Erforschung eines Ansatzes zur Systemvalidierung der sicherheitstechnischen Funktion von softwarebasierten Kransteuerungen

GRS - 560

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Erforschung eines Ansatzes zur Systemvalidierung der sicherheitstechnischen Funktion von softwarebasierten Kransteuerungen

Moritz Leberecht
Ewgenij Piljugin
Christian Müller
Felix Gärner
Dagmar Sommer

März 2020

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Kennzeichen 4717R01361 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

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

GRS - 560
ISBN 978-3-947685-45-5

Deskriptoren

Betriebserfahrung, Fehlerbaumanalyse, FMEA, Hebezeuge, Krananlagen, SimuLink

Kurzfassung

Ziel des Vorhabens 4717R01361 „Erforschung eines Ansatzes zur Systemvalidierung der sicherheitstechnischen Funktion von softwarebasierten Kransteuerungen“ war es, eine Methode zu entwickeln, die es ermöglicht die korrekte Umsetzung der Sicherheitsfunktionen im Steuerungssystem eines Kranes zu validieren.

In einem ersten Schritt wurde das für die Auslegung der Steuerung von Hebezeugen in Kernkraftwerken anzuwendende Regelwerk zusammengestellt. Bei den zentralen Regelwerken handelt es sich um die KTA-Regeln 3902 und 3903, wobei insbesondere KTA 3902 konkrete Anforderungen an die Ausführung von Schutzfunktionen stellt. Einzelnen Schutzfunktionen werden dort Performance Level zugewiesen, wie sie in DIN ISO 13849-1 definiert werden. DIN ISO 13849-1 enthält Anweisungen zur Berechnung der Performance Level abhängig von Zuverlässigkeitskenngrößen und dem Konzept der Steuerung. Alternativ können Safety Integrity Level nach DIN EN 61508 verwendet werden. Vorgaben zur Auslegung der elektrischen Schutzeinrichtungen mit Fokus auf die deterministischen, elektrotechnischen Parameter finden sich in DIN EN 60204-32.

Die typischen Hebezeuge in deutschen Kernkraftwerken, an die erhöhte oder zusätzliche Anforderungen im Sinne der KTA 3902 gestellt werden, wurden ermittelt. Für erhöhte Anforderungen sind dies die Reaktorgebäudekrane, die Halbportalkrane im Außenbereich von Druckwasserreaktoren und in einigen Fällen die Krane im Zwischenlager. Die Anzahl der Hebezeuge mit zusätzlichen Anforderungen im Sinne der KTA 3902 ist größer und im Einzelnen anlagenabhängig. Für die Brennelementlademaschinen werden in der KTA 3902 eigene Anforderungen spezifiziert. Die Reaktorgebäudekrane, die Brennelementlademaschinen, die Zwischenlagerkrane und die Hebezeuge, die in der Behandlung radioaktiver Abfälle eingesetzt werden, sind als rückbaurelevant einzustufen. Für die übrigen Hebezeuge ist dies abhängig vom anlagenspezifischen Rückbaukonzept.

Zur Auswertung der spezifischen Betriebserfahrung von Kranen wurden deutsche und internationale Ereignisse aus Kernkraftwerken untersucht. Für den Auswertezeitraum wurden insgesamt 135 Ereignisse mit Fehlfunktionen bzw. Fehlern an Hebezeugen gefunden. Diese Ereignisse wurden hinsichtlich ihrer Fehlerfolge, der fehlerverursachenden Einrichtung, der Fehlerart und der Frage, ob die Steuerung bei dem Fehler eine Rolle spielte, kategorisiert und gruppiert. Beobachtete Fehlerfolgen waren Lastabstürze,

Kollisionen mit einem Umgebungselement ungeplante Verbindungen zwischen Hebezeug und Last (Kollisionen oder ungeplante Hebevorgänge), Selbstschädigungen und unwirksame nuklearspezifische Verriegelungen (in Bezug auf Strahlenschutz oder Kritikalitätssicherheit).

Die Fehler, bei denen die Steuerung des Hebezeugs eine Rolle spielte, wurden dann detaillierter ausgewertet. Es zeigte sich, dass Fehler in der Steuerung selten zu Lastabstürzen, aber häufig zu Selbstzerstörungen und Kollisionen mit Umgebungselementen führten. Im Hinblick auf die Fehlerart handelte es sich verhältnismäßig häufig um Auslegungsfehler. Die Fehler ließen sich in vier weitere Untergruppen gliedern: 1. Komponentenausfälle, bei denen einzelne (in wenigen Fällen: mehrere) physische Komponenten ausgefallen waren. 2. Programmierfehler, bei denen die Software der Steuerung Logik- oder Rechenfehler enthielt 3. Parametrierfehler, bei denen Variablen in der Software der Steuerung mit unzulässigen Werten besetzt wurden und 4. Spezifikationsfehler, bei denen Sicherheitsfunktion nicht oder nicht mit der spezifizierten Zuverlässigkeit umgesetzt waren.

Es wurden verschiedene modellbasierte Vorgehensweisen zur Analyse digitaler Kransteuerung entwickelt und erprobt. Die Vorauswahl der Analysemethoden erfolgte auf der Basis der in der GRS bereits gesammelten Erfahrungen auf dem Gebiet der Analyse digitaler Leittechnik in Kernkraftwerken. Anschließend wurde ein vereinfachtes Modell einer Krananlage und der zugehörigen Kransteuerung entwickelt. Die Erprobung von Analysemethoden anhand der modellierten Kransteuerung erfolgte dann in drei Schritten:

- Modellbasierte Fehlerausfallart- und Auswirkungsanalyse (FMEA– Failure Mode and Effects Analysis),
- Fehlerbaummodellierung und -analyse,
- Analyse einer simulierten Kransteuerung (Simulationsanalyse).

Die o. g. eingesetzten Methoden haben erwartungsgemäß ihre Eignung für modellbasierte Analyse potenzieller Ausfälle leittechnischer Komponenten der Steuerung grundsätzlich demonstriert. Die FMEA kann helfen auf der Basis der getroffenen Annahmen die Auswirkungen potenzieller Einzelfehler auf die Funktion der modellierten Kransteuerung und/oder Kandidaten für systematische Ausfälle (Gemeinsam Verursachter Ausfall,

GVA) zu ermitteln. Die Fehlerbaumanalysen lieferten im Wesentlichen die Ausfallkombinationen von SILT-Komponenten, die zum Lastabsturz führen können. Bei der Fehlerbaummodellierung wurden Ergebnisse der modellbasierten FMEA als Basiselemente eingesetzt. Die Quantifizierung erfolgte auf Basis von Schätzungen. Die Sensitivitäts- und Minimalschnittanalysen der im Vorhaben durchgeführten Fehlerbaumanalyse sind für die modell-basierten Analysen besonders wichtig, weil damit auch die Modellunsicherheiten erkannt und reduziert werden können. Die Simulationsanalysen bieten wesentliche Erweiterungen für Analysen dynamischer Abläufe bei Bewegungen der Krananlage und zur Validierung der FMEA und Fehlerbaumanalysen.

Bereits bei der Modellierung der Kransteuerung wurde festgestellt, dass für die Anwendung der Analysemethoden viele Detailinformationen zum Aufbau und zur Funktion sowohl einzelner Komponenten als auch des gesamten Systems der Krananlage erforderlich sind. Hierzu gehören u. a. Angaben zu Betrieb und Prüfung der Krananlage und deren Steuerung, zur Überwachung der Krananlage und Zuverlässigkeitskenndaten vom Hersteller oder aus der Betriebserfahrung.

Für die Bewertung der Wirksamkeit einzelner Funktionen der Kransteuerung ist eine konsistente, umfassende Modellierung der Krananlage, des Bewegungsraums und der zu bewegenden Lasten erforderlich. Eine weitere Verbesserung der Aussagefähigkeit der modellbasierten Fehlerbaum- und Simulationsanalyse kann durch Berücksichtigung der betrieblichen Funktionen der Kransteuerung und der mechanischen Sicherungseinrichtungen bei der Modellierung der Krananlage und -steuerung erreicht werden. Damit können die potenziellen Gefährdungen und ggf. das Schadensausmaß aussagefähig abgeschätzt werden. Bei dem im Vorhaben erreichten Stand der Modellentwicklung der Krananlage ist diese Abschätzung noch nicht möglich.

Abstract

The aim of the project 4717R01361 "System validation of safety functions of software-based crane control systems" was to develop a method for validating the correct implementation of the safety functions of the control system of a crane.

As a first step, the rules and regulations to be applied for the design of the control system for lifting equipment in nuclear power plants were compiled. The central regulations are KTA Safety Standards 3902 and 3903, with KTA 3902 giving the specific requirements on the design of safety functions. For each safety function a performance levels as defined in DIN ISO 13849-1 is assigned. DIN ISO 13849-1 contains instructions for calculating the performance levels depending on reliability parameters and the concept of the control system. Alternatively, Safety Integrity Levels as defined in DIN EN 61508 can be used. Specifications for the design of the electrical safety functions and devices with a focus on the deterministic, electrotechnical parameters can be found in DIN EN 60204-32.

The typical lifting equipment in German nuclear power plants, for which increased or additional requirements in the sense of KTA 3902 are made, were determined. For increased requirements, these are the reactor building cranes, the semi-gantry cranes in the outside area of pressurized water reactors and, in some cases, the cranes in the interim storage. The number of cranes with additional requirements as specified in KTA 3902 is larger and depends on the individual plant. Separate requirements are specified in KTA 3902 for the fuel assembly loading machines. The reactor building cranes, the fuel assembly loading machines, the interim storage cranes and the lifting equipment used in the treatment of radioactive waste shall be classified as relevant for decommissioning. For the other lifting equipment this depends on the plant-specific decommissioning concept.

German and international events from nuclear power plants were assessed in order to evaluate the specific operating experience of cranes. For the evaluation period, a total of 135 events with faults or failures in lifting equipment were found. These events were categorized and grouped according to their consequence, the equipment causing the failure, the type of failure and whether the control system played a role in the failure. Observed failure consequences were load crashes, collisions with surrounding elements, unplanned connections between hoist and load (both collisions and unplanned

lifting operations), self-inflicted damages and ineffective nuclear-specific interlocks (related to radiation protection or criticality safety).

The events where the control system of the lifting equipment played a role were then evaluated in a more detailed manner. It turned out that failures in the control system rarely lead to load crashes, but often to self-inflicted damages and collisions with surrounding elements. Regarding the type of failure, design errors were relatively common. The events could be further divided into four sub-groups: 1. component failures, in which individual (in a few cases: several) physical components failed 2. programming errors, in which the software of the control system contained logical or calculation errors 3. parameterization errors, in which impermissible values were assigned to variables in the software of the control system and 4. specification errors, in which the safety function was not implemented at all or not implemented with the specified reliability.

Various model-based methods for the analysis of digital crane control systems were developed and tested. The pre-selection of the analysis methods was based on the experience already gained at GRS in the field of analyzing digital I&C systems in nuclear power plants. Subsequently, a simplified model of a crane system and the corresponding crane control system was developed. The testing of analysis methods based on the modelled crane control system was then carried out in three steps:

- Model-based Failure Mode and Effects Analysis (FMEA),
- Fault tree modelling and analysis,
- Analysis of a simulated crane control system (simulation analysis).

As expected, the methods given above have fundamentally demonstrated their suitability for model-based analysis of potential failures of I&C components of the control system. Based on the assumptions made, the FMEA can help to determine the effects of potential individual faults on the function of the modelled crane control system and/or candidates for systematic failures (Common Cause Failure, CCF). The fault tree analyses essentially provided the failure combinations of SILT components that can lead to load crashes. For the fault tree modeling, results of the model based FMEA were used as basic elements. The quantification was based on estimates. The sensitivity and minimal cut set analyses of the fault tree analysis carried out in the project are particularly important for the model-based analyses, because they also allow for the identification and reduction of the model uncertainties. The simulation analyses offer essential extensions for analyses of dynamic

processes during crane system movements and for the validation of FMEA and fault tree analyses.

During the modelling of the crane control system it was already determined that a lot of detailed information on the design and function of individual components as well as of the entire crane system is required for the application of the analysis methods. This includes information on the operation and testing of the crane system and its control system, on the monitoring of the crane system and reliability data from the manufacturer or from operating experience.

In order to evaluate the effectiveness of individual functions of the crane control system, a consistent, comprehensive modelling of the crane system, the movement space and the loads to be moved is required. A further improvement of the significance of the model-based fault tree and simulation analysis can be achieved by taking into account the operational functions of the crane control system and the mechanical safety devices when modelling the crane and its control system. This allows the potential hazards and, if necessary, the extent of damage to be estimated in a meaningful way. This assessment is not yet possible given the current state of model of the crane system developed in this project.

Inhaltsverzeichnis

1 Einleitung

In kerntechnischen Anlagen wird eine Vielzahl von Hebezeugen für verschiedenste Zwecke eingesetzt. Ein Versagen dieser Hebezeuge kann eine Einwirkung von Innen zur Folge haben, was zu einer Gefährdung der kerntechnischen Sicherheit zum einen durch den Absturz und die Freisetzung von Kernbrennstoffen oder sonstigen radioaktiven Stoffen und zum anderen durch die Beschädigung von Sicherheitseinrichtungen führen kann. Ein Lastabsturz muss daher bei der Auslegung berücksichtigt oder zuverlässig ausgeschlossen werden. Ein wesentliches Element zum sicheren Betrieb von Hebezeugen ist die Steuerung von diesen, die Fehlbedienungen verhindert, Fehler erkennt und Schutzfunktionen auslöst. Die zuverlässige Funktion der Kransteuerungen, die zunehmend mit softwarebasierter Leittechnik umgesetzt sind, ist daher eine wichtige Voraussetzung für den sicheren Betrieb dieser Hebezeuge. Die deutsche Betriebserfahrung hat jedoch wiederholt Fehlfunktionen in der Steuerung der Brennelement-Lademaschinen und weiterer Hebezeuge in kerntechnischen Anlagen gezeigt, die z. B. auf Programmierungsfehlern oder Auslegungsmängeln in der Steuerung beruhten. In deutschen Kernkraftwerken sind verschiedene Hebezeuge auch noch längerfristig für sicherheitstechnisch relevante Aufgaben erforderlich, z. B. im Rahmen von Beladekampagnen für Transport- und Lagerbehälter. Die Anforderungen an die sichere Auslegung und den sicheren Betrieb von Hebezeugen gelten somit auch für Anlagen in der Nachbetriebs- bzw. Stilllegungsphase. In dem in diesem Bericht dargestellten Forschungsvorhaben sollen daher basierend auf der verfügbaren Betriebserfahrung Methoden zur Systemvalidierung von Kransteuerungen untersucht werden, mit denen die sichere Funktion der Steuerung umfassend geprüft werden kann.

Im Vorhaben wurden zunächst die geltenden Anforderungen des nuklearen und nichtnuklearen Regelwerks im Bereich der Kransteuerungen erfasst. Im Kapitel 2.1 sind diese zusammenfassend dargestellt. In einem nächsten Schritt wurden eine Recherche des derzeitigen Standes der Technik im Bereich der Kransteuerungen durchgeführt und die typischen Einsatzorte in Kernkraftwerken erfasst, an denen Krane für sicherheitstechnisch relevante Transportvorgänge oder in der Nähe von sicherheitstechnischen Einrichtungen genutzt werden. Die Ergebnisse sind in den Kapiteln 2.2 respektive 2.3 zusammengefasst. Die deutsche und internationale Betriebserfahrung zu Hebezeugen in Kernkraftwerken und ausgewählten anderen nukleartechnischen Anlagen wurde systematisch ausgewertet. Relevante Fehlerfolgen, -arten und die jeweiligen fehlerverursachenden Einrichtungen wurden bestimmt. Fehlfunktionen in der Steuerung wurden einer

separaten detaillierteren Untersuchung unterzogen und ihre Modellierbarkeit mit den typischen Methoden der Zuverlässigkeitsanalyse wurde eingeschätzt. Die Ergebnisse dieser Auswertung sind in Kapitel 2.4 dargestellt.

Ein Überblick über verschiedene, potenziell geeignete Methoden zur Zuverlässigkeits- und Sicherheitsanalyse von Kransteuerungen wird in Kapitel 3.1 gegeben. Die als zur Anwendung besonders geeigneten Methoden werden detaillierter beschrieben. In Kapitel 3.2 wird zunächst dargestellt, wie die Methoden aus Kapitel 3.1 für die weitere Analyse kombiniert werden. Außerdem wird das für die Untersuchung verwendete Modell einer Krananlage und der zugehörigen Kransteuerung beschrieben. In Kapitel 3.3 wird das Modell dann unter Verwendung einer Kombination der bisher beschriebenen Methoden analysiert, wobei verschiedene Anforderungs-, Ausfall- und Ereignisszenarien betrachtet werden.

Kapitel 4 fasst die Ergebnisse zusammen und gibt einen Ausblick auf potenzielle Ansätze zur weiteren Verbesserung der erarbeiteten Modelle und Methoden.

2 AP 1: Erfassung von Einsatzbereichen, anzuwendendem Regelwerk, verwendeter Technik und Auswertung der spezifischen Betriebserfahrung

2.1 Regelwerksanforderungen

Das für Hebezeuge und ihre Steuerungssysteme unmittelbar relevante Regelwerk sind die KTA-Regeln KTA 3902 „Auslegung von Hebezeugen in Kernkraftwerken“ /KTA 19a/ und KTA 3903 „KTA 3903 Prüfung und Betrieb von Hebezeugen in Kernkraftwerken“ /KTA 19b/. Die Anforderungen an Steuerungen aus diesen Regeln werden im folgenden Unterkapitel kurz zusammengefasst. Es zeigte sich, dass dabei insbesondere die DIN-Regeln DIN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze“ /DIN 16a/, DIN EN 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ /DIN 11a/ bis /DIN 11f/ und DIN EN 60204-32 „Sicherheit von Maschinen – Teil 32: Anforderungen für Hebezeuge“ /DIN 09/ umfangreich referenziert werden. Diese DIN-Normen werden in einem zweiten Unterkapitel zusammengefasst. Weitere relevante DIN-Normen und die BGV/DGUV-Vorschriften von untergeordneter Relevanz werden in einem dritten Unterkapitel etwas knapper zusammengefasst.

2.1.1 Nukleares Regelwerk: KTA 3902 und 3903

Die beiden für Hebezeuge in Kernkraftwerken relevanten KTA-Regeln sind KTA 3902 und KTA 3903. KTA 3902 befasst sich schwerpunktmäßig mit der Auslegung, KTA 3903 mit Prüfungen und Betrieb von Hebezeugen.

2.1.1.1 KTA 3902 Auslegung von Hebezeugen in Kernkraftwerken

KTA 3902 schreibt zunächst vor, dass die konventionellen Arbeitsschutzvorschriften und die Vorschrift der Träger der gesetzlichen Unfallversicherungen erfüllt werden müssen (Kapitel 3). In Kapitel 4 werden dann abhängig von der sicherheitstechnischen Bedeutung zusätzliche Kategorien eingeführt. Diese sind:

- Aufzüge im Reaktorsicherheitsbehälter (Kapitel 4.1 und Kapitel 5, für das Projekt nicht relevant und daher im Folgenden nicht weiter diskutiert)
- Hebezeuge mit zusätzlichen Anforderungen (Kapitel 4.2 (Definition) und Kapitel 6 (Anforderungen))

- Hebezeuge mit erhöhten Anforderungen (Kapitel 4.3 (Definition) und Kapitel 7 (Anforderungen))
- BE-Wechselanlagen (Kapitel 4.4 (Definition) und Kapitel 8 (Anforderungen))

Bei diesen Kategorien gilt, dass die Anforderungen im Allgemeinen ansteigen (mit einigen Ausnahmen beim Vergleich von KTA 3902 4.3- und 4.4-Hebezeugen).

Hebezeuge mit zusätzlichen Anforderungen sind in Kapitel 4.2 definiert als Hebezeuge, bei deren Versagen…

- … die Gefahr einer Aktivitätsfreisetzung, als deren Folge eine Strahlenexposition von Personen in der Anlage mit einer effektiven Dosis durch innere Exposition über 1 mSv oder durch eine externe Exposition über 5 mSv eintreten kann, zu besorgen ist

oder

- …ein nicht absperrbarer Reaktorkühlmittelverlust oder eine über die Redundanz hinausgehende Beeinträchtigung von Sicherheitseinrichtungen, die notwendig sind, den Reaktor jederzeit abzuschalten, in abgeschaltetem Zustand zu halten oder die Nachwärme abzuführen, zu besorgen ist.

und gleichzeitig keine Gefahren wie bei Hebezeugen mit erhöhten Anforderungen zu besorgen sind.

Hebezeuge mit erhöhten Anforderungen sind in Kapitel 4.3 definiert als Hebezeuge, bei deren Versagen…

- …die Gefahr eines Kritikalitätsunfalls

oder

- die Gefahr einer Aktivitätsfreisetzung, als deren Folge die maximal zulässigen Ableitungen in die Umgebung gemäß Genehmigung überschritten werden können oder die Strahlenexposition in der Umgebung des Kernkraftwerkes für Einzelpersonen der Bevölkerung oberhalb der Grenzwerte der StrlSchV liegen kann, zu besorgen ist.

Für Hebezeuge mit zusätzlichen Anforderungen sind die steuerungsrelevanten Anforderungen in Kapitel 6.5 von KTA 3902 zu finden.

Dort werden Sicherheitsfunktionen vorgeschrieben, die bei unzulässigen Betriebszuständen oder unzulässigen Überschreitungen von Begrenzungen (Wege, Geschwindigkeiten und Lasten), die Antriebe abschalten und die Bremsen einlegen. Die Steuerung wird in eine betriebliche Steuerung und eine Sicherheitssteuerung unterteilt, die voneinander unabhängig zu gestalten sind. Die Sicherheitssteuerung soll die Einhaltung der sicherheitstechnisch wichtigen Grenzwerte überwachen und ggf. das Hebezeug in einen sicheren Zustand überführen. Für Vorgaben zur Ausführung der Steuerung wird auf Anhang E der KTA 3902 verwiesen. Dort wird den Funktionen der Steuerung abhängig von der Einstufung des Hebezeugs in Kapitel 4 ein Performance Level nach DIN EN ISO 13849-1 zugewiesen. Funktionen, die in Performance Level c, d und e eingestuft sind, sind in der Sicherheitssteuerung auszuführen. Bei Verwendung softwarebasierter Sicherheitssteuerungen ist DIN EN 62138 Abschnitt 6 /DIN 10/ einzuhalten. Anstelle der Performance Level können auch die „Safety Integrity Levels“ (SIL) aus DIN EN 61508 verwendet werden, wobei die Anforderungen für SIL 2 als gleichwertig mit den Anforderungen für Performance Level „d“ und die Anforderungen für SIL 3 als gleichwertig mit den Anforderungen für Performance Level „e“ gelten. Sicherheitsfunktionen des Performance Level „d“ sind mindestens in Kategorie 3 und Sicherheitsfunktionen des Performance Level „e“ in Kategorie 4 nach DIN EN ISO 13849-1 auszuführen. Außerdem sind für Sicherheitsfunktionen der Performance Level „c“ bis „e“ die in DIN EN 61513 /DIN 13a/ für Funktionen der Kategorie B enthaltenen Anforderungen einzuhalten. Grundsätzlich sind Maßnahmen vorzusehen, die eine Identifizierung des Versionsstands von Hard- und Software für Funktionen ermöglichen, die in Performance Level „c“ bis „e“ eingestuft sind. Die Prüfbarkeit der gesamten Signalpfade (einschließlich der Sicherheitswegbegrenzer im Vier-Augen-Prinzip) ist sicherzustellen. Auch Fehler in den Prüfeinrichtungen sind bei Funktionen der Performance Level „c“ bis „e“ zu berücksichtigen. Für die Realisierung sind zwangsläufig öffnende im Ruhestromprinzip wirkende Schalter oder sicherheitstechnisch äquivalente Technik einzusetzen.

Verschiedene elektrische Schutz- und Überwachungseinrichtungen werden vorgeschrieben. Hier sollen lediglich diejenigen aufgeführt werden, die nicht in Anhang E nochmals aufgegriffen werden:

- Die Wicklungen für Hubwerksmotoren müssen temperaturüberwacht sein.
- Hubwerkbremsen müssen einzeln und unabhängig angesteuert werden.

- Für elektrisch gesteuerte Lastaufnahmemittel wird eine Stellungsanzeige und eine elektrische Lastfreigabeverriegelung vorgeschrieben.
- Bezüglich der vorzusehenden Sicherheits- und Begrenzungsfunktion wird für Fahrwerke und Hubwerke ein betrieblicher Wegendbegrenzer und ein Sicherheitswegbegrenzer nach Anhang E vorgeschrieben (Ausnahme: Fahrwerke mit mechanischen Fahrwegendbegrenzungen).
- Elektronische Wegmesssysteme für Sicherheitsfunktionen der Performance Level „c“ bis „e“ müssen eine im Normalbetrieb verblockbare Justierfunktion (z. B. durch Schlüsselschalter), redundante Geber oder eine Überwachung zur Erkennung eines mechanisch bedingten Geberausfalls und bei Verwendung von Absolutwertgebern einen schlupffreien Antrieb besitzen.
- Wird der betriebliche Wegbegrenzer erreicht, muss das Hebezeug vor Erreichen des Sicherheitswegbegrenzers zum Stillstand kommen. Es wird eine vorgelagerte Geschwindigkeitsüberwachung gefordert. Ausnahmen gelten für Fahrwerke mit mechanischen Wegendbegrenzungen, die auf Nenngeschwindigkeit ausgelegt sind, und für Fahr- und Hubwerke, die ausreichend Nachlaufweg zwischen Sicherheitswegbegrenzer und mechanischer Wegendbegrenzung besitzen.
- Für die Befehls- und Eingabegeräte wird vorgegeben, dass beim Einschalten des Hebezeugs (auch bei betätigtem Steuerorgan) kein Anlaufen von Antrieben erfolgen darf.
- Bei Antrieben mit Geschwindigkeitsstufen darf die Steuerung der Geschwindigkeit nur von Null über die einzelnen Geschwindigkeitsstufen auf die maximale Geschwindigkeit möglich sein.
- Die Steuerung muss ohne Selbsthaltung und selbstrückstellend sein oder durch einen Freigabetaster im Steuerorgan eine Nullrückstellung elektronisch realisiert sein.
- Die Bewegungsrichtungen müssen eindeutig gekennzeichnet sein.
- Es muss ein „Not-Halt“-Schalter vorhanden sein, der nach DIN EN 60204-32 in Stopp-Kategorie „0“ oder Stopp-Kategorie „1“ ausgeführt ist.
- Bei Transportvorgängen die Gefährdungen nach KTA 3902 Kapitel 4.2 oder 4.3 verursachen können, muss eine Abschalteinrichtung mit ausreichendem Überblick über den jeweiligen Arbeitsbereich, z. B. ein zusätzlicher „Not-Halt“, vorhanden sein.

- Bei Hebezeugen mit mehreren Steuerstellen darf nur eine Stelle gleichzeitig im Eingriff sein.
- Drahtlose Steuerungen müssen den Anforderungen gemäß DIN EN 60204-32 genügen.
- Meldungen (für Betriebszustände und Verriegelungen) sind optisch, Warnungen und Störungen sind optisch und akustisch anzuzeigen. Sie sind prüfbar und quittierbar auszuführen, wobei die optische Anzeige bei weiterem Anstehen des Zustands erhalten bleiben muss (Ruhelicht statt Blinklicht).

Für Hebezeuge mit erhöhten Anforderungen gelten die oben genannten Anforderungen ebenso. Anforderungen bezüglich der Steuerung, die nur für Hebezeuge mit erhöhten Anforderungen gelten, sind in Kapitel 7.5 von KTA 3902 aufgeführt. Wieder werden hier lediglich die Aspekte aufgeführt, die nicht in Anhang E von KTA 3902 noch einmal aufgegriffen werden:

- Das Wiedereinschalten nach dem Ausfall eines Bauteils ist nur mittels Schlüsselschalter vom elektrischen Betriebsraum aus zulässig.
- Eine kontinuierliche Lastanzeige ist an der Steuerstelle vorzusehen und sofern Lastbegrenzungen im Teillastbereich für bestimmte Transporte erforderlich sind, ist ein entsprechender separat einstellbarer Überlastgrenzwert einzurichten.
- Bei Hubwerken mit einfacher Triebwerkskette ist eine Überwachung vorzusehen, die bei Getriebe- oder Wellenbruch die Sicherheitsbremse auslöst.

