Observed Population Records (Komponentengruppen)	Komponentengruppenjahre	Anzahl ICDE-Ereignisse
Batterien	391	5.187	77
Leistungsschalter	1.355	18.886	108
Kreiselpumpen	1.646	33.909	376
Rückschlagarmaturen	1.222	18.062	114
Steuerstäbe und Antriebe	490	5.681	173
Diesel	311	5.238	241
Softwarebasierte Leittechnik	4	41	4
Ventilatoren	724	12.299	32
Wärmetauscher	601	12.419	55
Umformer	17	312	1
Füllstandsmessungen	583	8.645	155

Komponentenart	Anzahl der Observed Population Records (Komponentengruppen)	Komponentengruppenjahre	Anzahl ICDE-Ereignisse
Frischdampfisolationsventile	187	2.889	2
Motorbetätigte Absperrarmaturen	1.377	24.767	168
Sicherheitsventile	721	12.947	250
Komponentengruppenübergreifende GVA			5
Summe	9.630	161.282	1.761

A.3.2 Berichte des ICDE-Projektes

Um die Arbeiten des ICDE-Projektes der Fachwelt transparent zu machen, berichtet der ICDE-Lenkungskreis über die Ergebnisse der Auswertungen zu den einzelnen Komponentenarten bzw. über spezifische, komponentengruppenübergreifende Themen wie z. B. „GVA-Ereignisse durch äußere Einwirkungen“ im Rahmen der Schriftenreihe der OECD/NEA/CSNI. Ziele dieser Berichte sind üblicherweise:

- Entwicklung qualitativer Erkenntnisse über die Ereignisse, ausgedrückt durch Ereignisursachen, Kopplungsfaktoren und Korrekturmaßnahmen,
- Identifizierung von Verbesserungs- und Vorsorgemöglichkeiten,
- Formulierung von gewonnenen Erkenntnissen und Empfehlungen.

Bisher waren bereits folgende Berichte erschienen:

- Komponentenbericht: Kreiselpumpen 1 /NEA 99/,
- Komponentenbericht: Notstromdiesel /NEA 00/,
- Komponentenbericht: Motorbetätigte Absperrarmaturen /NEA 01/,
- Komponentenbericht: Sicherheits- und Entlastungsventilen /NEA 02/,
- Komponentenbericht: Rückschlagarmaturen /NEA 03/,
- Komponentenbericht: Batterien /NEA 03a/,
- Komponentenbericht: Leistungsschalter /NEA 08a/,

- Komponentenbericht: Füllstandsmessungen /NEA 08b/,
- Komponentenbericht: Kreiselpumpen 2 /NEA 13a/ (Update zu /NEA 99/),
- Komponentenbericht: Steuerstäbe und -antriebe /NEA 13b/,
- Komponentenbericht: Wärmetauscher /NEA 15a/,
- Themenbericht: GVA-Ereignisse durch äußere Einwirkungen /NEA 15b/.

Im Vorhabenszeitraum wurden Berichte zu folgenden Komponentenarten bzw. Themen erstellt und im Rahmen der OECD/NEA/CSNI-Schriftenreihe veröffentlicht:

- Komponentenbericht: Notstromdiesel 2 (Update zu /NEA 00/) /NEA 17/,
- Themenbericht: GVA-Ereignisse an Notstromdieselgeneratoren, bei denen die komplette Komponentengruppe betroffen war /NEA 18/.

Aktuell befinden sich folgende Berichte im QS-Prozess bzw. werden bei der OECD/NEA zur Veröffentlichung vorbereitet:

- Themenbericht: GVA-Ereignisse infolge von Modifikationen an der Anlage,
- Themenbericht: Mehrblockanlagen,
- Themenbericht: Verbessern des Testens,
- Themenbericht: Systemübergreifende GVA.

Im Internet wird das ICDE-Projekt von der OECD/NEA (<http://www.oecd-nea.org/jointproj/icde.html>) vorgestellt, dort sind auch die oben erwähnten Berichte frei und öffentlich erhältlich. Darüber hinaus sind die Berichte sowie weitere öffentlich zugängliche Dokumente auf der Internetseite des Operating Agent (<https://projectportal.afconsult.com/ProjectPortal/icde>) verfügbar.

