Internationales GVA-Datenaustauschprojekt ICDE 2023 bis 2026

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

GRS - 848

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Internationales GVA-Datenaustauschprojekt ICDE 2023 bis 2026

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

Abschlussbericht

Julia Simon
Jan Stiller

August 2026

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) unter dem Förderkennzeichen 4723R01275 durchgeführt.

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

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

GRS - 848
ISBN 978-3-911727-41-9

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 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 Kenntnis über GVA-Phänomene nicht aus. Daher ist es notwendig, auch die Betriebserfahrung anderer Länder 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 30 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,
  - belastbare Grundlagen für Zuverlässigkeitskennzahlen für GVA-Ereignisse im Rahmen von probabilistischen Sicherheitsanalysen zu erhalten,
  - in probabilistischen Sicherheitsanalysen (PSA) verwendete GVA-Wahrscheinlichkeiten bzw. GVA-Raten beurteilen zu können.

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-Lenkungskreis 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 „Kreiselpumpen“, „Notstromdieselgeneratoren“, „Motorbetätigte Absperrarmaturen“, „Sicherheits- und Entlastungsventile“, „Rückschlagarmaturen“, „Batterien“, „Leistungsschalter“, „Füllstandsmessungen“, „Steuerstäbe und Steuerstabantriebe“, „Wärmetauscher“, „Frischdampfisolationsventile“, „Lüfter“, „Softwarebasierte Leittech-

nik“, „Wechselrichter“ und „komponentengruppenübergreifende GVA“ statt. Im Berichtszeitraum wurde die deutsche Betriebserfahrung in Bezug auf systematische Ausfälle für alle Komponentenarten für die Anlagen KRB-II B, KRB-II C, GKN II, KKE und KKI 2 bis zum Ende des Jahres 2023 in die ICDE-Datenbank eingegeben. Hierbei wurde auf die im Rahmen der Vorhaben zur aktualisierten Bewertung von gemeinsam verursachten Ausfällen (Vorhaben 4720R01350, 4722R01280, 4719R01371 und vorherige Vorhaben) durchgeführte Auswertung der deutschen Betriebserfahrung bezüglich GVA aufgebaut.

In der ICDE-Datenbank sind zurzeit insgesamt 2210[1] Ereignisse, davon 173 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 Ventilatoren von insgesamt 33 Ereignissen in der ICDE-Datenbank nur zwei Ereignisse aus deutschen Anlagen). Insbesondere aus den USA und Frankreich mit ihrer großen Anzahl von Anlagen liegen 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 Anlagen bewerten zu können.

Während der Laufzeit des jetzt abgeschlossenen Vorhabens 4723R01275 befasste sich der ICDE-Lenkungskreis in vier Workshops mit Ereignissen aus der ICDE-Datenbank im Hinblick auf verschiedene Fragestellungen. Dabei wurden in einem Workshop Ereignisse, die ihre Ursache in Defiziten der Sicherheitskultur haben, untersucht. Hierbei wird Sicherheitskultur umfassend verstanden, d. h. sie umfasst informelle Aspekte (Sicherheitskultur im engeren Sinn) und formalisierte Aspekte wie ein formales Managementsystem. Um die Ereignisse näher zu charakterisieren, wurde ein Kodierungssystem entwickelt, erprobt und angewandt. Es zeigte sich, dass für den überwiegenden Teil der ausgewerteten Ereignisse ein oder mehrere Defizite in der Sicherheitskultur, die zum Ereignis beigetragen hatten, identifiziert werden können. Die Erkenntnisse aus der Analyse, wie z. B., dass eine mangelnde Compliance mit unzureichender Arbeitsorganisation als auch mit Mängeln bei der Dokumentation der Arbeitsabläufe korreliert, wurden in dem Bericht „ICDE Topical report: Safety Culture Insights from Analysis of Common Cause Failure Events“ dokumentiert, der zurzeit den formalen Qualitätssicherungsprozess durchläuft. In zwei Workshops zu Alterung wurden bisher insgesamt 72 Ereignisse

[1] Die angegebenen Zahlen beziehen sich auf die Anzahl der Ereignisse, die bereits sämtliche Stufen des QS-Prozesses durchlaufen haben.

analysiert. Die Analyse der Ereignisse zeigte, dass Alterung als Ursache von GVA in den meisten Fällen zusammen mit anderen Ursachen wie Defiziten in der Instandhaltung oder ungeeigneten Umgebungsbedingungen auftritt. Ereignisse, die sich allein auf Alterung zurückführen lassen, sind demgegenüber selten. In einem weiteren Workshop wurden GVA identifiziert und analysiert, die durch konventionelle (d. h. nicht softwarebasierte) leittechnische Einrichtungen verursacht wurden. Hierbei zeigte sich, dass konventionelle und softwarebasierte Leittechnik teilweise gleiche Fehlermechanismen, z. B. falsch eingestellte Grenzwerte in Schutzeinrichtungen, aufweisen. Deshalb soll in Zukunft konventionelle und softwarebasierte Leittechnik zusammen analysiert werden.

Darüber hinaus hat die GRS 129 aus ausländischen Anlagen in die ICDE-Datenbank eingespeiste Ereignisberichte systematisch ausgewertet. In den Vorhaben SR 2545, 3608R01338, 3611R01335, 3614R01301 und 4720R01350 wurden bereits die in der ICDE-Datenbank zum jeweiligen Zeitpunkt vorhandenen Ereignisberichte zu Kreiselpumpen, 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/, /GRS 18/, /GRS 20/ und /GRS 23b/ beschrieben. In diesem Vorhaben wurde darauf aufbauend die neu angefallene ausländische Betriebserfahrung ausgewertet. Es wurden dabei auch in Deutschland noch nicht aufgetretene GVA-Phänomene gefunden.

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 knowledge 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 employing 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 co-initiated the setting up of an international common-cause failure working group. This working group has conceived 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 activities 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 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, and
- 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 different methods in collecting, evaluating, and modelling CCF events in different countries. Thus, knowledge is gained to facilitate further development of the methods including a possible standardisation.

The main focus of work within the ICDE Management Board is the creation of a uniform data basis with detailed breakdowns of failures 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,” “Digital I&C,” “Inverters,” and “Cross component CCF.” During the reporting period, the German operational experience was analysed for all component types until the end of 2023 for five plants.

In total, the ICDE database currently contains 2210 events. 173 of these events were complete CCF were all redundant components failed. The number of event reports from foreign countries surpasses the German sources many times (e.g., for control rods and control rod drives, of a total of 33 events in the ICDE database, only two events are from German plants). Especially from the USA and France with their large number of power plants, a large number of events originates. Extent and level of detail of the participants' event reports are usually sufficient to understand the observed failure mechanisms.

During this project 4723R01275, the ICDE Management Board held four workshops to analyse events from the ICDE database with respect to different questions. In one of these workshops, events that were caused by deficits in safety culture were examined. Here, safety culture is understood comprehensively, i.e., it includes informal aspects (safety culture in the narrower sense) and formalised aspects such as a formal (safety)

management system. To characterise the events in more detail, a coding system was developed and applied. The analysis revealed that a large proportion of events are related to one or more identifiable deficits in safety culture. The findings from the analysis such as that a lack of adherence to the procedures is highly correlated to both inadequate work management and deficits of work procedure documentation will be published in the upcoming report „ICDE Topical report: Safety Culture Insights from Analysis of Common Cause Failure Events“. In two workshops on ageing, 72 events have been analysed. In most cases, ageing occurs as a cause of CCF in conjunction with other causes, such as maintenance deficiencies or unsuitable environmental conditions. Incidents that can be attributed solely to ageing, by contrast, are rare. In a further workshop, CCFs caused by conventional (i.e. not software based) I&C equipment were identified and analysed. This revealed that conventional and software-based control systems may exhibit similar failure mechanisms, e.g., incorrectly set limit values in protective devices. Consequently, conventional and software based I&C will be analysed together in future.

In addition, GRS has systematically assessed the 129 new event reports that were provided by organisations from the other countries to the ICDE database. In the previous projects SR 2545, 3608R01338, 3611R01335, 3614R01301, and 4720R01350, 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, breakers, batteries, control rod drive assemblies and heat exchangers had been analysed with regard to the observed CCF phenomena. These phenomena had been compared to the phenomena already known in German plants. The results were documented in /GRS 08a/, /GRS 08b/, /GRS 11a/, /GRS 11b/, /GRS 14a/, /GRS 14b/, /GRS 18/, /GRS 20/ and /GRS 23b/. In this project, the new foreign operating experience was evaluated and new CCF phenomena that had not yet occurred in Germany were found.

Inhaltsverzeichnis

Kurzfassung I

Abstract V

1 Einführung und Zielsetzung 1

2 Organisation des ICDE-Projekts 5

2.1 Aufgabenverteilung innerhalb des Projekts 5

2.1.1 ICDE-Lenkungskreis 5

2.1.2 NEA-Sekretariat 7

2.1.3 Operating Agent 7

2.2 Vertraulichkeit der ICDE-Daten 7

2.3 Zustimmung der deutschen Betreiber 8

3 Abstimmung von Art und Umfang der für den ICDE-Datenaustausch vorgesehenen Informationen 9

3.1 Allgemeine ICDE-Kodieranleitung 9

3.2 Komponentenartspezifische Kodieranleitungen 10

3.3 Erweiterung für Anlagen im Nachbetrieb 11

3.4 Kodieranleitung zur Ereignisanalyse 12

3.5 ICDE-Datenbank 14

3.5.1 Struktur der ICDE-Datenbank 15

3.5.2 Weiterentwicklung der ICDE-Datenbank 18

3.6 GVA-Datenbasis der GRS 18

4 Ergebnisse des ICDE-Projekts 19

4.1 Stand des ICDE-Datenaustauschs 19

4.2 Berichte des ICDE-Projektes 20

4.3 Workshops des ICDE-Projekts 22

4.3.1 Workshops zum Thema „Sicherheitskultur“ 24

4.3.2 Workshops zum Thema „Alterung” 24

4.3.3 Workshop zum Thema „Konventionelle Leittechnik” 25

5 Sammlung, Analyse und Bereitstellung von Informationen zu deutschen GVA-Ereignissen für den Datenaustausch 27

5.1 Stand der deutschen ICDE-Betriebserfahrungsauswertung 27

6 Auswertung der ICDE-Ereignisse aus anderen Ländern 31

6.1 Datenbasis und Vorgehensweise 32

6.2 Komponentenart Batterien 34

6.3 Komponentenart Digitale Leittechnik 34

6.4 Komponentenart Frischdampfisolationsventile 36

6.5 Komponentenart Füllstandsmessungen 37

6.6 Komponentenart Kreiselpumpen 38

6.7 Komponentenart Leistungsschalter 44

6.8 Komponentenart Ventilatoren 44

6.9 Komponentenart Motorbetätigte Armaturen (MOVs) 45

6.10 Komponentenart Notstromdiesel 47

6.11 Komponentenart Rückschlagarmaturen 53

6.12 Komponentenart Sicherheits- und Entlastungsventile 54

6.13 Komponentenart Wechselrichter 57

6.14 Zusammenfassung der Auswertung 59

6.15 Hinweise 59

7 Zusammenfassung und Ausblick zum ICDE-Projekt 63

Literaturverzeichnis 67

Tabellenverzeichnis 73

1 Einführung und Zielsetzung

Ereignisse mit gemeinsam verursachten Ausfällen (GVA) können die Verfügbarkeit des Sicherheitssystems in Kerntechnischen Anlagen wesentlich beeinträchtigen. Deshalb werden Informationen und Daten zu GVA-Ereignissen in vielen Ländern systematisch gesammelt und analysiert. Aufgrund der geringen Eintrittswahrscheinlichkeit von GVA und aufgrund der Stilllegung deutscher Kernkraftwerke (KKW) reicht die in Deutschland vorliegende Betriebserfahrung nicht für eine umfassende Bewertung von GVA-Ereignissen, den Vorkehrungen gegen GVA sowie der Modellierung von GVA in Probabilistischen Sicherheitsanalysen (PSA) aus. Deshalb ist es notwendig, auch die Betriebserfahrung anderer Länder zu nutzen.

Eine direkte Nutzung der qualitativen und quantitativen GVA-Datensammlungen anderer Länder wird 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 mitinitiiert. 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 vom BMUKN finanzierten Vorhaben SR 2276, SR 2418, SR 2468, SR 2545, 3608R01338, 3611R01335 und 3614R01301, 4717R01337 und 4720R01350 und wurde im Rahmen des am 24.08.2023 abgeschlossenen und mit diesem Bericht dokumentierten Eigenforschungsvorhaben 4723R01275 fortgeführt.

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 und um probabilistischen Sicherheitsanalysen (PSA) verwendete GVA-Wahrscheinlichkeiten bzw. GVA-Raten beurteilen zu können.

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 verbreitet. Dies ermöglicht die Entwicklung von Vorsorgemaßnahmen auch gegen solche GVA-Phänomene, die in der deutschen Betriebserfahrung 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 internationalen 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.

Im vorliegenden Bericht wird zunächst das ICDE-Projekt vorgestellt. Dazu werden die organisatorischen Arbeiten und Entwicklungen beschrieben, die zur Lenkung des Projektes bis jetzt im Rahmen des laufenden Vorhabens notwendig waren. Dabei werden auch die wesentlichen organisatorischen Rahmenbedingungen des Projekts in ihren aktuellen Fassungen miterläutert. Danach werden der aktuelle Stand des ICDE-Datenaustauschs, die vom ICDE-Lenkungskreis erarbeiteten Auswerteberichte sowie die vom ICDE-Lenkungskreis durchgeführten Workshops zur Nutzung der ICDE-Daten vorgestellt. Anschließend werden die während der bisherigen Laufzeit des Vorhabens durchgeführten Auswertungen deutscher Betriebserfahrung mit GVA-Ereignissen und die dabei erzielten Ergebnisse beschrieben.

Mit den Berichten /GRS 08a/, /GRS 08b/, /GRS 11a/, /GRS 11b/, /GRS 14a/, /GRS 14b/, /GRS 18/, /GRS 20/ sowie /GRS 23b/ 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 schon bekannt und für deutsche Kernkraftwerke relevant sind. In diesem Vorhaben wurde darauf aufbauend die seit diesen Erstauswertungen neu angefallene ausländische Betriebserfahrung ausgewertet. In Kapitel 6 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 Anlagen verhindert werden könnten.

Die Arbeitsergebnisse des Vorhabens werden in zwei Berichten dokumentiert. Dieser Bericht (GRS-A-4215) enthält auch gemäß den dem ICDE-Projekt zugrundeliegenden Vereinbarungen zugangsbeschränkte Informationen und ist folglich nur für die Verbreitung in einem beschränkten Kreis (BMUKN, BASE, GRS) vorgesehen. Die generischen Erkenntnisse der Auswertung ohne zugangsbeschränkte, projektinterne Informationen werden in einem frei zugänglichen GRS-Bericht (GRS-848) veröffentlicht.

2 Organisation des ICDE-Projekts

2.1 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 „Nuclear Energy Agency“ (NEA) der „Organisation for Economic Co-operation and Development“ (OECD) die formale Verwaltung des ICDE-Projekts übernommen.

Die Steuerung des Projekts erfolgt durch den ICDE-Lenkungskreis („Management Board“, vormals „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 Lenkungskreis 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 IX“) läuft noch bis Ende 2026.

2.1.1 ICDE-Lenkungskreis

Der ICDE-Lenkungskreis (englisch „Management Board“) 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 und seines Vertreters,

- 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,
- Steuerung und Überwachung der Arbeiten des Operating Agents,
- Bestimmung des Informationsflusses (öffentliche Information und Vertraulichkeit),
- Aufbau und Inhalt der Projektberichte und
- 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) und UJV (Tschechische Republik). In den Heimatländern der beteiligten Organisationen befinden sich 203 Kernkraftwerksblöcke im Leistungsbetrieb – dies ist etwas weniger als die Hälfte der sich weltweit im Leistungsbetrieb befindende Blöcke.

Die spanische Aufsichtsbehörde hat angekündigt, in der nächsten ICDE-Periode, die am 01.01.2027 beginnen wird, am Projekt teilzunehmen. Zurzeit sind sieben Reaktoren in Spanien in Betrieb.