Für BE-Lademaschinen gelten die Anforderungen an Hebezeuge mit zusätzlichen und erhöhten Anforderungen analog. Zusätzlich werde weitere Anforderungen in Kapitel 8.5 gestellt. Wieder werden lediglich Anforderungen aufgeführt, die nicht in Anhang E von KTA 3902 noch einmal aufgegriffen werden:

- Die Endstellungen „auf“ und „zu“ des Greifers und alle zugehörigen Verriegelungen müssen optisch gemeldet werden. Solange eine der beiden Endstellungen nicht erreicht ist, darf eine Bewegung des Hubwerkes nicht möglich sein. Die Position des Greifers muss immer angezeigt werden.
- Der Netzanschlussschalter der Brennelement-Wechselanlage darf nur eingeschaltet werden können, wenn dieser mit einem Schlüsselschalter o. ä. vom Reaktorleitstand oder gleichwertiger Stelle aus freigegeben worden ist. Zwischen dieser Stelle und

allen Steuerstellen muss entweder unmittelbarer Sprechverkehr möglich sein oder eine notstromversorgte Gegensprechanlage bestehen. Eine Rücknahme der Freigabe darf keine Abschaltung des Netzanschlussschalters auslösen, muss aber nach Abschalten eine erneute Einschaltung verhindern.

- Fahrbewegungen dürfen nur möglich sein, wenn sich der Greifer in einer zulässigen Höhenlage befindet. Zur Begrenzung der Fahrbewegungen auf den sicherheitstechnisch zulässigen Fahrbereich ist neben dem betrieblichen Wegbegrenzer ein von diesem unabhängiger Sicherheitswegbegrenzer vorzusehen.

- Sind händische und motorische Bewegungen von Teilen der Lademaschine möglich, darf der motorische Antrieb nicht eingeschaltet oder einschaltbar sein, solange eine Bewegung von Hand möglich ist.

- Es ist sicherzustellen, dass beim Überfahren des Flutkompensators bei Siedewasserreaktoren und der Dichtmembran bei Druckwasserreaktoren keine Hub- oder Senkbewegungen des Haupthubwerks möglich sind.

- Die elektrische Verriegelung ist so auszuführen, dass der Steuerbefehl zum Abschlagen der Last nur bei gleichzeitiger Freigabe durch zwei voneinander unabhängige Kriterien (z. B. Hubhöhe und Last) ausgeführt werden kann.

Ein zentraler Teil der Vorgaben in KTA 3902 findet sich in der Tabelle E-1 in Anhang E, in der die geforderten Performance Level nach DIN EN ISO 13849-1 für die jeweiligen Funktionen der Steuerung aufgeführt sind, woraus sich schlussendlich Anforderungen an Redundanz, Diversität, Prüfbarkeit und die Zuverlässigkeit der einzelnen Bauteile ergeben. Tabelle 2.1 führt diese Zuweisung im Detail auf.

Tab. 2.1 Zuweisungen von Performance Leveln zu den einzelnen Funktionen eines Hebezeugs nach KTA 3902 Anhang E

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
Allgemein:						
1	Ein-/Ausschalten des Hebezeuges, Wartenfreigabe	6.5.2 (1), 8.5 b)	a	a	a	
2	Not-Halt	6.5.4.1 (5)	d	d	d	Bei drahtlosen Steuerungen: „Stopp“
3	Not-Halt für die Überwachungsperson bei Anwendung des „Vier-Augen-Prinzips“	6.5.4.1 (6)	d	d	-[1)]	Bei drahtlosen Steuerungen: „Stopp“
4	Betriebs-, Stör- und Warnmeldungen	6.5.4.2	a	a	a	
5	Betriebszustandsmeldungen, die solche Zustände signalisieren, die von sicherheitsrelevanten Handlungen ausgelöst werden oder von denen sicherheitsrelevante Handlungen abgeleitet werden	6.5.4.2	b	b	b	z. B. Rückmeldung einer Lastgrenzwertumschaltung
6	Bedienfunktionen und Antriebssteuerung	6.5.4.1	a	a	a	z. B. Steuerfunktionen der Meisterschalter, Betriebsartenschalter, Steuerbefehle für Antriebsregler (z. B. Sollwertsignale)

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
7	Betriebsstunden- oder Lastkollektivzähler, Zähler für den Einfall der Sicherheitsbremse	6.5.2 (5), 7.5 b)	a	a	a	
8	Gegenseitige Verriegelung der Steuerstellen	6.5.4.1 (7)	a	a	a	Not-Halt muss auch an abgeschalteten Steuerstellen wirksam sein (Ausnahme: Stopp-Funktion auf drahtlosen Steuerungen).
9	Drehfeld- und Außenleiterüberwachung	6.5.2 (2)	a	a	a	
10	Überlastschutz für Motoren	6.5.2 (3)	a	a	a	
Hubwerke und Fahrwerke:						
11	Geschwindigkeitsbegrenzung am Fahrbereichs- und Hubwegende	6.5.3 (5)	a	a	a	
12	a) Abschaltung bei Überschreitung der zulässigen Geschwindigkeit am Fahrbereichsende	6.5.3 (5)	c	c	d	
	b) Abschaltung bei Überschreitung der zulässigen Geschwindigkeit am Hubwegende Erste Abschalteinrichtung	6.5.3 (5), 7.5	d	e	e	

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
	Zweite Abschalteinrichtung [3]		-[1]	c	-[1]	
13	Betrieblicher Wegbegrenzer	6.5.3 (1) und (3)	a	a	a	Abschaltung am betrieblich zulässigen Fahr- oder Hubbereichsende
14	Sicherheitswegbegrenzer von Fahrwerken	6.5.3 (1)	c	c	d	
15	Stillstandsüberwachung	6.5.2 (8)	b	b	b	
16	Nullstellungszwang	6.5.4.1 (1)	a	a	a	
17	Richtungsüberwachung beim Anfahren aus dem Stillstand bei umrichterbetriebenen Antrieben	6.5.2 (8)	b	b	b	
18	Verriegelung von Fahr- oder Hubbewegungen	6.5.3 (6)	c	c	-[2]	
19	Verriegelung der Fahr- und Hubbewegung sowie Begrenzung der Fahrbewegung	8.5 a), 8.5 f),8.5 g), 8.5 l)	-[2]	-[2]	d	
Zusätzliche Funktionen für Hubwerke:						
20	Lastanzeige	7.5 g)	-[1]	a	a	
21	Abschaltung bei 110 % der maximalen Betriebslast (Überlastsicherung)	6.5.2 (4)	c	d	d	

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
22	Vorgelagerte variable Überlastsicherung	7.5 h)	-[1)]	b	-[2)]	Lastgrenzwert, der entsprechend der jeweils transportierten Last eingestellt wird. Kategorie „B“ für betriebliche Begrenzungen. Sofern Schutzfunktionen erfüllt werden müssen, sind die an „Überlastabschaltungen bei 110 % der maximalen Betriebslast“ gestellten Anforderungen gemäß lfd. Nr. 21 einzuhalten.
23	Vorgelagerte betriebsartenabhängige Überlastsicherung	8.5 d)	-[2)]	-[2)]	c	Lastgrenzwert, der betriebsartenabhängig aktiviert wird, z. B. in Abhängigkeit von der transportierten Last.
24	Unterlastsicherung, Schlaffseil	8.2.1.3.1 (7)	-[2)]	-[2)]	d	Störmeldung siehe 8.5 e)
25	Einfall der Betriebs- und Zusatzbremse bei sicherheitsrelevanten Antriebsabschaltungen	6.5.1 (1)	d	d	d	
26	Hubwerksabschaltung bei Ausfall eines Bauteils innerhalb einer doppelten Triebwerkskette oder einer Triebwerkskette mit Sicherheitsbremse	7.5 e)	-[2)]	b	b	

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
27	Überwachung der Hilfsmedien von Systemen zur Aufnahme oder zur Dämpfung des Lastumlagerungsstoßes	7.5 f)	-[2)]	b	b	
28	Überwachung des ordnungsgemäßen Aufwickelns des Seiles auf der Trommel	6.5.2 (11)	b	b	b	
29	Außenleiterüberwachung des Hubwerksmotors	7.5 a)	-[1)]	b	b	
30	Abschaltung bei Überschreitung der zulässigen Hub- oder Senkgeschwindigkeit	6.5.1 (1)	c	c	c	
31	Getriebebruchüberwachung mit Ansteuerung der Sicherheitsbremse	7.5 b)				
	Erste Überwachungseinrichtung		-[2)]	e	e	
	Zweite Überwachungseinrichtung [3)]		-[1)]	c[4)]	-[1)]	
32	Bremsenüberwachungen	6.5.2 (6) und 7.5 b)	a	a	a	Stellungsüberwachungen und Bremsbelagsüberwachungen
33	a) Sicherheitswegbegrenzer Richtung Heben	6.5.3, 7.5 d)				

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
	Erste Begrenzungseinrichtung		d	e	e	
	Zweite Begrenzungseinrichtung [3]		-[1]	c	-[1]	
	b) Sicherheitswegbegrenzer Richtung Senken	6.5.3, 6.2.2.3 (3)	c	e	e	
34	Überwachung der korrekten Reihenfolge beim Aus- und Einfahren von Hubwerkskomponenten	8.5 i)	-[2]	-[2]	c	Z. B. durch Überwachung der höhenabhängigen Last am Seil
35	Aufsetzverhinderung	8.5 j)	-[2]	-[2]	a	Ergänzende Funktion, die bereits vor dem Ansprechen der Unterlastabschaltung wirksam werden soll.
Funktionen für elektrisch gesteuerte Lastgreifer:						
36	a) Öffnen des Greifers bei Vorhandensein einer mechanischen Öffnungsverriegelung	6.5.2 (10)	a	c	c	
	b) Öffnen des Greifers bei Fehlen einer mechanischen Öffnungsverriegelung	6.5.2 (10), 8.5 k)	d	Nicht zulässig	e	

Lfd. Nr.	Funktion	Anforderung nach KTA 3902	PL nach DIN EN ISO 13849-1 bei Einstufung nach Abschnitt			Bemerkung
			4.2	4.3	4.4	
37	Stellungs- und Zustandsanzeigen des Lastgreifers	6.5.2 (9)	a	a	a	

1) Die Funktion ist nicht erforderlich, da der Verzicht auf diese Funktion zu keinen unzulässigen sicherheitstechnischen Auswirkungen führt.
2) Die Funktion ist aus technischen Gründen nicht relevant. Zur Erfüllung der Anforderungen kommt eine andere Funktion zur Anwendung.
3) Nur wenn bei Versagen dieser Funktion als Folge eine Überschreitung der Störfallplanungswerte nach § 104 StrlSchV unterstellt werden muss und die Funktion mittels softwarebasierter Systeme ausgeführt wird.
4) Nicht erforderlich bei Hubwerken mit maximaler Betriebslast gleich oder kleiner als 5 t.

2.1.1.2 KTA 3903 Prüfung und Betrieb von Hebezeugen in Kernkraftwerken

KTA 3903 spezifiziert, welche Vorprüfunterlagen einzureichen sind. Die Steuerung des Hebezeugs fällt hierbei unter den Begriff elektrotechnische Funktionen bzw. elektrische Einrichtungen. Nach KTA 3903 5.1.8 sind folgende Dokumente einzureichen:

- Übersichtsschaltpläne
- Stromlaufpläne,
- Dispositionspläne für Schaltschränke, Schalttafeln und Steuergeräte,
- Stücklisten mit Angaben der technischen Daten,
- Datenblätter von Antriebskomponenten, Umrichtern und elektrischen Betriebsmitteln (*)
- Darstellung der Arbeitsweise der Mess-, Regel-, Überwachungs- und Sicherheitseinrichtungen,
- Zusammenstellung der vorgesehenen Maßnahmen zur Erfüllung der Anforderungen nach DIN IEC 61513 Kategorie B (*)
- bei Einsatz von frei programmierbaren Systemen (z. B. speicherprogrammierbaren Steuerungen) (*):
    - Beschreibung aller Verriegelungen und Abläufe der Anlage zur Erstellung des Anwenderprogramms sowie Beschreibung der Konzeption des Anwenderprogramms (z. B. Modularisierungskonzept) entsprechend den Festlegungen in DIN EN ISO 13849-1 Abschnitt 4.6.3,
    - Software-Anforderungsspezifikation nach DIN EN 62138 Abschnitt 6.3.3,
    - Anwenderprogramm (Ausdruck und Datenträger) sowie zugehörige Systemhandbücher,
    - Nachweis der Unabhängigkeit der Sicherheitssteuerung von der betrieblichen Steuerung z. B. mittels Fehlzustandsart- und -auswirkungsanalyse (FMEA) für die Schnittstellen.
- Konfigurations- und Identifikationsdokumentation (KID) der Hard- und Softwarekomponenten (*)

- Prüfanweisungen für die Abnahmeprüfung und für wiederkehrende Prüfungen

Mit (*) gekennzeichnete Punkte müssen nur für Funktionen erfüllt werden, die nach KTA 3902 Anhang E in Performance Level c, d oder e auszuführen sind.

KTA 3903 beschreibt den Umfang der Bauprüfung in Tabelle 7-1.4. Hinsichtlich der Steuerung enthält diese, für Hebezeuge, die nach KTA 3902 4.2 bis 4.4 ausgeführt sind, eine Prüfung der Ausführung und Kennzeichnung auf Übereinstimmung mit den Vorprüfunterlagen und eine Überprüfung der Leitungsverlegung, der Anschlüsse, der Leitungsdurchführungen und der Absicherungen.

Die Abnahmeprüfung nach KTA 3903 Tabelle 8-1 enthält im Hinblick auf die Steuerung vor allem Abgleiche auf die Konformität mit den Vorprüfunterlagen, der KTA 3902 und der Norm DIN EN 60204-32 zur Sicherheit von Maschinen. Für einzelne Prüfgebiete werden auch Vorgaben aus weiteren Regelwerken herangezogen, z. B. BGV D6 (Bedienungs- und Nothalteeinrichtungen, Funktionsprüfungen) /BGV 01/, BGV D8 (Funktionsprüfungen) /BGV 96/, BGV V3 /DGU 97/ (Schutz gegen Berühren, Kennzeichnungen), DIN EN 61000-6-4 und 61800-3 (EMV-Verträglichkeit), DIN 13557 (Funktionsprüfungen), DIN VDE 0105-100 (Funktionsprüfungen) oder DIN VDE 0100-520 (Stromzufuhr).

Tabelle 10-1 in KTA 3903 gibt den Umfang der wiederkehrenden Prüfungen vor. Tabelle 2.2 gibt diesen Prüfumfang für steuerungsrelevante Komponenten wieder.

Tab. 2.2 Wiederkehrende Prüfungen an elektrischen Einrichtungen nach KTA 3903 Tabelle 10-1

	Prüfgegenstand	Prüfung
Befehlseinrichtungen	Netzanschlussschalter, Trennschalter, Kranschalter (Not-Halt), Steuerschalter, Schütze, Überstromschutz, Wegbegrenzer, Verriegelungsschalter, drahtlose Steuerungen	Zustand, Funktion, Kennzeichnung, Einstellung, Schutzmaßnahmen gegen direktes und bei indirektem Berühren
Leitungen	Bewegliche Anschlussleitungen, Schleifleitungen, Isolatoren, Stromabnehmer, fest verlegte Leitungen	Befestigung, Zustand, Schutzmaßnahmen gegen direktes und bei indirektem Berühren
Verbraucher	Motoren, Bremslüfter, Widerstände, Heizung, Beleuchtung, Warn- und Signalanlagen	Zustand, Funktion, Kennzeichnung
Schutzmaßnahmen und -einrichtungen		Schutz gegen direktes Berühren, Schutz bei indirektem Berühren, Mitführung des Schutzleiters, Isolatoren in Steuerketten
Mess-, Regel-, Überwachungs- und Sicherheitseinrichtungen	Funktionen, die nach KTA 3902 Anhang E in Performance Level a bis e eingestuft sind	Zustand, Funktion, Kennzeichnung, Einhaltung der Anforderungen gemäß KTA 3902 Abschnitte 6.5, 7.5, 8.5.
	Alarmanlage, Notbeleuchtung	Zustand, Funktion
	Durch den Anwender programmierbare oder parametrierbare Systeme, die Funktionen ausführen, die nach KTA 3902 Anhang E in Performance Level c, d oder e eingestuft sind	Vergleich der Software und der Parameter mit dem zuletzt geprüften Stand

KTA 3903 enthält außerdem Vorgaben zu verwendbaren Werkstoffen (Kapitel 6), Betrieb, Wartung und Instandsetzung von Hebezeugen (Kapitel 9), der Dokumentation (Kapitel 13) und beschreibt ein vereinfachtes Verfahren zur Verwendung von Serienbauteilen und -elektrozügen (Kapitel 11 und 12). Hierbei sind keine steuerungsspezifischen Inhalte enthalten, daher werden diese Kapitel hier nicht detaillierter beschrieben.

2.1.2 Wichtige DIN-Normen

2.1.2.1 DIN ISO 13849-1 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze

Die Eigenschaft einer Steuerung eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird in DIN ISO 13849-1 einer von fünf Performance Level (PL) zugeordnet. Diese PL werden als Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion (Ausfall der Sicherheitsfunktion, der durch die Selbstüberwachung nicht detektiert wird) pro Stunde definiert.

Tab. 2.3 Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde abhängig vom Performance Level nach DIN ISO 13849-1 Tabelle 7

PL	Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]
a	$2^* 10^{-5}$
b	$5^* 10^{-6}$
c	$1{,}7^* 10^{-6}$
d	$2{,}9^* 10^{-7}$
e	$4{,}7^* 10^{-8}$

DIN ISO 13849-1 enthält unter anderem Verfahren für Steuerungen ein Performance Level (PL) an Hand der mittleren Betriebsdauer bis zum Ausfall[1] der einzelnen beteiligten Bauteile, des Diagnoseabdeckungsgrades[2] der einzelnen Bauteile und der Kategorie der Steuerung abzuleiten. Der DC bezeichnet den Anteil der gefährlichen Ausfälle, die vor einer Anforderung bemerkt werden. Die Kategorie bezeichnet eine Einstufung der sicherheitsbezogenen Teile der Steuerung bezüglich ihres Widerstands gegen Fehler und ihres Verhaltens nach Fehlern. Ein PL kann durch verschiedene Kombinationen von Kategorien, MTTFs der einzelnen Kanäle und DCs erreicht werden. Tabelle 2.4 gibt einen Überblick über die verschiedenen Optionen. In DIN ISO 13849-1 werden den hier verwendeten qualitativen Einschätzungen („hoch“, „niedrig“ etc.) auch konkrete Zahlenwerte bzw. -bereiche zugewiesen. Im Anhang werden Abschätzverfahren und generische Daten für gängige Bauteile und Überwachungsmaßnahmen genannt, sofern die

[1] Im Folgenden als MTTF (mean time to failure) abgekürzt

[2] Im Folgenden als DC (Diagnostic Coverage) abgekürzt

Zahlenwerte für MTTF und DC nicht bekannt sind. Diese Anhänge sind allerdings dem informativen Teil der Norm zugeordnet.

Tab. 2.4 Verschiedene Möglichkeiten zur Realisierung eines PL nach DIN 13849-1 Tabelle 6

PL	Anforderungen
a	Kategorie B, kein DC, niedriger MTTF eines Kanals oder Kategorie 2, niedriger DC, niedriger MTTF eines Kanals
b	Kategorie B, kein DC, mittlerer MTTF eines Kanals oder Kategorie 2, niedriger DC, mittlerer MTTF eines Kanals oder Kategorie 2, mittlerer DC, niedriger MTTF eines Kanals oder Kategorie 3, niedriger DC, niedriger MTTF eines Kanals
c	Kategorie 1, kein DC, hoher MTTF eines Kanals oder Kategorie 2, niedriger DC, hoher MTTF eines Kanals oder Kategorie 2, mittlerer DC, mittlerer MTTF eines Kanals oder Kategorie 3, niedriger DC, mittlerer MTTF eines Kanals oder Kategorie 3, mittlerer DC, niedriger MTTF eines Kanals
d	Kategorie 2, mittlerer DC, hoher MTTF eines Kanals (*) oder Kategorie 3, niedriger DC, hoher MTTF eines Kanals oder Kategorie 3, mittlerer DC, mittlerer MTTF eines Kanals oder Kategorie 3, mittlerer DC, hoher MTTF eines Kanals
e	Kategorie 4, hoher DC, hoher MTTF eines Kanals

Die mit (*) gekennzeichnete Variante der Umsetzung wird in KTA 3902 explizit ausgeschlossen und darf daher für Sicherheitsfunktionen in kerntechnischen Anlagen nicht angewendet werden.

Für die Einstufung einer Steuerung in eine Kategorie werden in der Norm weitere Anforderungen formuliert:
Kategorie B ist das Basislevel ohne besondere Anforderungen. Die Komponenten müssen lediglich den zu erwartenden Betriebsbeanspruchungen und äußeren Einflüssen soweit standhalten, dass die spezifizierten Aufgaben erfüllt werden.
Kategorie 1 stellt zusätzlich die Anforderung ausschließlich bewährte Bauteile zu verwenden.
Kategorie 2 setzt zusätzlich zu Kategorie 1 eine Testfunktion voraus, die regelmäßig die Sicherheitsfunktion testet und Steuerungsmaßnahmen einleitet, wenn ein Fehler erkannt wurde.
Kategorie 3 setzt zusätzlich zu Kategorie 1 voraus, dass einzelne Fehler nicht zum Verlust der Sicherheitsfunktion führen. Im Allgemeinen bedeutet dies eine redundante Ausführung der Steuerung. Erst durch eine unentdeckte Anhäufung von Fehlern kann die Sicherheitsfunktion verloren gehen.

Kategorie 4 setzt zusätzlich zu Kategorie 3 voraus, dass die MTTF der einzelnen Kanäle und die DC hoch sind, so dass eine Anhäufung von Fehlern rechtzeitig vor Verlust der Sicherheitsfunktion bemerkt wird.
KTA 3902 fordert über die DIN ISO 13849-1 hinausgehend für einige Sicherheitsfunktionen zwei parallel arbeitende Steuerungen, von denen eine mindestens PL e und eine mindestens PL c erfüllen muss.

DIN 13849-1 enthält außerdem Ansätze wie in Reihen arbeitende Steuerungen unterschiedlicher oder gleicher PLs zu einem Gesamt-PL zu verrechnen sind. Ab Kategorie 2 werden außerdem Maßnahmen gegen gemeinsam verursachte Ausfälle gefordert, mögliche Ansätze (z. B. physische Trennung, Diversität etc.) werden im informativen Anhang der Norm und unter Verweis auf weitere Normen gegeben.

Es werden außerdem Anforderungen an den Software-Entwicklungs- und Lebenszyklus der Embedded Software und der Anwendungssoftware gestellt. Hauptziel dieser Anforderungen ist es, lesbare, verständliche, testbare und wartbare[3] Software zu erhalten. Alle Tätigkeiten im Lebenszyklus von sicherheitsbezogener Embedded- oder Anwendungssoftware müssen hauptsächlich die Vermeidung von Fehlern berücksichtigen, die während des Software-Lebenszyklus eingebracht werden.

Die Norm enthält auch Verfahren zur Bestimmung der Notwendigen PL und zur Identifikation der Sicherheitsfunktionen, diese finden im Rahmen der Auslegung von Kransteuerungen nach KTA 3902 keine Anwendung, da die zu erreichenden PLs und notwendigen Sicherheitsfunktionen konkret in der KTA 3902 benannt sind.

2.1.2.2 DIN EN 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

Sowohl KTA 3902 als auch DIN ISO 13849-1 erlauben die Kategorisierung einer Sicherheitsfunktion nach sogenannten „Safety Integrity Levels“ (SIL), wie sie in DIN EN 61508 definiert werden. Einem geforderten PL d entspricht übereinstimmend ein SIL 2, einem PL e eine Einstufung nach SIL 3. DIN ISO 13849-1 führt außerdem aus, dass PL b und c SIL 1 entsprechen, diese Äquivalenz wird in KTA 3902 nicht aufgegriffen. DIN EN

[3] Unter Wartbarkeit ist hier die Durchführbarkeit von nachträglichen Änderungen an der Software zu verstehen

61508-1 enthält zu erreichende Vorgaben für die Häufigkeiten eines gefährlichen Ausfalls pro Stunde und Wahrscheinlichkeiten für einen gefährlichen Ausfall pro Anforderung. Diese sind in Tabelle 2.5 aufgelistet. Dabei werde allerdings keine konkreten Vorgaben für die Ausführung der Steuerung oder die Rechenwege wie diese Vorgaben erreicht werden angegeben. Der Schwerpunkt liegt auf der Beschreibung eines Prozesses wie während der gesamten Phase des Lebenszyklus (Konzept und Definition des Anwendungsbereichs, Risikoanalyse, Sicherheitsanforderungen, Planung, Realisierung, Inbetriebnahme, Betrieb und Instandhaltung, Modifikation und Nachrüstung, Außerbetriebnahme etc.) die Sicherheitsanforderungen adäquat berücksichtigt werden.

Tab. 2.5 Häufigkeit bzw. Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde und Anforderung abhängig vom SIL nach DIN ISO 61508-1 Tabelle 2&3

SIL	Häufigkeit eines gefährlichen Ausfalls [1/h]	Wahrscheinlichkeit eines gefährlichen Ausfalls pro Anforderung
1	≥ 10^-6 bis < 10^-5	≥ 10^-2 bis < 10^-1
2	≥ 10^-7 bis < 10^-6	≥ 10^-3 bis < 10^-2
3	≥ 10^-8 bis < 10^-7	≥ 10^-4 bis < 10^-3
4	≥ 10^-9 bis < 10^-8	≥ 10^-5 bis < 10^-4

Die Teile DIN EN 61508-2 und DIN EN 61508-3 spezifizieren die Anforderungen an den Lebenszyklus für Hardware und Software genauer. In den normativen Anhängen der Hardware-Norm 61508-2 finden sich zusätzliche Vorgaben:

- Welche Ausfallarten abhängig vom beanspruchten Diagnoseabdeckungsgrad (DC in DN ISO 113849-1) für typische Bauteile bei Betrachtungen des Ausfallverhaltens beachtet und abgefangen werden müssen
- Welche Diagnoseabdeckungsgrade mit welchen Maßnahmen für verschiedene Bauteile erreichbar sind.
- Maßnahmen gegen systematische Ausfälle (hierzu wird auf detailliertere Beschreibungen in dem informativen Teil von DIN EN 61508-7 verwiesen)
- Verfahren zur Vermeidung von Fehlern während der Spezifikation, der Entwicklung, der Integration, des Betriebs und der Instandhaltung und der Validierung
- Vorgaben zur Berechnung eines Diagnoseabdeckungsgrads und des Anteils sicherer Ausfälle
- Anforderungen für integrierte Schaltkreise mit On-Chip-Redundanzen

Die Teile DIN EN 61508-5, 61508-6 und 61508-7 der Norm enthalten Verfahren und Beispiele zur Bestimmung der notwendigen statistischen Kenngrößen zur Berechnung der Ausfallhäufigkeiten bzw. -wahrscheinlichkeiten. Sie sind allerdings lediglich informativ.

2.1.2.3 DIN EN 60204-32 Sicherheit von Maschinen – Teil 32: Anforderungen für Hebezeuge

DIN EN 60204-32 ist eine Norm, die auch für konventionelle Krananlagen gilt. KTA 3902 referenziert sie nur dahingehend, dass die Not-Halt-Schalter und die drahtlosen Fernsteuerungen an KTA-Kranen entsprechend den Anforderungen aus dieser Norm auszulegen sind. Des Weiteren wird in den Abnahmeprüfungen nach KTA 3903 geprüft, ob die Ausführung der elektrischen Einrichtungen, einschließlich der Steuerungen, den Anforderungen aus dieser Norm entspricht. Die Norm DIN EN 60204-32 gilt für die elektrische und elektronische Ausrüstung und Systeme von Hebezeugen (u. a. Krane und Winden aller Art) und für hiermit zusammenhängende Ausrüstungen. Sie enthält Anforderungen und Empfehlungen für die elektrische Ausrüstung von Hebezeugen, um

- die Sicherheit von Personen und Sachen,
- die Erhaltung der Funktionsfähigkeit und
- die Erleichterung der Instandhaltung

zu fördern. Abb. 2.1 zeigt ein Blockschaltbild einer typischen Krananlage mit zugehöriger Ausrüstung, einschließlich der Steuerung und Energieversorgung.