Ein wesentlicher Bestandteil des ICDE-Projekts ist die Präsentation von Arbeitsergebnissen bei internationalen Fachkonferenzen. Im Rahmen der Konferenz ESREL 2019 (European Safety and Reliability Conference), die vom 22. bis zum 26. September 2019 in Hannover stattfand, wurden das ICDE-Projekt, bisher erzielte Ergebnisse sowie Anwendungsmöglichkeiten im Rahmen der „Risk Assessment“ Session vorgestellt.

A.3.3 Workshops des ICDE-Projekts

Während der Laufzeit des Vorhabens 4717R01337 wurden sechs Workshops durchgeführt, in denen die in der Datenbank enthaltenen Ereignisse hinsichtlich bestimmter Themen ausgewertet wurden.

Die Themen der Workshops werden in den vorausgehenden Treffen des ICDE-Lenkungskreises festgelegt. Hierbei kann es sich sowohl um themen- wie auch komponentenspezifische Auswertungen handeln. Anschließend werden in Zusammenarbeit zwischen den Teilnehmern und dem Operating Agent Suchkriterien entwickelt, anhand derer Ereignisse identifiziert werden können, die für das ausgewählte Thema des Workshops relevant sind. Hierbei ist es zwingend erforderlich, auf automatisierte Suchverfahren zurückzugreifen, da der Umfang der Datenbank eine manuelle Betrachtung jedes einzelnen Ereignisses nicht mehr zulässt. Ziel der Vorauswahl ist es, einen Satz von 30 bis 50 Ereignissen zu erzeugen, die dann im Rahmen des eigentlichen Workshops vertieft analysiert werden.

Zur Durchführung des Workshops werden Gruppen aus 2 bis 3 Personen gebildet. Die Teilnehmer rekrutieren sich im Wesentlichen aus den Projektverantwortlichen der einzelnen Teilnehmerorganisationen. Die Teilnahme zusätzlicher Experten von Betreibern, Aufsichtsbehörden oder sonstigen Organisationen ist mit Zustimmung des Lenkungs-kreises ebenfalls möglich und hat sich als sehr nützlich erwiesen, um weitere inhaltliche Perspektiven in den Workshop zu integrieren. Je nach Zahl der Ereignisse und Teilnehmern muss jede Gruppe 6 – 10 Ereignisse analysieren. Dies geschieht anhand eines generischen Workshopformats, das um zusätzliche, themenspezifische Fragestellungen ergänzt wird.

Die Ergebnisse der Expertenanalysen werden in einem vorab definierten Format in der Datenbank abgelegt und anschließend in Zusammenarbeit von ICDE-Lenkungskreis und Operating Agent zunächst zu einem „Workshop Summary“ und nach Herausarbeiten der wesentlichen Inhalte zu einem Bericht verarbeitet, der dann im Rahmen der OECD/NEA/CSNI-Schriftenreihe veröffentlicht wird.

A.3.3.1 Workshop zum Thema „Intersystem dependencies“

Den Auftakt zur Studie über systemübergreifende Abhängigkeiten (engl. Intersystem dependencies) bildete ein im Anschluss an das 45. Lenkungskreistreffen vom 16. bis zum 19. Oktober 2017 durchgeführter Workshop. Gegenstand dieses Workshops waren Ereignisse aus der Betriebserfahrung mit KKW, bei denen ein einziger GVA-Ausfallmechanismus Komponenten in mehreren verschiedenen Systemen des KKW betraf.

Im Workshop wurden auch Ausfälle mehrerer Komponentengruppen in nur einem System betrachtet, auch wenn keine Hinweise vorlagen, dass andere Systeme betroffen gewesen sein könnten. Diese werden normalerweise nicht als systemübergreifende Ereignisse betrachtet, sind aber in diesem Bericht enthalten, da sie Abhängigkeiten zwischen Komponentengruppen beinhalten, die nicht speziell in einer PSA modelliert werden.

Die Auswahl der systemübergreifenden Ereignisse basierte auf Schlüsselwörtern in einer Suchfunktion und der Ereigniskodierung in der ICDE-Datenbank. Ebenso wurden Ereignisse, die zuvor im Datenbankfeld für interessante Ereignisse mit dem Code 8 (Multiple systems affected) markiert wurden, einbezogen. Darüber hinaus wurden weitere Ereignisse berücksichtigt, die von einzelnen ICDE-Mitgliedern aus ihren eigenen nationalen Beiträgen zum ICDE Datenaustausch bekannt waren und als relevant für dieses Thema erschienen. Insgesamt wurden 25 Ereignisse analysiert.