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 entsprechende eigene Daten eingespeist haben.

2.1.2 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. Weiterhin unterstützt sie die Sitzungsdurchführung. Die NEA bestimmt das Projektsekretariat, hat jedoch keinen Einfluss auf die inhaltliche Arbeit des Lenkungsausschusses.

2.1.3 Operating Agent

Die Aufgaben des Operating Agents werden von der schwedischen Firma „AFRY“ wahrgenommen. Die Kosten dafür werden von den teilnehmenden Organisationen anteilig übernommen. 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 /ICD 26/ 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“).

2.2 Vertraulichkeit der ICDE-Daten

Für den detaillierten Informationsaustausch zu GVA-Ereignissen innerhalb des ICDE-Projektes 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.

2.3 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 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. Dieser Informationsaustausch unterliegt in beiden Richtungen wegen seiner Sensitivität der besonderen Vertraulichkeit (siehe hierzu Abschnitt 2.2).

3 Abstimmung von Art und Umfang der für den ICDE-Datenaustausch vorgesehenen Informationen

Im Rahmen der Arbeiten, an denen die GRS in den vergangenen Jahren 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 Komponentenart die entsprechenden Besonderheiten. Zusätzlich sind Hinweise und Erläuterungen zur Analyse von GVA-Ereignissen enthalten. In der aktuellen Fassung 5 des General Coding Guide /ICD 26/ sind sowohl die allgemeinen Kodieranleitungen, die bis jetzt fertiggestellten komponentenspezifischen Kodieranleitungen, die Failure Analysis Coding Guidelines und die 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. Der General Coding Guide wird stetig fortgeschrieben.

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

3.1 Allgemeine ICDE-Kodieranleitung

Die allgemeine ICDE-Kodieranleitung /ICD 26/ 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 potenzielle GVA-Ereignisse sein können,
- wie die Beobachtungseinheiten (Komponentengruppen), für die ICDE-Ereignisse gesammelt 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 und
- welche Informationen zur Beschreibung und Klassifizierung eines beobachteten ICDE-Ereignisses erforderlich sind.

Die einzelnen Informationen werden in entsprechenden Feldern der ICDE-Datenbank abgelegt (siehe Abschnitt 3.4). 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.

3.2 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 und
- 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.

Neben den komponentenspezifischen Kodieranleitungen gibt es auch eine spezielle Kodieranleitung für Ereignisse, die mehrere Komponentengruppen betrafen (Komponentengruppenübergreifende GVA, „X-CCF“). Diese beschreibt die Kodierung eines solchen Ereignisses in einem speziellen Datensatz, der die Kodierung in den Komponentengruppen-spezifischen Datensätzen ergänzt.

3.3 Erweiterung für Anlagen im Nachbetrieb

Da die Betriebserfahrung Ereignisse enthält, die spezifisch für Anlagen im Nachbetrieb sind, weil sie z. B. durch technische Änderungen oder Änderungen der Betriebsweise nach endgültiger Beendigung des Leistungsbetriebs hervorgerufen worden sind, wurde im Lenkungskreis beschlossen, zukünftig Ereignisse und Beobachtungszeiten von Anlagen, die ihren Leistungsbetrieb beendet haben, speziell zu kennzeichnen. Entsprechend wurde die Kodieranleitung um ein binäres Merkmal (Flag) erweitert. Dieses Merkmal „C15 – Post Operation Phase“ wird für Beobachtungzeiten-Datensätze („Statistical Records“) ausgewählt, wenn sich diese auf eine Beobachtungzeit beziehen, in der der Leistungsbetrieb beendet worden war. Entsprechen sind für Anlagen nach Beendigung des Leistungsbetriebs mindestens zwei Statistical Records erforderlich: Ein Statistical Record beschreibt die Beobachtungszeit vor Beendigung des Leistungsbetriebs – hier ist

Merkmal C15 nicht ausgewählt – und ein Statistical Record beschreibt die Beobachtungszeit nach Beendigung des Leistungsbetriebs – hier ist Merkmal C15 ausgewählt (siehe auch Abschnitt 3.5.2). Auch Ereignisse mit einem nur für den Nachbetrieb relevanten GVA-Phänomen werden nun entsprechend speziell gekennzeichnet durch das Merkmal C15.

3.4 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 oder
  - bei denen mehrere Qualitätssicherungsmaßnahmen zur Verhinderung von GVA versagt hatten.
- Eine Liste von Schweregradklassen zur Bewertung von GVA mitsamt entsprechenden Filtern 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 hinaus enthält die Kodieranleitung zur Ereignisanalyse die verschiedenen zusätzlichen Klassifizierungen der Ereignisse, die in der Vergangenheit in den Auswerteberichten des ICDE-Projekts 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.
- Auslegungs-, 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, komponentenartspezifische 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 Komponentenarten mit Ausnahme von Lüftern, Frischdampfisolationsventilen, softwarebasierter Leittechnik und Wechselrichtern vor. Für die noch ausstehenden Komponentenarten ist die Zahl der in der Datenbank hinterlegten Ereignisse noch nicht groß genug, um im Rahmen eines Komponentenworkshops entsprechende Kategorien zu entwi-

ckeln. Sobald ein entsprechender Umfang an Betriebserfahrung vorliegt, werden die entsprechenden Codes für die noch ausstehenden Komponentenarten entwickelt und ausformuliert. Die entsprechenden Codes sind in Abschnitt A1.4 von /ICD 26/ zu finden.

3.5 ICDE-Datenbank

Die Oberfläche der ICDE-Datenbank basiert auf der Softwareumgebung „.NET“ 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 2.1), 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 zugriffs-

berechtigt 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 Auswertezeiträume erhält, für die sie auch eigene Beiträge geliefert hat.

3.5.1 Struktur der ICDE-Datenbank

Die ICDE-Datenbank beinhaltet zwei wesentliche Datenstrukturen:

- Observed Population Records und
- Event Records.

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 und
- Hersteller.

Darüber hinaus enthalten die OP-Record auch die zugehörigen statistischen Informationen in Form von Statistical Records. Ein Statistical Record beinhaltet Informationen zu einem Beobachtungszeitraum und einer Ausfallart. Dies umfasst

- Anfang des Beobachtungszeitraums,
- Ende des Beobachtungszeitraums,

- ausgewertete Ausfallart,
- Zahl der im ausgewerteten Beobachtungszeitraum aufgetretenen Einzelfehler an Komponenten der Komponentengruppe.

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 sind[2]. Für die deutschen KKW existieren aktuell 1.472 OP-Records, die eine Betriebserfahrung von 36.313,2 Komponentengruppenjahren sowie 285.445,4 Komponentenjahren abdecken.

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) und
- Art der Fehlerentdeckung (z. B. Test oder Anforderung).

[2] Eine diesbezügliche Ausnahme stellt die Komponentenart „Softwarebasierte Leittechnik“ dar. Hier ist es nicht erforderlich, die OP-Records vollständig zu ermitteln. Dementsprechend werden die Komponentengruppen im Allgemeinen erst angelegt, wenn ein GVA in der entsprechenden Komponentengruppe aufgetreten ist.

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 (Complete Failure – C): Die Komponente war nicht in der Lage, ihre sicherheitstechnische Funktion zu erfüllen (Beispiel: Eine Pumpe startet nicht).
- Geschädigt (Degraded – D): Die Komponente war im Wesentlichen in der Lage ihre spezifizierte sicherheitstechnische Funktion zu erfüllen, wies jedoch Einschränkungen auf (Beispiel: Die Fördermenge einer Pumpe ist gegenüber der Spezifikation reduziert, reicht jedoch zum Erfüllen der verfahrenstechnischen Anforderungen aus.).
- Schwach geschädigt (Incipient Failure – I): Die Komponente war in der Lage ihre spezifizierte sicherheitstechnische Funktion zu erfüllen und wies keine funktionsrelevanten Einschränkungen auf, war jedoch von einem GVA-Fehlermechanismus betroffen, der sich zu einem Funktionsausfall hätte entwickeln können (Beispiel: Nicht dauerfeste Lager, die langfristig zu einer Funktionseinschränkung führen würden).
- Funktionsfähig. (Working – W): Die Komponente war von dem GVA-Fehlermechanismus nicht betroffen.

Darüber hinaus wird kodiert, wie viele Komponenten der Komponentengruppe potenziell von dem wirksamen GVA-Fehlermechanismus betroffen waren („Number of Exposed Components“).

Im Ordner „Specifications“ ist für jeden einzelnen Komponentenausfall spezifiziert, wann dieser aufgetreten ist, wie er entdeckt wurde und wie lange die Latenzzeit zwischen Auftreten und Entdeckung des Fehlers war.

Weitere Details zum verwendeten Kodierungsschema sind im General Coding Guide /ICD 26/ enthalten.

3.5.2 Weiterentwicklung der ICDE-Datenbank

Die Datenbankstruktur und die Oberfläche werden kontinuierlich gepflegt und auf Anforderung des ICDE-Lenkungskreises weiterentwickelt.

Während des Vorhabens wurde die Datenbank dahingehend erweitert, dass eine transparente Kodierung von Ereignissen und Beobachtungszeiten von Anlagen, die ihren Leistungsbetrieb beendet haben, möglich ist (siehe Abschnitt 3.3). Hierzu wurden die Ereignisdatensätze und die Datensätze für Beobachtungsperioden („Statistical Records“) jeweils um ein binäres Merkmal erweitert. Entsprechend sind für Anlagen, deren Betriebserfahrung auch nach Beendigung des Leistungsbetriebs erfasst wird, mindestens zwei Statistical Records erforderlich: Ein Statistical Record beschreibt die Beobachtungszeit vor Beendigung des Leistungsbetriebs – hier ist das Merkmal „C15 – Post Operation Phase“ nicht ausgewählt – und ein Statistical Record beschreibt die Beobachtungszeit nach Beendigung des Leistungsbetriebs – hier ist Merkmal C15 ausgewählt. Durch diese Erweiterung ist die Datenbank kompatibel mit älteren Versionen; eine manuelle Bearbeitung bestehender Datensätze für Beobachtungszeiten vor Beendigung des Leistungsbetriebs ist nicht nötig.

Ereignisse mit Nachbetriebs-spezifischen Phänomenen werden ebenfalls mit dem Merkmal „C15 – Post Operation Phase“ gekennzeichnet.

Entsprechend dieser Erweiterungen wurden für die fünf Anlagen, für die die deutsche Betriebserfahrung erfasst wurde, 836 neue Statistical Records erzeugt.

3.6 GVA-Datenbasis der GRS

Die GRS pflegt – neben der Datenbank der deutschen GVA-Ereignisse /GRS 10/ – auch eine strukturierte Sammlung der aufgetretenen GVA-Phänomene, die so genannte GVA-Checkliste. Diese Datensammlung beinhaltete bisher nur GVA-Phänomene aus der deutschen Betriebserfahrung. Im Rahmen dieses Vorhabens wurde sie derart erweitert, dass nun auch GVA-Phänomene aufgenommen werden können, die in ausländischen ICDE-Ereignissen beobachtet wurden. Ein entsprechendes Feld wurde ergänzt, in dem die Ereignis-Codes des ICDE eingegeben werden können. Im Zuge der Erweiterung wurde die Datenbankoberfläche neu erstellt, da die bisherige Oberfläche mit einer mittlerweile überholten Programmierumgebung erstellt worden war.

4 Ergebnisse des ICDE-Projekts

4.1 Stand des ICDE-Datenaustauschs

Während des Berichtzeitraums erfolgten Updates für neue Beobachtungszeiträume zu den Komponentenarten Batterien, Leistungsschalter, Kreiselpumpen, Rückschlagarmaturen, Steuerstäbe und Steuerstabantriebe, Notstromdieselgeneratoren, Lüfter, Wärmetauscher, Füllstandsmessungen, Frischdampfisolationsventile, motorbetätigten Absperrarmaturen, Sicherheits- und Entlastungsventile sowie Wechselrichter. Weiterhin wurden ein neues Ereignis als komponentengruppenübergreifender GVA kodiert.

In Tab. 4.1 ist ein Überblick über die im ICDE-Projekt ausgetauschten Datensätze zu den einzelnen Komponentenarten (Stand 30.06.2026) gegeben.

Tab. 4.1 Umfang der ICDE-Datenbank

Komponentenart	Anzahl der OP-Records (Komponentengruppen)	Komponenten-gruppenjahre	Anzahl ICDE-Ereignisse	Anzahl vollständiger GVA
Batterien	403	6.384,40	94	5
Leistungsschalter	1.363	26.512,43	121	7
Kreiselpumpen	1.734	40.294,79	464	48
Rückschlagarmaturen	1.233	25.146,59	126	15
Steuerstäbe und Steuerstabantriebe	491	7.784,43	190	4
Diesel	320	7.265,08	399	36
Softwarebasierte Leittechnik	11†	59,16†	10	5
Ventilatoren	736	13.445,94	33	4
Wärmetauscher	606	17.153,60	59	4
Wechselrichter	21	407,18	6	2
Füllstandsmessungen	599	11.693,10	178	10
Frischdampf-isolationsventile	188	3.885,04	14	1
Motorbetätigte Absperrarmaturen	1.444	32.572,46	201	10
Sicherheitsventile	763	17.467,45	306	22

Komponentenart	Anzahl der OP-Records (Komponentengruppen)	Komponentengruppenjahre	Anzahl ICDE-Ereignisse	Anzahl vollständiger GVA
Komponentengruppenübergreifende GVA	nicht anwendbar	nicht anwendbar	9	0
Summe	**9.912**	**210.071,65**	**2.210**	**173**

† Bei der softwarebasierten Leittechnik besteht keine Anforderung, die OP-Records der beobachteten Population vollständig zu ermitteln und einzugeben. Somit ist davon auszugehen, dass im Wesentlichen OP-Records derjenigen Einrichtungen übermittelt werden, bei denen Ereignisse aufgetreten sind. Deshalb ist bei dieser Komponentenart die tatsächlich ausgewertete Betriebserfahrung wesentlich größer als die Anzahl angegebener OP-Records bzw. Komponentengruppenjahre.

Im Rahmen des aktuellen Projektes wurden sechs neue ICDE-Ereignis-Datensätze sowie ein Datensatz zu einem übergreifenden GVA (X-CCF) hinzugefügt. Es wurden keine zusätzlichen Observed Population Records, jedoch 836 neue Statistical Records erstellt. Details sind im Abschnitt 5.1 dargestellt.

4.2 Berichte des ICDE-Projektes

Um die Arbeiten des ICDE-Projekts der Fachwelt transparent zu machen, berichtet der ICDE-Lenkungskreis im Rahmen der Schriftenreihe der OECD/NEA/CSNI über die Ergebnisse der Auswertungen zu den einzelnen Komponentenarten bzw. über spezifische, komponentengruppenübergreifende Themen wie z. B. latente, d. h. nicht sofort, sondern erst im Anforderungsfall oder bei Prüfungen erkennbare GVA durch menschliche Fehlhandlungen. Ziele dieser Berichte sind üblicherweise:

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

Während der Laufzeit der Vorgängervorhaben 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 03a/,
- Komponentenbericht: Batterien /NEA 03b/,
- 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/,
- Komponentenbericht: GVA-Ereignisse an Notstromdieselgeneratoren, bei denen die komplette Komponentengruppe betroffen war /NEA 17/,
- Themenbericht: Notstromdiesel 2 (Update zu /NEA 00/) /NEA 18/,
- Themenbericht: GVA-Ereignisse infolge von Modifikationen an der Anlage /NEA 20/,
- Themenbericht: Systemübergreifende GVA /NEA 22a/,
- Themenbericht: Mehrblockanlagen /NEA 22b/,
- Themenbericht: Verbessern von Prüfungen /NEA 22c/.