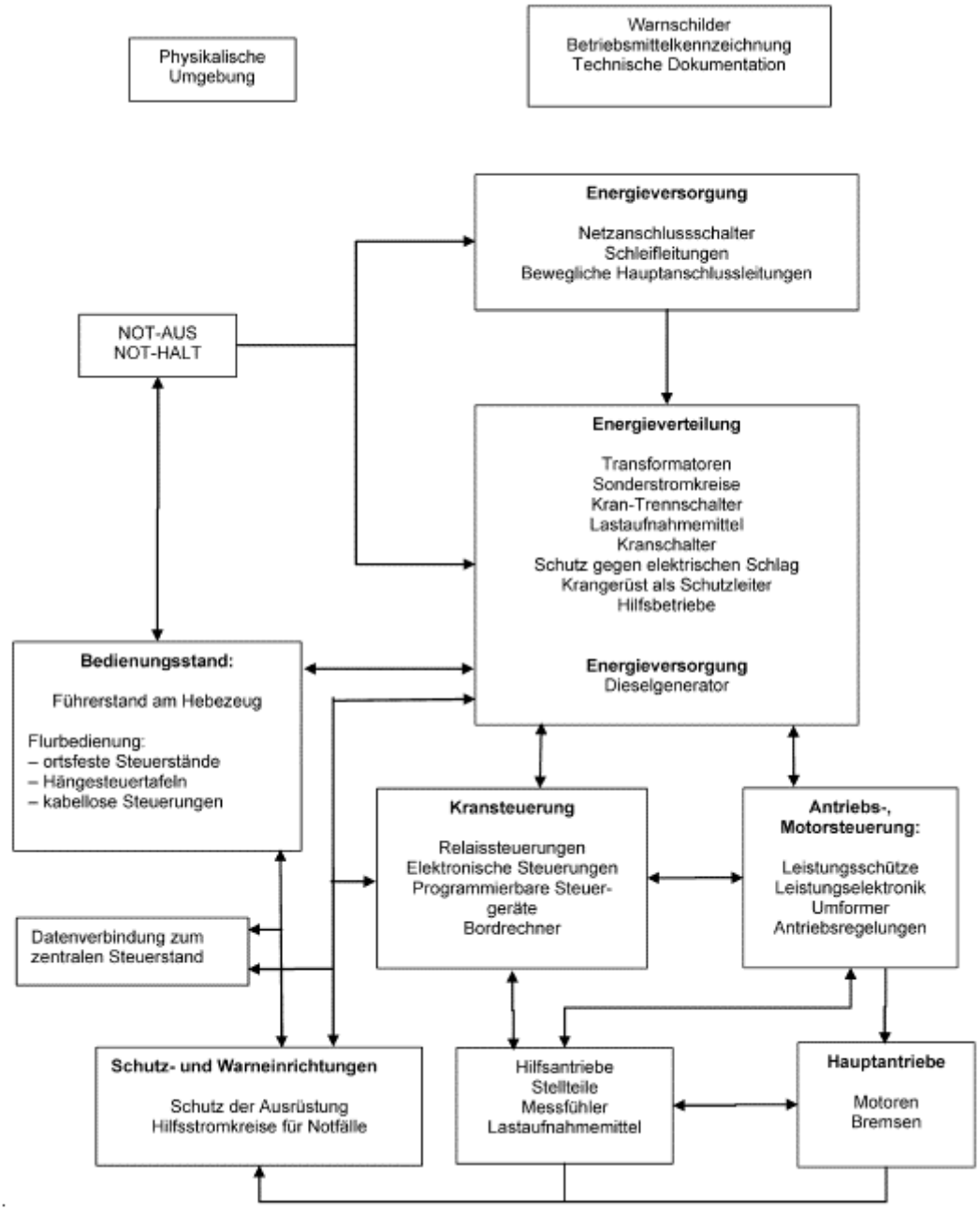

Abb. 2.1 Übersicht der elektrischen Ausrüstung einer Krananlage aus DIN EN 60204-32

Das Steuerungskonzept einer sicherheitsrelevanten Krananlage besteht aus einer zentralen, betrieblichen Steuerung der Antriebe und einer zentralen Mensch-Maschine-Schnittstelle und einer Sicherheitssteuerung. Es müssen die für einen sicheren Betrieb notwendigen Sicherheitsfunktionen und/oder Schutzmaßnahmen (z. B. Verriegelungen) vorgesehen werden. Maßnahmen müssen ergriffen werden, um nach jedem Anhalten des Hebezeuges eine unbeabsichtigte oder unerwartete Bewegung des Hebezeuges zu

verhindern (z. B. durch die Aufhebung eines gesperrten Zustandes, Fehler in der Energieversorgung, Batteriewechsel, Signalausfall bei drahtlosen Steuerungen). Die Einleitung des Betriebes (z. B. einer Bewegung) darf nur möglich sein, wenn alle relevanten Sicherheitsfunktionen und/oder Schutzmaßnahmen in der entsprechenden Stellung (Ausgangsignal), funktionsfähig und betriebsbereit sind. Wo eine Betriebsgrenze (z. B. Last, Position, Geschwindigkeit, Druck) überschritten werden und damit zu einer gefahrbringenden Situation führen kann, müssen Mittel vorgesehen werden (z. B. Stellungsgeber, Endschalter), um das Überschreiten dieser Grenze zu erfassen und eine angemessene Steuerungsaktion einzuleiten. Die Grenzen und einzuleitenden Steuerungsaktion werden durch die Risikobeurteilung des Hebezeuges festgelegt.

Falls es für die Sicherheit oder für den kontinuierlichen Betrieb erforderlich ist, dass bestimmte Funktionen an dem Hebezeug in wechselseitiger Beziehung zueinander stehen, muss eine passende Koordinierung durch geeignete Verriegelungen sichergestellt werden. Für eine Gruppe von Hebezeugen, die koordiniert zusammenarbeiten und die mehr als eine Steuerung besitzen, müssen Vorkehrungen getroffen werden, um den Betrieb der Steuerungen, soweit erforderlich, aufeinander abzustimmen. KTA 3902 schränkt dies für KTA-Krane weiter ein, dort darf grundsätzlich nur eine Steuerung gleichzeitig im Eingriff sein.

Alle Schütze, Relais und andere Steuergeräte, die Teile des Hebezeugs steuern und deren gleichzeitige Betätigung einen gefahrbringenden Zustand herbeiführen kann (z. B. solche, die gegenläufige Bewegungen einleiten), müssen gegen unsachgemäßen Betrieb verriegelt sein. Wendeschütze (z. B. solche, die die Drehrichtung eines Motors steuern) müssen so verriegelt sein, dass im Normalbetrieb beim Schalten kein Kurzschluss entstehen kann. Alle sicherheitsrelevanten Signale werden über die Sicherheitskreise mit entsprechenden Schaltgeräten und Schutzeinrichtungen verknüpft, wobei zur Erhöhung der Zuverlässigkeit der Sicherheitsfunktionen redundante Signalverarbeitung (u. a. Signale von Sensoren, Weg- und Endschalter der Krananlage) eingesetzt wird. Für die Sicherheitsfunktionen der Kransteuerung wird der Einsatz von qualifizierten Geräten gefordert.

Des Weiteren muss bei sicherheitstechnisch relevanten Steuerungsfunktionen berücksichtigt werden, dass Hebezeuge mehrere Betriebsarten haben können und hierzu für jede Betriebsart entsprechende Vorkehrungen realisiert werden müssen. Die Betriebsartenwahl allein darf keinen Betrieb des Hebezeugs auslösen. Eine getrennte Betätigung der Startsteuerung muss hierzu erforderlich sein. Wenn durch eine Betriebsartenwahl

eine gefahrbringende Situation entstehen kann, muss eine unbefugte und/oder unbeabsichtigte Auswahl durch geeignete Mittel verhindert werden (z. B. Schlüsselschalter, Zugangscode). Eine Bewegung oder Aktion eines Hebezeuges oder eines seiner Teile, die zu einem gefahrbringenden Zustand führen kann, muss überwacht werden.

Jenseits dieser Vorgaben zur Steuerung enthält die Norm außerdem folgende Anforderungen:

- Anforderungen zu den für die elektrische Ausrüstung zu berücksichtigenden Umgebungsbedingungen (Spannungs- und Frequenzschwankungen im AC wie auch im DC-Netz, EMV, Temperatur, Luftfeuchte, Höhenlage, Verschmutzungen, Strahlung, Vibrationen und mechanische Einwirkungen, Transport-, Lager- und Handhabungsbedingungen),
- Anforderungen zu den elektrischen Einrichtungen, also z. B. zur Energieversorgung des Hebezeugs (Netzanschluss),
- Anforderungen zu den Einrichtungen zum Trennen und Schalten der Einspeisung (Trennschalter, Not-Halt-Schalter etc.: Dimensionierung, Anordnung und Aufbau),
- Anforderungen zum Schutzerdungssystem und zum Potentialausgleich sowie zum Schutz gegen direktes und indirektes Berühren stromführender Bauteile.
- Außerdem werden Vorgaben zur Ausführung des Komponentenschutzes gemacht. Dieser umfasst Schutzmechanismen gegen den Überstrom, der bei einem Kurzschluss entsteht, gegen Überlaststrom, gegen anormale Temperaturen, gegen einen Ausfall der Versorgungsspannung oder Unterspannung, gegen Überdrehzahl bei Motoren, gegen Erdschluss, gegen ein falsch gepoltes Drehfeld und gegen Überspannungen durch Blitzschlag oder Schalthandlungen.
- Für die Bedienerschnittstelle werden Spezifikationen angegeben (Farben, Kennzeichnungen, Blinksignale, Lage und Art von Eingabegeräten etc.).
- Ebenso werden Vorgaben zur Verkabelung und Verdrahtung (Strombelastbarkeit, Berührungsschutz, Schutzleiter, Färbung, Dimensionierung der Leitungskanäle etc.) gemacht.
- Weitere Regelungen betreffen die verwendeten Motoren, die Beleuchtung, die Kennzeichnung, die erforderliche Dokumentation und das Prüfkonzept.

2.1.3 Sonstige Regelwerke

Bei der DIN 62061 „Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“ /DIN 16b/ handelt es sich um eine anwenderorientierte Norm, die insbesondere beschreibt, wie ein System aus bekannten Subsystemen aufgebaut werden kann und dessen resultierende SIL bestimmt werden kann. Dabei wird umfangreich DIN 61508 referenziert. Wird zur Realisierung der Anforderungen aus KTA 3902 nicht das Konzept der Performance Level PL und Kategorien, sondern der Safety Integrity Level SIL herangezogen, so ist die Anwendung der Norm möglich. Eine explizite Anforderung die Norm zu verwenden findet sich weder in KTA 3902 noch in den Normen DIN EN 61508-1 bis -3.

Die DIN EN 61513 „Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Allgemeine Systemanforderungen“ enthält Anforderungen an leittechnische Systeme und Geräte, die für die Ausführung sicherheitstechnisch wichtiger leittechnischer Funktionen in Kernkraftwerken eingesetzt werden. Sie spezifiziert die in DIN EN 61508 enthaltenen allgemeinen Anforderungen für die Anwendung im nuklearen Bereich. Sie enthält Anforderungen und Empfehlungen für die gesamte leittechnische Architektur. Gemäß KTA 3902 sind für die elektrischen Einrichtungen von Hebezeugen mit zusätzlichen oder erhöhten Anforderungen die Anforderungen entsprechend leittechnischer Einrichtungen der Kategorie B einzuhalten. Andere Einrichtungen in Kernkraftwerken, an die vergleichbare Anforderungen gestellt werden, sind beispielsweise die Begrenzungssysteme.

Die DIN EN 62138 „Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C“ enthält in Kapitel 6 Anforderungen an die Software leittechnischer Systeme, die Funktionen der Kategorie B ausführen. Nach KTA 3902 sind für softwarebasierte Sicherheitssteuerungen bei der Entwicklung der Software diese Anforderungen einzuhalten.

Die Berufsgenossenschaften und die deutsche gesetzliche Unfallversicherung veröffentlichen Unfallverhütungsvorschriften, deren Erfüllung rechtlich verbindlich für die versicherten Unternehmen ist. Die BG-Vorschriften werden sukzessive durch die DGUV-Vorschriften ersetzt. Für Hebezeuge in Kernkraftwerken sind die Vorschriften BGV D6

„Unfallverhütungsvorschrift Krane“ /BGV 01/, BGV D8 „Winden, Hub- und Zuggeräte“ /BGV 96/ relevant und werden in den KTA-Regeln zitiert (inhaltlich entsprechen diesen die DGUV-Vorschriften 53 /DGU 01/ und 55 /DGU 00/). Es handelt sich dabei um relativ allgemeine Vorschriften ohne detailliertere Vorgaben zu Zahlenwerten o. ä., da diese Vorschriften grundsätzlich für alle Krananlagen gelten, also auch z. B. für Krane in Logistik- oder Bauunternehmen. Der Fokus der Vorschriften liegt auf dem Bereich Arbeitssicherheit. Einige der Vorschriften sind trotzdem steuerungsrelevant, z. B. die Forderung §15 zum Vorhandensein von Notendhalteinrichtungen oder §16 für Lastmomentbegrenzer (Überlastüberwachung). Die Erfüllung der Vorschriften wird im Rahmen der Abnahmeprüfungen nach KTA 3903 geprüft. Es gibt auch weitere DGUV-Vorschriften, die zwar Vorgaben mit Bezug auf Hebezeuge enthalten, im KTA-Regelwerk referenziert werden, aber keine nuklearspezifischen, steuerungsrelevanten Vorgaben enthalten. Beispiele sind der DGUV Grundsatz 309-001 /DGU 12/ zu durchzuführenden Prüfungen, der Vor-, Bau-, Abnahme-, Inbetriebsetzungs- und wiederkehrende Prüfungen für konventionelle Krananlagen beschreibt, DGUV Regel 100-500 /DGU 08/, die Regeln zum Betrieb von Lastaufnahmemitteln umfasst oder DGUV Vorschrift 3 /DGU 97/, die Unfallverhütungsvorschrift für elektrische Anlagen und Betriebsmittel allgemein beinhaltet.

Neben den hier dargestellten steuerungsrelevanten Regelwerken gibt es auch umfangreiche Normen und Regelwerke zu der mechanischen Auslegung von Hebezeugen aus dem konventionellen Bereich. Einige dieser Normen enthalten, obwohl sie sich nicht schwerpunktmäßig mit Steuerungen beschäftigen, einzelne Kapitel mit entsprechenden Anforderungen. Häufig wird dabei auf die oben genannten Normen verwiesen. Im Folgenden sind zwei Beispiele ohne Anspruch auf Vollständigkeit genannt:
DIN EN 13135: „Krane - Sicherheit - Konstruktion - Anforderungen an die Ausrüstungen“ /DIN 18/ enthält ein Unterkapitel zur elektrischen Ausrüstung, hier wird sich auf DIN 60204-32 bezogen. Außerdem werden Drehmomentanforderungen für die zu verwendenden Motoren definiert. Hinsichtlich der technischen Sicherheitsfunktionen wird bezüglich der zu erreichenden Zuverlässigkeit DIN ISO 13849-1 herangezogen.
DIN EN 14492-2 „Krane – Kraftgetriebene Winden und Hubwerke –Teil 2: Kraftgetriebene Hubwerke“ /DIN 07a/ hat ebenfalls ein Kapitel zur elektrischen Ausrüstung von Hubwerken. Hier wird vor allem DIN 60204-32 referenziert.

Darüber hinaus gibt es eine größere Anzahl weiterer DIN-Normen, die sich mit spezifischen Anforderungen zu einzelnen Bauteilen, die in einer Steuerung verwendet werden können, beschäftigen. Beispielsweise (wieder ohne Anspruch auf Vollständigkeit) enthalten DIN EN 61131-6 „Speicherprogrammierbare Steuerungen – Teil 6: Funktionale

Sicherheit“ /DIN 13b/ Anforderungen zur Auslegung von speicherprogrammierbaren Steuerungen und DIN EN 61800-5-2 „Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit“ /DIN 17/ Anforderungen zur Auslegung von Antrieben. Auch hier wird in der Regel auf DIN ISO 13849-1 und DIN EN 61508 verwiesen oder Bezug genommen.

2.2 Ermittlung der verwendeten Technik für die Modellierung der Kransteuerung

Für die Modellierung einer Kransteuerung in AP2 ist es sinnvoll neben den grundsätzlichen Anforderungen aus dem Regelwerk auch die tatsächliche praktische Umsetzung zu berücksichtigen, um sicherzustellen, dass ein beispielhaft gewähltes Modell auch von realistischen Randbedingungen ausgeht und einer realen Anlage entsprechen könnte. Dementsprechend wurden verschiedene Fachveranstaltungen zu Recherchezwecken besucht und ergänzende Informationen durch den Austausch mit Betreibern eruiert, um ein realistisches Modell einer typischen Krananlage und ihrer Kransteuerung in einem deutschen Kernkraftwerk zu erstellen. Das verwendete Modell der Krananlage und der Kransteuerung wird in Kapitel 3.2 dieses Berichts genauer beschrieben.

2.3 Einsatzbereiche von Hebezeugen in deutschen KKW

Hebezeuge werden bei verschiedensten Montage-, Betriebs- und Instandhaltungsprozessen in Kernkraftwerken eingesetzt. Die Einsatzzwecke reichen beispielsweise vom Kernbrennstofftransport im Reaktorgebäude mit dem Reaktorgebäudekran und der Brennelementlademaschine über Hebevorgänge bei Instandhaltungsarbeiten an Sicherheitseinrichtungen, wie z. B. der Notstromerzeugung und den Nebenkühlwasserpumpen, bis zu betrieblichen Vorgängen. Um mögliche Fehlerfolgen differenziert bewerten zu können, erfolgt zunächst eine Erfassung der Einsatzbereiche von KTA-Hebezeugen in Kernkraftwerken. Bei dieser Betrachtung wird insbesondere berücksichtigt, welche Kernbrennstoffe und sonstigen radioaktiven Stoffe transportiert werden, welche Sicherheitseinrichtungen in der Nähe von Hebezeugen betrieben werden und welche Lasten mit diesen bewegt werden. Hierfür erfolgte eine Literaturrecherche in bei der GRS vorhandenen Betriebsunterlagen. Als wesentliche Quelle konnten dabei die bei der GRS vorliegenden Betriebshandbücher und Systembeschreibungen genutzt werden, um wesentliche Transportvorgänge zu identifizieren und die ungefähre Anzahl und Art der Hebezeuge zu bestimmen.

Die folgende Darstellung unterscheidet sicherheitsrelevante Hebezeuge, die sich in allen in Betrieb befindlichen Reaktoren finden und Hebezeuge, die sich zwar grundsätzlich in allen Reaktoren befinden, bei denen es allerdings anlagenspezifische Unterschiede im Detail gibt. Letztere werden generisch beschrieben.

Tab. 2.6 am Ende des Unterkapitels 2.3 enthält eine zusammenfassende Übersicht aller Hebezeuge.

2.3.1 Hebezeuge in Druckwasserreaktoren

Bei der Durchsicht der bei der GRS vorhandenen Unterlagen wurde festgestellt, dass sich die Abläufe beim Transport von Kernbrennstoffen und sonstigen radioaktiven Stoffen bei allen deutschen Druckwasserreaktoren grundsätzlich sehr ähneln, die räumliche Aufteilung zu einer ähnlichen Platzierung der Sicherheitseinrichtungen führte und daher nur unwesentliche Unterschiede zwischen den Reaktormodellen seit der Errichtung der Anlage Biblis zu beobachten sind. Erkenntnisse zu den einzelnen Anlagen sind daher weitgehend übertragbar.

Es wurden für deutsche DWR-Anlagen folgende Hebezeuge als relevant für den Transport von Kernbrennstoffen identifiziert:

- BE-Lademaschine
  Einbauort: BE-Bühne bzw. Bedienflur im Sicherheitsbehälter im Reaktorgebäude, fährt über BE-Becken und RDB
  Typische Lasten: Brennelemente, Steuerelemente, Drosselkörper, Neutronenquellen, kleinere Abfallbehälter, ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten
  Rückbaurelevanz: Ja, u. a. für Transport abgebrannter Brennelemente und Demontage der Kerneinbauten
  Einstufung nach KTA 3902: 4.4, für Hilfshub teilweise 4.3

- Reaktorgebäudekran
  Einbauort: Kuppel des Reaktorgebäudes
  Typische Lasten: RDB-Deckel, Transport- und Lagerbehälter, Abschirmriegel, RDB-Einbauten (oberes und unteres Kerngitter etc.), Dichtschütz, Trennschütz, allgemeine Transportvorgänge von Großkomponenten
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Brennelementgestelle des

BE-Lagerbeckens, RDB mit Kerneinbauten, Flutkompensator, Hauptkühlmittelpumpen
Rückbaurelevanz: Ja, u. a. für Transport abgebrannter Brennelemente sowie Demontage der Kerneinbauten, RDB, Dampferzeuger und HKMP
Einstufung nach KTA 3902: 4.3

- Halbportalkran
  Einbauort: Vor Materialschleuse auf der Außenseite des Reaktorgebäudes im Freien
  Typische Lasten: Transport- und Lagerbehälter, Prüfgewichte, ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Keine
  Rückbaurelevanz: Ja, Transport von Transport- und Lagerbehältern
  Einstufung nach KTA 3902: 4.3

- Konsolkran Reaktorgebäude
  Einbauort: BE-Bühne bzw. Bedienflur im Sicherheitsbehälter im Reaktorgebäude, montiert an Zylinderring des Sicherheitsbehälters, läuft über Randbereich des Bedienflurs, insbesondere über Bereich zwischen Materialschleuse und Luke zum Lager für unbestrahlte Brennelemente
  Typische Lasten: Unbestrahlte Brennelemente (Transport aus Entladestation in Lager für unbestrahlte BE) , ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: BE-Trockenlager, FD-Leitungen, Leitungen DE-Bespeisung, Druckspeicher, Umluftanlage
  Rückbaurelevanz: Keine zwingende Rückbaurelevanz
  Einstufung nach KTA 3902: 4.2

- Kran im Lager für unbestrahlte Brennelemente
  Einbauort: Lager für unbestrahlte Brennelemente (Reaktorgebäude im Sicherheitsbehälter, Ebene unterhalb des Bedienflurs)
  Typische Lasten: Unbestrahlte Brennelemente
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Unbestrahlte Brennelemente
  Rückbaurelevanz: Keine zwingende Rückbaurelevanz
  Einstufung nach KTA 3902: 4.2

2.3.2 Hebezeuge in Siedewasserreaktoren

Die räumliche Aufteilung und das Vorgehen bei Transportvorgängen ist auch in allen deutschen SWR ähnlich, sodass auch hier eine Übertragung der Erkenntnisse zwischen den Anlagen möglich ist, um etwaige Lücken in der Dokumentation zu kompensieren. Die beiden betrachteten Reaktormodelle vom Typ SWR-69 und SWR-72 ließen folgende Hebezeuge als relevant erkennen:

- BE-Lademaschine
  Einbauort: BE-Bühne bzw. Bedienflur, oberste Ebene im Reaktorgebäude, fährt über BE-Becken und RDB
  Typische Lasten: Brennelemente, Steuerelemente, Drosselkörper, Neutronenquellen, kleinere Abfallbehälter, ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten, Flutkompensator
  Rückbaurelevanz: Ja, u. a. für Transport abgebrannter Brennelemente und Demontage der Kerneinbauten
  Einstufung nach KTA 3902: 4.4, für Hilfshub teilweise 4.3

- Reaktorgebäudekran
  Einbauort: Decke des Reaktorgebäudes
  Typische Lasten: RDB-Deckel, SHB-Deckel, Flutkompensator, Transport- und Lagerbehälter, Abschirmriegel, RDB-Einbauten (oberes und unteres Kerngitter etc.), Beckenschütz, Dampfabscheider, Dampftrockner, allgemeine Transportvorgänge von Großkomponenten
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten, Behälter mit Vergiftungslösung (System TW)
  Rückbaurelevanz: Ja, u. a. für Transport abgebrannter Brennelemente und Demontage der Kerneinbauten
  Einstufung nach KTA 3902: 4.3

- Schwenkkran
  Einbauort: Reaktorgebäude Bedienflur über Hauptmontageöffnung
  Typische Lasten: Unbestrahlte Brennelemente, ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Unbestrahlte Brennelemente, Umluftanlage Bedienflur

Rückbaurelevanz: Keine zwingende Rückbaurelevanz
Einstufung nach KTA 3902: 4.2 (teilweise auch 4.3)

- Kran im Lager für unbestrahlte Brennelemente
  Einbauort: Lager für unbestrahlte Brennelemente (Reaktorgebäude außerhalb des Sicherheitsbehälters, Ebene unterhalb des Bedienflurs)
  Typische Lasten: Unbestrahlte Brennelemente
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Unbestrahlte Brennelemente
  Rückbaurelevanz: Keine zwingende Rückbaurelevanz
  Einstufung nach KTA 3902: 4.2 (teilweise auch 4.3)

2.3.3 Hebezeuge in Zwischenlagern

In den deutschen Zwischenlägern werden Krane zum Transport von Transport- und Lagerbehältern innerhalb der Halle genutzt. Diese wurden in den letzten Jahren nachgerüstet, um die erhöhten Anforderungen der KTA 3902 zu erfüllen. Die genaue Anzahl der Krane pro Zwischenlager variiert, die sonstigen Parameter sind im Rahmen dieser Betrachtungstiefe vergleichbar.

- Zwischenlagerkran
  Einbauort: Zwischenlager
  Typische Last: Transportbehälter, insbesondere CASTOR
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: andere Transportbehälter
  Rückbaurelevanz: Ja, Einlagerung und späterer Abtransport der Transportbehälter
  Einstufung nach KTA 3902: 4.2 oder 4.3

2.3.4 Weitere Hebezeuge und Hilfsmittel mit KTA-Einstufung

Neben den oben aufgeführten Hebezeugen, die es in jedem Kernkraftwerk gibt, sind in einem Kernkraftwerk noch weitere Hebezeuge mit KTA-Einstufung vorhanden, die sich allerdings im Detail von Anlage zu Anlage unterscheiden. Gemeinsam ist diesen Hebezeugen, dass es sich nach KTA 3902 um Hebezeuge der Einstufung 4.2 handelt.

- Hebezeuge für den Transport radioaktiver Abfälle
  Einbauort: Typischerweise Hilfsanlagengebäude
  Typische Lasten: Filter, Fässer mit mittel- und schwachradioaktivem Abfall, ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Behälter mit mittel- und

schwachradioaktivem Abfall, Filteranlagen, Komponenten und Systeme zur Behandlung von schwachradioaktivem Abfall
Rückbaurelevanz: Ja, während dem Rückbau erfolgt laufende Behandlung von Abfall
Einstufung nach KTA 3902: 4.2

Typische derartige Hebezeuge sind beispielsweise Krane im Fasslager, die dazu dienen die abgepackten Fässer einzulagern und zu bewegen oder Hebezeuge, die in der Filterwechselanlage zum Tausch der Filter eingesetzt werden. Bei der Filterwechselanlage handelt es sich um eine Vorrichtung zum Tausch von Filtern, die Primärkreismedium filtern. Diese Filter erreichen dabei durch die Anreicherung von aktivierten Korrosionsprodukten relativ hohe Dosisleistungen. Die entsprechenden Hebezeuge gibt es in jedem Kraftwerk, die genaue Anzahl und die exakten Einbauorte sind anlagenspezifisch. Je nach Anlage kann es außerdem noch Hebezeuge zum Transport von radioaktiven Abfällen oder zum Transport von sonstigen Lasten über Lager von radioaktiven Abfällen hinweg geben. Diese sind ebenfalls nach KTA 3902 4.2 eingestuft.

- Hebezeuge zum Transport von aktivierten oder größeren Komponenten im Kontrollbereich
  Einbauort: Reaktorgebäude, Ringraum oder Hilfsanlagengebäude
  Typische Lasten: Komponenten, ggf. Werkzeuge und Material
  Sicherheitstechnisch relevante Einrichtungen in der Nähe: Die entsprechenden Komponenten, sofern sicherheitsrelevant, ggf. auch andere aktivierte Komponenten, z. B. in der heißen Werkstatt
  Rückbaurelevanz: Keine zwingende Rückbaurelevanz
  Einstufung nach KTA 3902: 4.2

Typische derartige Hebezeuge wären beispielsweise Krane in der heißen Werkstatt des Hilfsanlagengebäudes. Weiterhin existieren in den meisten Kernkraftwerken Hebezeuge (Katzen, Schwenkkrane oder Hilfszüge), die speziell für den Ein- und Ausbau bestimmter größerer Komponenten gedacht sind. Beispiele wären hier Hebezeuge zum Transport der HD-Förderpumpen oder raumspezifische Hebezeuge. Je nach Anlage sind einige dieser Komponenten nach KTA 3902 4.2 eingestuft. Wenn das Einstufungskriterium nicht die potenzielle Aktivitätsfreisetzung, sondern der potenzielle Kühlmittelverlust oder die Beeinträchtigung von Sicherheitseinrichtungen ist, werden oft administrative Regelung vorgenommen, die sicherstellen, dass das Hebezeug nur in Anlagenzuständen genutzt wird, in denen diese Sicherheitseinrichtungen nicht benötigt werden, respektive kein Kühlmittelverlust auftreten kann (also z. B. nur im Anlagenstillstand). Dann können

diese Hebezeuge auch nach KTA 3902 3.0 eingestuft werden. Es muss dann lediglich das konventionelle Regelwerk erfüllt werden.