Für die Klassifizierung von systemübergreifenden Ereignissen wurden die beiden Parameter „Schweregrad der Beeinträchtigung“ und „Gleichzeitigkeit“ definiert. Der „Schweregrad der Beeinträchtigung“ der betroffenen Systeme wird bestimmt, indem beurteilt wird, wie stark die Systeme beeinträchtigt und geschädigt wurden (tatsächliche oder potentielle Ausfälle in mehreren Systemen). Die Gleichzeitigkeit (hoher bzw. niedriger Zeitfaktor) der systemübergreifenden Ereignisse wird durch die Zeit zwischen der Erkennung des Fehlers im ersten und im zweiten System bestimmt. Durch deren Kombination wurde die folgende Klassifikation erstellt:

Tatsächliche systemübergreifende Abhängigkeit

Ausfälle, die mehrere Systeme mit einem hohen Zeitfaktor betreffen. Beobachtete Ereignisse zeigen Anzeichen dafür, dass mehrere Systeme betroffen sind.

Partielle / beginnende systemübergreifende Abhängigkeit

Ausfälle oder Beeinträchtigungen, die mehrere Systeme mit einem niedrigen Zeitfaktor betreffen. Beobachtete Ereignisse zeigen Anzeichen dafür, dass mehrere Systeme von einem ähnlichen Problem (Ausfallmechanismus) betroffen sind, z. B. dass sie die gleiche vom Ausfallmechanismus betroffene Unterkomponente enthalten.

Mögliche systemübergreifende Abhängigkeit

Ausfälle nur in einem System, aber andere Systeme könnten aufgrund der Art des Ausfallmechanismus betroffen gewesen sein. Beobachtete Ereignisse zeigen Anzeichen für eine potenzielle systemübergreifende Abhängigkeit, z. B. dadurch, dass der aufgetretene Fehlermechanismus zwar in mehreren Systemen auftrat, aber nur in einem Schaden hervorrief.

Für die Ereignisse, bei denen mehrere CCCGs (Common Cause Component Groups) betroffen waren, wobei jedoch alle betroffenen CCCGs zu einem System gehören, wurde das oben erwähnte Klassifikationsschema um folgende Definition erweitert:

Inter-CCCG-Abhängigkeit

Ausfälle oder Schädigungen mehrerer CCCGs in nur einem System ohne Hinweise darauf, dass auch andere Systeme betroffen gewesen sein könnten.

Dies sind keine gewöhnlichen systemübergreifenden Ereignisse, aber interessant, da sie Abhängigkeiten zwischen den CCCGs beinhalten.

Nach der Erstellung einer ersten internen Arbeitsgrundlage (Worknote) und mehreren Kommentierungen im Laufe der Projektphase wurde zuletzt eine im ICDE-Lenkungskreis abgestimmte Berichtsversion der Program Review Group (PRG) des CSNI zum Review vorgelegt. Diese erhielt die Zustimmung und wird demnächst veröffentlicht.

A.3.3.2 Workshop zum Thema „Pre-initiator human failure events“

Ein Pre-Initiator Human Failure Event (HFE) ist ein Ereignis, das sich auf die Verfügbarkeit von Komponenten in sicherheitsrelevanten Systemen auswirken kann und durch unangemessene Handlungen oder menschliches Fehlverhalten, wie z. B. Ausrichtungs-

fehler und Fehlkalibrierungen, verursacht wird. Eine Definition aus "Standard For Probabilistic Risk Assessment For Nuclear Power Plant Applications, ANSI/ASME RA-S-2002" /ANSI 02/ lautet:

"A basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction or inappropriate action."

Ein Basisereignis, das einen Ausfall oder eine Nichtverfügbarkeit einer Komponente, eines Systems oder einer Funktion darstellt, die durch menschliche Untätigkeit oder unangemessene Handlungen verursacht wird.

Vom ICDE-Lenkungskreis wurden in zwei Workshops, die im April und Oktober 2018 durchgeführt wurden, insgesamt 51 vollständige GVA-Ereignisse, also Ereignisse, bei denen alle Redundanzen einer Komponentengruppe ausgefallen waren, betrachtet. Die ingenieurtechnische Analyse hatte u. a. den Zweck, die Ereignisursache bzw. den Ereignisauslöser, den Kopplungsfaktor, der die Umstände beschreibt, durch den sich ein Fehler auf mehrere Komponenten auswirkt und die Latenzzeit, also die Zeit, über die der Fehler unbemerkt vorlag, sowie Korrekturmaßnahmen zu bestimmen.