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

- Komponentenbericht: Sicherheits- und Entlastungsventile (ICDE Project Report: Common-Cause Failures of Safety and Relief Valves, NEA/CSNI/R(2020)17) /NEA 24/,
- Themenbericht: GVA durch externe Einwirkungen auf Komponenten (ICDE Topical Report Operational Experience on Common-Cause Failures due to External Environmental Factors, NEA/CSNI/R(2020)15) /NEA 25a/,

- Komponentenbericht: Motorbetätigte Armaturen (ICDE Project report: Lessons Learnt from Common-Cause Failures of Motor-Operated Valves, NEA/CSNI/R(2021)7) /NEA 25b/,
- Projektbericht: Überblick über die VIII. Phase des ICDE (ICDE Project Report: Summary of Phase VIII of the International Common-Cause Failure Data Exchange Project, NEA/CSNI/R(2023)9) /NEA 25c/,
- Themenbericht: Latente GVA durch menschliche Fehlhandlungen (ICDE Topical Report: Collection and Analysis of Common-Cause Pre-Initiator Human Failure Events, NEA/CSNI/R(2022)1) /NEA 25d/,
- Komponentenbericht: Batterien (ICDE Topical Report: Lessons Learnt from Common-Cause Failures of Batteries, NEA/CSNI/R(2023)8, /NEA 26/.

Aktuell befindet sich folgender Bericht im Qualitätssicherungsprozess:

- Themenbericht: Erkenntnisse zur Sicherheitskultur durch Analyse von GVA (ICDE Topical Report: Safety Culture Insights from Analysis of Common Cause Failure Events).

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 veröffentlichten 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 „Probabilistic Safety Assessment and Management & Asian Symposium on Risk Assessment and Management (PSAM 17 und ASRAM2024)“, die vom 7. bis 11. Oktober 2024 in Sendai/Japan stattfand, wurden das ICDE-Projekt und ausgewählte bisher erzielte Ergebnisse sowie Anwendungsmöglichkeiten vorgestellt. Das Konferenzpaper /STI 24/ ist frei verfügbar.

4.3 Workshops des ICDE-Projekts

Während der Laufzeit des aktuellen Vorhabens 4723R01275 wurden vier Workshops durchgeführt, in denen die in der Datenbank enthaltenen Ereignisse hinsichtlich bestimmter Themen ausgewertet wurden.

Die Themen der Workshops werden jeweils im Vorfeld der Treffen des ICDE-Lenkungskreises festgelegt. Hierbei kann es sich sowohl um themen- als auch um 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 bestimmen, die dann im Rahmen des eigentlichen Workshops vertieft analysiert werden.

Zur Durchführung des Workshops werden Gruppen aus zwei bis fünf 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 Lenkungskreises ebenfalls möglich und hat sich als sehr nützlich erwiesen, um weitere inhaltliche Perspektiven in den Workshop zu integrieren. Zum Beispiel nahmen am Workshop über Alterung im Rahmen des 60. Treffens zusätzliche Experten der finnischen Aufsichtsbehörde sowie der Organisation des Operating Agents, AFRY, teil. Je nach Zahl der Ereignisse und Teilnehmern muss jede Gruppe 5 - 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.

Tab. 4.2 Übersicht der ICDE-Workshops

ICDE-Treffen	**Thema des Workshops**
Nr. 57 (Saclay bei Paris)	Sicherheitskultur (3. Workshop)
Nr. 60 (Solna bei Stockholm)	Alterung (1. Workshop)
Nr. 61 (Paris)	Alterung (2. Workshop)
Nr. 62 (Boulogne-Billancourt bei Paris)	Konventionelle Leittechnik

Auf den 58. und 59. ICDE-Treffen fanden statt Workshops Diskussionen über die aktuellen Berichte statt. Hierbei wurde insbesondere über die Arbeiten zur Quantifizierung, d. h. der Bestimmung von GVA-Wahrscheinlichkeiten bzw. -Raten aus den ICDE-Daten, diskutiert.

Die Ergebnisse der Workshops werden im Folgenden kurz zusammengefasst. Hierbei wird auch auf Arbeiten eingegangen, die der Vor- und Nachbereitung der Workshops dienten.

4.3.1 Workshops zum Thema „Sicherheitskultur“

Im Rahmen der Studie über Defizite in der Sicherheitskultur als Ursache von GVA, die während des Vorgängervorhabens 4720R01350 begonnen worden war (siehe /GRS 23b//GRS 23b/), wurde ein weiterer Workshop durchgeführt. Hierbei wurden jeweils in mehreren Gruppen von Experten weitere Ereignisse analysiert, die potenziell durch Defizite in der Sicherheitskultur verursacht wurden und gemäß dem zuvor entwickelten Kodierungsschema kodiert.

Die in allen drei Workshops zum Thema Sicherheitskultur betrachteten Ereignisse wurden im Überblick analysiert. Dabei zeigte sich, dass für den überwiegenden Teil der ausgewerteten Ereignisse jeweils ein oder mehrere Defizite in der Sicherheitskultur als kausale Faktoren identifiziert werden können. Die Erkenntnisse aus der Analyse, wie z. B., dass eine mangelnde Compliance sowohl mit unzureichender Arbeitsorganisation als auch mit Mängeln bei der Dokumentation der Arbeitsabläufe korreliert, sind im Bericht „ICDE Topical report: Safety Culture Insights from Analysis of Common Cause Failure Events“ dokumentiert. Er wurde an die externen Workshop-Teilnehmer der OECD/NEA Arbeitsgruppen „Working Group on Human and Organisational Factors“ (WGHOF) und „Working Group on Leadership and Safety Culture“ (WGLSC) zur Kenntnisnahme versandt. Auf der 62. Sitzung des Management Boards wurde beschlossen, den Bericht bei der CSNI einzureichen.

4.3.2 Workshops zum Thema „Alterung”

Eines der aktuellen Themenschwerpunkte sind GVA durch Alterung. Die Arbeiten wurden mit einem Workshop im Rahmen der 60. Sitzung des Lenkungskreises im April 2025 begonnen und auf einem zweiten Workshop im Rahmen der 61. Sitzung im September/Oktober 2025 fortgesetzt. Es wurden bisher insgesamt 72 Ereignisse analysiert. Die

Analyse der Ereignisse lieferte u. a. die vorläufige qualitative Erkenntnis, dass Alterung als Ursache von GVA in den allermeisten Fällen zusammen mit anderen Ursachen wie Defiziten in der Instandhaltung, ungeeignete Umgebungsbedingungen usw. auftritt. Ereignisse, die sich allein auf Alterung zurückführen lassen, sind selten. Dies kann dahingehend interpretiert werden, dass in den Anlagen meist ein Alterungsmanagement vorhanden ist, das eine effektive Vorkehrung gegen alterungsbedingte systematische Ausfälle darstellt. Erst wenn weitere Ursachen hinzukommen oder Defizite in dem Alterungsmanagement auftreten, werden alterungsbezogene GVA beobachtet. Den meisten untersuchten alterungsbezogenen GVA lagen mechanische Schädigungsmechanismen wie mechanische Abnutzung oder Ermüdung zugrunde.

4.3.3 Workshop zum Thema „Konventionelle Leittechnik”

Im Rahmen der 62. Sitzung des Lenkungskreises im April 2026 wurde ein Workshop zum Thema konventionelle (d. h. nicht softwarebasierte) Leittechnik durchgeführt. Hierzu hatte der Operating Agent eine Datenbank-Suchabfrage entwickelt, die auf die Identifikation von Ereignissen abzielte, bei denen die GVA-Ursache in Betriebsmitteln der konventionellen Leittechnik liegt und die innerhalb der Komponentenabgrenzung liegt (Konventionelle Leittechniksysteme wie z. B. das Reaktorschutzsystem sind derzeit nicht Teil der Datensammlung des ICDE). Die so gefundenen Ereignisse wurden in fünf Gruppen von jeweils zwei bis drei Teilnehmern näher analysiert. Dazu wurde zunächst bewertet, ob tatsächlich konventionelle leittechnische Einrichtungen die Ursache des GVA waren. Hierbei zeigte sich, dass dies in vielen Fällen nicht der Fall war. Dann wurden jeweils die für die Detailanalyse in Workshops entwickelten Kodierungen für Ausfallmechanismus, Ausfallursache und ggf. effektiver Vorkehrung ermittelt sowie eine kurze textliche Charakterisierung des Fehlermechanismus erstellt. Die abschließende Diskussion ergab verschiedene Aspekte, die vor einem weiteren Workshop zu diesem Thema behandelt werden müssen. Zum einen ist die Datenbank-Suchabfrage nicht trennscharf genug. In der ICDE-Datenbank sind keine Kodierungen vorgesehen, die ein einfaches Identifizieren von relevanten Ereignissen erlauben. Weiterhin waren die gefundenen Ereignisse teilweise durch konventionelle, teilweise durch softwarebasierte Leittechnik verursacht. Bei der Analyse zeigte sich, dass eine Beschränkung auf konventionelle Leittechnik nicht sinnvoll ist, da konventionelle und softwarebasierte Leittechnik teilweise gleiche Fehlermechanismen, z. B. falsch eingestellte Grenzwerte in Schutzeinrichtungen, aufweisen. Somit erscheint es sinnvoll, Ereignisse mit Ursache in leittechnischen Einrichtungen unabhängig von der verwendeten Technologie zusammen zu analysieren. Darüber hinaus zeigte sich, dass unter den Teilnehmern verschiedene Abgrenzungen

und Begriffsdefinitionen in Bezug auf konventionelle und softwarebasierte Leittechnik verwendet werden. Daher wurde vereinbart, basierend auf dem vom Operating Agent zu erstellenden Bericht über den Workshop, auf der nächsten Sitzung des Management-Boards die weitere Vorgehensweise zu diesem Thema zu diskutieren.

5 Sammlung, Analyse und Bereitstellung von Informationen zu deutschen GVA-Ereignissen für den Datenaustausch

5.1 Stand der deutschen ICDE-Betriebserfahrungsauswertung

Im Anschluss an den sogenannten Erstrundendatenaustausch, in dessen Rahmen für eine zuvor neu definierte Komponentenart ein Beobachtungszeitraum von mindestens fünf Jahren ausgewertet wird, wird im ICDE-Projekt eine regelmäßige Aktualisierung der Daten durchgeführt. Hierfür werden für Komponentenarten, bei denen bereits ein erster Datenaustausch stattgefunden hat, regelmäßig immer weitere Beobachtungszeiträume ausgewertet. Es werden hierbei im ICDE-Lenkungskreis keine Mindestauswertezeiträume vorgegeben, sondern es wurde jedem Projektteilnehmer freigestellt, in welchem Rhythmus bzw. Modus (z. B. komponenten- oder anlagenweise) er Datenupdates liefern will. Die neuesten Daten der teilnehmenden Länder sollen dabei nicht älter als acht Jahre sein. Um hierbei das Gegenseitigkeitsprinzip aufrecht zu erhalten, wurde beschlossen, den Datenbankzugang so zu regeln, dass ein Teilnehmer für diejenigen Komponentenarten und den Beobachtungszeitraum, für den er einen vollständigen eigenen Beitrag für alle Kernkraftwerke aus seinem Herkunftsland liefert, Zugang zu den in der ICDE-Datenbank gespeicherten Informationen der entsprechenden Komponentenarten und Zeiträume erhält. Zudem ermöglichen die neuen Regelungen allen Teilnehmern des ICDE-Projektes Zugriff auf alte Datensätze bis zum Jahr 2000. Die Teilnehmer des ICDE-Projektes sind angehalten, den Zeitraum ohne Datenaktualisierung kleiner als acht Jahre zu halten.

Im Rahmen des Vorhabens 3614R01301 wurde die Auswertung der Betriebserfahrung für 13 der 17 deutsche Anlagen bis zum 31.12.2010 abgeschlossen und mit der Auswertung für die Anlage KKG wurde für den Zeitraum 01.01.2011 bis 31.12.2015 begonnen. Die Auswertung erfolgt hierbei anlagenweise, d. h. es werden alle Komponentenarten einer Anlage für den entsprechenden Betrachtungszeitraum durch die GRS ausgewertet, in Kooperation mit dem Betreiber der Anlage und dem Operating Agent des ICDE-Projekts qualitätsgesichert und anschließend in die Datenbank eingespeist. Im Vorhaben 3617R01337 bzw. 4720R01337 wurde die Auswertung bis 2010 für alle Anlagen abgeschlossen und mit der Auswertung für den Zeitraum bis 2015 für die Anlagen, die nach 2011 noch eine Berechtigung zum Leistungsbetrieb hatten, fortgefahren. Diese Aktualisierung betraf die Anlagen Isar 2, Grohnde, Philippsburg 2 und Brokdorf. Im Vorhaben

4720R01350 wurden die Daten für die Anlagen Gundremmingen B und C, Neckarwestheim 2, Emsland, Brokdorf, Grohnde, Grafenrheinfeld und Isar 2 bis einschließlich 2017 und für die Anlage Philippsburg 2 bis einschließlich 2019 aktualisiert. Aus Effizienzgründen erfolgte die Bearbeitung nun parallel, d. h. die einzelnen Arbeitsschritte wurden für alle Anlagen gleichzeitig ausgeführt. Im aktuellen Vorhaben 4723R01275 wurden die Anlagen Gundremmingen B und C, Neckarwestheim 2, Emsland und Isar 2 bis einschließlich Ende 2023 aktualisiert. Bei den Arbeiten wurde – wenn möglich – auf die Ergebnisse der GRS-Vorhaben zur Auswertung der deutschen Betriebserfahrungen in Bezug auf GVA (4722R01280, 4719R01371 und vorherige Vorhaben, siehe /GRS 23a/) zurückgegriffen. Es wurden jeweils alle im ICDE erfassten Komponentenarten berücksichtigt.

Der aktuelle Stand der Auswertung ist in Tab. 5.1 dargestellt.

Tab. 5.1 Stand der ICDE-Auswertung der deutschen Betriebserfahrung

Kernkraftwerk	Ende Auswertungszeitraum
Gundremmingen B (KRB-II B)	31.12.2023
Gundremmingen C (KRB-II C)	31.12.2023
Neckarwestheim 1 (GKN I)	31.12.2010
Neckarwestheim 2 (GKN II)	31.12.2023
Krümmel (KKK)	31.12.2010
Biblis A (KWB-A)	31.12.2010
Biblis B (KWB-B)	31.12.2010
Emsland (KKE)	31.12.2023
Brunsbüttel (KKB)	31.12.2010
Unterweser (KKU)	31.12.2010
Isar 1 (KKI 1)	31.12.2010
Philippsburg 1 (KKP 1)	31.12.2010
Grafenrheinfeld (KKG)	31.12.2015
Brokdorf (KBR)	31.12.2017
Grohnde (KWG)	31.12.2017
Isar 2 (KKI 2)	31.12.2023
Philippsburg 2 (KKP 2)	31.12.2019

In Tab. 5.2 wird der aktuelle Stand der deutschen ICDE-Betriebserfahrungssammlung aufgeschlüsselt nach Komponentenarten dargestellt. Die neuen OP- und Event-Records

bezeichnen hierbei diejenigen Datenbankeinträge, die im Verlauf des aktuellen Vorhabens 4723R01275 neu erstellt wurden. Entsprechend der jüngst entwickelten Erweiterungen der ICDE-Datenbank um Betriebserfahrung aus der Nachbetriebsphase (siehe Abschnitt 3.5.2) wurden für die fünf Anlagen, für die die deutsche Betriebserfahrung erfasst wurde, 836 neue Statistical Records erzeugt.

Tab. 5.2 Deutsche ICDE-Betriebserfahrung aufgeschlüsselt nach Komponentenarten

Komponente	Anzahl dt. OP-Records	Anzahl dt. Event Records	Neue OP-Records	Neue Event-Records
Batterien	51	10	0	0
Leistungsschalter	125	10	0	0
Kreiselpumpen	150	33	0	0
Rückschlagarmaturen	345	19	0	0
Steuerstäbe und Steuerstabantriebe	59	6	0	0
Diesel	37	37	0	4
Softwarebasierte Leittechnik	4	4	0	0
Ventilatoren	149	3	0	1
Wärmetauscher	49	15	0	0
Wechselrichter	17	1	0	0
Füllstandsmessungen	155	10	0	0
Frischdampf-ISO-Ventile	51	0	0	0
Motorbetätigte Absperrarmaturen	193	19	0	1
Sicherheitsventile	100	26	0	0
Übergreifende GVA	n. a.	10	n. a.	1
Gesamt	**1.485**	**203**	**0**	**7**

Zum Zeitpunkt der Berichtserstellung ist die Auswertung der deutschen Betriebserfahrung für den deutschen Beitrag zum Erstrundendatenaustausch für alle in Tab. 5.2 dargestellten Komponentenarten abgeschlossen. Der aktuelle Stand der Auswertung für alle Kernkraftwerke ist im Detail in Tab. 5.1 dargestellt. Die Auswertezeiträume beziehen

sich jeweils auf alle im ICDE betrachteten Komponentenarten. Für die deutschen Anlagen, die nach 2011 noch in Betrieb waren, ist somit die Betriebserfahrung bis zum Ende 2017 (Brokdorf und Grohnde), 2019 (Philippsburg 2) bzw. 2023 (Gundremmingen B und C, Emsland und Isar 2) vervollständigt.