Neben den bisher aufgeführten Hebezeugen gibt es in jedem Kernkraftwerk eine größere Anzahl (höherer zweistelliger Bereich) an rein betrieblichen Hebezeugen. Durch diese können keine sicherheitstechnischen Gefahren herbeigeführt werden, deswegen werden sie nach KTA 3902 3.0 (Erfüllung konventionelles Regelwerk) eingestuft. Ein Beispiel für ein solches Hebezeug wäre der Kran des Maschinenhauses. Darüber hinaus besteht auch die Option insbesondere für einmalig durchzuführende Transporte temporär montierbare Hebezeuge zum Einsatz zu bringen.

2.3.5 Lastaufnahmemittel und Anschlagmittel

Demontierbare Lastaufnahmemittel und Anschlagmittel, die nicht für jeden Transport benötigt werden, werden separat nach KTA 3902 eingestuft. Abhängig davon, welche Last transportiert wird und über welche Komponenten und Systeme mit dieser Last gefahren wird, können sich die Einstufungen auch für Lastaufnahmemittel und Anschlagmittel desselben Hebezeugs unterscheiden. Für viele Lastaufnahmemittel gibt KTA 3902 Anhang A eine beispielhafte Einstufung vor, allerdings kann diese durch eine anlagenspezifische Betrachtung der potenziellen Versagensfolgen auch geändert werden.

Beispiele für Lastaufnahmemittel, die nach KTA 3902 4.3 einzustufen wären, sind im Folgenden aufgeführt. Grund für die Einstufung nach 4.3 ist entweder, dass direkt Brennelemente transportiert werden oder, dass Lasten über dem BE-Lagerbecken transportiert werden oder beides:

- BE-Greifer
- Lastaufnahmemittel für den Transport der Brennstabwechsel- und BE-Reparaturvorrichtungen
- Traversen und Gehänge für den Transport von Lagerbehältern (Castor, Mosaik etc.) und ihrer Deckel
- Traversen für den Transport des Dicht- oder Beckenschützes
- Traversen und Gehänge für den Transport von Abschirmriegeln, z. B. DH/HKMP/Reaktorraum/BE-Becken (teilweise auch nur nach KTA 3902 4.2 eingestuft)

- Lastaufnahmemittel und Gehänge für Transportvorgänge in Zusammenhang mit Filterwechseln (BE-Becken)
- Traversen für den Transport von Flutkompensator, Dampfabscheider und Dampftrockner (SWR)
- Traversen und Gehänge für den Transport der Hilfsbrücke
- Arbeitskorb mit Abschirmung für Arbeiten auf dem Beckenflur
- Lastaufnahmemittel für den Transport von Gasflaschen

Beispiele für Lastaufnahmemittel, die nach KTA 3902 4.2 einzustufen wären, sind:

- Lastaufnahmemittel für den Transport des RDB-Deckels (teilweise auch nach KTA 3902 4.3 eingestuft), der RDB-Schrauben und zugehöriger Führungsstangen
- Traversen für den Transport des Kernbehälters oder des oberen und unteren Kerngerüsts (Traverse für oberes Kerngerüst teilweise auch nach KTA 3902 4.3 eingestuft)
- Traversen für den Transport des Trennschützes
- Traversen für den Transport der Kerninstrumentierungslanzenreparaturstation
- Traversen für den Transport von Transportbehältern für unbestrahlte Brennelemente
- Gestell und Gehänge für den Transport von Prüfgewichten

2.3.6 Rückbaurelevanz

Die Rückbaurelevanz von einzelnen Hebezeugen ist nur in Ausnahmefällen eindeutig zu benennen. Wie oben bereits ausgeführt, sind für den Abtransport der abgebrannten Brennelemente die BE-Lademaschine und der Reaktorgebäudekran zwingend erforderlich. Auch für die Demontage von Kerneinbauten und RDB sind diese Hebezeuge notwendig.

Da während des gesamten Rückbauprozesses im Kontrollbereich schwach radioaktive Abfälle anfallen, ist außerdem davon auszugehen, dass die Hebezeuge für den Transport radioaktiver Abfälle bis zum Abschluss des Rückbaus Verwendung finden.

Für alle übrigen Hebezeuge ist eine pauschale Aussage zur Rückbaurelevanz nicht möglich. Grundsätzlich können sie natürlich bei Demontagearbeiten für beliebige Lasten (demontierte Komponenten, Werkzeuge etc.) innerhalb ihrer Auslegung herangezogen werden. Eine zwingende Notwendigkeit ergibt sich jedoch nicht, da ggf. auch auf temporär montierte Hebezeuge zurückgegriffen werden kann. Dies wird z. B. für den Abtransport von Großkomponenten des Sekundärkreises so gehandhabt.

Tab. 2.6 Übersicht über typische sicherheitsrelevante Hebezeuge in Kernkraftwerken

Bezeichnung	Einbauort	Typische Lasten	Sicherheitstechnisch relevante Einrichtungen in der Nähe	Rückbaurelevanz	Einstufung nach KTA 3902
BE-Lademaschine (DWR)	BE-Bühne bzw. Bedienflur im Sicherheitsbehälter im Reaktorgebäude, fährt über BE-Becken und RDB	Brennelemente, Steuerelemente, Drosselkörper, Neutronenquellen, kleinere Abfallbehälter, ggf. Werkzeuge und Material	Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten	Ja, u. a. für Transport abgebrannter Brennelemente und Demontage der Kerneinbauten	4.4, für Hilfshub teilweise 4.3
Reaktorgebäudekran (DWR)	Kuppel des Reaktorgebäudes	RDB-Deckel, Transport- und Lagerbehälter, Abschirmriegel, RDB-Einbauten (oberes und unteres Kerngitter etc.), Dichtschütz, Trennschütz, allgemeine Transportvorgänge von Großkomponenten	Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten, Flutkompensator, Hauptkühlmittelpumpen	Ja, u. a. für Transport abgebrannter Brennelemente, sowie Demontage der Kerneinbauten, RDB, Dampferzeuger und HKMP	4.3
Halbportalkran (DWR)	Vor Materialschleuse auf der Außenseite des Reaktorgebäudes im Freien	Transport- und Lagerbehälter, Prüfgewichte, ggf. Werkzeuge und Material	Keine	Ja, Transport von Transport- und Lagerbehältern	4.3
Konsolkran Reaktorgebäude (DWR)	BE-Bühne bzw. Bedienflur im Sicherheitsbehälter im Reaktorgebäude, montiert an Zylinderring des Sicherheitsbehälters	Unbestrahlte Brennelemente (Transport aus Entladestation in Lager für unbestrahlte BE) , ggf. Werkzeuge und Material	BE-Trockenlager, FD-Leitungen, Leitungen DE-Bespeisung, Druckspeicher, Umluftanlage	Keine zwingende Rückbaurelevanz	4.2

Bezeichnung	Einbauort	Typische Lasten	Sicherheitstechnisch relevante Einrichtungen in der Nähe	Rückbaurelevanz	Einstufung nach KTA 3902
Kran im Lager für unbestrahlte Brennelemente (DWR)	Lager für unbestrahlte Brennelemente (Reaktorgebäude im Sicherheitsbehälter, Ebene unterhalb des Bedienflurs)	Unbestrahlte Brennelemente	Unbestrahlte Brennelemente	Keine zwingende Rückbaurelevanz	4.2
BE-Lademaschine (SWR)	BE-Bühne bzw. Bedienflur, oberste Ebene im Reaktorgebäude, fährt über BE-Becken und RDB	Brennelemente, Steuerelemente, Drosselkörper, Neutronenquellen, kleinere Abfallbehälter, ggf. Werkzeuge und Material	Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten, Flutkompensator	Ja, u. a. für Transport abgebrannter Brennelemente und Demontage der Kerneinbauten	4.4, für Hilfshub teilweise 4.3
Reaktorgebäudekran (SWR)	Decke des Reaktorgebäudes	RDB-Deckel, SHB-Deckel, Flutkompensator, Transport- und Lagerbehälter, Abschirmriegel, RDB-Einbauten (oberes und unteres Kerngitter etc.), Beckenschütz, Dampfabscheider, Dampftrockner, allgemeine Transportvorgänge von Großkomponenten	Brennelementgestelle des BE-Lagerbeckens, RDB mit Kerneinbauten, Behälter mit Vergiftungslösung (System TW)	Ja, u. a. für Transport abgebrannter Brennelemente und Demontage der Kerneinbauten	4.3
Schwenkkran (SWR)	Reaktorgebäude Bedienflur über Hauptmontageöffnung	Unbestrahlte Brennelemente, ggf. Werkzeuge und Material	Unbestrahlte Brennelemente, Umluftanlage Bedienflur	Keine zwingende Rückbaurelevanz	4.2 (teilweise auch 4.3)
Kran im Lager für unbestrahlte Brennelemente (SWR)	Lager für unbestrahlte Brennelemente (Reaktorgebäude außerhalb des Sicherheitsbehälters, Ebene unterhalb des Bedienflurs)	Unbestrahlte Brennelemente	Unbestrahlte Brennelemente	Keine zwingende Rückbaurelevanz	4.2 (teilweise auch 4.3)

Bezeichnung	Einbauort	Typische Lasten	Sicherheitstechnisch relevante Einrichtungen in der Nähe	Rückbaurelevanz	Einstufung nach KTA 3902
Hebezeuge für den Transport radioaktiver Abfälle	Typischerweise Hilfsanlagengebäude	Filter, Fässer mit mittel- und schwachradioaktivem Abfall, ggf. Werkzeuge und Material	Behälter mit mittel- und schwachradioaktivem Abfall, Filteranlagen, Komponenten und Systeme zur Behandlung von schwachradioaktivem Abfall	Ja, während dem Rückbau erfolgt laufende Behandlung von Abfall	4.2
Hebezeuge zum Transport von aktivierten oder größeren Komponenten im Kontrollbereich	Reaktorgebäude, Ringraum oder Hilfsanlagengebäude	Komponenten, ggf. Werkzeuge und Material	Entsprechende Komponenten, sofern sicherheitsrelevant, ggf. auch andere aktivierte Komponenten, z. B. in der heißen Werkstatt	Keine zwingende Rückbaurelevanz	4.2
Zwischenlagerkran	Zwischenlager	Transportbehälter, insbesondere CASTOR	andere Transportbehälter	Ja, Einlagerung und späterer Abtransport der Transportbehälter	4.2 oder 4.3

2.4 Nationale und internationale Betriebserfahrung zu Vorkommnissen an Hebezeugen in Kernkraftwerken

Im folgenden Kapitel sollen durch eine Betrachtung der deutschen und internationalen Betriebserfahrung relevante Fehlermechanismen für Hebezeuge bestimmt werden. Da insbesondere Fehler durch softwarebasierte Steuerungssysteme erfasst werden sollen, ist die jüngere Betriebserfahrung aufgrund des in diesem Zeitraum verstärkten Einsatzes solcher Kransteuerungen von besonderem Interesse. Um also einerseits schwerpunktmäßig Ereignisse an Hebezeugen mit einem einigermaßen aktuellen technischen Stand zu betrachten und andererseits den Gesamtaufwand der Auswertung zu begrenzen, wurde die Auswertung von Kranereignisse auf den Zeitraum nach 2000 begrenzt. Es wurden daher die VERA-Datenbank der GRS und die IRS-Datenbank der IAEA auf relevante Ereignisse seit dem Jahr 2000 durchsucht.

Die Datenbank VERA (Vertiefte Auswertung) beinhaltet alle meldepflichtigen Ereignisse aus deutschen Leistungs- und Forschungsreaktoren. Diese Datenbank ist in Bezug auf meldepflichtige Ereignisse in der deutschen Betriebserfahrung vollständig.

Die Datenbank IRS (International Reporting System) beinhaltet besondere, durch die Mitgliedsländer veröffentlichte Ereignisse aus dem Anlagenbetrieb. Eine Meldepflicht besteht für Ereignisse ab einer INES-Einstufung der Stufe 2. Ereignisse an Krananlagen erreichen eine derartige Einstufung in der Regel nicht. Nationale Aufsichtsbehörden können aber nach eigenem Ermessen auch Ereignisse unterhalb dieser Einstufung in die Datenbank einpflegen, sofern sie dem Ereignis eine besondere sicherheitstechnische Bedeutung beimessen. Es kann daher nicht davon ausgegangen werden, dass die IRS-Datenbank alle Ereignisse an Hebezeugen vollständig darstellt, sie gibt aber einen Überblick über wesentliche Ereignisse.

Für den Zeitraum seit 2000 bis zum 30.05.2017 (Beginn des Vorhabens), der als Stichtag für die Berücksichtigung von Ereignissen gewählt wurde, sind in der IRS Datenbank 1275 Einträge und in der VERA 1861 Einträge vorhanden. Ereignisse nach diesem Stichtag konnten in der Auswertung nicht mehr berücksichtigt werden.

Während der Laufzeit des Vorhabens sind noch 175 Ereignismeldungen in der VERA-Datenbank und 171 Meldungen in der IRS-Datenbank hinzugekommen, die jedoch auf

Grund des Meldezeitpunkts nicht mehr für die folgende, detailliertere Auswertung herangezogen und bearbeitet werden konnten. Ein zusätzliches, verkürztes Screening zum Projektabschluss ergab, dass hiervon acht Schädigungsmechanismen verteilt auf ebenso viele Meldungen in der VERA-Datenbank und acht Schädigungsmechanismen verteilt auf drei Meldungen in der IRS-Datenbank Ereignisse an Hebezeugen sind. Davon sind wiederum zwei Schädigungsmechanismen potenziell steuerungsrelevant: Einmal ein einzelner Ausfall eines Weggebers zur Positionsmessung eines Hubwerks (deutsches Ereignis, bei Prüfung entdeckt, Ausfallursache zurzeit noch nicht abschließend geklärt) und einmal eine Unterbrechung der Signalübertragung auf Grund eines Kabelschadens (internationales Ereignis, detailliertere Ausführungen zur Ursache nicht vorhanden). Es handelt sich dabei nicht um neuartige Phänomene. Ähnliche Ereignisse sind in der Auswertung bereits enthalten und in Kapitel 2.4.5 aufgeführt.

Die Datenbanken wurden in einem mehrstufigen Prozess ausgewertet. In einem ersten Schritt wurden zunächst alle Ereignisse in den Datenbanken durchsucht und überprüft, ob Hebezeuge überhaupt eine Rolle spielten. Dies wurde an Hand des vollständigen Meldetextes der VERA- bzw. des Feldes „Basic Data“ in der IRS-Datenbank festgestellt. Im Ergebnis wurden innerhalb des Auswertezeitraums 51 meldepflichtige Ereignisse in deutschen Kernkraftwerken, bei denen Hebezeuge eine Rolle spielten, identifiziert. In der IRS-Datenbank fanden sich für den Auswertezeitraum 37 Ereignisse an Hebezeugen. Aus den oben dargelegten Gründen stellt dies nur einen Ausschnitt aus der internationalen Betriebserfahrung dar.

Aus Gründen der Vollständigkeit wurden außerdem ausgewählte Ereignisse an Krananlagen in anderen kerntechnischen Anlagen, von denen die GRS im Rahmen ihrer Tätigkeiten auf dem Gebiet der Auswertung der Betriebserfahrung kerntechnischer Anlagen Kenntnis hatte, in der Auswertung berücksichtigt. Dadurch erhöhte sich der Umfang der Auswertung um weitere sechs Ereignisse.

In einem zweiten Schritt wurden die 94 für die weitere Auswertung identifizierten Ereignismeldungen im Detail untersucht und eine Eingruppierung in Bezug auf typische Fehlerarten, -effekte und –folgen vorgenommen. Im Rahmen dieser genaueren Untersuchung zeigte sich, dass einige Meldungen mehrere Einzelereignisse umfassen. Daher wurden schlussendlich 135 Fehlermechanismen verteilt auf 94 Ereignismeldungen in der Auswertung berücksichtigt.

Als nächstes wurden die identifizierten Ereignisse je nach vorgefundenen Fehlerarten und -folgen und fehlerverursachenden Einrichtungen in verschieden Gruppen eingeteilt. Die genaue Beschreibung der verwendeten Gruppierungsschemata wird in den folgenden Unterkapiteln dargestellt. Für die Eingruppierung der Fehler wurden einige Ereignisse mehrfach berücksichtigt. Dies ist dann der Fall, wenn mehrere Fehler oder Abweichungen in Kombination auftraten oder verschiedene Fehlerfolgen möglich erscheinen.

2.4.1 Vorgehen bei Gruppierung nach Fehlerfolgen und -effekten (Ereignisarten)

Bei der Gruppierung nach Fehlerfolgen wurden insgesamt fünf Kategorien verwendet. Hierbei handelt es sich um die unterschiedlichen Arten von Konsequenzen, die sich aus den vorgefundenen Abweichungen ergeben. Wichtig ist, dass an dieser Stelle nicht zwischen einer potenziellen und einer tatsächlich eingetretenen Folge unterscheiden wurde.

- Lastabsturz
  Um einen Lastabsturz handelt es sich, wenn das zu transportierende Objekt oder Teile davon sich aus der Lastaufnahmeeinrichtung lösen und herabfallen. Dabei kommt es in der Regel zu Folgeschäden an Last und Umgebung. Ebenfalls in diese Kategorie fallen Ereignisse, bei denen auf Grund von Schädigungen beim Heben einer Last ein Absturz möglich wäre, obwohl die Spezifikationen der Last sich im Auslegungsbereich des Hebezeugs befanden. Auch die Unverfügbarkeit von Sicherheitseinrichtungen, die Lastabstürze verhindern sollen, fallen in diese Kategorie.

- Selbstzerstörung oder -schädigung
  In diese Kategorie fallen Ereignisse, bei denen durch Betrieb unter nicht auslegungsgemäßen Randbedingungen einzelne Komponenten der Krananlage beschädigt werden oder Schutzeinrichtungen zur auslegungsgemäßen Auslösung gebracht werden. Die Folge ist, dass die Anlage dann nicht mehr weiter betrieben werden kann oder bei potenziellen Ausfällen eine baldige Unverfügbarkeit absehbar ist. Allerdings ist in Abgrenzung zu den entsprechenden Fehlerfolgen ohne weitere Ausfälle oder Fehler kein Lastabsturz und keine Kollision möglich.

- Kollision mit Umgebungselementen
  Bei diesen Ereignissen kam es zu einem ungeplanten Kontakt des Hebezeugs oder der Last mit anderen Gegenständen oder Teilen der Umgebung. Als Umgebung werden in diesem Zusammenhang Gegenstände betrachtet, die im Rahmen des Trans-

portvorgangs plangemäß nicht bewegt werden sollen. Häufig gehen auch diese Kontakte mit Schäden an Last oder Umgebung einher. Auch die Unverfügbarkeit von Sicherheitseinrichtungen, die derartige Kollisionen verhindern sollen, fallen in diese Kategorie. Diese Fehlerfolge ist zu unterteilen in:

- Fehler, bei denen sich das Element der Umgebung an unzulässiger Position befindet
- Fehler, bei denen sich die Last während des Transports in unzulässiger Position befindet
- Fehler, bei denen der Kran auf eine unzulässige Position fährt

- Unvorhergesehener Kontakt Hebezeug-Last
  Gemeint ist hier nicht der ordnungsgemäße Kontakt zwischen Lastaufnahme- oder Tragmittel und Last bei einem normalen Hebevorgang, sondern ein nicht auslegungsgemäßer Kontakt zwischen Teilen des Hebezeugs und der Last, beispielsweise durch Schwing- oder Pendelvorgänge der Last. Bei dem Teil des Hebezeugs kann es sich aber prinzipiell auch um das Lastaufnahmemittel handeln, beispielweise bei einer versehentlichen Kollision zwischen dem ungeöffnetem Lastaufnahmemittel und der Last oder bei fehlerhaften Ausklink- oder Absetzvorgängen, bei denen die Verbindung irrtümlich bestehen bleibt. Die Folgen sind potenzielle Schäden an Hebezeug und Last. Diese Fehlerfolge ist zu unterteilen in:
  - Fehler, bei denen das Lastaufnahmemittel nicht aufnahmebereit ist
  - Fehler, bei denen sich die Last vor, während oder nach Transport in unzulässiger Position befindet
  - Fehler, bei denen die falsche Last gehoben wird
  - Fehler, bei denen der Kran auf eine unzulässige Position fährt

- Nuklearspezifische Verriegelung nicht wirksam
  Es gibt eine größere Anzahl an häufig anlagen- und hebezeugspezifischen Verriegelungen, die besondere sicherheitstechnische Einschränkungen, die für Hebezeuge in Nuklearanlagen gelten, abbilden. Beispielsweise kann es Beschränkungen für den Transport von schweren Lasten über sicherheitstechnisch relevante Komponenten hinweg geben, um eine auslegungsüberschreitende Belastung für diese Komponenten bei einem Lastabsturz zu verhindern. Aus Gründen des Strahlen-

schutzes oder der Kritikalitätssicherheit kann es Beschränkungen hinsichtlich der zulässigen Kranbewegungen und Abstellplätze geben, die abhängig von der Positionierung dritter Komponenten, die am Hebevorgang an sich nicht beteiligt sind (z. B. Abschirmungen oder andere Brennelemente), geben. Ereignisse, bei denen diese Verriegelungen oder Regelungen nicht funktionsfähig waren, werden in dieser Kategorie gesammelt. Dabei muss es in der Folge nicht zwingend zu Schäden gekommen sein, es ist ausreichend, wenn unzulässige Vorgänge durchgeführt wurden oder möglich gewesen wären.

2.4.2 Vorgehen bei der Bestimmung der fehlerverursachenden Einrichtung

Normalerweise sind Abweichungen an einer oder mehreren (Teil-)Einrichtungen des Krans für das Auftreten des Fehlers und seiner Fehlerfolgen ursächlich. Hierbei wurde unterschieden zwischen:

- Abweichungen an der Last selbst
- Abweichungen an den Lastaufnahmemitteln (Körbe, Transportgestelle, Traversen o. ä.)
- Abweichungen an den Anschlagmitteln (Seile oder ähnliche Verbindungen mit denen das Lastaufnahmemittel mit dem Tragmittel verbunden wird)
- Abweichungen an den Tragmitteln (Greifer, Haken o. ä.). Diese sind im Unterschied zu Lastaufnahmemitteln permanent mit dem Hebezeug verbunden.
- Abweichungen an Hubseilen, auch Ereignisse an Haltekabeln oder Stahlseilen werden in diese Kategorie eingestuft
- Abweichungen an der Laufkatze oder den Laufschienen
- Abweichungen am Antriebsstrang bzw. der Triebwerkskette: Diese besteht aus einem oder mehreren Motoren, Antriebswellen, ggf. auch Getrieben. Motorschutzeinrichtungen und Leistungsschalter oder -schütze der Elektromotoren wurden auch in diese Kategorie eingestuft.
- Abweichungen an der Bremse (Wellen und Naben, die die Bremse mit der Seiltrommel verbinden, sind in der Auswertung der Bremse zugeschlagen, da bei einem Bruch die Bremse unverfügbar wird). Grundsätzlich könnte eine Bremse,

die nicht als separate Sicherheitsbremse getrennt von der Triebwerkskette ausgeführt ist, auch der Triebwerkskette selbst zugeschlagen werden. Da für viele ausgewertete IRS-Ereignisse, der Aufbau des Hebezeugs nicht in einem Detaillierungsgrad bekannt ist, der eine derartige Unterscheidung zuließe, wurde beschlossen Ereignisse an den Bremsen grundsätzlich in eine separate Kategorie zu überführen.

- Abweichungen an der mechanischen Krankonstruktion (Türme, Masten, Stützen oder sonstige Teile des Tragwerks o. ä.)
- Abweichungen an Laufrädern, dies umfasst auch Abweichungen an den Achsen, Wellen und insbesondere den Lagern von Laufrädern
- Abweichungen an der Seiltrommel
- Abweichungen in der Steuerung, dies wurde noch einmal weiter unterteilt in die Unterkategorien
    - Messwerterfassung,
    - Signalverarbeitung,
    - Parametrierung,
    - Signalübertragung
    - und Eingabe- und Ausgabegeräte.
- Abweichungen an Armaturen/Schiebern/Verschlüssen: Diese Kategorie betrifft Ereignisse an den BE-Lademaschinen von Schwerwasser-, RBMK- oder AGR-Reaktoren. Bei diesen werden die entsprechenden BE-Wechselvorgänge im Leistungsbetrieb der Anlage durchgeführt, weshalb sie auch mit Primärkühlmittel gefüllte und entsprechend dem Kühlmitteldruck unter Druck stehende Aufnahmegefäße aufweisen. Für die Befüllung und Entleerung zu Prüfzwecken und für andere betriebliche Vorgänge gibt es dort auch Armaturen und Schieber, die unter den genannten Betriebsbedingungen arbeiten müssen und Verschlüsse, die zu Revisionszwecken geöffnet werden und im Leistungsbetrieb Dichtheitsanforderungen erfüllen müssen.
- Abweichungen an einem Element der Umgebung, das weder zum Hebezeug noch zur Last gehört. Diese Kategorie wurde typischerweise bei Kollisionsereignissen gewählt, wenn das Hebezeug mit einer fehlplatzierten Komponente, die

nicht zu Hebezeug oder Last gehört, kollidierte. In Abgrenzung zu der Einstufung „Abweichungen in Bezug auf den Fahrweg“ liegt in diesen Fällen eine unzulässige Positionierung des Umgebungselements oder eine anderweitige mangelnde Gängigkeit, z. B. durch Schäden am Umgebungselement, vor.

- Abweichungen in Bezug auf den Fahrweg: Unter diese Zuordnung fallen Ereignisse, die darauf zurückzuführen sind, dass von der Betriebsmannschaft ein im konkreten Fall unzulässiger Fahrweg gewählt wurde. Die Folge ist häufig eine Kollision mit einem Umgebungselement. In einigen Fällen kommt es aber auch zur Verletzung von nuklearspezifischen Verriegelungen, wenn beispielsweise Abschirmeinrichtungen nicht platziert wurden. In Abgrenzung zu der Einstufung „Abweichungen an einem Element der Umgebung“ war die Positionierung des Gegenstandes, mit dem das Hebezeug kollidierte, in diesen Fällen ordnungsgemäß.

- Fehlpositionierung: Diese Zuordnung betrifft Transporte von Brennelementen. Abhängig von der jeweiligen Anreicherung und dem bisherig erreichten Abbrand sieht der Beladeplan für RDB, BE-Becken oder Transportbehälter aus Gründen der Kritikalitätssicherheit oder der Nachwärmeabfuhr für jedes Brennelement eine bestimmte Positionierung vor. Kommt es irrtümlich zu Abweichungen vom Beladeplan, liegt eine Fehlpositionierung vor. Dabei kommt es nicht zu Kollisionen oder Schäden an Kran, Last oder Umgebungselementen. Der Transportvorgang selbst funktioniert quasi ordnungsgemäß, es werden allerdings in Folge des Transportvorgangs Vorgaben zur Unterkritikalität, zum Nachwärmeeintrag oder zur zulässigen Ortsdosisleistungen verletzt.

- Sonstige Abweichungen: Ein Sammelbegriff für alle technischen Fehler, die nicht in die obigen Kategorien einstufbar sind. In der Auswertung wurde Malwarebefall und fehlerhafte Prüfanweisungen, sowie Ausfälle an Schiebern (Linearaktoren) als Ereignisse, die in diese Sammelkategorie fallen, identifiziert.

2.4.3 Vorgehen bei Gruppierung nach Fehlerarten

Bei der Eingruppierung nach Fehlerarten wurde zwischen folgenden Fehlerarten unterschieden:

- Bedienfehler (Human Factor)
  Diese Fehlerart bezeichnet Ereignisabläufe, bei denen das vor Ort handelnde Personal bei einem Hebevorgang entweder vorgesehene Handlungen unterlässt (z. B. indem Hindernisse im Fahrweg nicht geräumt werden), falsch ausführt (z. B. wenn Hindernisse „zu knapp“ umfahren werden) oder Handlungen vornimmt, die nicht vorgesehen sind (z. B. Überbrückung der Fahrwegsbegrenzung)

- Herstellungsfehler
  Diese Fehlerart wird für Ereignisse verwendet, bei denen es im Herstellungsprozess von einzelnen Komponenten oder Bauteilen des Hebezeugs zu Abweichungen kam, auf Grund denen die Komponenten oder Bauteile nicht die in den Spezifikationen vorgesehenen Eigenschaften besitzen (z. B. Einschlüsse in einer Welle oder einem Haken, durch die der effektive lasttragende Querschnitt verringert wird). Verantwortlich ist hierbei das Personal in der Produktion des Herstellers.

- Montagefehler
  Ereignisse werden unter dieser Fehlerart eingestuft, wenn sie ihre Ursache in der nicht sachgerechten Montage, also im Aufbau des Hebezeugs vor der Inbetriebsetzung, haben (z. B. nicht sauber zentrierte Bauteile, nicht wie spezifiziert angezogene Schrauben). Verantwortlich kann abhängig von Bauteil und Montagezeitpunkt Personal des Herstellers oder des Betreibers des Hebezeugs sein.