Zu den wesentlichen Erkenntnissen der beiden Workshops zählen:

- Fehlerhafte Prozeduren waren die Hauptursache für GVA bezogen auf die Gesamthäufigkeit von Pre-Initiator-HFEs (74 %). Menschliche Fehlhandlungen zeigen sich häufig bei der Erstellung von Prozeduren, weshalb die Festschreibung von Prozeduren alleine nicht als hinreichende Vorsorgemaßnahme gewertet werden kann. Aspekte wie die Ausbildung des Personals, die Sicherheitskultur und das Anlagenmanagement spielen eine wichtige Rolle bei der Vermeidung von HFE.
- Zu den häufigsten Kopplungsfaktoren zählen neben fehlerhaften Prozeduren, die Arbeitsplanung, mangelndes Training des Personals und handschriftliche Arbeitsanweisungen.
- Bei der Gesamtanalyse wurde folgende Punkte als wichtig hervorgehoben:
 - Das Kraftwerksmanagement spielt die entscheidende Rolle bei der Qualitätssicherung von Prozeduren. Diese beinhaltet den Umfang und die Angemessenheit der Prozeduren sowie die Sicherstellung der Fachkunde des Personals.

- Das sichere Einhaltung von Verfahren und schriftlichen Arbeitsplänen. Zum Beispiel sollen keine Tests in einem ungeeigneten Anlagenbetriebszustand oder gleichzeitig an mehreren Redundanzen durchgeführt werden.
- Überprüfung der Funktionsfähigkeit nach Wartungsarbeiten (Installationen, Änderungen und Austausch) und nach Tests (z. B. korrekte Stellung von Schaltern usw.)
- Die Pre-Initiator-HFE aus der ICDE-Datenbank liefern wertvolle Einblicke in Abhängigkeiten, da viele dieser Abhängigkeiten in der Regel nicht bei den in PSA durchgeführten Analysen menschlicher Handlungen modelliert sind.

Der Bericht liegt derzeit als Entwurf vor. Geplant ist die Fertigstellung und Übergabe an die PRG zum nächsten Lenkungskreistreffen im Oktober 2020.

A.3.3.3 Workshop zum Thema „Motor operated valves“

Im Juli 2001 wurde der Bericht „ICDE Project Report: Collection and Analysis of Common-Cause Failures of Motor Operated Valves“ /NEA 01/ veröffentlicht. Dieser fasst die Ergebnisse aus der Analyse von 87 GVA-Ereignissen mit motorbetätigten Armaturen zusammen. Seit dieser Veröffentlichung hat sich die Anzahl dieser Ereignisse in der Datenbank auf 172 erhöht und umfasst nun den Zeitraum von 1980 bis 2017. Während des 48. Treffens des ICDE-Lenkungskreises, das vom 9. bis zum 11. April 2019 in Paris stattfand, wurde ein Workshop mit dem Ziel eine Aktualisierung des Berichts vorzubereiten durchgeführt.

Ziel des Expertenaustauschs während des Workshops war es, Gemeinsamkeiten der vorliegenden Ereignisse zu erkennen, um diese statistisch auswerten zu können. Dabei sollten im Wesentlichen folgende Fragen beantwortet werden:

- Welche gemeinsamen Fehlermechanismen sind aufgetreten?
- Welche gemeinsamen Ereignisauslöser gab es?
- Kann man Schlüsse aus Ereignissen mit ähnlichem Schweregrad ziehen?
- Wo lagen gemeinsame Ursachen?
- Welche Verbesserungsmöglichkeiten oder Vorkehrungen wurden getroffen?