6 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 substanziell 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 (siehe /GRS 14a/, /GRS 14b/).

Im Rahmen des Vorhabens 3614R01301 wurden erstmals auch die Komponentenarten Lüfter, Frischdampfisolationsventile und softwarebasierte Leittechnik erfasst /GRS 18/. Hinzu kamen im Vorhaben 4720R01337 die Komponentenart Wechselrichter und die komponentenübergreifenden GVA /GRS 20/.

Während der Laufzeit des aktuellen Vorhabens 4723R01275 wurden vom ICDE keine neuen Komponentenarten hinzugefügt, sondern die Auswertungen der bisherigen Komponentenarten um weitere Auswertezeiträume erweitert. Die so neu hinzugekommenen Ereignisse aller Komponentenarten wurden analysiert. Dies ist im Folgenden dargestellt.

6.1 Datenbasis und Vorgehensweise

Seit der letzten Auswertung der ICDE-Ereignisse im Jahr 2023 hat sich die Zahl der ausländischen Ereignisse um 129 erhöht. Eine Übersicht über die im Rahmen der Vorgängervorhaben (siehe /GRS 08a/, /GRS 11b/, /GRS 14b/, /GRS 18/, /GRS 20/ und /GRS 23b/**Fehler! Verweisquelle konnte nicht gefunden werden.**/GRS 23b/) ausgewertete sowie die in der ICDE-Datenbank seitdem zusätzlich verfügbare Betriebserfahrung mit GVA ist in Tab. 6.1 dargestellt. Der höchste Zuwachs an Ereignissen ist in der Komponentenart Notstromdiesel zu verzeichnen.

Tab. 6.1 Vergleich bereits ausgewerteter und neuer, bisher nicht ausgewerteter ausländischer ICDE-Ereignisse

Komponentenart	Ausgewertete ausländische ICDE-Ereignisse		
	Gesamtzahl zum Vorhabensbeginn	Anzahl neuer Ereignisse	Gesamtzahl zum Vorhabensende
Batterien	75	2	77
Digitale Leittechnik	0	5	5
Frischdampfisolationsventile	12	1	13
Füllstandsmessungen	155	8	163
Komponentenübergreifender GVA	0	0	0
Kreiselpumpen	381	33	414
Leistungsschalter	103	2	105
Ventilatoren	30	1	31
Motorbetätigte Armaturen	164	9	173
Notstromdiesel	288	47	335
Rückschlagarmaturen	101	3	104
Sicherheits- und Entlastungsventile	247	14	261
Steuerstäbe und Steuerstabantriebe	171	0	171
Wärmetauscher	44	0	44
Wechselrichter	0	4	4
Summe	**1.771**	**129**	**1.900**

Die von Deutschland in die ICDE-Datenbank eingespeisten Ereignisse wurden hier nicht betrachtet, da deren Fehlermechanismen und Ursachen bereits durch die nationale Vorkommnisauswertung erfasst worden sind.

In den folgenden Abschnitten werden für die in diesem Vorhaben ausgewerteten Komponentenarten zunächst jeweils die in der ausländischen Betriebserfahrung identifizierten Fehlermechanismen vorgestellt und kurz beschrieben. Es wurden nur Fehlermechanismen diskutiert, die mehrere Komponenten betroffen haben oder potenziell zu einem GVA mehrerer Komponenten hätten führen können. Ereignisse, bei denen die Ursache unbekannt ist oder bei denen die Ursache der Beschreibung nicht entnommen werden kann, wurden nicht berücksichtigt. Ebenso wurden Ereignisse nicht berücksichtigt, wenn die Ausfälle Folgefehler eines Ausfalls technischer Einrichtungen außerhalb der Komponentengrenze ohne GVA-Charakter sind, z. B. Ausfall einer einzelnen Versorgungseinrichtung für mehrere redundante Komponenten. Deshalb ist die Anzahl diskutierter Ereignisse im Allgemeinen kleiner als die Anzahl bewerteter Ereignisse.

Es wurde jeweils nur der Fehlermechanismus betrachtet, unabhängig davon, wie viele Komponenten auf Grund dieses Fehlermechanismus ausgefallen waren. Wenn eine größere Anzahl von verschiedenen Fehlermechanismen verblieb, wurden diese gruppiert; die Gruppierung erfolgte hierbei hinsichtlich der aufgetretenen Ursachen, betroffenen Einrichtungen (z. B. Bauteilen) oder anderer Gemeinsamkeiten. Anschließend wurde im Rahmen einer Expertendiskussion zunächst erörtert, ob die identifizierten Fehlermechanismen auch für deutsche Anlagen relevant sein können. Ein Fehlermechanismus wurde dabei als für deutsche Anlagen 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 Anlagen relevanten Fehlermechanismen wurde anschließend diskutiert, ob der beobachtete Fehlermechanismus eine Weiterleitungsnachricht erforderlich erscheinen lässt oder ob er in Form eines sicherheitstechnischen Hinweises im Rahmen dieses Berichtes aufgegriffen wird. Es wurde ein für eine Weiterleitungsnachricht relevanter Fehlermechanismus (Verlust von Speicherinhalten durch entladene Batterien, die nicht rechtzeitig ersetzt wurden, siehe Abschnitt 6.13) identifiziert; für diesen wurde eine Weiterleitungsnachricht (WLN 2026/01 „Ausfälle/Fehlfunktionen von Baugruppen in mehreren kerntechnischen Anlagen aufgrund nicht funktionsfähiger Pufferbatterien“) erstellt. Darüber hinaus wurde kein Fehlermechanismus identifiziert, der eine Weiterleitungsnachricht notwendig gemacht hätte und zu dem noch keine Weiterleitungsnachricht verfasst wurde.

Im Folgenden werden jeweils die in den Ereignissen wirksamen GVA-Mechanismen kurz charakterisiert und dann – ggf. für mehrere Ereignisse zusammen – in Bezug auf deutsche Anlagen bewertet.

6.2 Komponentenart Batterien

Im Verlauf des Vorhabens wurden zwei neue ausländische ICDE-Ereignisbeschreibungen übermittelt. Diese beiden Ereignisbeschreibungen beziehen sich auf dasselbe Ereignis, das zwei verschiedene Komponentengruppen derselben Anlage betraf.

Bei dem Ereignis wurde eine unzulässig reduzierte Kapazität an allen vier bzw. an drei von vier redundanten Batterien entdeckt. Die Untersuchung ergab als wahrscheinlichste Ursache verschiedene Defizite bei der Herstellung: Unvollständiges Befüllen der Platten, Beschädigung der Platten, Verschmutzung an den Separatoren und zu fest angezogene Befestigungen. Diese haben wahrscheinlich zu einer schnelleren Alterung geführt, so dass die erwartete Lebensdauer von 20 Jahren nicht erreicht wurde. Darüber hinaus wurde herausgefunden, dass im Rahmen von Prüfungen die Batterien teilweise zu tief entladen wurden. Dies hat wahrscheinlich ebenfalls zu einer beschleunigten Alterung beigetragen.

Auch aus Deutschland sind latente Schäden an Batterien durch Defizite bei der Herstellung bekannt. Eine systematische Schädigung durch zu tiefes Entladen ist ebenfalls aufgetreten. Zu Schäden an Batterien hat die GRS bereits mehrere Weiterleitungsnachrichten verfasst.

6.3 Komponentenart Digitale Leittechnik

Bezüglich digitaler Leittechnik wurden fünf neue ausländische Ereignisse übermittelt.

Bei einem Ereignis wurde während der Revision aufgrund einer Fehlplanung eine Schiene der elektrischen Energieversorgung abgeschaltet, die eine Redundante der Leittechnik der Neutronenflussmessung versorgte, während eine weitere Redundante gerade wegen einer Prüfung unverfügbar war.

Fehlplanungen, die zu unzulässigen gleichzeitigen Unverfügbarkeiten von Einrichtungen führen, insbesondere auch durch Abschaltung der elektrischen Energieversorgung, sind auch aus Deutschland bekannt.

Bei einem Ereignis versagte die Drehzahlregelung beider Zwangsumwälzpumpen eines SWR, da die Drehzahl-Steuerungseinrichtungen der Pumpen ausgefallen waren. Die

Ausfälle wurde durch eine Überlastung des Datennetzwerkes, an der die Steuerungseinrichtungen angeschlossen waren, verursacht. Auch andere an das Netzwerk angeschlossene Steuerungseinrichtungen waren ausgefallen. Die Ursache der Überlastung konnte nicht aufgeklärt werden. Als Vorsorgemaßnahme wurden vor den Steuerungseinrichtungen Firewalls installiert.

Systematische Ausfälle von Datennetzwerken durch Überlastung sind grundsätzlich auch in Deutschland bekannt. Allerdings bestand im übermittelten Ereignis der Ausfallmechanismus gemäß Ereignisbeschreibung und weiterer öffentlich verfügbarer Information aus einem Ausfall der Steuerungseinheiten infolge der Überlastung, nicht aufgrund der durch die Überlastung beeinträchtigten Datenübertragung. Hieraus ergibt sich auch die Vorkehrungsmaßnahme der Anlage in Form von Firewalls, die eine Überlastung der Netzwerksegmente verhindern sollen, an der die Steuerungseinrichtungen angeschlossen sind. Ein Ausfall („Absturz“) von Steuereinrichtungen durch Netzwerkbelastungen ist aus der deutschen Betriebserfahrung nicht bekannt.

Bei dem übermittelten Ereignis ist auch wesentlich, dass die redundanten Pumpen an dasselbe Netzwerk angeschlossen waren, d. h., dass es hier keine Redundanztrennung gab. Insofern ist dieses Phänomen für Systeme, bei denen es eine Redundanztrennung gibt, nicht relevant.

Bei einem Ereignis kam es durch Fehlanregungen aufgrund eines Whiskers an einer Diode in einer digitalen Leittechnikbaugruppe zu einer Fehlauslösung. Die Ursachenanalyse ergab ein ungeeignetes Überzugsmaterial von Platinen, das Whiskerbildung begünstigte.

Probleme mit Whiskerbildung sind auch in Deutschland bekannt. Hierzu hat die GRS in der Vergangenheit die Weiterleitungsnachrichten WLN 2002/01 und 2002/01A verfasst. Von den deutschen Anlagen wurden entsprechende umfassende Vorkehrungen getroffen. Ein interessanter Aspekt des ausländischen Ereignisses ist, dass trotz langer bekannter und gut untersuchter Problematik das Schädigungsphänomen weiterhin auftreten konnte.

In einem Ereignis war in einer Softwareversion der Schutzbegrenzungsrechner eine nicht spezifikationsgemäße Reaktion auf den gleichzeitigen selbstgemeldeten Ausfall beider redundanter analoger Eingabemodule eines Strangs implementiert: Statt in die-

sem Strang ein Abschaltsignal auszulösen, wurden die letzten von den analogen Eingabemodulen als „gültig“ gelieferten Werte weiterverarbeitet, so dass die Auslösung im Anforderungsfall bei Ausfall beider Eingabemodule nicht erfolgt wäre. Die fehlerhafte Software war auf allen vier redundanten Rechnern vorhanden.

Eine nicht spezifikationsgemäße Programmierung ist auch aus der deutschen Betriebserfahrung bekannt. Die inkorrekte Verarbeitung ungültiger Messwerte in softwarebasierter digitaler Leittechnik ist auch aus Deutschland bekannt. Ebenso ist es bekannt, dass systematische Fehler durch ein Update eingebracht werden können.

Beim letzten Ereignis hatte ein Prozessor die Verarbeitung aus unbekanntem Grund gestoppt. Es konnte nicht geklärt werden, ob dieses Ereignis überhaupt eine systematische Ursache hat. Der Ausfall hatte nur Auswirkungen auf die Anlage aufgrund menschlicher Fehlhandlungen bei der Fehlerbehebung.

Fehlhandlungen bei der Fehlerbehebung sind auch aus der deutschen Betriebserfahrung bekannt.

Die Ereignisse zeigen einen neuen, noch nicht beobachteten Schädigungsmechanismus, den „Absturz“ aufgrund Überlastung eines Datennetzwerkes, der zum gleichzeitigen Ausfall mehrerer Einrichtungen führt, die mit überlasteten Netzwerksegmenten verbunden sind. Sind mehrere redundante Einrichtungen mit einem solchen Datennetzwerk verbunden, so ist ihr gemeinsamer Ausfall zu befürchten.

Darüber hinaus verdeutlichen die Ereignisse, dass die häufig deutliche größere Komplexität softwarebasierter Leittechnik, z. B. bezüglich der Verarbeitung ungültiger Messwerte oder des Ausfallverhaltens, hohe Anforderungen an den Menschen bei Programmierung und Instandhaltung stellt und zu unerwarteten Fehlern bzw. Ausfällen führen kann.

6.4 Komponentenart Frischdampfisolationsventile

Für die Komponentenart Frischdampfisolationsventile wurde ein neues ausländisches Ereignis übermittelt. Der Ereignisbeschreibung und -kodierung ist lediglich zu entnehmen, dass das Öffnen von mehreren Vorsteuerventilen zu langsam erfolgte, was zu einem zu langsamen Schließen zweier Frischdampfisolationsventile führte, und dass Änderungen der Instandhaltung als Vorkehrung implementiert wurden.

Hieraus ergeben sich keine neuen Erkenntnisse.

6.5 Komponentenart Füllstandsmessungen

Für die Auswertung wurden acht neue ausländische Einträge bewertet.

In einem Ereignis wurden bei Prüfungen an acht von neun Messumformern Fehlkalibrierungen festgestellt, wobei ein Messumformer die zulässige Abweichung überschritt. Als Vorkehrung wurde der Instandhaltungsprozess verbessert.

Systematische Fehlkalibrierungen an Messumformern sind aus Deutschland ebenfalls bekannt.

In einem Ereignis wurden nach einem Kurzschluss zwei redundante Messumformer unverfügbar, weil sie durch dieselbe Sicherung abgesichert waren.

Ein solches Ereignis ist ausgeschlossen, wenn eine Redundanztrennung in der elektrischen Energieversorgung vorliegt.

In einem Ereignis zeigten während der Revision zwei von vier RDB-Niveaumessungen zu hohe Werte an, weil die entsprechenden Redundanzen der Temperaturmessungen der Kühlmitteltemperaturkompensation unverfügbar waren. Bei der Planung der Revisionsarbeiten war die Abhängigkeit der Niveaumessungen von den Temperaturmessungen nicht berücksichtigt worden.

Fehler bei der Freischaltungsplanung in der Form, dass Abhängigkeiten nicht berücksichtigt werden, sind ein auch aus Deutschland bekanntes Phänomen.

Bei einem Ereignis traten bei drei von 16 Grenzwertgebern Drifts im Auslösewert auf aufgrund von Alterung von Potentiometern auf.

Die Drift von Potentiometern durch Alterung ist aus Deutschland bereits bekannt.

Bei den zwei weiteren übermittelten Ereignissen konnte die Ursache nicht geklärt werden bzw. es handelt sich um einen Einzelausfall.

6.6 Komponentenart Kreiselpumpen

Die Komponentenart Kreiselpumpen enthält Gruppen redundanter Pumpen mit sicherheitstechnischer Bedeutung, insbesondere in den redundant ausgelegten Sicherheitsteilsystemen. Sie 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. 33 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. 6.2 sind die mehrfach aufgetretenen Fehlerkategorien mit der jeweiligen Ereignisanzahl dargestellt.