- Alterung bzw. Wartungs- und Instandhaltungsfehler
  Bei diesen Ereignissen wurden im Rahmen der Wartung und vorbeugenden Instandhaltung notwendige Tätigkeiten entweder unterlassen oder fehlerhaft ausgeführt, so dass es in der Folge zu einem Ausfall kam. Auch alterungsbedingte Ausfälle (z. B. ein Ermüdungsbruch) fallen in diese Kategorie, weil in derartigen Fällen ein rechtzeitiger Austausch der betroffenen Komponente oder eine anders geartete vorbeugende Instandhaltung angezeigt gewesen wäre.

- Auslegungsfehler
  In diese Fehlerart werden Ereignisse eingestuft, bei denen entweder Komponenten sich im Betrieb anders verhielten als in der Auslegung geplant (z. B. wenn eine Komponente schwerer ist, als in der mechanischen Auslegung angenommen und

dadurch eine Überbelastung entsteht) oder Betriebsbedingungen auftreten, die während der Auslegung nicht unterstellt wurden (z. B. wenn Komponenten Kräfte abtragen müssen, ohne dass dies geplant war).

- Unbekannt
  In einigen Fällen lagen der GRS nicht genug Informationen vor, um eine Einstufung bezüglich der Fehlerart vorzunehmen. Dies ist üblicherweise dann der Fall, wenn zwar die ausgefallene Komponente oder das ausgefallene Bauteil benannt wurden, aber nicht weiter spezifiziert wurde, weshalb es ausfiel.

- Sonstiges
  Diese Einstufung wurde für ein Ereignis gewählt, bei dem nach einem Lastabsturz festgestellt wurde, dass die mit dem Hebezeug transportierten Lasten Anforderungen an die mechanische Festigkeit nicht immer erfüllen und daraufhin das Hebezeug und insbesondere die Steuerung angepasst wurden, um auch diese Lasten transportieren zu können. Ein Fehler im eigentlichen Sinne bezüglich der ursprünglichen Auslegung bestand nicht.

2.4.4 Gruppierung der Ereignisse und Auswertung

Werden die Ereignisse nun nach Fehlerfolgen, wie in Kapitel 2.4.1 dargestellt, gruppiert, ergibt sich eine Darstellung wie Abb. 2.2.

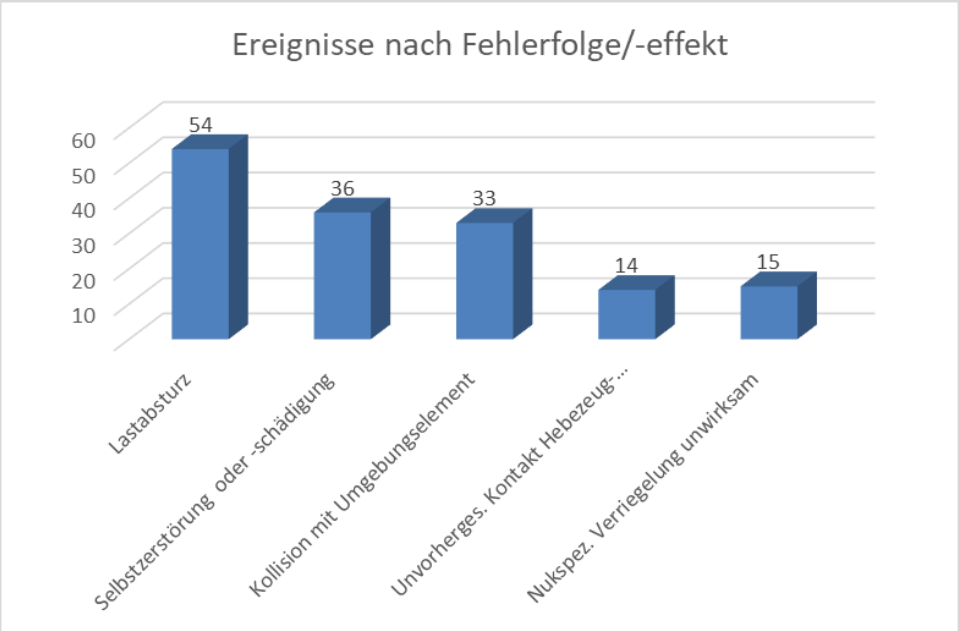

Abb. 2.2 Ereignisse an Krananlagen nach Fehlereffekt/-folge gruppiert

Man kann die Ereignisse noch genauer unterscheiden, z. B. zwischen Ereignissen, bei denen es lediglich potenziell zu entsprechenden Fehlerfolgen hätte kommen können, dies aber z. B. bei Prüfungen bemerkt wurde und Ereignissen, bei denen es tatsächlich zu entsprechenden Fehlern und Fehlerfolgen kam. Dies ist insbesondere bei den schwerwiegenderen Fehlerfolgen wie z. B. Lastabstürzen eine wichtige Distinktion. Außerdem fällt auf, dass die Gesamtanzahl der in Abb. 2.2 aufgeführten Ereignisse größer als die in Kapitel 2.4 angegebenen 135 Ereignisse ist. Dies liegt daran, dass einige Ereignisse mehrere potenzielle Fehlerfolgen und -effekte haben. In Abb. 2.3 sind die Säulen noch einmal farblich aufgeteilt in potenzielle (grün) und tatsächliche Ereignisse (blau). Ereignisse mit mehreren Fehlereffekten sind als (MF) gekennzeichnet und farblich abgehoben (tatsächliche Ereignisse rot, potenzielle Ereignisse lila). Diese farbliche Konvention wird im ganzen folgenden Kapitel beibehalten.

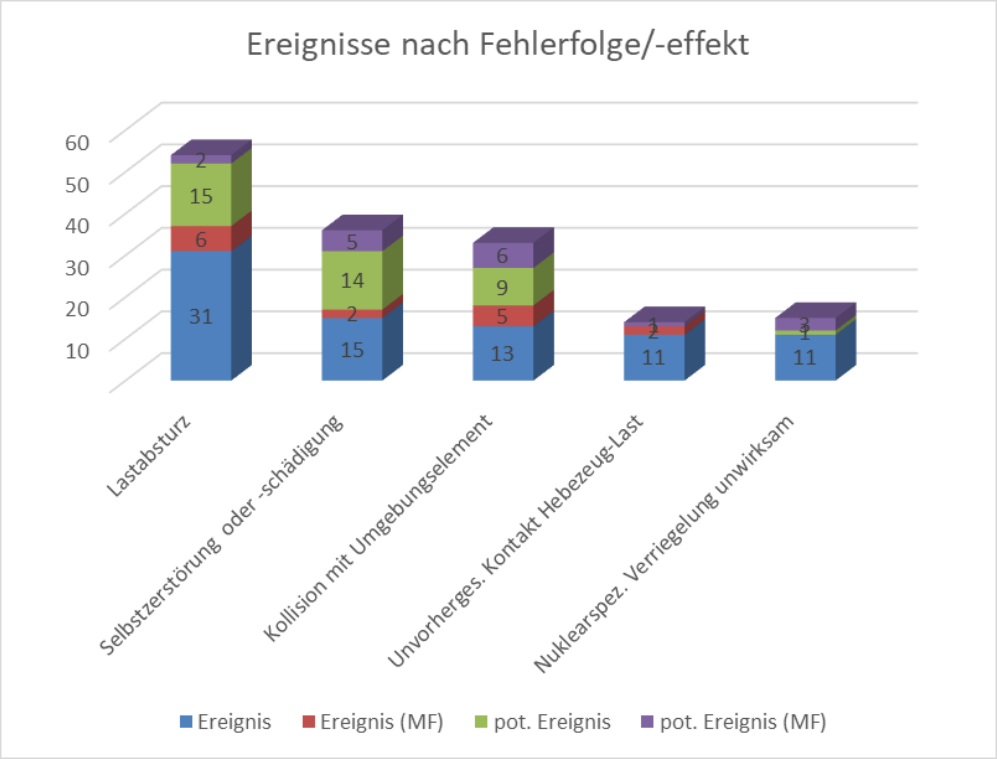

Abb. 2.3 Ereignisse an Krananlagen nach Fehlereffekt/-folge gruppiert mit Unterscheidung nach potenziellen und tatsächlichen Ereignissen und mit Hervorhebung von Ereignissen mit mehreren Fehlereffekten

Es fällt in diesem Zusammenhang auf, dass potenzielle Ereignisse sich hauptsächlich auf die Fehlereffekte Lastabsturz, Selbstzerstörung oder -schädigung und Kollision mit einem Umgebungselement verteilen.

2.4.4.1 Lastabsturz

Unterscheidet man die 54 identifizierten Ereignisse mit der Fehlerfolge Lastabsturz gemäß den jeweils für den potenziellen oder tatsächlichen Lastabsturz ursächlichen Einrichtung entsprechend der Darstellung in Kapitel 2.4.2, so ergibt sich die in Abb. 2.4 dargestellte Aufteilung. In die Gruppe Sonstige fällt ein Ereignis mit Schadsoftwareeintrag, bei dem keine realen Ausfälle beobachtet wurden, da die Schadsoftware dafür nicht geeignet war. Potenziell wären allerdings sehr vielfältige Fehlereffekte und beeinflussbare Einrichtungen durch eine Schadsoftware denkbar.

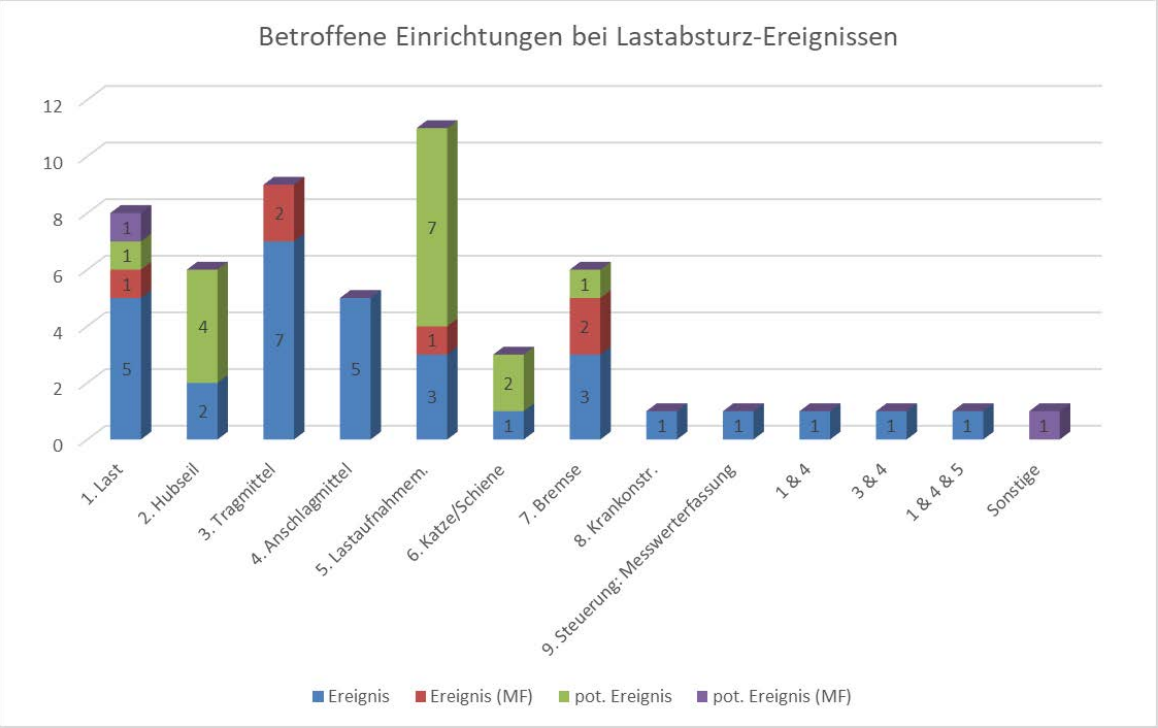

Abb. 2.4 Lastabsturz-Ereignisse gruppiert nach fehlerauslösender Einrichtung

Gruppiert nach Fehlerarten entsprechend den Definitionen in Kapitel 2.4.3 ergibt sich Abb. 2.5. Bei dem Ereignis, dass unter „Sonstige“ eingestuft wurde, wurden auf Grund

eines Lastabsturzes die Auslegungsgrundlagen eines Hebezeugs angepasst. Die zu transportierende Last war zerbrochen, da sie Vorschädigungen aufwies. Neben anderen Maßnahmen zur Vermeidung von Vorschädigungen, wurden auch Maßnahmen ergriffen um entsprechend vorgeschädigte, mechanisch instabilere Lasten transportiert zu können. Dadurch war es notwendig verschiedene Parameter der Steuerung anzupassen (z. B. maximale Geschwindigkeit etc.).

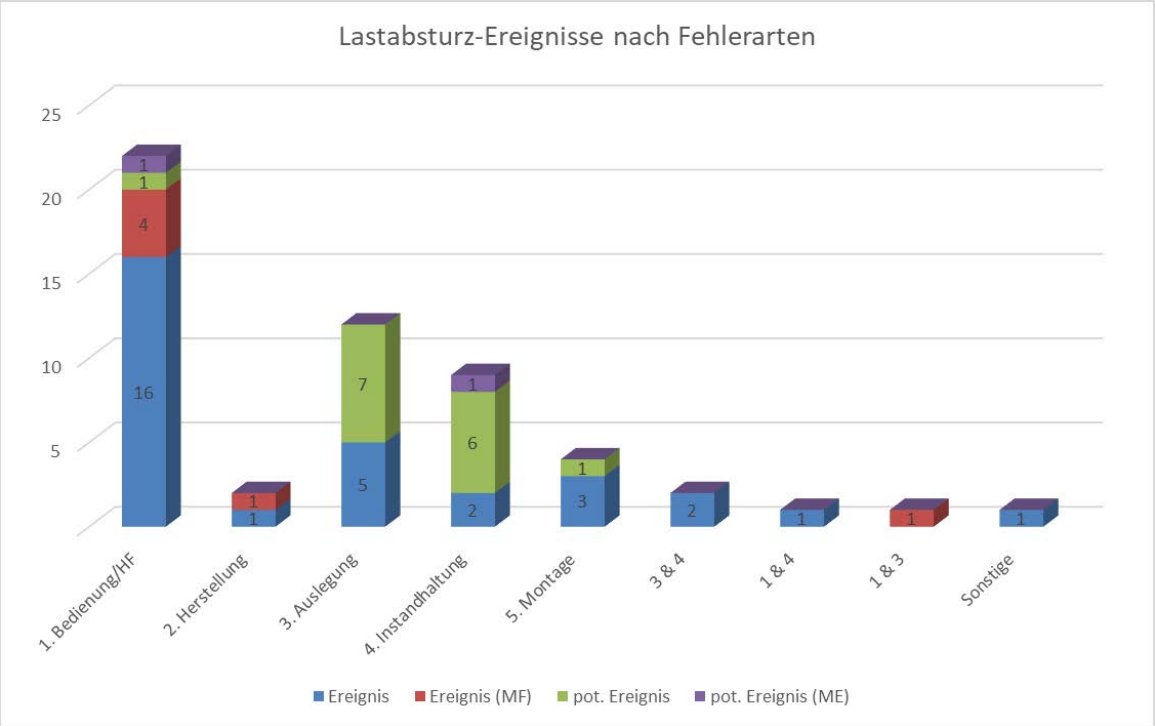

Abb. 2.5 Lastabsturz-Ereignisse gruppiert nach Fehlerart

Im Rahmen der Auswertung der Lastabsturz-Ereignisse wurden verschiedene Schwerpunkte festgestellt:

- Es wurden insgesamt sechs Ereignisse bei denen Lastaufnahmeeinrichtungen oder Katzen bzw. Schienen nicht ausreichend gegen Erdbeben qualifiziert oder ausgelegt waren gefunden (Auslegungsfehler). Bei diesen Ereignissen handelt es sich schwerpunktmäßig um IRS-Ereignisse aus den Vereinigten Staaten, es kam dabei nicht zu tatsächlichen Lastabstürzen.
- Es wurden insgesamt vier Ereignisse gefunden, bei denen Lasten gehoben wurden, die schwerer als für das Hebezeug zulässig waren. In der Folge kam es zu Lastabstürzen. Es handelt sich auch hierbei um IRS-Ereignisse.

- Es wurden insgesamt sieben Ereignisse gefunden, bei denen Tragmittel nicht korrekt geschlossen oder geöffnet hatten. Dies wurde trotz teilweise bestehenden Meldefunktionen jeweils vor dem Fortsetzen des Hebevorgangs nicht bemerkt (Bedienfehler/HF). Diese Ereignisse verteilen sich auf alle ausgewählten Quellen, es kam in der Folge jeweils zu tatsächlichen Lastabstürzen.
- Es wurden insgesamt sieben Ereignisse gefunden, bei denen Seil, Spleiss- oder Schlingverbindungen entweder unfachmännisch oder mit nicht dafür zugelassenen Seilen eingerichtet worden waren. Abgesehen von einer Ausnahme handelt es sich hierbei um IRS-Ereignisse aus Russland. Es kam in der Folge jeweils zu tatsächlichen Lastabstürzen.

2.4.4.2 Selbstschädigung oder -zerstörung

Von den 36 ausgewerteten Ereignissen des Fehlereffekts „Selbstschädigung oder -zerstörung“ hatten 21 ihre Ursache in Ausfällen von Steuer- und Überwachungseinrichtungen.

Gruppiert nach den Kategorien der fehlerverursachenden Einrichtungen, wie sie in Kapitel 2.4.2 definiert wurden ergibt sich für diese Ereignisse Abb. 2.6. In die Gruppe Sonstiges fällt dabei ein Ereignis mit Schadsoftwareeintrag, bei dem keine realen Ausfälle beobachtet wurden, da die Schadsoftware dafür nicht geeignet war. Potenziell wären allerdings sehr vielfältige Fehlereffekte und beeinflussbare Einrichtungen durch eine Schadsoftware denkbar.

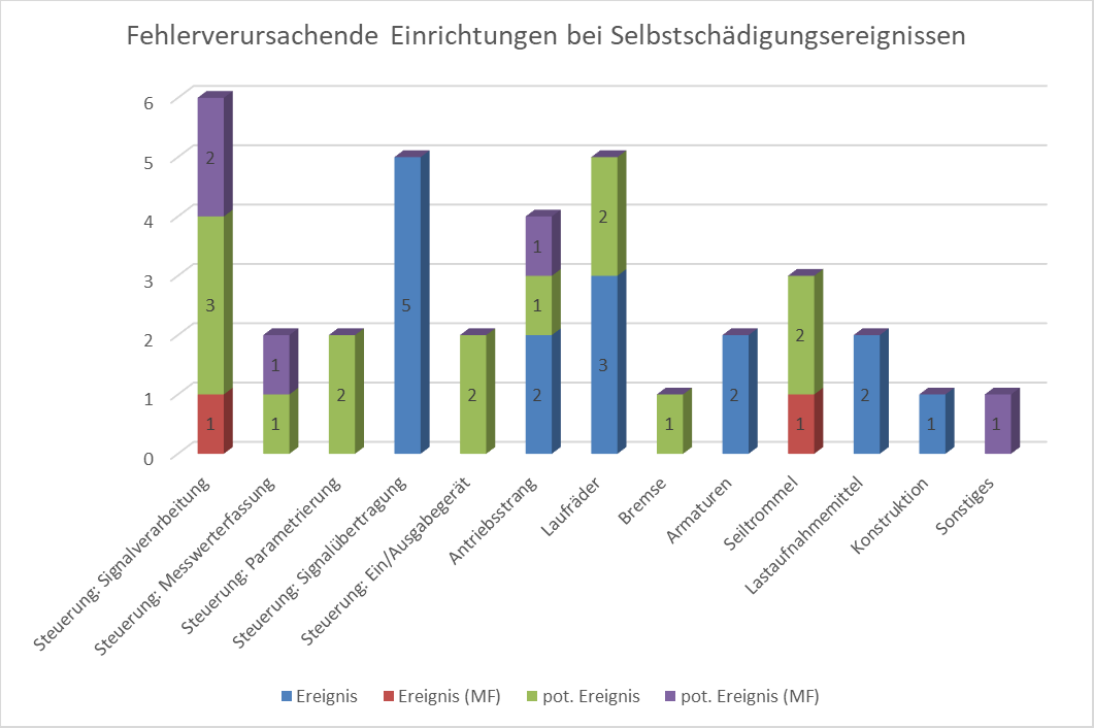

Abb. 2.6 Selbstschädigungsereignisse gruppiert nach der fehlerverursachenden Einrichtung

Gruppiert nach Fehlerarten entsprechend den Definitionen in Kapitel 2.4.3 ergibt sich Abb. 2.7. Mit der Fehlerart „Unbekannt“ wurden Ereignisse eingestuft, bei denen eine detailliertere Ursachenanalyse nicht vorliegt oder die Ursache nicht so genau ermittelt werden konnte, dass eine Einstufung der Fehlerart möglich wäre.

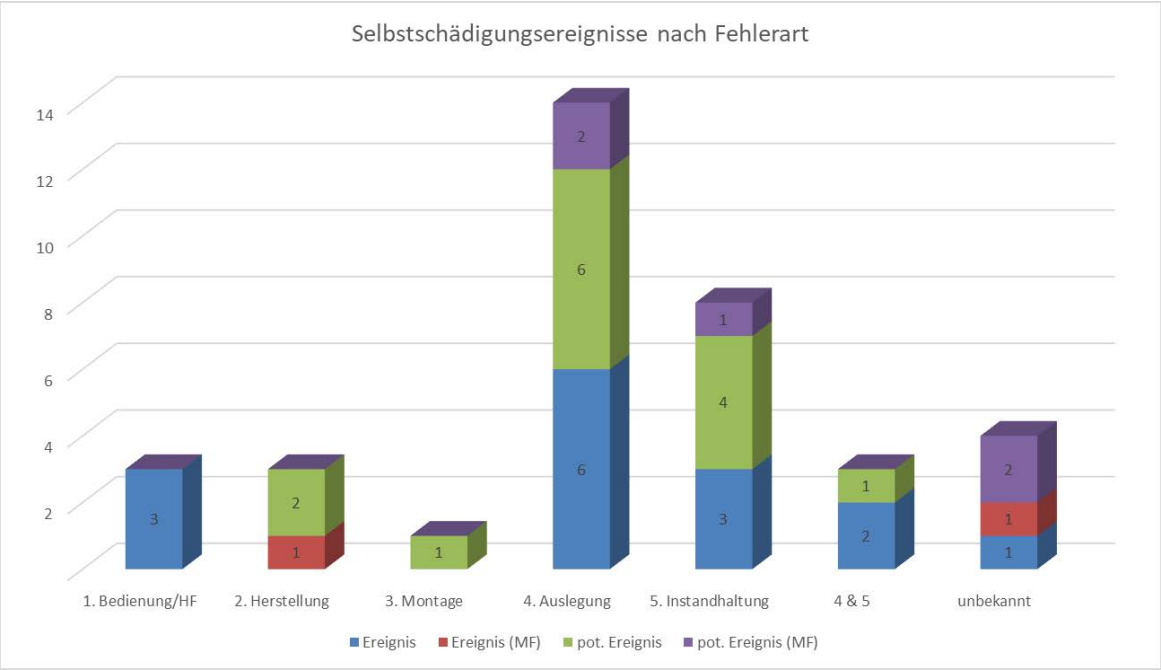

Abb. 2.7 Selbstschädigungsereignisse gruppiert nach Fehlerarten

Im Rahmen der Auswertung der Selbstschädigungsereignisse wurden drei Schwerpunkte festgestellt:

- Fünf der ausgewerteten Ereignisse basierten auf einer Serie von meldepflichtigen Ereignissen in einer deutschen Anlage, bei der mehrere Abweichungen in der Steuerung der BE-Lademaschine gefunden wurden. Die GRS hat zu diesen Ereignissen auch zwei Weiterleitungsnachrichten verfasst.
- Sieben der ausgewerteten Ereignisse basierten auf einem meldepflichtigen Ereignis in einer deutschen sonstigen kerntechnischen Anlage, die im Rahmen der Auswertung von zusätzlichen Ereignissen in die Auswertung aufgenommen wurde und hierbei für die Bewertung in mehrere Teilereignisse aufgeteilt wurde. Auch hier wurde eine größere Anzahl von Abweichungen festgestellt, mehrheitlich im Bereich der Steuerung. Die sicherheitstechnische Bedeutung der Ereignisse ist allerdings zum Teil sehr gering und wären für einige Ereignisse für sich genommen auch nicht meldepflichtig.
- Es wurden insgesamt fünf Ereignisse gefunden, bei denen Probleme an Kabelschleppsystemen oder anderen Kabelläufen ursächlich waren. Die Folge waren dann Unterbrechungen der Kabelverbindungen. Betroffen waren sowohl Signal- als auch Leistungskabel. Es ließ sich kein Schwerpunkt bezüglich der Herkunft der Ereignisse feststellen.

2.4.4.3 Kollision mit einem Umgebungselement

Dem Fehlereffekt „Kollision mit einem Umgebungselement“ waren 33 der ausgewerteten Ereignisse zuzuordnen.

Gruppiert nach den Kategorien der fehlerverursachenden Einrichtungen, wie sie in Kapitel 2.4.2 definiert wurden, ergibt sich für diese Ereignisse Abb. 2.8. Ereignisse, bei denen die Krananlage selbst keine Fehler aufwies, sind dabei in der Mehrzahl. Die Kategorien „Umgebungselement“ und „Last“ enthalten Ereignisse, bei denen die Krananlage ebenfalls fehlerfrei arbeitete, aber Abweichungen an der Last oder Umgebungselementen zu einer Kollision führten. In der Regel handelt es sich dabei um schadensbedingt hervorstehende Teile, die zu einer Kollision führten. In die Kategorie Sonstiges fällt ein Ereignis mit Schadsoftwareeintrag, bei dem keine realen Ausfälle beobachtet wurden,

da die Schadsoftware dafür nicht geeignet war. Potenziell wären allerdings sehr vielfältige Fehlereffekte und beeinflussbare Einrichtungen durch eine Schadsoftware denkbar. Ein weiteres Ereignis in dieser Kategorie ist ein Ereignis bei dem defizitäre Prüfunterlagen dazu führten, dass Sicherheitseinrichtungen nicht geprüft und somit potenziell weniger zuverlässig waren

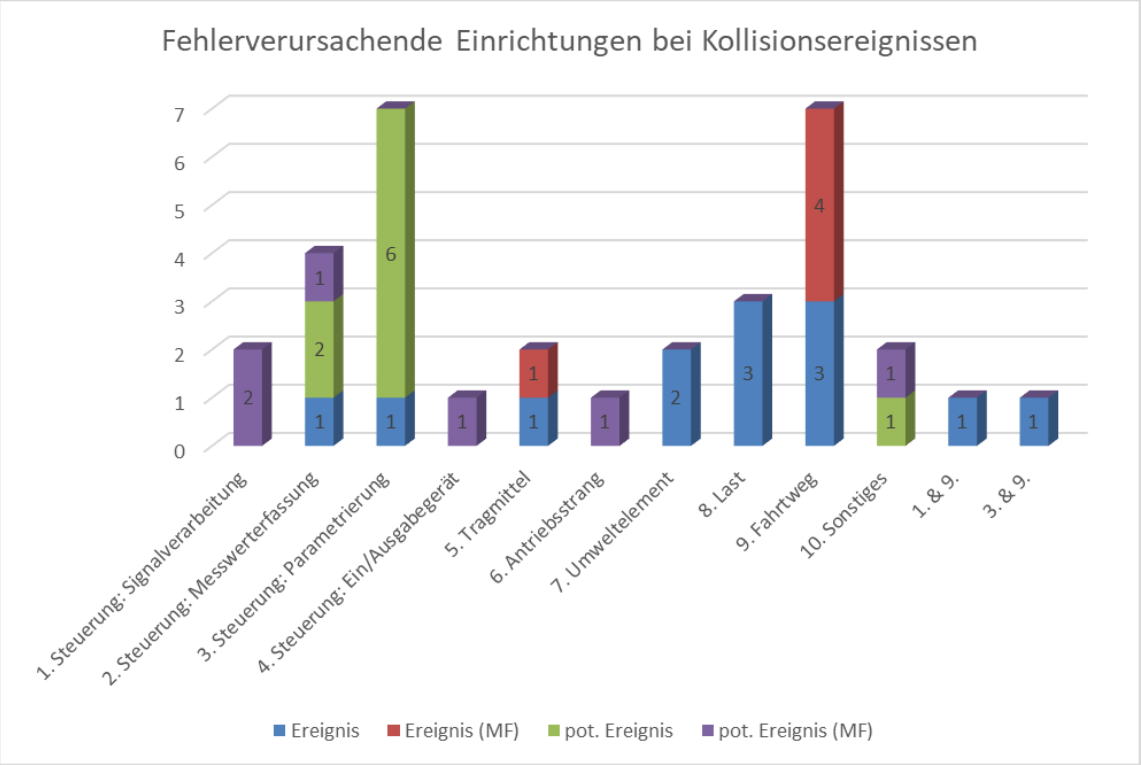

Abb. 2.8 Kollisionsereignisse gruppiert nach der fehlerverursachenden Einrichtung

Gruppiert nach Fehlerarten entsprechend den Definitionen in Kapitel 2.4.3 ergibt sich für Ereignisse mit dem Fehlereffekt Kollision mit einem Umgebungselement Abb. 2.9. Hierbei wurde noch unterschieden, ob ursächlich für die Kollision Abweichungen am Hebezeug selbst, an der Last oder an dem Umgebungselement, mit dem das Hebezeug oder die Last kollidierte, waren. Mit der Fehlerart „Unbekannt“ wurden Ereignisse eingestuft, bei denen eine detailliertere Ursachenanalyse nicht vorliegt oder die Ursache nicht so genau ermittelt werden konnte, dass eine Einstufung der Fehlerart möglich wäre.