Zum Schluss des Workshops wurden allgemeine Empfehlungen aus der Beantwortung dieser Fragen gezogen. Zusammen mit der statistischen Auswertung konnten dabei folgende wesentliche Schlüsse gezogen werden:

- Mängel in der Konstruktion führen in der Regel zu schwerwiegenden Ereignissen für MOVs, und die meisten Fehler werden durch Probleme in der elektrischen Ansteuerung und der Leittechnik verursacht. Am häufigsten waren dabei falsch eingestellte Drehmomentschalter Ursache für die aufgetretenen Fehler.
- Wiederkehrende Prüfungen an den Drehmomentschaltern und deren Verifizierung nach Test und Wartung sind geeignete Maßnahmen, um das GVA-Risiko zu reduzieren und sollten implementiert werden.
- Die Schädigung der motorbetätigten Armaturen vollzieht sich häufig über einen langen Zeitraum. Folglich sollten Alterungsmanagement und betriebliche Maßnahmen implementiert werden, die in der Lage sind, Schädigungen zu erkennen, bevor ein vollständiges Versagen der Komponente eintritt.
- Bedienfehler führen zu schweren Ereignissen. Um solche Fehler zu vermeiden, sind angemessene Verfahren, schriftliche Arbeitspläne, Schulung des Personals und generell eine gut etablierte Sicherheitskultur unerlässlich.

Der Bericht liegt derzeit als Erstentwurf vor. Geplant ist die Fertigstellung und Übergabe an die PRG zum Lenkungskreistreffen im Frühjahr 2021.

A.3.3.4 Workshop zum Thema „External factors update“

Im Anschluss an das 48. Lenkungskreistreffen wurde neben dem Workshop zu motorbetätigten Armaturen ein kurzfristig organisierter, kleinangelegter Workshop zur Aktualisierung des Berichts zu Ereignissen aufgrund äußerer Einflüsse /NEA 15b/ durchgeführt. Seit dieser Veröffentlichung wurden 24 zusätzliche Ereignisse in die ICDE-Datenbank eingetragen, die die Auswahlkriterien zu diesem Thema erfüllen. Sieben dieser Ereignisse waren vollständige GVA, vier weitere waren teilweise GVA³.

³ Ein teilweiser GVA (partial CCF) bezeichnet den vollständigen Funktionsausfall von mindestens zwei Komponenten einer Komponentengruppe, wenn nicht die gesamte Komponentengruppe betroffen ist, wobei die Fehlerzustände gleichzeitig existieren müssen und diese das direkte Ergebnis einer gemeinsamen Ursache sind.

Durch den Workshop konnte im Wesentlichen die Erkenntnis gewonnen werden, dass bei etwa 31 % der Ereignisse die Hauptursache für einen GVA ausschließlich oder überwiegend durch fehlerhaftes Design ausgelöst wurde und Umwelteinflüsse einen wesentlichen Beitrag leisteten. Ein ebenso großer Anteil der Ereignisse wurde durch Umwelteinflüsse ausgelöst, bei denen das Eintreten dieses Umwelteinflusses nicht in Betracht gezogen wurde.

Derzeit befindet sich der Bericht im finalen Entwurf. Geplant ist die Verabschiedung durch den ICDE-Lenkungskreis beim nächsten Treffen im Oktober 2020.

A.3.3.5 Workshop zum Thema „Safety and Relief Valves“

Während des 49. Treffens des ICDE-Lenkungskreises vom 15. bis zum 17. Oktober 2019 in Washington, wurde ein Workshop mit dem Ziel einer Aktualisierung des Komponentenberichts zu Sicherheits- und Abblaseventilen durchgeführt. Der erste Bericht /NEA 02/ wurde im Jahr 2002 veröffentlicht. Von damals 149 Ereignissen in der Datenbank hat sich die Zahl bis heute auf 271 erhöht. Hieraus ergab sich die Notwendigkeit diesen Bericht zu aktualisieren und dabei neue Werkzeuge, wie die formale Fehleranalyse nach der „Failure analysis guideline“ (siehe /GRS 17/), das neueste Berichtsformat und die „Root cause analysis (siehe Abschnitt 3.4), anzuwenden.

Der Workshop wurde nach dem gleichen Muster wie zuvor der Workshop zu motorbetätigten Armaturen durchgeführt. Die erste Auswertung steht noch aus.

A.3.3.6 Workshop zum Thema „Interesting events“

Während des 50. Treffens des ICDE-Lenkungskreises, das vom 21. bis zum 23. April 2020 im Rahmen einer Videokonferenz stattfand, wurden Ereignisse diskutiert, in deren Verlauf die Sicherheitsfunktion von Systemen im Betrieb angefordert wurde und ausfiel. Der Fokus lag auf Ereignissen, die nicht während der routinemäßigen Prüfungen erkannt wurden und zusätzlich im Zusammenhang mit der Sicherheitskultur standen und / oder bei denen alle Redundanzen betroffen waren

Derzeit werden Arbeiten zur Erstauswertung (Worknote) des Workshops durchgeführt.