Tab. 6.2 Kategorisierung der identifizierten Fehlermechanismen an Kreiselpumpen

Fehlerkategorien	**Ereignisanzahl**[3]
Alterung	6
Nicht konforme Bauteile	3
Auslegungsfehler - davon Auslegungsfehler der Komponente - davon Auslegungsfehler der Anlage	3 1 2
Fehler bei der Instandhaltung - davon Fehlkalibrierungen - davon Verwendung falscher Teile - davon Planungsfehler - davon unzureichende Entlüftung - davon unzureichende Reinigung	7 2 2 1 1
Unzureichende Schmierung	3
Fehler in Zusammenhang mit Modifikationen	2

[3] Weil manche Ereignisse keine GVA sind bzw. weil das betreffende GVA-Phänomen unbekannt oder nicht aus der Ereignisbeschreibung ermittelbar ist, ist hier und bei den anderen Komponentenarten die Anzahl der diskutierten Ereignisse teilweise kleiner als die Anzahl ausgewerteter neuer ausländischer Datensätze. Weiterhin können für einzelne Ereignisse mehrere Kategorien zutreffend sein. Hierauf wird im Folgenden nicht jedes Mal explizit hingewiesen.

Weitere Mechanismen, wie Defizite der Ersatzteilversorgung, traten jeweils nur einmal auf.

Im Folgenden sind die einzelnen aufgetretenen Ereignisse und GVA-Mechanismen beschrieben.

In einem Ereignis trat eine erhebliche Fehlmessung des Durchflusses einer Pumpe auf, weil sich beim gleichzeitigen Betrieb einer Kolbenpumpe eines anderen Systems Druckstöße über das Medium ausbreiteten. Die Dämpfung der Kolbenpumpe ist auf hohen Druck ausgelegt und bei niedrigem Gegendruck kaum wirksam. Ursache ist somit, dass die Auswirkungen des parallelen Betriebs der Pumpen nicht bedacht worden waren. Ob dies bei der ursprünglichen Auslegung der Anlage geschehen war, indem ein solcher Betriebszustand nicht berücksichtigt wurde, aber in der Anlagendokumentation auch nicht ausgeschlossen wurde, oder bei einer eventuellen späteren Änderung der Anlagendokumentation, die eine solche Betriebsweise zuließ, ist der Ereignisbeschreibung nicht zu entnehmen. Die Ereignisbeschreibung enthält auch keinen Hinweis auf menschliche Fehlhandlungen, so dass nicht von einem Verstoß gegen die Betriebsanweisungen auszugehen ist.

Zwei redundante An- und Abfahrpumpen erbrachten nicht den erforderlichen Druck und Durchfluss. Grund war eine zu hohe Temperatur des Fördermediums, die zu Kavitation in der Pumpe führte. Grund war ein Auslegungsfehler, der durch Modifikation der Anlage behoben wurde.

Auslegungsfehler sind auch aus der deutschen Betriebserfahrung bekannt. Die beschriebenen GVA-Mechanismen können jedoch auch dann auftreten, wenn Systeme in veränderter Weise betrieben werden.

Bei zwei redundanten Pumpen des gesicherten Nebenkühlwassers kam es nach Ergänzung von Schmiermittel zu einer Erhöhung der Lagertemperatur, die sich nach wenigen Stunden wieder normalisierte. Als Ursache wurde verhärtetes Schmiermittel identifiziert, das durch den Nachfüllvorgang abgelöst und in das Lager gedrückt wurde.

Die Alterung von Schmiermitteln ist aus der deutschen Betriebserfahrung grundsätzlich bekannt. Das hier beobachtete Phänomen ist allerdings insofern speziell, als dass es

sich nicht um einen langsam ablaufenden Vorgang handelt, sondern es durch das gleichzeitige Nachfüllen von Schmiermittel in mehreren Redundanten zu einer schnell auftretenden gleichzeitigen Beeinflussung mehrerer Pumpen kam.

Bei einem Ereignis konnte die Abschaltung von gesicherten Nebenkühlwasserpumpen nicht erfolgen, da falsche Relais (mit 24 V Spannung statt 48 V) eingebaut worden waren. Durch diesen Fehler wäre eine Umschaltung zwischen den zwei redundanten Pumpen eines Stranges nicht möglich gewesen.

Auch aus der deutschen Betriebserfahrung ist der Einsatz von falschen Bauteilen, insbesondere solcher mit falscher Nennspannung, bekannt.

Als Ursache eines Pumpenausfalls wurde entdeckt, dass ein Kurzschluss der LED-Kontrollleuchte der Pumpe zu einer Überstrom-Abschaltung des Leittechnikschrankes der Ansteuerung der Pumpe und damit zu ihrem Ausfall führte. Die LEDs waren als Ersatz der ursprünglich für die Anzeige verwendeten Glimmlampen verwendet worden. Eine mögliche Rückwirkung war bei der Modifikation nicht bedacht worden. Die LEDs wurden wieder durch Glimmlampen ersetzt. Dieser latente Fehler war bei vier Komponentengruppen vorhanden. Es waren jeweils zwei von vier Redundanten betroffen.

Der Ausfall von Schienen durch Überstrom aufgrund eines Kurzschlusses einer Kontrollleuchte ist auch aus Deutschland bekannt, während systematische Probleme durch Umrüstung auf LED bisher nicht aufgetreten sind. Das grundsätzliche Phänomen, dass durch Änderungen unerwartete neue Fehler und Ausfallmöglichkeiten, insbesondere durch Rück- oder Wechselwirkungen entstehen können, ist allerdings auch aus Deutschland bekannt.

Bei zwei von vier Pumpen waren die Strommessungen fehlkalibriert, was jeweils eine falsche Regelung der Pumpe verursachte. Dieser Fehler war bei einem Austausch im Rahmen eines Modernisierungsprojektes aufgetreten.

Systematische Fehlkalibrierungen sind auch aus Deutschland bekannt.

Ein Kabelbrand trat in einem Kabelanschlusskasten einer Pumpe auf. An einer redundanten Pumpe trat zwei Monate später Brandgeruch auf. Die Anschlusskästen aller redundanten Pumpen sollen durch Anschlusskästen eines anderen Designs ersetzt werden.

Systematische Schäden an der Isolierung in Anschlusskästen sind auch aus der deutschen Betriebserfahrung bekannt.

Zwei Brunnenwasserpumpen versagten mehrfach beim Start. Als Fehlerursache wurden ihre Leistungsschalter identifiziert. In einem Fall wurde eine Schwergängigkeit aufgrund ausgetrockneten Fetts identifiziert; in einem Fall ein Versagen des Verriegelungsmechanismus durch beschleunigte Alterung. Die Ursachen von zwei weiteren Schalterausfällen konnten nicht abschließend geklärt werden.

Die gefundenen Schädigungsmechanismen sind auch aus der deutschen Betriebserfahrung bekannt.

Eine Pumpe ließ sich nicht starten, weil es Kontaktprobleme in Sockeln von Leittechnikbaugruppen gab. Diese wurden durch Alterung des Elastomers, aus dem die Sockel gefertigt worden waren, verursacht. Von der Alterung waren auch die entsprechenden Leittechnikbaugruppen in den anderen Redundanten betroffen.

Alterung von Kunststoffsockeln von Bauelementen in Leittechnikbaugruppen ist auch aus Deutschland bekannt.

Redundante Pumpen zeigten eine reduzierte Leistung aufgrund der teilweisen Verstopfung ihrer Saugsiebe. Eine Inspektion der Behälter, aus denen sie ansaugten, identifizierte Farbreste und Schlamm auf dem Boden. Der Schlamm bestand aus Korrosionsprodukten und Material, das bei der Errichtung oder bei Instandhaltungsarbeiten eingebracht wurde. Offenbar waren notwendige Reinigungen nicht erfolgt. Ein zur Reinhaltung des Wassers vorgesehenes System konnte die Sedimente nicht herausfiltern, da der geringe Durchfluss, der beim Betrieb des Reinigungssystems entsteht, nicht zum Aufwirbeln von Sedimenten führt.

Auch aus deutschen Anlagen ist die Beeinträchtigung von Pumpen durch Material, das nach Arbeiten im System verblieben ist, bekannt. Bei dem beobachteten Phänomen handelt es sich jedoch um ein Zusammenwirken von einem unzureichenden Reinigungssystem und systematischen Fehlern bei der Reinigung nach Instandhaltungsarbeiten.

Eine Rohrleitung in der Ansaugleitung einer Nebenkühlwasserpumpe vibrierte stark. Befestigungen der Leitung hatten sich gelöst. Am redundanten Strang wurden dieselben

Probleme gefunden. Die Befestigungen wurden in ordnungsgemäßen Zustand gebracht und zusätzliche Befestigungen wurden installiert.

Schäden durch Schwingungen von Leitungen sind auch aus Deutschland bekannt.

In allen vier Redundanten wurden falsche Sicherungen (falsche Spannung) verwendet. Als Ursachen wurden Fehler im Ersatzteil-Management und das Fehlen einer Kontrolle vor dem Einbau identifiziert.

Der Einsatz von Sicherungen mit falschen Charakteristika (Strom, Spannung, Trägheit) ist auch aus Deutschland bekannt.

Durch mangelhafte Entlüftung fiel eine Pumpe des gesicherten Nebenkühlwassers aus. Auch die redundanten Pumpen mussten entlüftet werden.

Systematische Ausfälle durch unzureichende Entlüftung sind aus Deutschland bekannt.

Eine Nachkühlpumpe fiel durch Fehlanregung der Überstromauslösung des Leistungsschalters aus. Ursache war eine falsche Einstellung. Dieselbe falsche Einstellung war bei der redundanten Pumpe vorhanden.

Systematische Fehlkalibrierungen sind auch aus Deutschland bekannt.

Bei zwei Pumpen des gesicherten Nebenkühlwassers löste sich die innere Polyurethan-Beschichtung des Gehäuses. Bei einer dieser Pumpen kam es bereits zu einer Beeinträchtigung des Freilaufs des Rotors.

Eine Ablösung der Innenbeschichtung von Komponenten ist auch aus Deutschland bekannt.

An Wellen aller vier redundanter Pumpen des Zwischenkühlkreises wurden nicht konforme Kontermuttern entdeckt. Ein Versagen der Pumpen konnte nicht ausgeschlossen werden. Angaben über die Ursachen sind der Ereignisbeschreibung nicht zu entnehmen.

Eine Verwendung falscher Teile an mehreren redundanten Komponenten ist auch aus Deutschland bekannt.

Während Prüfungen wurden mit vier von sechs unzulässig viele gesicherte Nebenkühlwasserpumpen freigeschaltet. Ursache waren Fehler in der Freischaltungsplanung und die unzureichende Abstimmung des Wartenpersonals.

Fehler in der Planung und Durchführung von Freischaltmaßnahmen sind auch aus Deutschland bekannt.

An einer Pumpe trat eine Leckage auf. Die Ursache lag wahrscheinlich in einer nicht vollständig parallelen Ausrichtung der Dichtflächen, die zu einer ungleichmäßigen Abnutzung führte. Dieser Fehler lag auch an einer weiteren Pumpe vor.

Probleme mit der exakten Ausrichtung von Dichtflächen sind auch aus Deutschland bekannt.

In den weiteren Ereignissen, die im Folgenden aufgeführt werden, lassen sich keine weiterreichenden Informationen entnehmen, da die Phänomene nicht oder nicht ausreichend beschrieben sind.

An zwei von vier redundanten Pumpen des Zwischenkühlkreises wurde ein zu niedriger Schmiermittelstand entdeckt, der bei Anforderung zu einem Versagen der Pumpen innerhalb der Mission Time geführt hätte. Eine Ursache ist nicht angegeben.

Bei drei Pumpen des Zwischenkühlkreises trat ein nicht näher beschriebener Schaden auf, der ein Versagen der Pumpen befürchten ließ. Leitungen des Zyklonabscheiders der Sperrwasserversorgung mussten erneuert werden.

Bei zwei redundanten Pumpen des gesicherten Nebenkühlwassers kam es im Abstand von zwei Wochen zu einer Erhöhung der Lagertemperatur, so dass die Pumpen abgeschaltet werden mussten. Die Ursache ist nicht angegeben.

An allen acht Nebenkühlwasserpumpen und Zwischenkühlwasserpumpen mussten Schütze vorbeugend ersetzt werden. Die Ursache ist nicht angegeben.

Zwei von drei redundanten Pumpen versagten durch Überstromabschaltung aus ungeklärter Ursache.

An zwei von vier redundanten Pumpen traten starke Vibrationen auf. Als Ursache wurden Lagerschäden aus ungeklärter Ursache identifiziert.

Ein weiteres Ereignis wurde als GVA von Pumpen übermittelt; ihm liegt aber ein systematischer Ausfall von Rückschlagklappen zugrunde. Deshalb wird es in Abschnitt 6.11 diskutiert.

6.7 Komponentenart Leistungsschalter

Die Datensammlung der Komponentenart Leistungsschalter umfasst diejenigen sicherheitstechnisch wichtigen Leistungsschalter, die nicht innerhalb der Komponentengrenzen aktiver Komponenten wie Pumpen, Lüfter oder Dieselaggregaten sind. Neben den Schaltern zur Ausführung der Reaktorschnellabschaltung handelt es sich um Kuppelschalter zwischen verschiedenen Schienen. Für die Auswertung wurden zwei neue ausländische ICDE-Ereignisse analysiert.

Beiden Ereignissen, die verschiedene Komponentengruppen derselben Anlage betrafen, lag ein identischer, langsam ablaufender Schädigungsmechanismus zugrunde, der bei Wiederkehrenden Prüfungen entdeckt wurde. Bei einem Ereignis wurde eine Erhöhung des Kontaktwiderstandes von Hilfsschützen an zwei von acht Leistungsschaltern, bei dem anderen Ereignis an zwei von vier Hilfsschützen beobachtet. Zur Behebung wurden die Schalter umgerüstet mit Hilfsschützen eines neuen Designs.

Die Erhöhung des Widerstandes von Kontakten durch Alterung ist auch aus der deutschen Betriebserfahrung bekannt.

6.8 Komponentenart Ventilatoren

Ein neues ausländisches ICDE-Ereignis betraf die Komponentenart Ventilatoren.

Bei dem Ereignis kam es zum Ausfall von beiden Redundanten von Zuluftventilatoren, weil sich aufgrund spezieller Wetterbedingungen (niedrige Temperatur und hohe Luftfeuchtigkeit) eine dicke Eisschicht an den Jalousien der Lufteinlassöffnungen bildete, die zu einer völligen Verstopfung führte.

Ein systematischer Ausfall von Zuluftsträngen aufgrund von Eisbildung ist aus deutschen Anlagen nicht bekannt. Jedoch ist dieses Phänomen im Rahmen der RSK (496. Sitzung der RSK am 06.09.2017) bereits diskutiert worden.

6.9 Komponentenart Motorbetätigte Armaturen (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 sowie die
- Absperrventile vor den Druckhalterabblaseventilen.

Den Ventilen sind die jeweiligen elektro- und leittechnischen Einrichtungen zugeordnet, die alleinig dem Betrieb der jeweiligen Komponenten dienen, wie z. B. die Antriebssteuerung und der Leistungsschalter.

Seit der letzten Auswertung wurden neun neue ausländische ICDE-Ereignisse zu der Datenbank hinzugefügt.

Bei keinem der Ereignisse betraf der GVA das Betriebsmittel „Ventil“; vielmehr lagen die Ursachen bei dem elektrischen Anschluss, der Einstellung von Drehmoment- und Wegendschaltern sowie in einem Fall bei der auslegungsüberschreitenden Beanspruchung durch einen Instandhaltungsfehler.

Bei drei Ereignissen waren Probleme mit elektrischen Kontakten ursächlich:

In einem Ereignis wurde eine erhöhte Ausfallwahrscheinlichkeit von Schützen beobachtet, die teilweise zum Ausfall von Ventilen führten. Als vorbeugende Maßnahme wurden die Schütze erneuert.

Erhöhte Ausfallwahrscheinlichkeiten von Schützen sind auch aus Deutschland bekannt.