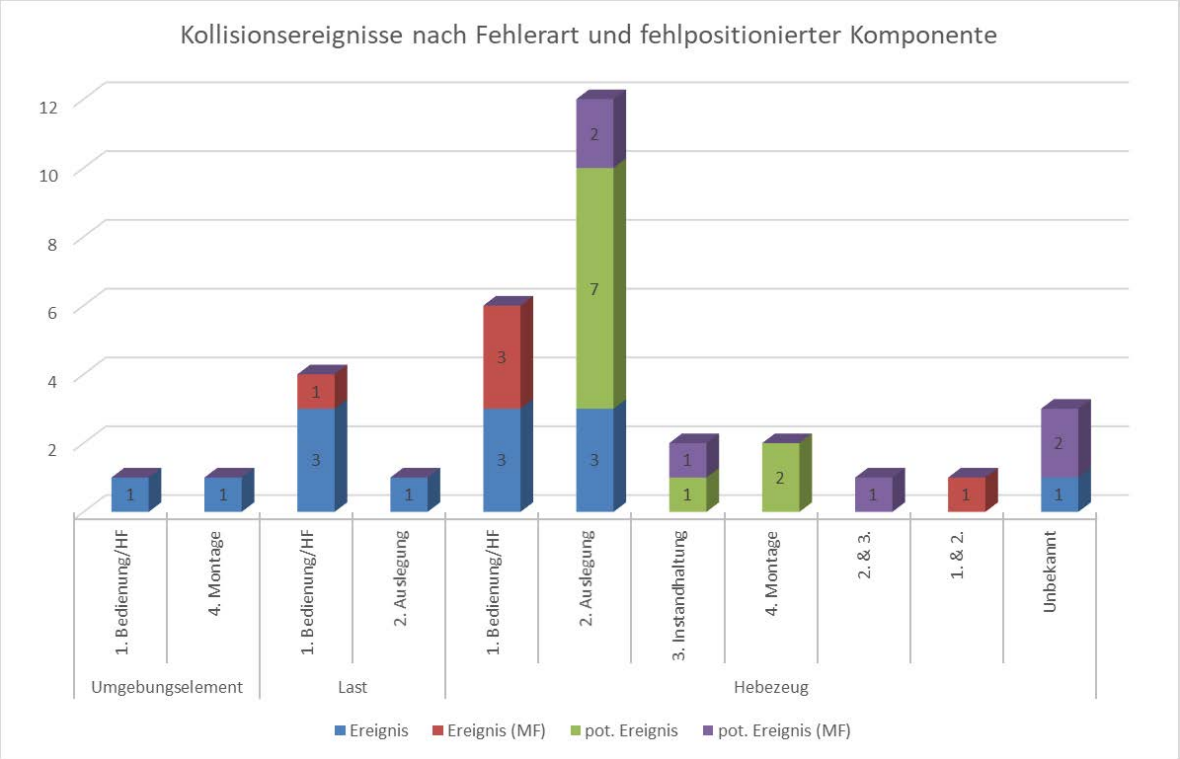

Abb. 2.9 Kollisionsereignisse gruppiert nach Fehlerarten

Im Rahmen der Auswertung der Kollisionsereignisse wurden zwei Schwerpunkte festgestellt:

- Es wurden insgesamt neun Einzelereignisse mit Auslegungsfehlern, die potenziell zu einer Kollision des Hebezeugs mit der Umgebung führen könnten, beobachtet. Sechs dieser Einzelereignisse basieren auf zwei meldepflichtigen Ereignissen in deutschen Anlagen, bei denen verschiedene einzelne separate Abweichungen und Fehler in der Steuerung festgestellt wurden. Im Rahmen der Auswertung wurden diese Abweichungen jeweils als separate Einzelereignisse betrachtet. Die GRS hat zu einem dieser Ereignisse auch zwei Weiterleitungsnachrichten verfasst.
- Ein weiterer Schwerpunkt waren mit vier Einzelereignissen Vorkommnisse, bei denen die Zentrierung des Hebezeugs beim Heben oder Absetzen von Brennelementen mit der BE-Lademaschine unzureichend waren, wodurch es zu Kollisionen bzw. einem ungeplanten Aufsetzen kam. Weitere Ereignisse dieser Art sind dem Fehlereffekt „Ungeplanter Kontakt Kran - Last“ zuzuordnen.

2.4.4.4 Unvorhergesehener Kontakt Hebezeug – Last

Dem Fehlereffekt „Unvorhergesehener Kontakt Hebezeug - Last“ waren 14 der ausgewerteten Ereignisse zuzuordnen.

Gruppiert nach den Kategorien der fehlerverursachenden Einrichtungen, wie sie in Kapitel 2.4.2 definiert wurden, ergibt sich für die Ereignisse mit diesem Fehlereffekt Abb. 2.10. Es handelt sich dabei fast ausschließlich um Ereignisse, bei denen die Krananlage selbst keine Fehler aufwies. Die Kategorie „Lastaufnahmemittel“ und „Tragmittel“ enthalten hier Ereignisse, die zumeist auf menschliches Fehlverhalten zurückzuführen sind. Dabei handelt es sich beispielsweise um Ereignisse, bei denen die Last zu früh freigegeben wurde, wodurch sie sich am Hebezeug verkantete. Bei anderen Ereignissen wurde die Last irrtümlich gar nicht freigegeben oder Haltebolzen oder Lastaufnahmemittel wurden nicht ordnungsgemäß demontiert, so dass es beim weiteren Verfahren des Hebezeugs zu einem teilweisen Wiederanheben der Last kam oder ähnliches. In die Kategorie Sonstiges fällt ein Ereignis mit Schadsoftwareeintrag, bei dem keine realen Ausfälle beobachtet wurden, da die Schadsoftware dafür nicht geeignet war. Potenziell wären allerdings sehr vielfältige Fehlereffekte und beeinflussbare Einrichtungen durch eine Schadsoftware denkbar. Außerdem wurde ein Ereignis in diese Kategorie eingestuft, bei dem durch den Betrieb einer Beckenpumpe während des Transports einer Last im BE-Becken diese zu Schwingungen angeregt wurde, wodurch es zu einer Kollision und nachfolgend zu einem Verhaken der Last mit dem Hebezeug kam. Außerdem wurde ein Ereignis in einem Schwerwasserreaktor dieser Kategorie zugeordnet, bei dem ein Schieber (Linearaktor), der die Brennelemente horizontal bewegt, einen Defekt aufwies.

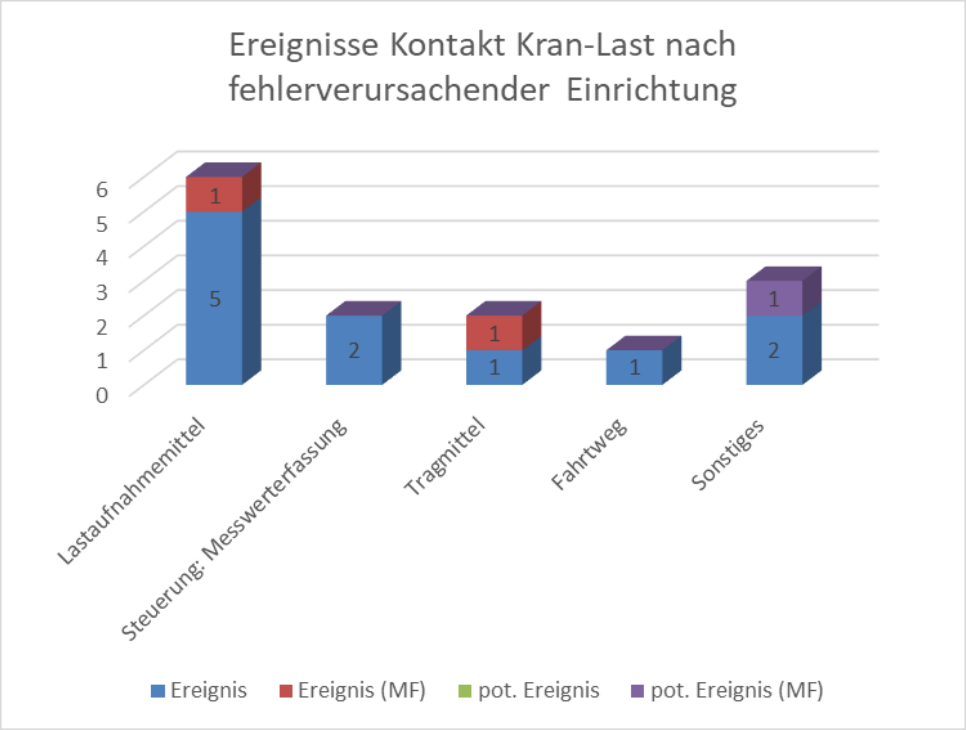

Abb. 2.10 Ereignisse mit unvorhergesehenem Kontakt zwischen Kran und Last gruppiert nach der fehlerverursachenden Einrichtung

Gruppiert nach Fehlerarten entsprechend den Definitionen in Kapitel 2.4.3 ergibt sich für Ereignisse mit dem Fehlereffekt unvorhergesehenem Kontakt zwischen Kran und Last Abb. 2.11. Mit der Fehlerart „Unbekannt“ wurden Ereignisse eingestuft, bei denen eine detailliertere Ursachenanalyse nicht vorliegt oder die Ursache nicht so genau ermittelt werden konnte, dass eine Einstufung der Fehlerart möglich wäre.

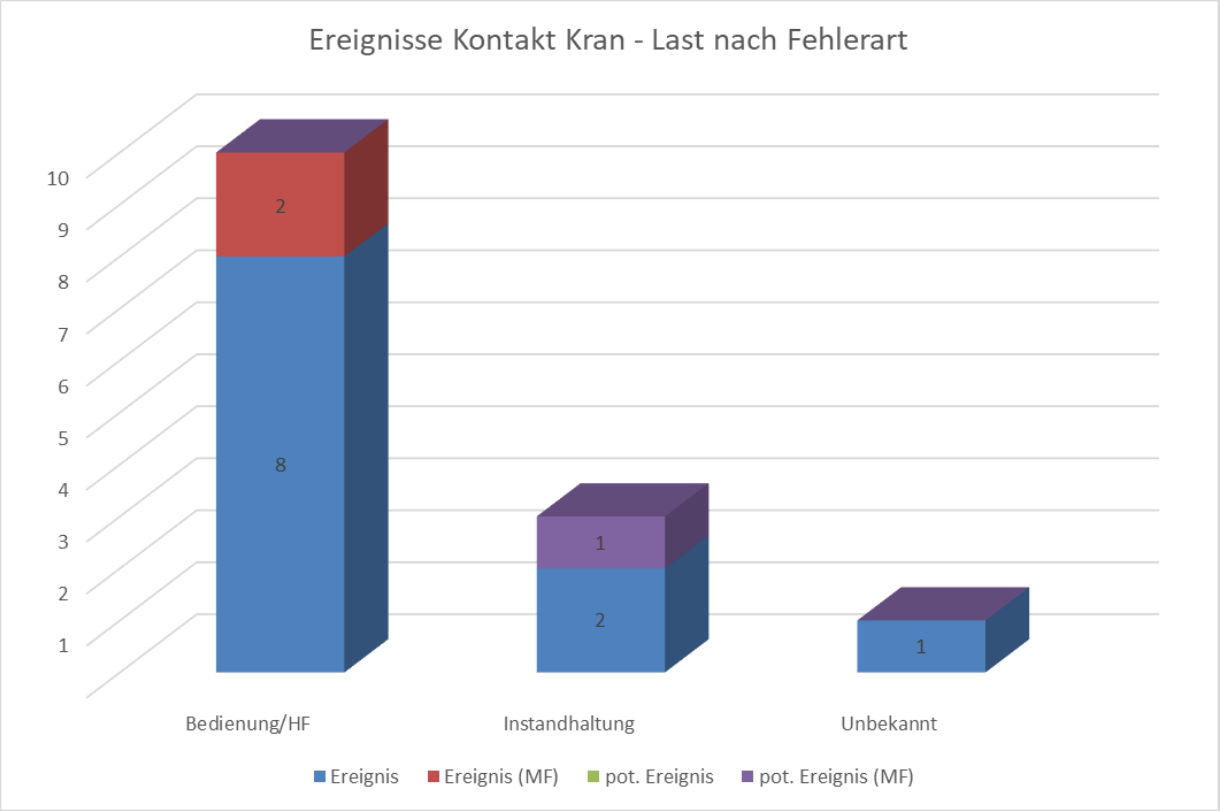

Abb. 2.11 Ereignisse mit unvorhergesehenem Kontakt zwischen Kran und Last gruppiert nach der Fehlerart

Im Rahmen der Auswertung der Ereignisse mit unvorhergesehenem Kontakt zwischen Kran und Last wurden drei Schwerpunkte festgestellt:

- Fünf Ereignisse betrafen Bedienfehler, bei denen Halterungen, Haltebolzen, Seile, die als Anschlagmittel verwendet worden waren oder direkt ein Greifer als Tragmittel irrtümlich vor dem Anheben des Hebezeugs nicht gelöst bzw. demontiert worden waren.
- Bei drei Ereignissen kam es zu Zentrierproblemen, wie sie bereits in Kapitel 2.4.4.3 thematisiert wurden. Im Unterschied zu den dort genannten Ereignissen handelt es sich hier um Ereignisse, bei denen es beim Absenken oder Anheben des Hebezeugs dann zu einem Verhaken der Last mit dem Hebezeug kam.
- Außerdem fällt eine gewisse Häufung von Ereignissen auf, bei denen es zu Problemen an den Absperrarmaturen, Linearaktoren und Tragmitteln der Lademaschinen von Schwerwasserreaktoren kam. Insgesamt wurden drei derartige Ereignisse beobachtet. Dies ist bei genauerer Betrachtung zu erwarten, da alle Probleme an den Teilsystemen zur Bewegung der Brennelemente und Befüllung

der Druckröhren entweder zu dem Fehlereffekt Selbstschädigung oder zu einer Kollision Kran - Last führen.

2.4.4.5 Nuklearspezifische Verriegelung unwirksam

Dem Fehlereffekt „Nuklearspezifische Verriegelung unwirksam“ waren 15 der ausgewerteten Ereignisse zuzuordnen.

Gruppiert nach den Kategorien der fehlerverursachenden Einrichtungen, wie sie in Kapitel 2.4.2 definiert wurden, ergibt sich für die Ereignisse mit diesem Fehlereffekt Abb. 2.12. In die Kategorie Sonstiges fällt ein Ereignis mit Schadsoftwareeintrag, bei dem keine realen Ausfälle beobachtet wurden, da die Schadsoftware dafür nicht geeignet war. Potenziell wären allerdings sehr vielfältige Fehlereffekte und beeinflussbare Einrichtungen durch eine Schadsoftware denkbar.

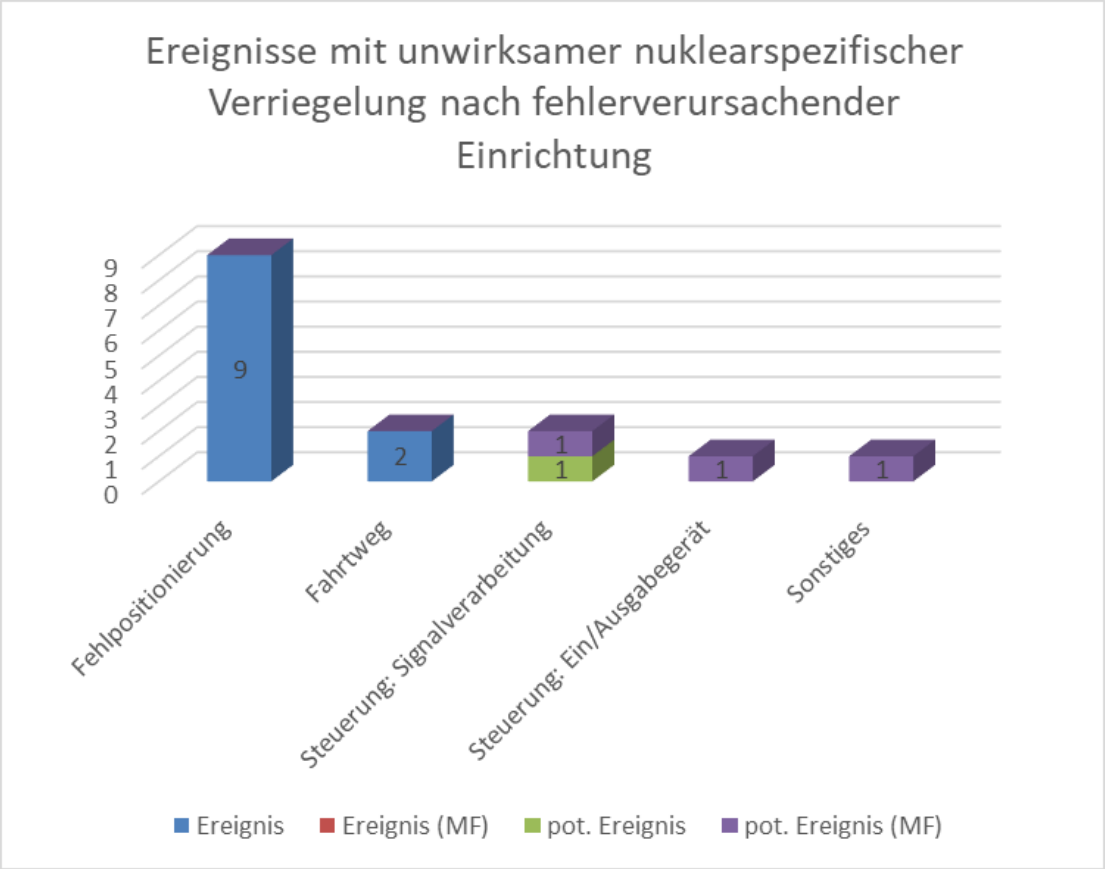

Abb. 2.12 Ereignisse mit unwirksamen nuklearspezifischen Verriegelungen gruppiert nach der fehlerverursachenden Einrichtung

Gruppiert nach Fehlerarten entsprechend den Definitionen in Kapitel 2.4.3 ergibt sich für Ereignisse mit dem Fehlereffekt „Nuklearspezifische Verriegelung unwirksam“ Abb. 2.13.

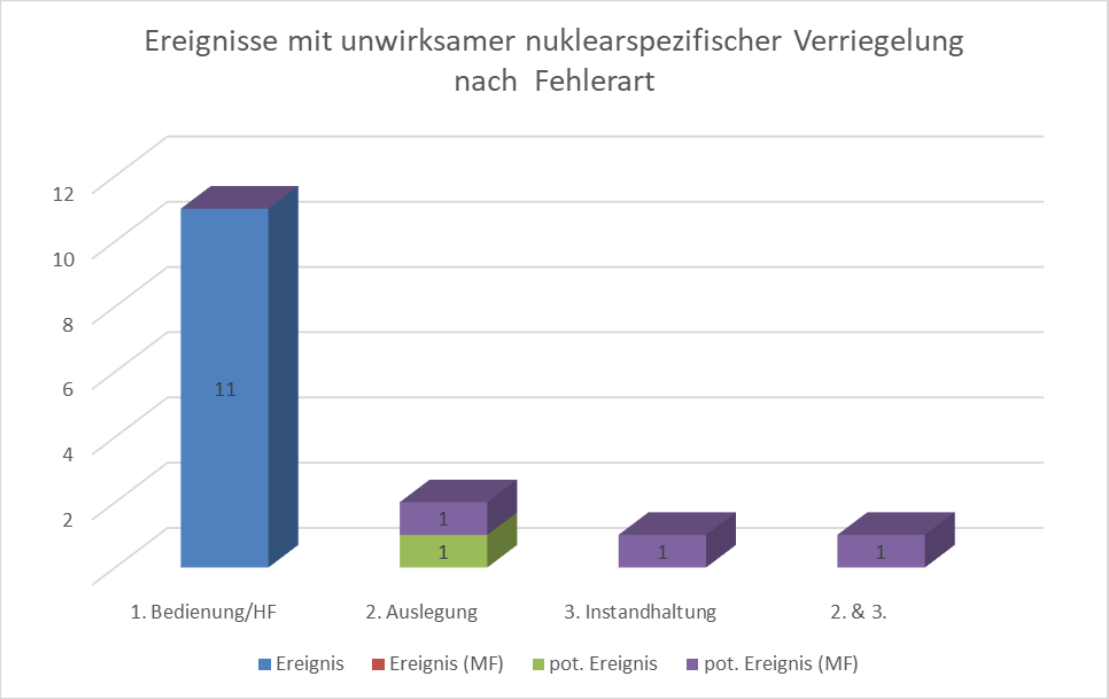

Abb. 2.13 Ereignisse mit unwirksamen nuklearspezifischen Verriegelungen gruppiert nach der Fehlerart

Im Rahmen der Auswertung der Ereignisse mit unwirksamen nuklearspezifischen Verriegelungen wurde ein Schwerpunkt festgestellt: Es fanden sich insgesamt neun Ereignisse bei denen Brennelemente bei der Beladung des BE-Lagerbeckens und in einem Fall bei der Beladung des Reaktordruckbehälters fehlpositioniert wurden. Dabei handelt es sich um ausschließlich um IRS-Ereignisse, mehrheitlich aus den Vereinigten Staaten.

2.4.5 Detailauswertung von Ereignissen mit Bezug zur Steuerung des Hebezeugs

Von den 135 insgesamt ausgewerteten Ereignissen wurde bei 43 ein Bezug zur Steuerung der Krananlage festgestellt. Im Folgenden werden diese Ereignisse hinsichtlich ihrer Ursachen noch einmal genauer untersucht. Außerdem werden Überlegungen angestellt, wie die Ereignisse im Rahmen einer Modellierung berücksichtigt werden können. Gruppiert man diese Ereignisse nach den Fehlerfolgen, so ergibt sich Abb. 2.14. Wie bereits im vorherigen Kapitel gilt: Farblich unterschieden wird zwischen Ereignissen, bei denen es tatsächlich zu der Fehlerfolge kam (blau) und potenziellen Ereignissen (grün), bei denen es bei weiterem unentdeckten Vorliegen oder Fortschreiten des Fehlermechanismus zu der Fehlerfolge hätte kommen können, die aber noch vor dem Eintritt der Fehlerfolge entdeckt wurden. Einige Ereignisse sind nicht nur einer Fehlerfolge zuzuordnen, sie sind mit dem Kürzel (MF) gekennzeichnet. Dies kann sich z. B. daraus ergeben,

dass es sich um potenzielle Ereignisse (lila) handelt, deren genaue Folge von den weiteren Betriebsbedingungen im Augenblick eines Komponentenversagens abhängen oder um tatsächliche Ereignisse (rot) bei denen unterschiedliche Einzelfehler zu unterschiedlichen Folgen führten oder ein kaskadierendes Versagen mit mehreren Fehlerfolgen auftrat (z. B. Erst Kollision mit einem Umgebungselement, dann folgend Lastabsturz).

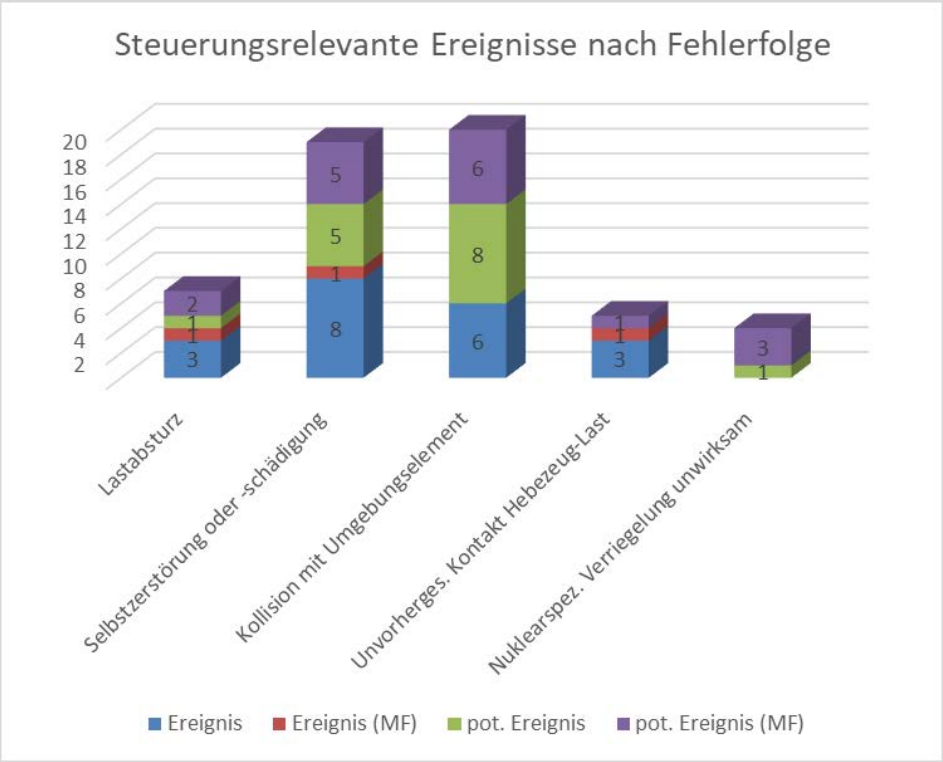

Abb. 2.14 Ereignisse mit Steuerungsbezug gruppiert nach der Fehlerfolge

Vergleicht man die Häufigkeiten der auftretenden Fehlerfolgen mit denen der Grundgesamtheit aller Ereignisse (siehe Abb. 2.15) zeigt sich, dass es bei Abweichungen in der Steuerung in der Folge häufig zu Selbstschädigungen oder Kollisionen mit einem Umgebungselement kommt. Die Fehlerfolgen „Unvorhergesehener Kontakt Hebezeug-Last“ und „Nuklearspezifische Verriegelung unwirksam“ treten in etwas so oft auf, wie man auf Grund ihrer insgesamt geringeren Häufigkeit in den ausgewerteten Ereignissen erwarten würde. Die Fehlerfolge Lastabsturz tritt deutlich seltener auf als an Hand ihrer Häufigkeit in der Grundgesamtheit zu erwarten. Es fällt außerdem auf, dass die Häufigkeiten der einzelnen Fehlerfolgen in der Summe höher ist als die Summe der Erwartungswerte. Dies ist darauf zurückzuführen, dass es sich bei Ereignissen mit Abweichungen in der Steuerung überproportional häufig um Ereignisse handelt, die mehreren Fehlerfolgen zuzuordnen sind.