A.4 Zusammenfassung und Ausblick zum ICDE-Projekt

Im Rahmen des ICDE-Projekts der OECD/NEA wird seit mehr als 20 Jahren auf internationaler Ebene Betriebserfahrung zum Thema "gemeinsam verursachte Ausfälle" (GVA, oder Common Cause Failure, CCF) systematisch in einer Datenbank gesammelt, ausgetauscht und analysiert. Beteiligt an diesem Projekt sind sowohl Behörden als auch Gutachterorganisationen und Forschungseinrichtungen. Der internationale Austausch bezüglich GVA ist erforderlich, da derartige Ausfälle zum einen große Auswirkungen auf das Sicherheitssystem kerntechnischer Anlagen haben können, zum anderen jedoch – verglichen mit Einzelfehlern – deutlich seltener auftreten. Aus diesem Grund ist die nationale Betriebserfahrung nicht ausreichend, um die Thematik abdeckend zu erfassen.

Mit dem abgeschlossenen Vorhaben 4717R01337 „Systematische Aufbereitung der weltweiten Betriebserfahrung mit gemeinsam verursachten Ausfällen (GVA) im Rahmen einer internationalen Expertengruppe ICDE (Internationales GVA Datenaustauschprojekt der OECD/NEA)“ wurden drei übergeordnete Ziele verfolgt und umgesetzt:

- Sicherstellung der weiteren Beteiligung am ICDE-Projekt durch systematische Erfassung und Einspeisung der deutschen Betriebserfahrung mit GVA,
- Auswertung der internationalen Betriebserfahrung im Hinblick auf für deutsche KKW relevante GVA-Effekte und GVA-Fehlermechanismen und
- Fortschreibung des Standes von Wissenschaft und Technik bezüglich GVA.

Während des Vorhabenszeitraums wurde die GVA-Betriebserfahrung des Zeitraums 01.01.2003 bis zum 31.12.2015 von insgesamt vier deutschen Anlagen ausgewertet und für die Einspeisung in die ICDE-Datenbank aufbereitet. Da der Zugang zu den Daten innerhalb des Projekts nach dem Quid-pro-quo-Prinzip organisiert ist, d. h., dass jeder in dem Maße Zugang zu den Daten der anderen Projektteilnehmer erhält, in dem er selber Informationen bereitstellt, ist nur durch einen kontinuierlichen Beitrag sichergestellt, dass die GRS auch weiterhin Zugriff auf die ausländische Betriebserfahrung hat.

Die Auswertung der ausländischen Betriebserfahrung mit GVA umfasste insgesamt 63 GVA-Ereignisse, wobei erstmals auch Ereignisse der Komponentenart Lüfter ausgewertet wurden. Bei zwei Ereignissen wurden im Rahmen dieses Vorhabens generische sicherheitstechnische Hinweise formuliert, wie die im Rahmen der Ereignisse beobachteten Effekte bei deutschen KKW verhindert werden können.

Während der Laufzeit des Vorhabens wurden im Rahmen der halbjährlichen Treffen des ICDE-Lenkungskreises insgesamt sechs Workshops durchgeführt. Beteiligt waren jeweils die Mitglieder des Lenkungskreises sowie ggf. weitere Personen (z. B. von Behörden oder auch Anlagen) auf Einladung des Lenkungskreises.

Im Zuge der Workshops wurden sowohl komponenten- wie auch themenspezifische Auswertungen bezüglich GVA-Phänomene durchgeführt. So wurde:

- ein neuer Bericht zu systemübergreifenden GVA erarbeitet und
- themenspezifische Workshops durchgeführt zu
 - GVA-Ereignissen aufgrund menschlichem Fehlverhalten,
 - GVA-Ereignissen, die bei Anforderung von Sicherheitssystemen erkannt wurden und
 - zur Aktualisierung des Berichts zu GVA auf Grund von äußeren Einflüssen.

Weiterhin wurden komponentenspezifische Workshops zur Aktualisierung der Berichte zu motorbetätigten Armaturen und Sicherheits- und Abblaseventilen durchgeführt. Im Vorhabenszeitraum wurden vier CSNI-Berichte zu GVA-spezifischen Themen fertiggestellt. Darunter zählen je ein Themenbericht zu

- GVA-Ereignissen an Notstromdieselgeneratoren, bei denen die komplette Komponentengruppe betroffen war,
- GVA-Ereignissen infolge von Modifikationen an der Anlage,
- Verbesserungen im Bereich "Wiederkehrende Prüfungen & Inspektionen" („Improving Testing“),
- GVA-Ereignissen, bei denen der GVA Fehlermechanismus in mehr als einem Kraftwerksblock aufgetreten ist,

und ein Update des Komponentenberichts bezüglich GVA an Notstromdieseln.