Zwei Ereignisse wurden durch Erneuerungen verursacht. Hier wurden jeweils Schütze nicht korrekt beschaltet:

In einem dieser Ereignisse öffneten Ventile, die normalerweise in halb geöffneter Position sind, auf Anforderung nicht vollständig. Ursache waren Fehlverkabelungen von Schützen, die bei einer Modernisierung aufgetreten waren. Für alle Armaturen war ein einheitlicher Schaltplan statt individuell projektierter Schaltpläne verwendet worden. Es war nicht berücksichtigt worden, dass diejenigen Armaturen, die normalerweise in halb geöffneter Position sind, eine abweichende Beschaltung benötigen. Nach der Implementation der Änderungen war kein Test in Bezug auf das vollständige Öffnen durchgeführt worden.

Im anderen Ereignis wurden bei einer Prüfung Fehlverkabelungen mehrerer Armaturen festgestellt. Die Fehler entstanden bei der Durchführung einer Modernisierung. Nachdem auch mehrere weitere Fehlverkabelungen entdeckt worden waren, wurden sämtliche Versorgungen sicherheitsrelevanter Verbraucher, die modernisiert worden waren, neu hergestellt.

Fehlverkabelungen sind aus der deutschen Betriebserfahrung bekannt.

Vier Ereignisse hatten falsch eingestellte Schalter als Ursache:

Bei einem der Ereignisse kam, obwohl die Armatur geschlossen war, die „geschlossen“-Meldung nicht, da der Wegendschalter falsch eingestellt war. Eine technische Verbesserung der Konstruktion wird untersucht.

Bei den drei weiteren Ereignissen betraf die Fehleinstellung die Drehmomentabsteuerung:

Im ersten Ereignis war der Abschaltwert zu niedrig eingestellt. Die Ursache war, dass die Drehmomentabsteuerungen auf einen Wert +/- 5 % des Nominalwertes eingestellt wurden. Durch verschiedene Betriebsbedingungen, wie wechselnde Temperaturen, Abnutzung und andere Einflüsse, kann sich das erforderliche Drehmoment so verändern, dass die Absteuerung zu früh erfolgt. Als Vorkehrung wurde die zulässige Einstelltoleranz dahingehend verändert, dass keine Einstellungstoleranz nach unten mehr zulässig ist.

In den zwei weiteren Ereignissen wurden Drehmomentabsteuerungen ebenfalls zu niedrig eingestellt.

Systematische Probleme mit der Einstellung von Drehmoment- und Wegendschaltern sind aus der deutschen Betriebserfahrung wohlbekannt.

In einem Ereignis kam es zu einer Schutzabschaltung des Stellantriebes wegen Überhitzung, dies führte zu einem Versagen der Armatur in halb geöffneter Stellung. Die Ursache war ein ununterbrochenes Auf- und Zufahren. Dieses wurde verursacht durch oszillierende Durchflussmessungen, die auf eine unzureichende Entlüftung des Systems zurückzuführen waren. Ein GVA der Armaturen wäre zu befürchten gewesen, wenn in mehreren Redundanten eine fehlerhafte Entlüftung vorgelegen hätte.

Der Ausfall von Antrieben durch Überhitzung aufgrund auslegungsüberschreitender, andauernder Betätigung ist bekannt. Ebenso sind systematische Messabweichungen durch Luftansammlungen bekannt. Der hier vorliegende spezielle Mechanismus, ein ständiges Verfahren einer Armatur durch oszillierende Durchflussmessungen, die durch unzureichende Entlüftung bedingt waren, ist jedoch so noch nicht beobachtet worden.

Bei einem Ereignis war die leittechnische Ansteuerung defekt. In mehreren Redundanzen ließen sich die entsprechenden Schieber nur nach mehrmaligen Versuchen fahren. Eine Oxidation von Kontakten der zugehörigen Leittechnikmodule wurde als Ursache vermutet.

Die Oxidation von elektrischen Kontakten ist ein auch aus Deutschland bekannter Fehlermechanismus.

Unter den Ereignissen dieser Komponentenart sind die systematischen Fehler hervorzuheben, die durch Modernisierungen verursacht wurden. In einem Fall war die Ausführung fehlerhaft, in einem anderen die Planung. Hier wurden zur Korrektur jeweils die Arbeiten neu ausgeführt bzw. neu geplant und ausgeführt.

6.10 Komponentenart Notstromdiesel

Die Komponentenart Notstromdiesel umfasst das Notstromdieselaggregat mit dem zugehörigen Notstromgenerator und Generatorschalter sowie die Leittechnik zur Steuerung der Komponente. Es wurden seit der letzten Auswertung 47 neue ausländische Ereignisse zu der Datenbank hinzugefügt. Die Ausfallmechanismen wurden ausgewertet und nach der unten dargestellten Tab. 6.3 in Kategorien nach Gemeinsamkeiten mehrerer Ereignisse, wie Ursachen und Auswirkungen, gruppiert.

Tab. 6.3 Kategorisierung der identifizierten Fehlermechanismen an Notstromdieselaggregaten

Ausfallkategorie	Ereignisanzahl
Auslegungsfehler - resultieren in Vibrationen, die zu Schäden führen	8 6
Schäden durch Vibrationen - davon aufgrund eines Auslegungsfehlers - davon bei technischen Änderungen	7 6 2
Fehler beim Betrieb	2
Fehler bei der Instandhaltung - davon aufgrund unzureichender Dokumentation	5 1
Alterung	5
Leckagen	7

Im Folgenden sind die GVA-Phänomene kurz dargestellt und diskutiert. Hierbei sind, wie in den folgenden Abschnitten, ggf. mehrere ähnliche Ereignisse zusammen bewertet.

Bei einem Ereignis brach durch Vibrationen eine Befestigung einer Kühlwasserleitung. Die Kühlwasserleitung und ihre Befestigung wurden modifiziert.

Nach Entfernen einer Rohrhalterung wurden in einem weiteren Ereignis starke Vibrationen der Rohrleitung beobachtet. Der Modifikation war vom Hersteller zugestimmt worden. Der Ursprungszustand wurde wiederhergestellt.

Materialermüdung durch Vibrationen führten zu Rissen an Kraftstoffleitungen, die Kraftstoffleckagen verursachten. Es traten mehrere Leckagen an zwei Dieseln auf. Ursache war eine hohe Belastung der Leitungen an der Stelle, wo sie in einen Dichtungskonus führen.

Ein Diesel fiel wegen zu hoher Kühlwassertemperatur aus. Es stellte sich heraus, dass die Messung fehlerhaft war. Der Temperatursensor war durch Vibrationen geschädigt worden. Dies wurde durch eine ungünstige Konstruktion verursacht: Der Sensor hatte in seiner Befestigung mehrere Millimeter Spiel. Diese ungünstige Konstruktion war bei allen redundanten Dieseln vorhanden.

In Dieseln in mehreren Blöcken waren Signalkabel des Überdrehzahlschutzes lose. Es war zu befürchten, dass sie sich bei längerer Betriebsdauer der Diesel durch Vibrationen lösen könnten und einen Ausfall der Diesel verursachen könnten.

Kühlwasserleitungen für alle vier Diesel wurden erneuert. Wegen unzureichender Dokumentation der ursprünglichen Ausführung wurde eine neue Auslegung entwickelt und an allen vier Dieseln implementiert. Nach nur einem Jahr traten Schädigungen durch schwingungsbedingte Ermüdung auf, die zu Leckagen und der Unverfügbarkeit eines Diesels führten. Alle redundanten Diesel wurden modifiziert; hierbei wurden als Vorkehrung gegen GVA zwei verschiedene Auslegungen gewählt. Als mittelbare Ursache wurden Defizite im Auslegungsprozess identifiziert.

Auch aus der deutschen Betriebserfahrung sind Schäden aufgrund von Vibrationen, insbesondere auch durch ungünstige Auslegung, wohlbekannt.

An einer Kraftstoffleitung trat durch einen Abriss an der Lötverbindung zwischen Leitungssegmenten aus Kohlenstoffstahl und Leitungssegmenten aus Kupfer eine Leckage auf. Solche Risse waren schon zuvor beobachtet worden. Diese ungünstige Konstruktion, die eine Rissbildung bei Vibrationen begünstigt, war bei allen redundanten Dieseln vorhanden. Als Vorkehrung gegen Wiederholung wurde ein Austausch der Leitungen gegen Leitungen aus Kohlenstoffstahl geplant.

Aus deutschen Anlagen sind bisher keine entsprechenden Probleme an Dieseln aufgetreten. Typischerweise sind entsprechende Leitungen aus Stahl ausgeführt.

Zwei Diesel fielen wegen Ausfall von Dioden im Erreger aus. Eine erhöhte Ausfallrate dieser Dioden war zuvor schon beobachtet worden.

GVA von Dioden sind auch aus Deutschland bekannt.

In zwei redundanten Dieseln wurde eine unzulässig hohe Menge Dieselkraftsoff im Schmieröl festgestellt, so dass von einem Ausfall bei längerem Betrieb auszugehen war. Diese wurde durch eine interne Leckage im Rückschlagventil der Kraftstoffrücklaufleitung auf Grund einer defekten bzw. fehlenden Dichtung verursacht.

Bei einem Ereignis kam es zu einer Leckage an einer Dichtung der Kühlwasserpumpe. Es war zu befürchten, dass das austretende Wasser zu Schäden am Diesel führt. Ursache war die Nichtdurchführung der vom Hersteller empfohlenen Überholungen der Kühlwasserpumpen aller vier redundanter Diesel.

In einem Ereignis trat ein Startversagen eines Diesels durch eine interne Startluftleckage aufgrund einer zerstörten Gummidichtung auf. Auch in den redundanten Dieselaggregaten wurden geschädigte Dichtungen gefunden. Als Ursache wurde Abnutzung und der Kontakt mit Öl identifiziert.

An der Kühlwasserversorgung zweier Diesel trat Korrosion auf.

Bei zwei Ereignissen traten Leckagen an der Kühlwasserversorgung zweier Diesel auf.

An zwei redundanten Dieseln traten Ölleckagen an jeweils einer Zylinderbaugruppe auf.

Interne und externe Leckagen aus verschiedenen Ursachen sind auch aus Deutschland bekannt. Diese betrafen Schmieröl, Kraftstoff, Startluft, Kühlwasser und Abgase.

Als Vorkehrung gegen Überspannung durch Blitzschlag durch ein aufziehendes Unwetter sollten in mehreren Blöcken einer Anlage jeweils eine Notstromschiene vom Netz getrennt und durch einen Notstromdiesel versorgt werden. Hierzu sollte zunächst der Diesel im Netzparallelbetrieb betrieben werden. In zwei Blöcken kam es dabei zu einem Abschalten der Diesel durch Rückleistung, da jeweils die Leistung der Diesel manuell reduziert wurde. In einem Fall wurde eine falsche Anzeige abgelesen, im anderen Fall legt der Verlauf eine Unkenntnis des Bedieners über die Vorgehensweise und die technischen Hintergründe des Netzparallelbetriebs nahe. Dies führte zu einer Unverfügbarkeit der Diesel. Das gleichzeitige mehrfache Auftreten ähnlicher Fehlhandlungen in mehreren Blöcken einer Anlage lässt als mittelbare Ursache eine nicht ausreichende Fachkunde und Defizite in den Prozeduren wahrscheinlich erscheinen.

Bei einem Ereignis kam es zu erhöhten Lagertemperaturen im Generator. Ursache war ein falsches Schmieröl. Statt dem für den Generator vorgesehenen Öl war ein anderes bei der Instandhaltung der Dieselaggregate verwendetes Öl nachgefüllt worden. Zur menschlichen Fehlhandlung trug bei, dass die Instandhaltungsanweisung die Teilenummer des zu verwendenden Öls nicht enthielt.

Die Verwendung eines falschen Schmiermittels ist aus der deutschen Betriebserfahrung bekannt.

Zwei redundante Diesel waren unverfügbar durch Fehleinstellungen von Spannung bzw. Frequenz.

Menschliche Fehlhandlungen, wie sie den letztgenannten Ereignissen zugrunde liegen, – insbesondere durch Schulungsdefizite und Defizite in der Instandhaltungsdokumentation – sind auch aus Deutschland bekannt.

In einem weiteren Ereignis kam es kurz hintereinander zu Ausfällen von drei von vier redundanten Dieseln. Diese Ausfälle hatten unterschiedliche unmittelbare Ursachen (Ausfall des Spannungsreglers, Verstopfung des Startluftventils durch Fremdstoffe, lose Druckluftleitung am Startluftventil). Da allerdings drei unabhängige Ausfälle in kurzer Zeit sehr unwahrscheinlich wären, ist eine tieferliegende systematische Ursache wie unzureichende Qualität der Instandhaltungsarbeiten zu vermuten.

In einem Ereignis war die Kühlwasserversorgung für zwei von vier redundanten Dieseln unverfügbar, da Armaturen geschlossen waren. Ursache der Fehlbedienung waren falsche Kennzeichnungen.

Falsche Kennzeichnungen von Komponenten bzw. Betriebsmitteln sind auch aus der deutschen Betriebserfahrung bekannt.

Zwei von drei Diesel starteten wegen einer defekten Leittechnikbaugruppe nicht automatisch. Ein gleicher Defekt war bei einem der Diesel schon zuvor aufgetreten.

Auch in der deutschen Betriebserfahrung wurde ein Startversagen von Dieseln aufgrund des Ausfalls von Leittechnikbaugruppen schon beobachtet.

Die Spannungsregelung eines Diesels funktionierte nicht, da ein Bolzen gebrochen war, der das Getriebe des Drehzahlreglers mit der Motorwelle verband. Der Bruch war vermutlich wegen Schwergängigkeit des Getriebes durch Alterung des Schmiermittels verursacht worden. Das Getriebe war nicht von der vorbeugenden Instandhaltung erfasst.

Schwergängigkeit durch Alterung von Schmiermitteln ist auch aus Deutschland bekannt.

In zwei Blöcken hatte sich die Innenbeschichtung der jeweiligen Kühlwasserbehälter zweier redundanter Diesel durch Oxidation teilweise gelöst und Blasen gebildet. Es war zu befürchten, dass sich Teile der Beschichtung vollständig ablösen und die Kühlmittelversorgung der Diesel blockieren.

Die Ablösung von Innenbeschichtungen ist ein auch aus Deutschland bekanntes GVA-Phänomen.

Beim Test eines Diesels trat eine starke Rauchentwicklung an einer elastischen Kupplung auf. Das Material der Kupplung, der Polyurethan-Elastomer PUR, ist nur für einen Temperaturbereich von -40 °C bis +80 °C geeignet. Aufgrund der dynamischen Belastung erhöhte sich die Temperatur darüber hinaus, was zur Materialzerstörung durch Oxidation führte. Dasselbe Material wurde in den elastischen Kupplungen des redundanten Diesels verwendet.

Auch aus der deutschen Betriebserfahrung sind Diesel-GVA aufgrund eines Auslegungsfehlers der elastischen Kupplungen bekannt mit ähnlichen Auswirkungen (Zerstörung des Gummi-Elastomers). Der hier beschriebene konkrete Mechanismus (Materialzersetzung durch Oxidation aufgrund von Überhitzung durch dynamische Belastung) ist jedoch noch nicht beobachtet worden.

Zwei Diesel wurden unverfügbar aufgrund des Ausfalls der gemeinsamen Startluftversorgung.

In Deutschland sind die verschiedenen Redundanten getrennt, so dass ein solcher GVA nicht zu befürchten ist.

Bei zwei weiteren Ereignissen war keine Ursache zu ermitteln:

In zwei Anlagen waren jeweils bei zwei redundanten Dieseln die Befestigungsbolzen der Kühler der Turbolader lose bzw. gebrochen. Die Ursache ist nicht angegeben.

In einem Ereignis fielen Drehzahlregler zweier redundanter Diesel aus. Die Ursache konnte vom Betreiber nicht geklärt werden.

6.11 Komponentenart Rückschlagarmaturen

Drei neue ausländische ICDE-Ereignisse wurden übermittelt und bewertet.