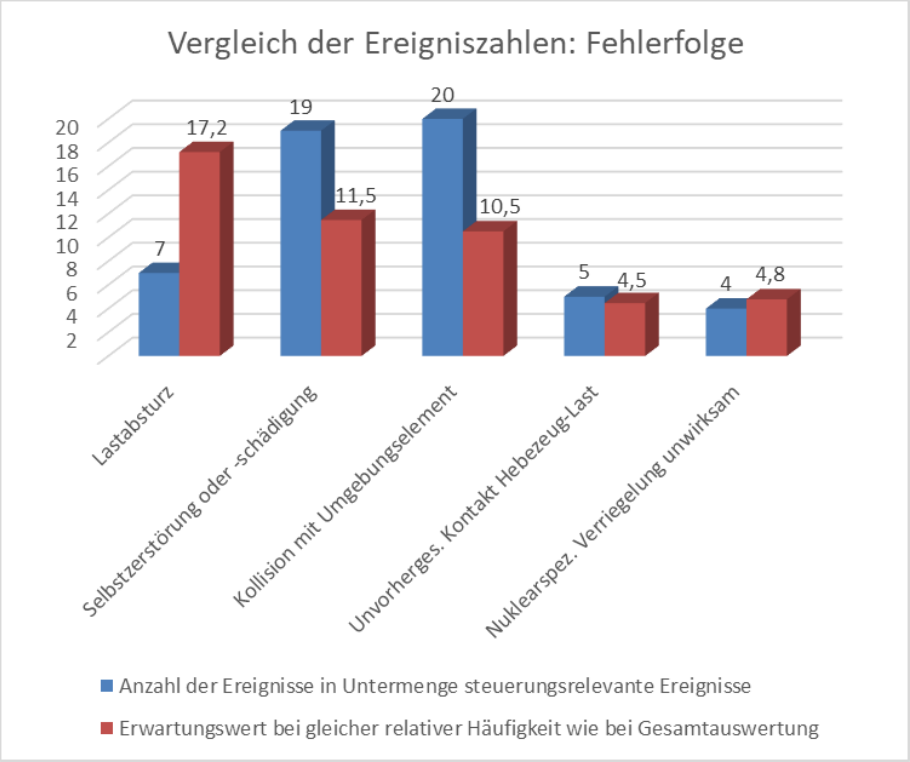

Abb. 2.15 Vergleich der Häufigkeiten der einzelnen Fehlerfolgen

Gruppiert man die Ereignisse nach Fehlerarten, ergibt sich Abb. 2.16. Es waren keine Ereignisse der Fehlerart „Herstellung“ oder der Fehlerartkombination „Human Factor“ und „Instandhaltung“ zuzuordnen, diese sind lediglich aus Gründen der Vollständigkeit aufgeführt, da sie bei der Auswertung der Grundgesamtheit aller Ereignisse aufgetreten waren. Bei dem Ereignis, dass unter „Sonstige“ eingestuft wurde, wurden auf Grund eines Lastabsturzes die Auslegungsgrundlagen eines Hebezeugs angepasst. Die zu transportierende Last war zerbrochen, da sie Vorschädigungen aufwies. Neben anderen Maßnahmen zur Vermeidung von Vorschädigungen, wurden auch Maßnahmen ergriffen um entsprechend vorgeschädigte, mechanisch instabilere Lasten transportiert zu können. Dadurch war es notwendig, verschiedene Parameter der Steuerung anzupassen (z. B. maximale Geschwindigkeit etc.). Bei den Ereignissen mit der Fehlerart „Unbekannt“ war eine Bestimmung der Fehlerart an Hand der vorliegenden Informationen nicht möglich. Dabei handelt es sich ausnahmslos um Hardwareausfälle von Steuerungskomponenten, bei denen die genaue Ausfallursache der betroffenen Komponente nicht zu ermitteln war.

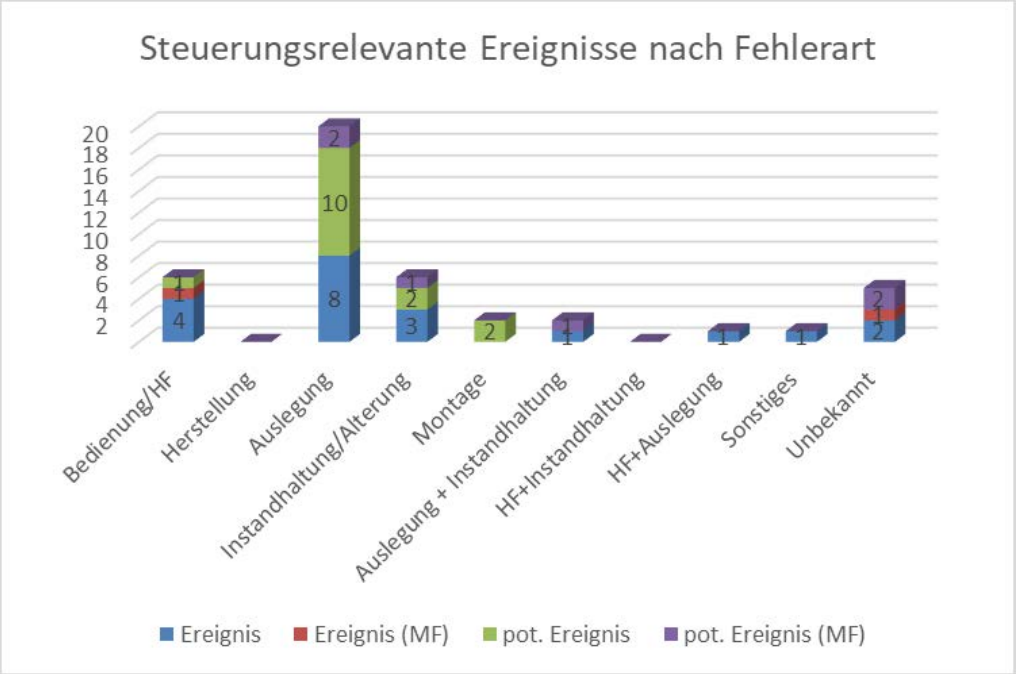

Abb. 2.16 Ereignisse mit Steuerungsbezug gruppiert nach der Fehlerart

Vergleicht man die Häufigkeiten der auftretenden Fehlerarten mit denen der Grundgesamtheit aller Ereignisse (siehe Abb. 2.17) fällt auf, dass „Human Factor“-Ereignisse, also Bedienfehler, deutlich seltener als in der Grundgesamtheit aller Ereignisse sind. Dem gegenüber steht ein überproportional häufiges Auftreten von Auslegungsfehlern und Fehlern, deren Fehlerart als „Unbekannt“ eingestuft wurde. Die übrigen Fehlerarten treten in etwa so oft auf, wie man auf Grund ihrer Häufigkeit in den insgesamt ausgewerteten Ereignissen erwarten würde.

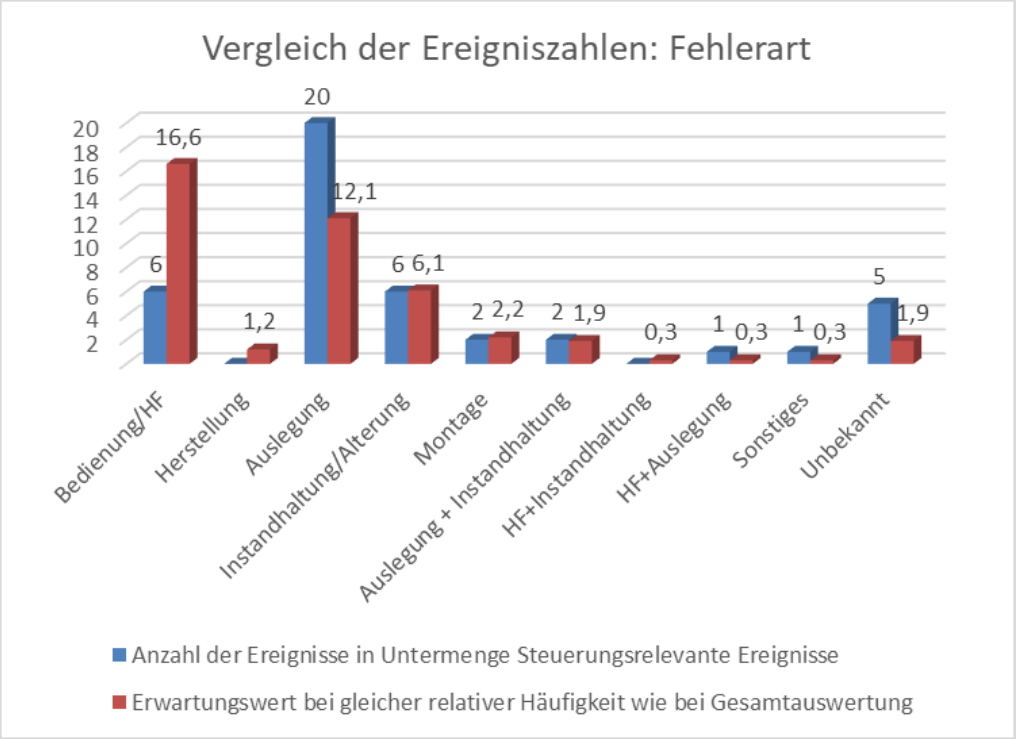

Abb. 2.17 Vergleich der Häufigkeiten der einzelnen Fehlarten

Betrachtet man die Ereignisse im Detail, so kann man die Ereignisse mit steuerungsrelevanten Aspekten aufteilen: Einerseits in Ereignisse, bei denen es zu Ausfällen der Hardware kam, bei denen also physische Defekte von Komponenten oder Bauteilen vorlagen. Andererseits in Ereignisse, bei denen es zu Problemen mit der Software kam, bei denen aber alle beteiligten Komponenten oder Bauteile für sich genommen funktionsfähig waren.

Bei einer Betrachtung der Hardwaredefekte fällt auf, dass sich zwei Schwerpunkte bilden lassen: Einmal Ausfälle in der Messwerterfassung, bei denen Messwertgeber ausfielen, und andererseits Ausfälle in der Signalübertragung durch Kabelschäden, die in den gefundenen Fällen stets auf Mängel in der Kabelführung zurückzuführen sind. Die übrigen Hardwareausfälle werden in Abb. 2.18 unter dem Punkt „Sonstiges“ subsummiert. Bei einem Ereignis waren ein Messwertgeber und eine sonstige Komponente (Hydraulischer Schieber, Linearaktor) gleichzeitig defekt.

Bei Ereignissen mit Fehlern in der Software ist zwischen verschiedenen Fehlern zu unterscheiden: Erstens Programmier- und Logikfehler in der Software, bei denen die Software von beteiligten Komponenten mit korrekten Eingabeparametern zu falschen Ergebnissen kam. Es handelt sich dabei um einen Fehler in der programmiertechnischen Umsetzung der Anforderungsspezifikation. Dabei liegen mathematische oder logische

Fehler in der Software bei der Bildung einer Ausgangs- oder Hilfsgröße vor. Zweitens Parametrierfehler bei denen zwar die verwendete Mathematik und Logik zur Bildung einer Ausgangs- oder Hilfsgröße korrekt ist, aber eine dabei verwendete Variable, die nicht unmittelbar aus einer Messgröße abgeleitet wird, sondern in der Software selbst oder per externer Eingabe definiert wird (z. B. Fahrgeschwindigkeit), falsch eingegeben oder nicht spezifikationsgemäß bestimmt wurde. Drittens wurden Fehler in der Spezifikation selbst beobachtet. Dies bedeutet, dass die Steuerung selbst wie spezifiziert funktioniert, allerdings nicht anforderungsgerecht war, weil beispielweise notwendige Funktionen nicht oder nicht in der notwendigen Qualität umgesetzt waren. Bei zwei Ereignissen lag ein Spezifikationsfehler in Kombination mit einem Hardwarefehler vor. Dabei lagen einmal ein ausgefallener Messwertgeber und einmal ein Schaden an einem Eingabegerät (Fernbedienung) und einem Relais vor.

Abb. 2.18 zeigt wie sich die gefundenen steuerungsrelevanten Ereignisse auf die beschriebenen Software- und Hardwarefehler verteilen.

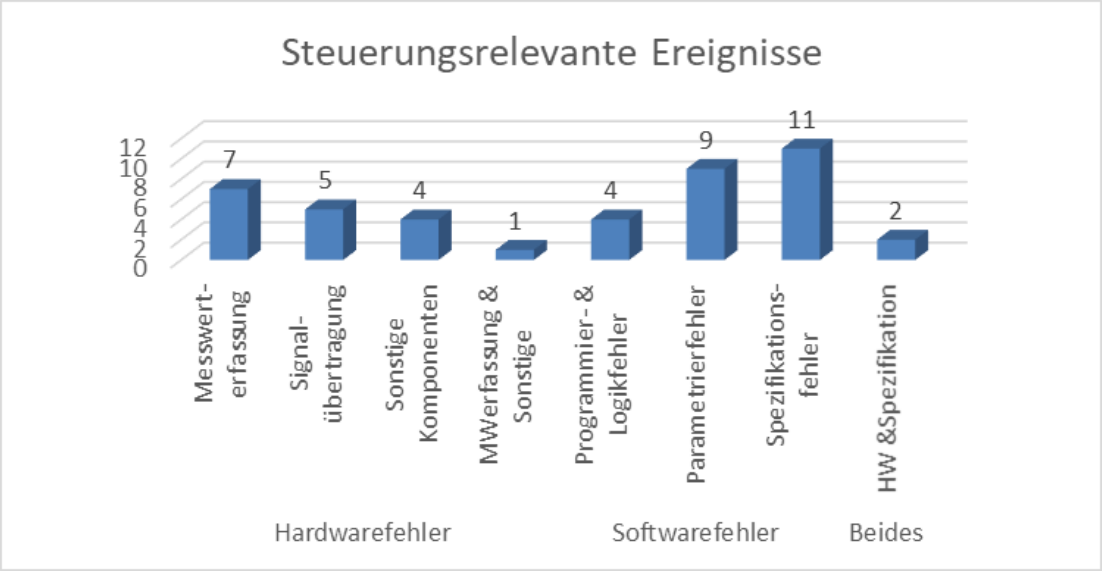

Abb. 2.18 Häufigkeiten der verschiedenen Hardware- und Softwarefehler

Bei den ausgefallenen Gebern der Messwerterfassung handelte es sich im Einzelnen um:

- Drehzahlgeber für die Wegmessung (GVA)
  Aus der Anzahl der Drehungen wird hier eine Position abgeleitet. Es kam hier zu einem Schaden an der Welle der Drehzahlgeber. Dadurch waren alle Geber an der

Welle hinter der Bruchstelle unverfügbar (Montagefehler beim Montieren der Lagerung). Betroffen war ein Lagerkran.

- Drehzahlgeber für die Geschwindigkeitsmessung

  Auch hier kam es zum Bruch der Welle des Drehzahlgebers, der in diesem Fall allein auf der Welle saß. Er wurde zur Geschwindigkeitsmessung genutzt. Betroffen war eine BE-Lademaschine (DWR). Gleichzeitig lag noch ein Spezifikationsfehler der Software vor.

- Wegendgeber für Absperrschieber bzw. hydraulische Schieber
  Insgesamt wurden zwei Ereignisse festgestellt. Die betroffenen Anlagen sind Schwerwasseranlagen.
  Bei einer betroffenen Anlage gibt es einen eigenen Behälter für den Transport von Kühlmittelkanälen. Dieser Transportbehälter wird mit dem Gebäudekran bewegt und hat einen eigenen, separaten Greifer im Inneren und einen Absperrschieber, um ein Herausfallen des Kanals zu verhindern. Die Wegendmessung bezieht sich auf die Positionierung dieses Absperrschiebers. Sie war bekanntermaßen unverfügbar, trotzdem wurden Transportvorgänge durchgeführt, da die sicherheitstechnische Bedeutung falsch eingeschätzt wurde. In der Folge kam es zur Kollision eines Kanals mit dem Schieber.
  Bei der anderen Anlage werden die Brennelemente durch die BE-Lademaschine waagerecht in den Reaktor eingeschoben, bei dem betroffenen hydraulischen Schieber handelt es sich um einen Linearaktor, der das Brennelement aus einem Transportmagazin in das Magazin zum direkten Einbringen in den Reaktor schiebt. Defekt war hier der Linearaktor (Hub abweichend, Alterungseffekt) und die Wegendüberwachung (Kenndatendrift). Da die defekte Überwachung aber nur die Detektion des Ereignisses verzögerte und die Folgen verschlimmerte (BE beschädigt statt Schutz aus), nicht aber das Ereignis verursachte, wurde dieses Ereignis im Gegensatz zu den übrigen Ereignissen in dieser Aufzählung nicht mit der Messwerterfassung als verursachender Einrichtung sondern mit „Sonstiges (Linearaktor)“ bewertet.

- Positionsgeber Greifer
  Es handelt sich um das gleiche Ereignis wie bei dem Wegendgeber des Absperrschiebers. Der Positionsmessung des Greifers im Transportbehälter war ebenfalls defekt. Das genaue Messprinzip ist hier nicht bekannt.

- Lastmessung Schlaffseilüberwachung
  Hierbei handelt es sich um eine Überwachungseinrichtung, damit die zulässige Geschwindigkeit beim Absenken von Lasten nicht überschritten wird. Betroffen war eine BE-Lademaschine. Beim irrtümlichen Aufsetzen eines BE kam es auf Grund der defekten Messung (Draht lose) zum Lastabsturz.

- Stellungsgeber Lastaufnahmemittel
  Mit dieser Überwachungseinrichtung wird überwacht, ob die Anschlagpunkte korrekt in den Lastaufnahmemitteln liegen. Im konkreten Fall war dies durch einen Bedienfehler nicht der Fall, wurde dann aber nicht gemeldet. Da die defekte Überwachung aber nur die Detektion des Ereignisses verzögerte und die Folgen verschlimmerte (Schaden an Lastaufnahmemittel statt Warnmeldung), nicht aber das Ereignis verursachte, wurde dieses Ereignis im Gegensatz zu den übrigen Ereignissen in dieser Aufzählung nicht mit der Messwerterfassung als verursachender Einrichtung sondern mit „Lastaufnahmemittel“ bewertet (da der Fehler beim Anlegen des Lastaufnahmemittels entstand).

- Weggeber zur Positionsmessung (teilweise GVA)
  Es wurden insgesamt zwei Ereignisse festgestellt.
  Bei einem Ereignis war der Weggeber einer BE-Lademaschine (SWR) defekt, was zu Fehlfahrten in horizontaler Richtung führte. Bei dem anderen Ereignis waren beide laserbasierten Weggeber eines Lagerkrans durch Nebel (Kran überfährt auch Außenbereich) beeinträchtigt, wodurch der Bremsvorgang bei Erreichen des Wegendes nicht eingeleitet wurde.

Komponenten der Messwerterfassung können beispielsweise in einem Fehlerbaum direkt ggf. auch mit verschiedenen Ausfallarten modelliert werden. Für diese Ereignisse sind daher keine besonderen Probleme bei der Methodenentwicklung zu erwarten.

Die fünf Ereignisse mit Problemen in der Signalübertragung sind jeweils auf Schäden an Steuerungs- und Leistungskabeln zurückzuführen. Zwei der Ereignisse sind auf beschädigte Halterungen, wodurch Kabelschleifen entstanden, die dann abgeschert wurden, zurückzuführen. Einmal wurde das Kabel über eine scharfe Kante geführt. Einmal entgleiste der Kabelschlepp aufgrund einer Kante an der Laufschiene. Einmal wurde das Kontrollpult für Arbeiten temporär versetzt und die Kabel dabei durch eine Tür verlegt, die dann ohne Rücksicht auf den Kabelstrang zu nehmen geschlossen wurde. Die Sig-

nalübertragung kann als Komponente beispielsweise in einem Fehlerbaum direkt modelliert werden. Für diese Ereignisse sind daher keine besonderen Probleme bei der Methodenentwicklung zu erwarten.

Bei den sonstigen Hardwareausfällen handelt es sich um folgende Komponenten:

- Relais
  Es wurden zwei Ereignisse festgestellt.
  Bei einem Ereignis waren Relaiskontakte verbacken, wodurch eine Überlastüberwachungseinrichtung unverfügbar war. Dies wurde bei einer Prüfung festgestellt.
  Bei dem anderen Ereignis war auf Grund einer zu großen Hysterese ein Relais geschaltet und dadurch eine Freigabe für Fahrbewegungen wirksam ohne dass ein entsprechender Befehl gegeben worden war. Dies hatte in Kombination mit einem weiteren Defekt (Eingabegeräte, siehe unten) und einem Spezifikationsfehler nicht angeforderte Fahrbewegungen zur Folge. Betroffen war der Reaktorgebäudekran eines Forschungsreaktors.

- Motorschutzschalter
  Es kam zu mehreren Fehlauslösungen und damit Stillsetzungen durch elektromagnetische Einkopplungen. Da der Schutzschalter bei dem betroffenen Lagerkran keine Sicherheitsfunktion hatte, war er bei der Qualifikation nicht ausreichend beachtet worden.

- Hydraulischer Schieber (Linearaktor)
  Dieses Ereignis wurde oben unter dem Unterpunkt Wegendgeber für hydraulische Schieber beschrieben.

- Eingabegerät
  Durch verschlissene Kontakte an einer Fernbedienung mit Joystick kam es sporadisch zur Auslösung von Fahrbefehlen ohne eine entsprechende Handeingabe. Zusammen mit einem defekten Relais (siehe oben) und einem Spezifikationsfehler führte dies zu nicht angeforderten Fahrbewegungen.

- Elektromotor
  Sporadischer Defekt eines Antriebs einer BE-Lademaschine, was zu Fehlfahrten in horizontaler Richtung führte.

- SPS-Baugruppe
  Fehlauslösung einer Notbremsung mit Einfall der Bremsen durch einen losen Draht auf der Baugruppe. Betroffen war die Lademaschine eines Forschungsreaktors.

Diese Komponenten können beispielsweise in einem Fehlerbaum direkt ggf. auch mit verschiedenen Ausfallarten modelliert werden. Für diese Ereignisse sind daher keine besonderen Probleme bei der Methodenentwicklung zu erwarten.

Bei den beobachteten Programmier- und Logikfehlern handelt es sich im Einzelnen um Folgende:

- Rundungsfehler und arithmetischer Überlauf
  Eine Variable für die relative Sollgeschwindigkeit (0 bis 1 entsprechen einer Sollgeschwindigkeit von bis zu 100 % der Nenngeschwindigkeit) konnte nach einer Division (spezifiziert: halbe Geschwindigkeit bei bestimmten Lasten) kleiner als die Anzahl der spezifizierten Nachkommastellen sein und wurde dann fehlerhaft auf Null gesetzt. In der weiteren Auswertelogik wurden allerdings nur Werte größer Null korrekt verarbeitet. Ein Wert Null der Variable führt dazu, dass der Wert als Eins interpretiert wird (Schutz gegen arithmetischen Überlauf), wodurch die relative Sollgeschwindigkeit auf 100 % der Nenngeschwindigkeit gesetzt wurde und es zu nicht angeforderten Beschleunigungsvorgängen des Fahrwerks kam. Betroffen war eine BE-Lademaschine (SWR).

- Dynamische Parametererfassung
  Bei der Übergabe von Parametern zwischen verschiedenen Baugruppen änderten sich die einzulesenden Parameter während des Einlesevorgangs. Da dies nicht berücksichtigt war, wurden dadurch unzulässige Parametersätze generiert. Dadurch kam es zu Fahrten des Hubwerks in die falsche Richtung. Dabei war außerdem die Überlastüberwachung unwirksam. Betroffen war eine BE-Lademaschine (SWR).

- Dynamische Parametererfassung und arithmetischer Überlauf
  Unter bestimmten Umständen kann eine Variable für die relative Sollgeschwindigkeit gelöscht werden (Sicherheitsmaßnahme bei unzulässigen Parametersätzen nach obigem Ereignis). Der Wert wurde danach allerdings nicht neu eingelesen, so dass er nach der Löschung auf dem Wert Null verblieb. Dies wurde analog zu dem arithmetischen Überlauf weiter oben als 100 % der Nenngeschwindigkeit interpretiert, wodurch es zu nicht angeforderten Beschleunigungsvorgängen des Fahrwerks kam. Betroffen war eine BE-Lademaschine (SWR).

- Malware
  Auf einer BE-Lademaschine wurde allgemein verbreitete Schadsoftware entdeckt. Diese war nicht geeignet irgendwelche Schäden hervorzurufen. Das Ereignis zeigte

aber Defizite in der Einhaltung der Schutzmaßnahmen an der Airgap bei Instandhaltungsvorgängen, durch die potenziell schädigende Software hätte eingetragen werden können.

Als fehlerverursachende Einrichtung wurde für alle obigen Ereignisse die Signalverarbeitung identifiziert. Lediglich das Malware-Ereignis wurde in die Kategorie „Sonstiges“ eingestuft.

Die aufgeführten Logikfehler können nicht direkt als Basiselemente in einer Fehlerbaumanalyse modelliert werden. Allerdings können die Komponenten, also in den vorliegenden Fällen Baugruppen, auf denen die defizitäre Software lief, mit entsprechenden Basiselementen als ausgefallen modelliert werden (Black-Box-Ansatz, siehe Kapitel 3.2.3). Je nach Art des Softwaredefizits können verschiedene Ausfallarten modelliert werden. Für diese Ereignisse sind daher keine besonderen Probleme bei der Methodenentwicklung zu erwarten.

Bei den beobachteten Parametrierfehlern handelt es sich im Einzelnen um:

- Fahrgeschwindigkeit x2
  Betroffen waren hierbei jeweils zulässige Höchstgeschwindigkeiten mit der das Fahrwerk des Hebezeugs an verschiedenen Punkten des Transportvorgangs verfahrbar ist.
  In einem Fall war die Fahrgeschwindigkeit einer BE-Lademaschine so hoch gewählt, dass es unter ungünstigen Randbedingungen zu Pendelbewegungen der Last kommen konnte. Um dann fällige Pausen zwischen Fahr- und Hubbewegungen zu vermeiden, wurde die Fahrgeschwindigkeit gesenkt.
  In einem weiteren Fall war die Sollgeschwindigkeit der Sicherheitsvorendschalter zu hoch eingestellt. Der Sicherheitsvorendschalter prüft, ob vor Erreichen des tatsächlichen Wegendpunkts der Bremsvorgang ordnungsgemäß eingeleitet wurde. Diese Prüfung fand dann effektiv nicht statt.

- Hubgeschwindigkeit x2
  Betroffen waren hierbei jeweils zulässige Höchstgeschwindigkeiten mit der das Hubwerk des Hebezeugs an verschiedenen Punkten des Transportvorgangs verfahrbar ist.
  In einem Fall erwies sich ein bestimmter Brennelement-Typ, wenn das Zeilensprungverfahren verwendet wurde (Beladeverfahren), als anfällig für ein Verhaken der Abstandshalter. Um ein Verhaken zu vermeiden, musste die Hebegeschwindigkeit

deutlich verringert werden. Diese war vorher speziell für dieses Beladeverfahren erhöht worden.

In einem anderen Fall sollten zukünftig auch Brennelemente mit gewissen Vorschädigungen mit der BE-Lademaschine transportiert werden ohne dass es zu weiteren Folgeschäden am Brennelement kommt. Dazu war es ebenfalls notwendig die Hebegeschwindigkeit zu verringern.

- Toleranzwert Richtungsüberwachung (Hubgeschwindigkeit)
  Die Richtungsüberwachung überwacht bei Hebevorgängen, ob die Richtung, in die sich das Hebezeug bewegt, mit dem gegebenen Befehl übereinstimmt. Bei dem betroffenen Hebezeug wurden dafür die Soll- und Ist-Geschwindigkeiten verglichen. Hierfür war ein Toleranzwert in der Steuerung definiert, der irrtümlich zu hoch eingegeben wurde, so dass nur bei höheren Fahrgeschwindigkeiten überhaupt eine Richtungsüberwachung wirksam war.

- Verzögerungszeit x2
  Bei diesem Parameter handelt es sich um eine spezifizierte Zeitdauer nach der Schutzaktionen einzuleiten sind.
  In einem Fall war die Zeitdauer zwischen dem Überfahren des ersten Vorendschalters und einer Prüfung, ob daraufhin ordnungsgemäß der Bremsvorgang eingeleitet wurde (Geschwindigkeitsvergleich) irrtümlich um den Faktor 100 zu groß eingestellt. Eine Überwachung des Bremsvorgangs vor Erreichen des 2. Endschalters fand also effektiv nicht statt.
  In einem anderen Fall war die Zeitdauer für die die Schlaffseilüberwachung (effektiv eine Lastmessung) ansprechen muss, bevor Schutzmaßnahmen ergriffen werden, zu hoch eingestellt. Dadurch konnte es, als die Antriebskette aus ihrer Führung rutschte, zu einem Verklemmen des Seils mit weiteren Folgeschäden kommen.

- Fahrbereichsgrenzen (Wegendschalter) x2
  Hierbei handelt es sich um Weggrenzen, die in der Steuerung hinterlegt werden, um Kollisionen mit Wänden oder anderen Umgebungselementen im Fahrbereich zu verhindern.
  In einem Fall waren nach Änderungen im BE-Lagebecken die Fahrbereichsgrenzen nicht mit angepasst worden, so dass einige Umgebungselemente nicht in den Fahrbereichsgrenzen abgebildet waren und die Gefahr von Kollisionen bestand. Bei diesem Ereignis handelt es sich um einen Grenzfall, dies kann auch als Spezifikationsfehler betrachtet werden.
  In einem anderen Fall waren nach Änderungen die Wegendschalter zwar angepasst

worden, bei der händischen Eingabe kam es aber zu einem Tippfehler, so dass der 2. Wegendschalter (Sicherheitswegendschalter) effektiv nicht wirksam war.

- Überlastüberwachung (Boole'sche Variable)
  Die Überlastüberwachung verhindert, dass mit dem Hubwerk Lasten transportiert werden, die das Hubwerk mechanisch überlasten oder aus anderen Gründen nicht transportiert werden dürfen.
  Im Rahmen einer Schulungsmaßnahme an dem Hebezeug wurde die Überlastüberwachung an der Bedienoberfläche versehentlich unscharf geschaltet. Dabei wurde nicht der Grenzwert, ab dem die Überwachung wirksam wird, geändert, sondern leittechnisch die gesamte Überlastüberwachung deaktiviert.