Darüber hinaus wurde im Rahmen des ICDE-Projekts aktiv an der Fortschreibung des Standes von Wissenschaft und Technik bezüglich GVA gearbeitet. So wurden beispielsweise neue Methoden zur Analyse der Ereignisursache erarbeitet und in die Datenbank integriert.

Literaturverzeichnis

- /ASME 02/ Standard For Probabilistic Risk Assessment For Nuclear Power Plant Applications, ANSI/ASME RA-S-2002
- /BBE 16/ Brück, B.; Kreuser, A.; Stiller, J.; Leberecht, M.
Expanding the Scope of ICDE: Systematic Collection of Operating Experience with Cross Component Group CCFs
PSAM 13, 02. – 07. Oktober 2016, Seoul, Korea
- /BMU 11/ Übereinkommen über nukleare Sicherheit
Bericht der Regierung der Bundesrepublik Deutschland für die 5. Überprüfungstagung im April 2011 (CNS 2011)
- /GRS 08a/ Kreuser, A., Holtschmidt, H., Stiller, J.C.
Auswertung von Ereignissen mit gemeinsam verursachten Ausfällen (GVA) aus dem internationalen GVA-Datenaustauschprojekt ICDE
GRS-A-3403, Januar 2008
- /GRS 08b/ Kreuser, A., Holtschmidt, H., Stiller, J.C.
Systematische Aufbereitung der weltweiten Betriebserfahrung mit gemeinsam verursachten Ausfällen (GVA) im Rahmen einer internationalen Expertengruppe, Abschlussbericht Phase 2005-2008
GRS-A-3399, Januar 2008
- /GRS 10/ Kreuser, A., Stiller, J.C., Voelskow, J.
Entwicklung einer Checkliste mit GVA-Phänomenen zur Überprüfung der in den deutschen Kernkraftwerken getroffenen Vorsorgemaßnahmen gegen GVA,
GRS-A-3546, Juli 2010
- /GRS 11a/ Kreuser, A., Arnold, S., Voelskow, J.
Internationales GVA-Datenaustauschprojekt ICDE,
Abschlussbericht Phase 2008-2010
GRS-A-3578, Januar 2011

- /GRS 11b/ Kreuser, A., Voelskow, J.
Auswertung von Ereignissen mit gemeinsam verursachten Ausfällen (GVA)
aus dem internationalen GVA-Datenaustauschprojekt ICDE, Teil 2
GRS-A-3588, Februar 2011
- /KWG 11/ Kernkraftwerk Grohnde (KWG), meldepflichtiges Ereignis „ Ausfall einer gesicherten Stromschiene bei gleichzeitigem Ausfall aller vier in Betrieb befindlichen Umformer “am 20.11.2011, Block-Vorkommnis-Nr. 06/2011, endgültige Meldung vom 07.08.2012
- /KRE 12/ Kreuser, A., Johanson, G.
General Insights from the International Common Cause Data Exchange (ICDE) Project
PSAM 11 ESREL2012, 25. – 29. Juni 2012, Helsinki Finland
- /KRE 14/ Kreuser, A., Johanson, G.
Recent Insights from the International Common Cause Data Exchange (ICDE) Project
PSAM 12, 22. – 27. Juni 2014, Honolulu, USA
- /KRE 16/ Kreuser, A., Johanson, G.
Recent Insights from the International Common Cause Data Exchange (ICDE) Project
PSAM 13, 02. – 07. Oktober 2016, Seoul, Korea
- /GRS 14a/ Brück, B., Kreuser, A., Simon, J.
Internationales GVA-Datenaustauschprojekt ICDE,
Abschlussbericht Phase 2011-2014
GRS-A-3748, Juni 2014
- /GRS 14b/ Brück, B., Kreuser, A., Simon, J.
Analyse von Ereignissen mit gemeinsam verursachten Ausfällen (GVA) aus dem internationalen GVA-Datenaustauschprojekt ICDE
GRS - 340, August 2014