Bei Ereignissen in zwei Blöcken einer Anlage wurden fehlende Teile an allen drei redundanten Rückschlagklappen gefunden. Deshalb war zu befürchten, dass diese im Anforderungsfall nicht oder nicht dicht schließen würden, d. h. eine interne Leckage auftreten würde. Der Fehler lag wahrscheinlich seit der Errichtung vor. Im Rahmen von Reinigungsarbeiten bei der Errichtung waren diese Teile entfernt, aber vermutlich nicht wieder eingebaut worden. Die Klappen wurden weder im Rahmen der Inbetriebsetzung noch danach in Bezug auf die betroffenen Teile inspiziert oder anforderungsgerecht geprüft. Neben den Klappen, deren Datensätze im Rahmen des ICDE-Projektes übermittelt wurden, waren auch weitere Klappen vom selben Fehler betroffen.

Fehlende Teile und interne Leckagen an Rückschlagklappen sind auch aus Deutschland bekannt.

Ebenfalls sind aus Deutschland Fälle bekannt, bei dem ein aus der Errichtung stammender Fehler über lange Zeiten unerkannt vorhanden war, da keine anforderungsgerechten Prüfungen durchgeführt worden waren.

In einem weiteren Ereignis[4] war es mehrfach zum Ausfall von Pumpen bei der Umschaltung von redundanten Pumpen gekommen. Ursache war das Nichtschließen von Rückschlagklappen, was zu einem Rückfluss führte. Insgesamt traten neun entsprechende Ausfälle auf, zwei davon nach einer grundlegenden Überholung aller redundanten Klappen. Nach Angaben des Betreibers ist unklar, warum in zwei anderen Blöcken derselben Anlage solche Ausfälle nicht auftreten. Als Ursache werden Defizite in der Instandhaltung vermutet.

Da die Instandhaltung in allen Blöcken in gleicher Weise durchgeführt wird, erscheint die Erklärung des Betreibers nicht schlüssig. Aus diesem Ereignis lassen sich keine Schlussfolgerungen für deutsche Anlagen ableiten.

[4] Dieses Ereignis wurde als GVA von Pumpen übermittelt.

Bei einem weiteren Ereignis kam es zu einem unvollständigen Schließen von zwei von acht Rückschlagarmaturen aufgrund von Schwergängigkeit. Die Ursache lag in der Konstruktion, aufgrund derer es schwierig ist, die Stopfbuchse so anzuziehen, dass einerseits die Armatur sich leicht genug schließen kann und andererseits keine Leckage auftritt. Die Armaturen sollen gegen Armaturen einer besseren Konstruktion ausgetauscht werden.

Auch in Deutschland sind entsprechende Fälle mit einer systematischen Fehleinstellung von Stopfbuchsen bekannt.

6.12 Komponentenart Sicherheits- und Entlastungsventile

Die Komponentenart „Sicherheits- und Entlastungsventile“ umfasst Sicherheitsventile, Entlastungsventile und Sicherheits- und Entlastungsventile (S&E-Ventile). Es wurden während der Vorhabenslaufzeit 14 neue ausländische Einträge übermittelt.

In Tab. 6.4 sind Kategorien, denen mehrere Ereignisse zugeordnet werden konnten, dargestellt.

Tab. 6.4 Kategorisierung der identifizierten Fehlermechanismen an Sicherheits- und Entlastungsventilen

Ausfallkategorie	**Ereignisanzahl**
Schäden durch Oxidation	2
Sitzverklebung durch Oxidation	2
Fehlkalibrierung	2
Unzureichende Druckluftversorgung durch Fehler bei Instandhaltungsarbeiten	2

Bei einem Ereignis wurde durch einen Alarm angezeigt, dass die leittechnische Ansteuerung der drei Sicherheitsventile des Druckhalters unzulässigerweise deaktiviert war.

Der Druckhalter hat für deutsche Anlagen keine sicherheitstechnische Bedeutung mehr. Das abstrakte Phänomen, dass es unterlassen wird, Signale zu reaktivieren, ist bekannt.

Bei einem weiteren Ereignis wiesen 4 von 18 federbelasteten Sicherheitsventile der Dampferzeuger einen um 0,1 bis 0,2 bar zu hohen Ansprechdruck auf. Ursache waren Fehleinstellungen.

Auch aus Deutschland sind systematische Einstellungsfehler bekannt.

In zwei Anlagen traten Ablagerungen in Zylinderbohrungen von magnetischen Vorsteuerventilen auf, die zum Schließversagen bzw. potentiell zum Schließversagen von S&E-Ventilen führten. Diese Ablagerungen wurden wegen ihres Cobaltgehaltes mit dem Anker in Verbindung gebracht, da diese als die einzig mögliche Cobaltquelle in Betracht kamen. Die Anker wurden gegen neue ausgetauscht. Trotzdem zeigten sich an einem Ventil nach dem Austausch wieder Ablagerungen. Weiterhin konnte nicht geklärt werden, wieso – bei schon langjährigem Betrieb – Ablagerungen erst bei längerer Betriebszeit und dann an mehreren Ventilen gleichzeitig auftraten. Es werden Abweichungen im Betrieb, in der Instandhaltung oder eine Kombination von beidem vermutet. Der Schadmechanismus trat später nicht wieder auf.

Auch aus Deutschland sind Ablagerungen in Vorsteuerventilen bekannt, die die Funktion beeinflussen – siehe u. a. WLN 2000/14. Dort führten Abweichungen im Herstellungsprozess in Kombination mit langen Stillstandphasen zum Eintrag von Korrosionsprodukten im Bereich der Ventilspindel und somit zur Schwergängigkeit. Ebenfalls traten Ablagerungen aufgrund der Zersetzung von Montagehilfsmitteln (Schmiermitteln) auf – siehe WLN 1996/11.

Bei der Modernisierung von Vorsteuerventilen von S&E-Ventilen kam es zu einem Herstellungsfehler von Bauteilen: Lagerbuchsen wurden mit Chrom beschichtet, anstatt die vorgesehene Nitrid-Plasma-Härtung durchzuführen. Diese Chrombeschichtung oxidierte schnell, was zu einem Festsetzen mehrerer Vorsteuerventile führte. Bei einem Probeeinsatz waren zunächst fünf Vorsteuerventile umgerüstet und ein Jahr lang betrieben worden. Obwohl diese bei der anschließenden Prüfung eine verlängerte Öffnungszeit zeigten, wurden alle weiteren Ventile in gleicher Weise umgerüstet. Die Umrüstungen waren erfolgt, da die ursprüngliche Konstruktion einen relativ hohen Instandhaltungsaufwand mit der Notwendigkeit regelmäßiger Überholungen beim Hersteller verursacht hatte.

An den gleichen Komponenten im anderen Block derselben Anlage kam es zu einem ähnlichen Ereignis. Hier wiesen alle Vorsteuerventile Schädigungen auf und zwei versagten. Ursache war neben dem oben bereits diskutierten Korrosionsprozess aufgrund eines Herstellungsfehlers ein zu geringer Abstand zwischen Bauteilen. In diesem Block waren sämtliche Vorsteuerventile gleichzeitig modernisiert worden, obwohl die ursprüngliche Planung eine Modifikation von zunächst nur fünf Ventilen vorgesehen hatte. Es konnte nicht geklärt werden, warum von der ursprünglichen Planung abgewichen wurde.

Auch aus Deutschland sind ähnliche Herstellungsfehler, bei denen von den Herstellungsspezifikationen abgewichen wurde und die zu unerwünschten Bauteileigenschaften führten, bekannt. Als Folge wurden entlang der Herstellungskette die Qualitätssicherungsmaßnahmen verstärkt, was sich in entsprechenden Anforderungen u. a. im KTA-Regelwerk wiederfindet – übergeordnet in KTA 1401 sowie detaillierter in den komponenten- bzw. bauteilspezifischen KTA-Regeln. Weiterhin wurden die Auswirkungen von Abweichungen beim Herstellungsprozess von Vorsteuerventilen von Sicherheitsventilen in WLN 2000/14 diskutiert.

In Deutschland ist jedoch bisher nicht aufgetreten, dass trotz Auffälligkeiten bei einem Probeeinsatz keine Ursachenklärung erfolgte, sondern die geplante Umrüstung aller verbleibenden gleichartigen redundanten Einrichtungen unverändert durchgeführt wurde bzw. von einer zuvor geplanten gestaffelten Umrüstung ohne nachvollziehbaren Grund abgewichen wurde.

In einem Ereignis traten bei mehreren Ventilen Risse und Abplatzungen der Chrombeschichtung im Kontrollzylinder sowie Oxidation und Risse im Hauptzylinder auf. Eines der betroffenen Ventile zeigte eine erhöhte Öffnungszeit. Daraufhin wurden betroffene Bauteile ersetzt bzw. die Chrombeschichtung entfernt.

Auch aus Deutschland sind Korrosionsprobleme mit Chrombeschichtungen bekannt.

Bei drei Ereignissen kam es zu einer verlängerten Öffnungszeit von mehreren S&E-Ventilen. Als Grund wurde interne Kondensation aufgrund einer ungünstigen Konstruktion angenommen.

Unerwünschte Kondensation als Ausfallursache ist auch aus Deutschland bekannt.

Bei einem Ereignis wurden Verformungen des Armaturengehäuses von fünf Vorsteuerventilen beobachtet. Als Ursache wurden Radiolysegasreaktionen aufgrund des Versagens der Rekombinatoren angenommen. Entsprechend wurden als Vorkehrung die Rekombinatoren getauscht. Das Thema Radiolysegasreaktion, insbesondere Wasserstoffexplosion in SWR-Anlagen ist ein weithin und seit langem bekanntes Thema.

Auch aus der deutschen Betriebserfahrung sind Radiolysegasreaktion bekannt, die zu Verformungen von S&E-Ventilen führten – siehe u. a. WLN 1987/09 und 1987/18. Weitere Radiolysegasreaktionen in anderen Systemen werden u. a. in WLN 2000/07 und 2002/04 behandelt. Mit möglichen Auswirkungen fehlerhafter bzw. ausgefallener Rekombinatoren befasst sich u. a. WLN 1983/09.

Bei zwei Ereignissen versagten jeweils zwei redundante S&E-Ventile, die durch pneumatisch betätigte Vorsteuerventile gesteuert werden. In einem Fall waren die Vorsteuerventile falsch eingestellt. Als Ursache wurde die Verwendung eines falschen Hilfsmittels (Simulationswerkzeug) oder die falsche Anwendung des Hilfsmittels angenommen. Als Vorkehrung gegen Wiederholung wurde die Instandhaltungsanweisung verbessert. Im zweiten Fall waren sowohl die Haupt- als auch die Vorsteuerventile nicht richtig eingestellt.

Fehleinstellungen von Vorsteuerventilen sind auch aus Deutschland bekannt, ebenso die Verwendung falscher Werkzeuge bzw. die falsche Anwendung von Werkzeugen.

Bei einem Ereignis kam es zum Versagen der pneumatischen Offenhaltung zweier S&E-Ventile, da die Absperrventile für die Anhebeluft verschlossen waren. Die Absperrventile waren nach Prüfungen nicht wieder geöffnet worden.

Auch aus Deutschland sind Fälle bekannt, wo es versäumt wurde, nach einer Prüfung den ordnungsgemäßen Zustand wiederherzustellen und Absperrventile geschlossen blieben.

6.13 Komponentenart Wechselrichter

In der Laufzeit des Vorhabens wurden vier neue ausländische ICDE-Ereignisse der Komponentenart „Wechselrichter“ übermittelt.

Beim ersten Ereignis startete ein Wechselrichter nach Reparaturarbeiten nicht mehr. Es stellte sich heraus, dass es zu einem Datenverlust in einem internen Speicher gekommen war, weil dessen Batterien leer waren. Sie hätten zuvor bereits getauscht werden müssen. Derselbe Fehler lag an zwei weiteren redundanten Wechselrichtern vor.

Verlust von Speicherinhalten durch entladene Batterien, die nicht rechtzeitig ersetzt wurden, sind auch aus Deutschland bekannt. Hierzu hat die GRS die Weiterleitungsnachricht WLN 2026/01 verfasst, in die auch Informationen aus dem genannten Ereignis eingeflossen sind.

Beim zweiten Ereignis wurde bei Instandhaltungsarbeiten an einem rotierenden Umformer Schutzsignale für die beiden redundanten Umformer sowie deren Bypassschalter ausgelöst. Die rotierenden Umformer schalteten ab, die Bypassschalter schlossen nicht und die betroffenen Schienen wurden stromlos.

Ursächlich für das Ereignis war, dass die Auswirkungen der Instandhaltungsarbeiten auf andere rotierende Umformer und Bypassschalter redundanter Schienen, d. h. die ausgelösten Schutzsignale und ihre Auswirkungen, bei der Planung nicht berücksichtigt worden waren. Die Schutzsignale hätten vor Arbeitsbeginn deaktiviert werden müssen.

Auch bei deutschen Anlagen ist bei rotierenden Umformern eine solche signaltechnische Abhängigkeit vorhanden, um zu verhindern, dass mehrere Einspeisewege gleichzeitig aktiv sind. Somit ist das Phänomen übertragbar. Ebenfalls sind auch aus Deutschland Fälle bekannt, in denen bei Instandhaltungsarbeiten in einer Redundante die Auswirklungen auf andere Redundanten nicht ausreichend bedacht wurden.

Laut der Ereignisbeschreibungen der zwei weiteren Datensätze wurde in einer Anlage eine erheblich erhöhte Häufigkeit von Ausfällen von Wechselrichtern beobachtet. Unter anderem kam es zu einem Kurzschluss eines Leistungstransistors. Der Betreiber erklärt dies mit einem Erreichen des Endes der Lebensdauer der Wechselrichter sowie hohen Umgebungstemperaturen. Die hohen Temperaturen führten teilweise unmittelbar zu einer Schutzabschaltung der Wechselrichter. Darüber hinaus führten sie gemäß der Ursachenanalysen zu einer beschleunigten Alterung elektronischer Bauteile.

Auch aus der deutschen Betriebserfahrung sind Fälle bekannt, bei denen

- es zu Ausfällen durch ungeeignete Umgebungsbedingungen, insbesondere zu hohen Temperaturen, kam,

- zu hohe Temperaturen zu einer beschleunigten Alterung führten bzw.
- am Ende der Lebensdauer eine erhöhte Ausfallrate auftrat.

6.14 Zusammenfassung der Auswertung

Im Rahmen von AP 2 des Vorhabens wurde die in der aktuellen ICDE-Datenbasis enthaltene internationale Betriebserfahrung mit GVA ausgewertet. Insgesamt wurden bis jetzt 1900 ausländische ICDE-Ereignisse ausgewertet; davon wurden 129 Ereignisse im Rahmen des aktuellen Vorhabens analysiert. Durch diese Auswertungen konnte der Erfahrungsumfang bezüglich GVA und somit auch bezüglich der zugrunde liegenden Fehlermechanismen im Vergleich zur rein deutschen Betriebserfahrung erheblich ausgeweitet werden.

Im Zuge der Auswertungen konnten neue Fehlermechanismen identifiziert und Häufungen von Fehlermechanismen in der ausgewerteten ausländischen Betriebserfahrung beobachtet werden, die in der deutschen Betriebserfahrung allein nicht zu beobachten sind. Sofern die beobachteten Fehlermechanismen auch für deutsche Anlagen relevant sind, wurden sicherheitstechnische Hinweise formuliert, die im Folgenden aufgeführt sind.

6.15 Hinweise

Wie im Abschnitt 6.1 beschrieben, wurde für die gefundenen neuen Fehlermechanismen jeweils unter Experten dahingehend diskutiert, ob der beobachtete Fehlermechanismus eine Weiterleitungsnachricht erforderlich erscheinen lässt oder ob er in Form eines sicherheitstechnischen Hinweises im Rahmen dieses Berichtes aufgegriffen wird. Es wurde dabei kein Fehlermechanismus identifiziert, der eine Weiterleitungsnachricht notwendig gemacht hätte und zu dem noch keine Weiterleitungsnachricht verfasst worden war bzw. in Bearbeitung war. Jedoch ergeben sich aus den Auswertungen folgende Hinweise, die zur Vorbeugung gegen GVA berücksichtigt werden sollten:

1. Technische Änderungen bedingen ein erhöhtes GVA-Potential. Dies umfasst die Modifikation von Komponenten, den Ersatz von Komponenten und die Änderungen von Systemen.