- /GRS 16/ S. Blum, B. Brück, A. Kreuser, H. Nitschke
Bericht zur Auswertung der meldepflichtigen Ereignisse der Jahre 2013-2015 im Hinblick auf fachkunde-relevante Aspekte
GRS-A-3874, Januar 2017
- /GRS 17/ B. Brück, A. Kreuser, D. Voß
Systematische Aufbereitung der weltweiten Betriebserfahrung mit gemeinsam verursachten Ausfällen im Rahmen einer internationalen Experten-
gruppe
GRS – 447, März 2018
- /IAEA 14/ Root Cause Analysis Following an Event at a Nuclear Installation: Reference Manual,
IAEA TECDOC No. 1756; ISBN: 978-92-0-110014-6; veröffentlicht 2014
- /ICDE 19/ Technical Note on the ICDE Project
General Coding Guidelines
Januar 2019
- /NEA 99/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report on Collection and Analysis of Common-Cause Failures of Centrifugal Pumps
NEA/CSNI/R(99)2, September 1999
- /NEA 00/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report on Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators
NEA/CSNI/R(2000)20, 19-Feb-2001
- /NEA 01/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report on Collection and Analysis of Common-Cause Failures of Motor Operated Valves
NEA/CSNI/R(2001)10, 27-Jul-2001

- /NEA 02/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report on Collection and Analysis of Common-Cause Failures
of Safety and Relief Valves
NEA/CSNI/R(2002)19, 03-Oct-2002
- /NEA 03/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report: Collection and Analysis of Common-Cause Failures
of Check Valves
NEA/CSNI/R(2003)15, May 2003
- /NEA 03a/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report: Collection and Analysis of Common-Cause Failures
of Batteries
NEA/CSNI/R(2003)19, September 2003
- /NEA 08a/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report: Collection and Analysis of Common-Cause Failures
Switching Devices and Circuit Breakers
NEA/CSNI/R(2008)1, January 2008
- /NEA 08b/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report: Collection and Analysis of Common-Cause Failures
Level Measurement Components
NEA/CSNI/R(2008)8, June 2008
- /NEA 12a/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
International Common Cause Failure Data Exchange (ICDE)
General Coding Guidelines, Updated Version
NEA/CSNI/R(2011)12, February 2012

- /NEA 13a/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report on Collection and Analysis of Common-Cause
Failures of Centrifugal Pumps
NEA/CSNI/R(2013)2, June 2013
- /NEA 13b/ Nuclear Energy Agency Committee on the Safety of Nuclear Installations
ICDE Project Report on Collection and Analysis of Common-Cause
Failures of Control Rod Drive Assemblies
NEA/CSNI/R(2013)4, June 2013
- /NEA 15a/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Project Report: Collection and Analysis of Common-Cause Failures
of Heat Exchangers
NEA/CSNI/R(2015)11, August 2015
- /NEA 15b/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
ICDE Workshop on Collection and Analysis of Common-Cause Failures
due to External Factors
NEA/CSNI/R(2015)17, Oktober 2015
- /NEA 17/ Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
Workshop on the Collection and Analysis of Emergency Diesel Generator
Common-Cause Failures Impacting Entire Exposed Populations
NEA/CSNI/R(2017)8, August 2017/NEA 18/Nuclear Energy Agency
Committee on the Safety of Nuclear Installations
Lessons Learnt from Common-Cause Failure of Emergency Diesel Genera-
tors in Nuclear Power Plants
NEA/CSNI/R(2018)5, September 2018
- /SJC 17/ Stiller, J.; Leberecht, M.; Kreuser, A.; Verstegen, C.
Common Cause Failure exceeding CCF Groups
PSAM 13, 02. – 07. Oktober 2016, Seoul, Korea

Tabellenverzeichnis

Tab. 2.1	Vergleich vorhandene und neue, bisher nicht ausgewertete GVA-Ereignisse	6
Tab. 2.2	Gruppierung der identifizierten Fehlermechanismen an Kreiselpumpen.....	8
Tab. 2.3	Gruppierung der identifizierten Fehlermechanismen an Notstromdieselaggregaten	11
Tab. 2.4	Gruppierung der identifizierten Fehlermechanismen an Lüftern	13
Tab. 2.5	Für deutsche KKW relevante systematische Fehlermechanismen bei Lüftern	15
Tab. 2.6	Umfang ICDE-Datenbank.....	36

**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 978-3-947685-78-3