2. Bei Ersatz von Einrichtungen durch solche einer anderen Technologie kann sich ein verändertes Ausfallverhalten ergeben. Insbesondere können sich andere Ausfallarten zeigen, so dass ggf. unerwartete Folge- oder Rückwirkungen auftreten können.

3. LED-Leuchten können eine gegenüber Glimmlampen erhöhte Kurzschlusswahrscheinlichkeit aufweisen.

4. Änderungen der Betriebsweise von Systemen und Komponenten bedingen ebenfalls ein erhöhtes GVA-Potential. Hierdurch können unter anderem latente Fehler, die bisher nicht wirksam geworden waren, zu systematische Ausfällen führen. Insbesondere kann das gleichzeitige Betreiben von Komponenten, die bisher nicht gleichzeitig betrieben wurden, zu unerwarteten Folge- und Wechselwirkungen führen.

5. Werden Kolbenpumpen bei einem niedrigen Gegendruck betrieben, so können Dämpfungseinrichtungen weniger wirksam werden und infolgedessen Druckstöße auftreten.

6. Die Vorteile und Risiken von Änderungen sollten ermittelt, abgewogen und die Überlegungen dokumentiert werden. Insbesondere bei technischen Änderungen betriebsbewährter Einrichtungen sollte der erwartete Nutzen mit möglichen Risiken kritisch abgewogen werden.

7. Wann immer möglich, sollten Änderungen nicht in allen Redundanten gleichzeitig, sondern versetzt ausgeführt werden. Die Betriebserfahrung an den modifizierten Systemen bzw. Einrichtungen sollte kritisch bewertet und eventuelle Abweichungen von dem erwarteten Verhalten und von dem Verhalten der nicht modifizierten Einrichtungen aufgeklärt werden. Wo sinnvoll möglich, sollten schon bei der Planung der Änderungen Kriterien für die Bewertung festgelegt und dokumentiert werden. Hinweisen auf mögliche Probleme sollte nachgegangen werden. Gegebenenfalls sollte die Umrüstung weiterer Redundanten verschoben werden, bis die Analysen abgeschlossen sind.

8. Bei Planänderungen sollten die Risiken erwogen werden. Hierbei sollte insbesondere die Dokumentation der ursprünglichen Planung und der dort diskutierten Risiken berücksichtigt werden. Die Überlegungen zur Planänderung sollten ebenfalls dokumentiert werden.

9. Nach technischen Änderungen sollten alle möglicherweise betroffenen Funktionen geprüft werden.

10. Bei der Auslegung, der Herstellung und der Änderung digitaler softwarebasierter Leittechnik sollte besonderes Augenmerk auf die Verarbeitung von ausgefallenen Eingängen und die Verarbeitung von als ungültig gekennzeichneten Signalen gelegt werden, da hier wegen der typischerweise großen Anzahl von Kombinationen möglicher Signalzustände ein unerwartetes und ggf. unzulässiges Ausfallverhalten entstehen kann. Insbesondere ist zu betrachten, ob statt aktueller, ungültiger Signale zu einem früheren Zeitpunkt gültige Signale fälschlicherweise weiterhin die Ausgangssignale beeinflussen können.

11. Arbeiten an Einrichtungen, aus denen Signale abgeleitet werden, die andere Redundanten beeinflussen können, erfordern eine besondere Vorsicht. Eventuelle Folgen sollten vorab detailliert analysiert und die Überlegungen dokumentiert sowie geeignete Vorkehrungen getroffen werden, z. B. Unterbrechen oder Simulieren von Signalen.

12. Stark belastete Datennetzwerke können den Ausfall („Absturz“) angeschlossener Einrichtungen verursachen. Auf diese Weise kann der Ausfall einzelner Einheiten derart, dass übermäßig viele Daten gesendet werden, zum Ausfall weiterer Einheiten führen. Dieser mögliche Ausfallmechanismus sollte – zusätzlich zu der behinderten Datenübertragung über das Netzwerk – bedacht werden.

13. Eine möglichst starke Trennung von Netzwerken, ggf. unter Verwendung von Firewalls, sollte erwogen werden. Insbesondere sollten Datennetzwerke soweit möglich redundanzweise getrennt werden.

14. Bei speziellen Wetterbedingungen (niedrige Temperatur und hohe Luftfeuchtigkeit) kann es, wenn keine geeigneten Vorkehrungen wie Beheizung vorhanden sind, zu einer Eisbildung an Jalousien von Lufteinlassöffnungen derart kommen, dass die Luftzufuhr vollständig ausfällt.

15. Die Qualität von Arbeiten, insbesondere von Fremdfirmen, kann erhebliche systematische Mängel aufweisen. Arbeitsergebnisse sollten stets umfassend überprüft werden.

16. Die Spezifikationen für Bauteile sollten entlang der Lieferkette klar kommuniziert werden.

17. Es sollte systematisch überprüft werden, ob gelieferte technische Einrichtungen den Spezifikationen entsprechen.

18. Eine gleichzeitige plötzliche Beeinflussung mehrerer redundanter Einrichtungen kann auch durch langsam ablaufende Alterungsvorgänge verursacht werden, wenn diese durch gleichzeitige Vorgänge (z. B. Instandhaltungsvorgänge) wirksam werden.

19. Durch Nachfüllen von Schmiermittel kann gealtertes Schmiermittel mit ungeeigneten Eigenschaften an die zu schmierende Orte gelangen.

Weiterhin wird auf die WLN 2026/01 „Ausfälle/Fehlfunktionen von Baugruppen in mehreren kerntechnischen Anlagen aufgrund nicht funktionsfähiger Pufferbatterien“ hingewiesen.

7 Zusammenfassung und Ausblick zum ICDE-Projekt

Im Rahmen des ICDE-Projekts der OECD/NEA wird seit 30 Jahren auf internationaler Ebene Betriebserfahrung zum Thema gemeinsam verursachte Ausfälle (GVA, englisch Common-cause Failures, 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 internationale Betriebserfahrung erforderlich, um die Thematik abdeckend zu erfassen.

Mit dem abgeschlossenen Vorhaben 4723R01275 „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 aktuelle Informationen über GVA, insbesondere auch für deutsche KKW relevante GVA-Effekte und GVA-Fehlermechanismen und
- Fortschreibung des Standes von Wissenschaft und Technik bezüglich GVA.

Im Rahmen des Vorhabens wurde die GVA-Betriebserfahrung des Zeitraums bis zum 31.12.2023 von insgesamt fünf 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 selbst 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 129 ICDE-Ereignisse, die analysiert und dargestellt wurden. Hierbei wurden auch GVA-Mechanismen gefunden, die noch nicht in der deutschen Betriebserfahrung beobachtet wurden. Insbesondere wurden auch neue GVA-Mechanismen gefunden, die durch die

Änderung des Betriebes von Komponenten bedingt waren und für den Übergang zum Nachbetrieb eine erhöhte Bedeutung haben.

Während der Laufzeit des Vorhabens wurden im Rahmen der halbjährlichen Treffen des ICDE-Lenkungskreises insgesamt vier Workshops durchgeführt. Beteiligt waren jeweils die Mitglieder des Lenkungskreises sowie teilweise weitere Personen z. B. von Aufsichtsbehörden oder Consultants auf Einladung des Lenkungskreises. Im Zuge der Workshops wurden sowohl komponenten- wie auch themenspezifische Auswertungen bezüglich GVA-Phänomene durchgeführt. So wurden

- ein Workshop zum Thema Sicherheitskultur,
- zwei Workshops zum Thema Alterung und
- ein Workshop zum Thema konventionelle (d. h. nicht softwarebasierte) Leittechnik

durchgeführt. Im Vorhabenszeitraum wurden sechs CSNI-Berichte veröffentlicht. Dies sind Berichte zu den Themen:

- GVA von Sicherheits- und Entlastungsventilen,
- GVA durch externe Einwirkungen auf Komponenten,
- GVA motorbetätigter Ventile,
- Latente GVA durch menschliche Fehlhandlungen,
- GVA von Batterien

sowie einen

- Projektbericht über die VIII. Phase des ICDE-Projekts.

Im formalen Qualitätssicherungsprozess befindet sich ein

- Themenbericht zu Erkenntnissen zur Sicherheitskultur durch Analyse von GVA,

während ein

- Projektbericht zur IX. Phase des ICDE-Projekts

zurzeit durch das Management Board erstellt wird.

Darüber hinaus wurde im Rahmen des ICDE-Projekts aktiv an der Fortschreibung des Standes von Wissenschaft und Technik bezüglich GVA auch zu weiteren Themen gearbeitet. Dies umfasst die Analyse von GVA durch Alterung, die Entwicklung einer systematischen Vorgehensweise zur Quantifizierung, d. h. zur Verwendung der ICDE-Daten für die Ermittlung von Zuverlässigkeitskenngrößen für Probabilistischen Sicherheitsanalysen sowie zu GVA konventioneller Leittechnik.

Literaturverzeichnis

/GRS 08a/ Kreuser, A., H. Holtschmidt, J. Stiller: Auswertung von Ereignissen mit gemeinsam verursachten Ausfällen (GVA) aus dem internationalen GVA-Datenaustauschprojekt ICDE, GRS-A-3403, Januar 2008.

/GRS 08b/ Kreuser, A., H. Holtschmidt, J. Stiller: 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/ A. Kreuser, J. Stiller, J. Voelskow: 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., S. Arnold, J. Voelskow: Internationales GVA-Datenaustauschprojekt ICDE, Abschlussbericht Phase 2008-2010, GRS-A-3578, Januar 2011.

/GRS 11b/ Kreuser, A., J. Voelskow: Auswertung von Ereignissen mit gemeinsam verursachten Ausfällen (GVA) aus dem internationalen GVA-Datenaustauschprojekt ICDE, Teil 2, GRS-A-3588, Februar 2011.

/GRS 14a/ Brück, B., A. Kreuser, J. Simon: Internationales GVA-Datenaustauschprojekt ICDE, Abschlussbericht Phase 2011-2014 GRS-A-3748, Juni 2014.

/GRS 14b/ Brück, B., A. Kreuser, J. Simon: Analyse von Ereignissen mit gemeinsam verursachten Ausfällen (GVA) aus dem internationalen GVA-Datenaustauschprojekt ICDE, GRS-340, August 2014.

/GRS 18/ Brück, B., A. Kreuser, D. Voß: Systematische Aufbereitung der weltweiten Betriebserfahrung mit gemeinsam verursachten Ausfällen im Rahmen einer internationalen Expertengruppe, GRS-447, März 2018.

/GRS 20/ Foldenauer, M., M. Homann, A. Kreuser, C. Lambertus: Internationales GVA-Datenaustauschprojekt ICDE 2017 bis 2020 – Systematische Aufbereitung der weltweiten Betriebserfahrung mit gemeinsam verursachten Ausfällen im Rahmen einer internationalen Expertengruppe, GRS-592, November 2020.

/GRS 23a/ Homann, M., A. Kreuser, M. Leberecht, J. Stiller: Forschung zur aktualisierten Bewertung von gemeinsam verursachten Ausfällen – Auswertung der Betriebserfahrung in deutschen Anlagen im Zeitraum 2011 bis 2018, GRS-676, ISBN 978-3-949088-67-4, August 2023.

/GRS 23b/ Lambertus, C., J. Simon, J. Stiller: Internationales GVA-Datenaustauschprojekt ICDE 2020 bis 2023 – Systematische Aufbereitung der weltweiten Betriebserfahrung mit gemeinsam verursachten Ausfällen im Rahmen einer internationalen Expertengruppe, GRS-723, ISBN 978-3-910548-14-5, Oktober 2023.

/ICD 26/ International Common-cause Failure Data Exchange (ICDE): General Coding Guidelines, Issue 5, Mai 2026, https://projectportal.afconsult.com/ProjectPortal/OpenDocumentFilePage.aspx?id=2676

/NEA 99/ Nuclear Energy Agency (NEA): 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 (NEA): 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, Februar 2001.

/NEA 01/ Nuclear Energy Agency (NEA): 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. Juli 2001.

/NEA 02/ Nuclear Energy Agency (NEA): 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, Oktober 2002.

/NEA 03a/ Nuclear Energy Agency (NEA): 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, Mai 2003.

/NEA 03b/ Nuclear Energy Agency (NEA): 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 (NEA): Committee on the Safety of Nuclear Installations, ICDE Project Report: Collection and Analysis of Common-Cause Failures of Switching Devices and Circuit Breakers, NEA/CSNI/R(2008)1, Januar 2008.

/NEA 08b/ Nuclear Energy Agency (NEA): 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, Juni 2008.

/NEA 13a/ Nuclear Energy Agency (NEA): 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, Juni 2013.

/NEA 13b/ Nuclear Energy Agency (NEA): 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, Juni 2013.

/NEA 15a/ Nuclear Energy Agency (NEA): 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 (NEA): 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 (NEA): 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 (NEA): Committee on the Safety of Nuclear Installations, Lessons Learnt from Common-Cause Failure of Emergency Diesel Generators in Nuclear Power Plants, NEA/CSNI/R(2018)5, September 2018.

/NEA 20/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, Collection and Analysis of Common-Cause Failures due to Nuclear Power Plant Modifications – Topical Report of the Nuclear Energy Agency International Common-Cause Failure Data Exchange Project, NEA/CSNI/R(2019)4, März 2020.

/NEA 22a/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Topical Report: Collection and Analysis of Intersystem Common-Cause Failure Events, NEA/CSNI/R(2020)1, Mai 2022.

/NEA 22b/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Topical Report: Collection and Analysis of Multi-Unit Common-Cause Failure Events, NEA/CSNI/R(2019)6, November 2022.

/NEA 22c/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Topical Report: Provision against Common-Cause Failures by Improving Testing, NEA/CSNI/R(2019)5, November 2022.

/NEA 24/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Project Report: Common-Cause Failures of Safety and Relief Valves, NEA/CSNI/R(2020)17, April 2024.

/NEA 25a/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Topical Report Operational Experience on Common-Cause Failures due to External Environmental Factors, NEA/CSNI/R(2020)15, April 2025.

/NEA 25b/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Project Report: Lessons Learnt from Common-Cause Failures of Motor-Operated Valves, NEA/CSNI/R(2021)7, April 2025.

/NEA 25c/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Project Report: Summary of Phase VIII of the International Common-Cause Failure Data Exchange Project, NEA/CSNI/R(2023)9, Juni 2025.

/NEA 25d/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Topical Report: Collection and Analysis of Common-Cause Pre-Initiator Human Failure Events, NEA/CSNI/R(2022)1, November 2025.

/NEA 26/ Nuclear Energy Agency (NEA): Committee on the Safety of Nuclear Installations, ICDE Topical Report: Lessons Learnt from Common-Cause Failures of Batteries, NEA/CSNI/R(2023)8, April 2026.

/STI 24/ Stiller, J., H. Chatri, G. Johanson, J. Wood: The International Common Cause Failure Data Exchange (ICDE) Project – Recent Insights, Proceedings of the 17th International Probabilistic Safety Assessment and Management Conference & Asian Symposium on Risk Assessment and Management (PSAM17&ASRAM2024), Sendai, Japan, Oktober 2024, https://www.iapsam.org/PSAM17/program/Papers/PSAM17&ASRAM2024-1014.pdf

Tabellenverzeichnis

Tab. 4.1 Umfang der ICDE-Datenbank 19

Tab. 4.2 Übersicht ICDE-Workshops 23

Tab. 5.1 Stand der ICDE-Auswertung der dt. Betriebserfahrung 28

Tab. 5.2 Deutsche ICDE-Betriebserfahrung aufgeschlüsselt nach Komponentenarten 29

Tab. 6.1 Vergleich bereits ausgewerteter und neuer, bisher nicht ausgewerteter ausländischer GVA-Ereignisse 32

Tab. 6.2 Kategorisierung der identifizierten Fehlermechanismen an Kreiselpumpen 38

Tab. 6.3 Kategorisierung der identifizierten Fehlermechanismen an Notstromdieselaggregaten 48

Tab. 6.4 Kategorisierung der identifizierten Fehlermechanismen an Sicherheits- und Entlastungsventilen 54

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-911727-41-9