Als fehlerverursachende Einrichtung gemäß den Kategorien aus Kapitel 2.4.2 wurde für die genannten Ereignisse in der Regel auch die Steuerung (Unterkategorie Parametrierung) identifiziert. Drei Ereignisse wurden abweichend kategorisiert: Erstens die Anpassung der Hubgeschwindigkeit für Brennelemente mit Vorschäden. Diese Anpassung war die Folge eines Lastabsturzes mit einem solchen geschädigten Brennelement. Fehlerverursachend war der Vorschaden am Brennelement also der Last. Zweitens die zu große Verzögerungszeit der Schlaffseilüberwachung. Hier war der Schaden an der Antriebskette (Einstufung somit Antriebsstrang) ursächlich, die Fehlparametrisierung vergrößerte nur die Auswirkungen.

Die genannten Ereignisse können nicht direkt modelliert werden. Allerdings können die Komponenten, auf denen die Software falsche Parameter enthielt, als ausgefallen modelliert werden. Je nach Art des Parametrierfehlers können verschiedene Ausfallarten modelliert werden. Für diese Ereignisse sind daher keine besonderen Probleme bei der Methodenentwicklung zu erwarten.

Bei den Spezifikationsfehlern handelt es sich im Einzelnen um:

- Überlastüberwachungen nicht spezifiziert x2
  Bei insgesamt zwei Ereignissen kam es zu sicherheitsrelevanten Schäden am Hebezeug oder zu Lastabstürzen, weil zu schwere Lasten gehoben wurden. Überlastüberwachungen wurden daraufhin nachgerüstet.

- Positionsmessung nicht spezifiziert
  Bei dem betroffenen Hebezeug handelte es sich um ein Hebezeug mit Haupt- und Hilfshub. Der Hilfshub hatte keine eigene Positionsmessung bzw. lediglich eine improvisierte, so dass eine Last irrtümlich zu hoch positioniert wurde. Nachdem die Last

am Haupthub ins Schwingen geriet, kam es zu einem Lastabsturz der Last am Hilfshub, da in Folge der Fehlpositionierung der Hilfshub Kräfte des Haupthubwerks mit abtragen musste.

- Fahr- und Hubbereichsgrenzen für besondere Fahrtbedingungen nicht spezifiziert
  In einem Fall war ein fest installiertes, aber nicht immer den Weg des Hebezeugs behinderndes Umgebungselement (klappbare Brücke) nicht in den Fahrbereichsgrenzen berücksichtigt worden.
  In einem anderen Fall war ein spezielles Greifwerkzeug in den Abmessungen abweichend von den Standardgreifern, so dass die normal wirksamen Hubbereichsgrenzen nicht galten ohne das Ersatzgrenzen definiert waren. Die Folgen waren in beiden Fällen Kollisionen.

- Sicherheitsrelevante Hilfssysteme nicht überwacht
  In einem Fall wurde ein Greifer durch Druckluft offengehalten. Es kam zu einer Kollision, weil auf Grund eines Druckabfalls der Greifer nicht mehr fähig war, alle Eingaben ordnungsgemäß auszuführen. Der Druck im Druckluftsystem wurde zwar gemessen und angezeigt, ging aber nicht in Alarme oder Verriegelungen ein.

- Nicht ausreichende Trennung von zu separierenden Funktionen x2
  Eine einzelne Drehzahlmessung wurde sowohl für die betriebliche als auch für die Sicherheitsleittechnik als Geschwindigkeitsmessung des Fahrwerks verwendet. Nach dem Ausfall der Messung kam es in der Folge zu einem Überfahren der Fahrbereichsgrenzen.
  In einem anderen Fall war die Fahrfreigabe eines Eingabegerätes so ausgeführt, dass die Fahrfreigabe für alle Fahrtrichtungen gleichzeitig durch einen einzelnen Taster gegeben wurde. Zusammen mit einem weiteren Komponentenausfall hatte dies Fehlfahrten in sonstige Fahrtrichtungen ohne Anforderung zur Folge.

- Abstellbarkeit in gefährlicherem Systemzustand
  In einem Fall konnte ein Schlüsselschalter, der zur Umschaltung zwischen verschiedenen Betriebsmodi dient, in einer Position abgezogen werden, in der das Hubwerk des Hebezeugs nicht verriegelt ist und sich normalerweise ein Betonriegel mit einer radiologischen Abschirmfunktion nicht in ordnungsgemäßer Position befindet.

- Verringerte Zuverlässigkeit von Überwachungsfunktionen x2
  In einem Fall konnte im Rahmen der WKP die Wegend-Überwachungsfunktionen (Vorend- und Endschalter) des Fahrwerks nicht mit maximaler Geschwindigkeit ge-

prüft werden, da diese Geschwindigkeitsstufe automatisch über den Schlüsselschalter WKP blockiert wurde.
In einem anderen Fall waren nicht alle vorhandenen Sensoren der Leckageüberwachung einer hydraulischen Dämpfungseinrichtungen in die Überwachung eingebunden.

- Quittierbarkeit von Störmeldungen durch nicht qualifiziertes Personal
  In einem Fall konnten Störmeldungen aus der Triebwerkskette ohne Schlüsselschalter und somit von nicht entsprechend qualifiziertem Personal quittiert werden.

Die genannten Ereignisse können nicht direkt im Fehlerbaum modelliert werden. Sie müssen durch die Verwendung eines strukturierten Ansatzes bei der Definition der notwendigen Sicherheitsfunktionen und der Anforderungen an diese abgefangen werden. Eine FMEA-Analyse ist hierfür beispielsweise geeignet.

3 AP 2: Entwicklung einer Methode zur Systemvalidierung des Steuerungssystems von Hebezeugen bezüglich der Umsetzung der Sicherheitsfunktionen und der Berücksichtigung der zu unterstellenden Ausfälle und Erprobung der Methode an einer Beispielsteuerung

3.1 Methoden der Zuverlässigkeit- und Sicherheitsanalyse

Eine umfassende Risikoanalyse soll die potenziellen Risiken einer automatisierten Krananlage bei der Auslegung erkennen und damit als Basis zur Erstellung eines Sicherheitskonzepts zur Fehlervermeidung und -beherrschung dienen. Generell werden bei der Auslegung einer Krananlage nur Einzelfehler bzw. -ausfälle betrachtet /GÜN 03/. Beim Einsatz einer Krananlage im Bereich mit hohem Risiko für Mensch und Umwelt kann es notwendig sein, auch Abläufe bzw. Ereignisse mit mehr als einem Fehler (Fehlerkombinationen) zu berücksichtigen. Für die Sicherheitssteuerung einer Krananlage in einer kerntechnischen Anlage ist es notwendig, dass vor der ersten Inbetriebnahme der Kransteuerung eine detaillierte sicherheitstechnische Bewertung (u. a. Nachweis der erforderlichen Zuverlässigkeit) durchgeführt wird und durch die entsprechenden Tests die Sicherheit der gesamten Krananlage nachgewiesen wird /KTA 19a/.

Für Zuverlässigkeits- und Sicherheitsanalysen analoger und digitaler Leittechnik in Kernkraftwerken wurden weltweit eine Vielzahl von Methoden entwickelt und eingesetzt. Die GRS hat mehrere Forschungsvorhaben zur Methodenentwicklung für die sicherheitstechnische Bewertung digitaler Leittechnik in Kernkraftwerken durchgeführt, wobei jeweils der Stand von Wissenschaft und Technik zu dieser Thematik ermittelt und fortgeschrieben wurde. Wesentliche Erkenntnisse hierzu wurden durch die Erprobung einiger Methoden (z. B. /GRS 15a/, /GRS 17/, /PIL 04/, /PIL 10/) und durch die Mitwirkung an internationalen Projekten (u. a. DIGREL /NEA 15/) gewonnen. In zahlreichen Forschungsvorhaben der GRS (z. B. /GRS 15a/, /GRS 17/) wurden wesentliche Merkmale von Methoden der Sicherheits- und Zuverlässigkeitsanalysen digitaler Leittechnik erfasst und bewertet. (s. Tab. 3.1)

Tab. 3.1 Vergleich verschiedener Methoden der Sicherheits- und Zuverlässigkeitsanalyse

	Geeignet für komplexe Systemarchi-tektur	Geeignet für Auslegung	Geeignet für Sicherheits-überprüfung	Vorgehens-weise: deduktiv/in-duktiv	Arbeits-aufwand	Akzeptanz und Nach-vollziehbar-keit	Verfügbarkeit von Analyse-werkzeugen
Fehlzustandsbaumanalyse (FTA - Fault Tree Analysis) /DIN 07b/	Ja	Ja	Ja	D	Hoch	Hoch	viele
Fehlzustandsart- und -auswir-kungsanalyse (FMEA – Failure Mode and Effect Analysis) /DIN 06a/, /DIN 11a/, /DIN 15a/	Nein	Nein / Ja[1]	Ja	I	Hoch	Hoch	viele
Zuverlässigkeitsblockdiagramm /DIN 06b/	Nein	Nein	Ja	D	Mittel	Mittel	viele
Markoff-Analyse /DIN 07c/	Ja	Ja	Ja	D	Mittel / Hoch	Mittel	viele
Petrinetze	Ja	Ja	Nein	D	Mittel / Hoch	Niedrig	viele
Monte-Carlo-Simulation	Ja	Ja	Ja (ergänzend)	Nicht zutreffend	Hoch	Modell-abhängig	viele
Modellbasierte Fehlersimulation (Fault injection)	Ja	Nein	Ja	I	Hoch	Modell-abhängig	viele

[1] grundsätzlich Ja, aber die Eignung der FMEA hängt von vielen Aspekten der Auslegung ab: z. B. welche Zielstellung soll die FMEA erfüllen, eine FMEA auf der Funktionsebene in Entwurfs- bzw. Konzeptphase oder während der detaillierten Auslegung eines Systems, wo die Auswirkungen der Komponentenausfälle im Rahmen der Validierung und Verifizierung (V&V Prozess)) analysiert werden sollten. Für die V&V-FMEA sind detaillierte Informationen zum System und dessen Komponenten erforderlich.

Die Auswahl der Methoden im Rahmen dieses Projekts erfolgte auf der Grundlage von den Merkmalen der Methoden gemäß Tabelle 3.1. Die Eignung für eine Sicherheitsüberprüfung (u.a. Verifizierung und Validierung der erforderlichen Nachweise im Rahmen der Betriebsgenehmigung) ist eine grundsätzliche Voraussetzung für die auszuwählenden Methoden. Weitere relevante Aspekte bei der Auswahl der Methoden sind eine hinreichende Akzeptanz und die Eignung der Methode für modellbasierte Analysen. Daraus ergaben sich die FMEA-Analyse und die Fehlerbaumanalyse als einsetzbare Methoden. Die Simulation sollte dazu eingesetzt werden, um die Annahmen in der FMEA-Analyse zu validieren und die Ergebnisse der Fehlerbaumanalyse zu überprüfen. Eine Simulation bietet sich insbesondere zur Analyse von dynamischen Abläufen an, weil diese für die Analyse (möglicher) Wechselwirkungen zwischen den Sicherheitsfunktionen und der Umgebung von Bedeutung sein können. In den nachfolgenden Abschnitten werden diese Methoden erläutert.

3.1.1 Fehlzustandsart- und Auswirkungsanalyse (FMEA)

Die FMEA (FMEA - Failure Mode Effect Analysis) ist eine weitverbreitete Methode zur qualitativen Sicherheits- und Zuverlässigkeitsanalyse technischer Einrichtungen und Systeme (z. B. Zuverlässigkeit, Verfügbarkeit, Risikobewertung). Die Vorgehensweise der FMEA-Methode ist in der Regel induktiv (Bottom-Up-Analyse), d. h. die Analyse beginnt bei einer vorher festgelegten Betrachtungseinheit (oder einem primären Ereignis) und beschäftigt sich dann mit deren Fehlzustandsarten sowie deren Einflüssen auf nachfolgende Einrichtungen, Systeme, Funktionen bzw. Abläufe. Die FMEA-Vorgehensweise wird in /DIN 06a/, /DIN 15a/ und /NEA 15/ detailliert beschrieben und kann iterativ in verschiedenen Lebenszyklusphasen genutzt werden. Darüber hinaus kann die FMEA auf verschiedene Ebenen einer Betrachtungseinheit oder eines Prozesses angewandt werden, von höchsten Hierarchieebenen bis hinunter auf die Ebene von Einzelfunktionen oder diskreten Bauteilen, Softwarebefehlen oder spezifischen Prozeduren. In der FMEA hängt die Definition von Fehlzustandsarten, -ursachen und Auswirkungen von der Ebene der Analyse und von den Systemausfallkriterien ab, wobei die Ausfallarten auf niedrigerer Ebene zu Ausfallursachen auf höherer Ebene werden können.

Eine detaillierte Kenntnis der Systemkomponenten und ihrer Fehlerarten ist Voraussetzung für die Durchführung einer FMEA. Üblicherweise wird die FMEA für die Bewertung bereits existierender Systeme und Einrichtungen angewendet, weil hierzu entweder

Kenntnisse/Informationen zu den Ausfallursachen vorliegen oder diese anhand von Versuchen ermittelt werden können. Dennoch besteht die Möglichkeit die FMEA anhand von Modellen durchzuführen, wobei die Annahmen zu den Ausfallursachen auf der Basis von generischen Informationen getroffen werden. In der Regel müssen die Ergebnisse der modellbasierten Analyse wegen Unsicherheiten vor oder während der Inbetriebnahme der Einrichtung durch Versuche verifiziert werden. Des Weiteren sollen bei einer Sicherheitsbewertung konservative Annahmen hinsichtlich der Fehlerauswirkungen in der FMEA getroffen werden, also z. B. unwirksame Fehlererkennung vor Anforderung.

Die FMEA wird auf der Basis von Expertenschätzungen durchgeführt und in einer relativ einfach gestalteten Analysematrix (z. B. orthogonale FMEA-Tabelle) dokumentiert, in der die Ursache und die Auswirkung in einem direkten Zusammenhang dargestellt werden. Die Analyse kann durch Softwarewerkzeuge unterstützt werden, z. B. RiskSpectrum FMEA (Lloyd's Register).

Für die Analyse der Fehlerfortpflanzung innerhalb von komplexen redundanten Strukturen einer Betrachtungseinheit ist die FMEA-Methode weniger geeignet, weil hierzu die Wechselwirkungen und die logischen Verknüpfungen redundanter Komponenten innerhalb und außerhalb der Betrachtungseinheit berücksichtigt werden müssen /GRS 17/.

3.1.2 FTA – Fault Tree Analysis: Fehlzustandsbaumanalyse

Die Fehlzustandsbaumanalyse (FTA – Fault Tree Analysis) ist eine systematische Methode der modellbasierten Analyse, um die Abhängigkeiten zwischen dem Ausfall eines Systems und dem Ausfall seiner Komponenten zu ermitteln und die Wahrscheinlichkeit des Ausfalls des Systems zu berechnen /BFS 05a/. Sie dient allgemein der Analyse der Fehlerfortpflanzung innerhalb von redundanten Strukturen, wobei logische Wechselwirkungen bzw. Zusammenhänge zwischen Bestandteilen von Strukturen berücksichtigt werden. Es handelt sich um ein deduktives Analyseverfahren (Top-Down-Analyse der Fehlerauswirkungen von einer höheren Systemebene zu einer niedrigeren Systemebene) mit dem Ziel, die Kombinationen von Ursachen (Minimalschnitte der Primär- oder Basisereignisse) besonders hervorzuheben, die zum festgelegten Hauptereignis führen können. Die Analyse kann qualitativer oder quantitativer Natur sein. Die qualitative Analyse fokussiert sich auf die Analyse von Minimalschnitten (Kombinationen von Ereignissen), die zu einem unerwünschten Hauptereignis führen. Die Variationen im Fehlerbaummodell können dazu eingesetzt werden, um Strategien zur Fehlerbeherrschung zu entwickeln.

Sind die Wahrscheinlichkeiten der Primärereignisse (z. B. Ausfallwahrscheinlichkeiten der Leittechnik-Komponenten) bekannt, können die Eintrittswahrscheinlichkeiten des Hauptereignisses sowie aller Zwischenereignisse im Rahmen einer quantitativen Analyse berechnet werden (siehe /DIN 07b/), wobei die Fehlererkennung und mögliche Reparaturen berücksichtigt werden können. Des Weiteren kann auf der Basis der Fehlerbaummodellierung eine Sensitivitätsanalyse durchgeführt werden, die die wichtigsten Parameter und Unsicherheitsquellen im Modell identifizieren /GRS 12/ und damit konkrete Hinweise darüber geben kann, wo das System oder der Kenntnisstand zu diesem zu verbessern ist. Für die Fehlerbaummodellierung und -analyse ist eine Vielzahl von anerkannten und qualifizierten Werkzeugen verfügbar /NEA 12/, u. a. RiskSpectrum PSA (Lloyd's Register, wird auch in der GRS eingesetzt), FinPSA (STUK/VTT, Finnland), SAPHIRE (US NRC).

3.1.3 Methoden der Simulationsanalyse

Die Simulationsanalysen werden vorwiegend modellbasiert durchgeführt und erfordern eine Nachbildung technischer Vorgänge, wobei Bedingungen und Verhältnisse so hergestellt werden sollen, wie sie in Wirklichkeit bestehen. Im Bereich digitaler Leittechnik sind auch die Analysen der Anwendersoftware und digitaler Hardware mittels Fehlersimulation (u. a. Fault Injection Methodology) bekannt (vgl. /HSU 97/, /KOO 12/), wobei Simulationsuntersuchungen an den realen Systemen aus Verfügbarkeits- und Kostengründen selten möglich sind. Sie werden in der Regel nur für die Validierung von Modellanalysen im Rahmen von Inbetriebnahme oder Qualifizierungstests durchgeführt. Dennoch ist auch dafür die Verfügbarkeit des zu untersuchenden Systems und des Testfeldes erforderlich.

Bei modellbasierten Analysen können nach Abschluss der Modellierung alle Abläufe von den Gefahrenquellen bis zu den Auswirkungen unter Berücksichtigung von verschiedenen Randbedingungen (u. a. ungestörter Betrieb, Anforderungsfall nach externen oder internen Störungen) simuliert werden. Hierzu existieren bereits viele Modellierungs- und Analysewerkzeuge, z. B. MATLAB/Simulink-Software für die Verifizierung und Validierung eines technischen Systems.

Zu den quantitativen Methoden der Zuverlässigkeitsbewertung eines technischen Systems gehört die Monte-Carlo-Simulation. Die grundlegende Idee der Monte-Carlo-Methode besteht darin, dass für zufällig gewählte Parameter über die entsprechenden Zusammenhänge (Ursache-Wirkung-Verknüpfung) die zugehörigen Ergebnis- oder

Zielgrößen nach Stichprobenverfahren (stochastische Simulation) ermittelt werden. Die Analyseergebnisse sind quantitative Zuverlässigkeitswerte, die bei der Bewertung eines Systems eingesetzt können. Auch der zeitliche Verlauf der Komponentenzustände innerhalb der Stichproben/Spiele kann in der Analyse berücksichtigt werden, so ist es möglich innerhalb eines Spiels den Einfluss von Komponentenausfällen auf das nachfolgende Verhalten anderer Komponenten zu berücksichtigen. So kann z. B. der Ausfall einer Komponente zur höheren Belastung einer anderen Komponente führen, was deren Ausfallverhalten (negativ) beeinflussen und bei ihrer Ausfallwahrscheinlichkeit berücksichtigt werden kann. Voraussetzung für die Monte-Carlo-Simulation ist allerdings das Vorhandensein von Daten in hinreichendem Stichprobenumfang (z. B. ausreichende Betriebserfahrung) und ein korrektes Modell des technischen Systems.

Des Weiteren kann die Monte-Carlo-Methode für Sensitivitätsanalysen eingesetzt und damit der Einfluss verschiedener Parameter auf die Zuverlässigkeit der Steuerungsfunktionen ermittelt werden. Im aktuellen Vorhaben wurden auch die Modellierung und die Simulationsanalysen der Kransteuerung mittels MATLAB/Simulink-Software erprobt.

3.2 Konzept zur Analyse der Kransteuerung

3.2.1 Methodische Vorgehensweise

Die Sicherheitsanalyse der automatisierten Krananlagen und deren Steuerung kann mit keiner der oben genannten Methoden allein erfolgen, weil einzelne Methoden nur Teilaspekte der Analyse der rechnerbasierter und programmierbarer Leittechnik von Kransteuerungen umfassen. Deshalb wurde zunächst ein Konzept (s. Abb. 3.1) entwickelt, in dem die Methoden bzw. deren Elemente so zusammengesetzt wurden, dass diese den Anforderungen an die Nachweisführung (s. Kapitel 2.1 und 3.1) entsprechen.

Die einzelnen Methoden, die bei der im Konzept festgelegten Vorgehensweise verwendet werden, wurden auf Basis von GRS-Erfahrungen mit Analysen und Bewertungen rechnerbasierter und programmierbarer Leittechnik und Studien zum Stand von Wissenschaft und Technik in zuvor bei der GRS durchgeführten Forschungsvorhaben (u. a. /GRS 15a/, /GRS 15b/, /GRS 17/) ausgewählt.

Die modellbasierten Methoden aus dem Konzept zur Analyse einer Kransteuerung (s. Abb. 3.1) machten es erforderlich, zunächst einige grundsätzliche Festlegungen zur Erstellung eines Modells der Kransteuerung zu treffen:

- Modellannahmen zur Krananlage selbst, um deren Steuerungs- und Schutzfunktionen modellieren zu können,
- Festlegung der zu modellierenden Steuerungs- und Schutzfunktionen und der Abstraktionslevel der Modellierung der Leittechnik der Kransteuerung (Randbedingungen zur Erstellung von Funktionsblockdiagrammen)

Des Weiteren trägt die im Konzept dargestellte Vorgehensweise dazu bei, dass die Schnittstellen zu weiteren Aspekten der Bewertung einer gesamten Krananlage identifiziert werden. Diese Schnittstellen (u. a. Kranfahrer, mechanische Komponenten der Krananlage, Bauwerk) sollen dazu dienen, dass eine ganzheitliche Sicherheitsbewertung einer realen Krananlage systematisch bis zur Ermittlung von potenziellen Gefährdungen für Mensch und Umwelt durchgeführt werden kann. Hierzu gehören Wechselwirkungen mit den weiteren Komponenten der Krananlage (u. a. Antriebstechnik, Hub- und Fahrwerktechnik), des Bewegungsraums, der Energieversorgung und mit der Mensch-Maschine-Schnittstelle (einschließlich Arbeitsanweisungen und Personalhandlungen).

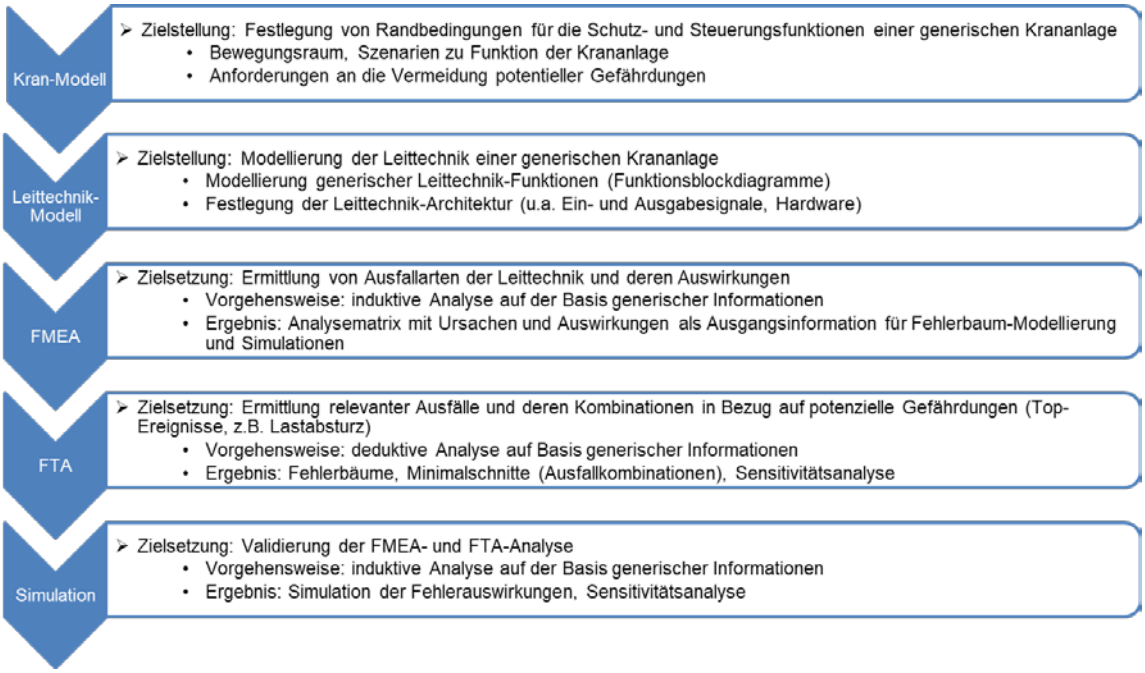

Abb. 3.1 Konzept der modellbasierten Analyse einer Kransteuerung

3.2.2 Modell der Krananlage

Bei der modellbasierten Vorgehensweise ist es erforderlich, die Funktionen der Kransteuerung zunächst anhand eines stark vereinfachten Modells einer Krananlage festzulegen. Im Vorhaben wurde eine typische sicherheitsrelevante Krananlage im Kernkraftwerk (Reaktorgebäudekran) ausgewählt und die Funktionen dieser Krananlage wurden auf der Basis von Informationen aus der KTA 3902 /KTA 19a/ spezifiziert. Der Reaktorgebäudekran besteht aus einer Brücke, die im Bewegungsraum seitlich verfahren werden kann. Entlang der Spannweite der Brücke fährt eine Laufkatze mit dem Hubwerk (siehe Abb. 3.2). Hierzu wurde die Ausrichtung des Bewegungsraums so nach Himmelsrichtungen festgelegt, dass sich die Laufkatze mit dem Hubwerk in Richtung Ost-West (Achse Y) und die Kranbrücke in Richtung Nord-Süd (Achse X) bewegen. Die Bewegungsrichtung für das Hubwerk und die Traglast wird zunächst in vertikaler Richtung (Achse Z in Abb. 3.2) festgelegt.

Der ungestörte Betriebsablauf der Krananlage beim Heben und Bewegen von Lasten ist fast immer gleich, wobei aus funktioneller Sicht die Lastabgabe analog zur Lastaufnahme erfolgt /GÜN 03/:

- Katz- und Kranfahren in die erforderliche Position,
- Senken des Lastaufnahmemittels,

- Greifen der Last,
- Verriegeln des Lastaufnahmemittels,
- Heben des Lastaufnahmemittels mit gegriffener Last,
- Kran- und Katzfahren zur Zielposition.

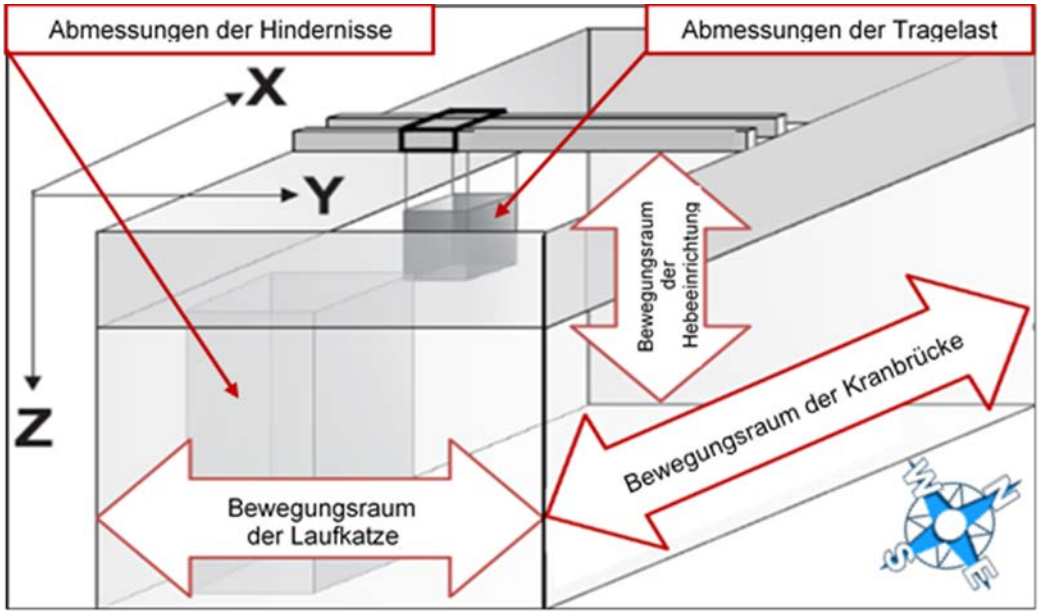

Abb. 3.2 Modell des Bewegungsraums der Krananlage (Gebäudekran)

Störungen beim Betrieb der Krananalage können prinzipiell bei allen o. g. Abläufen eintreten und ggf. zum Verletzen der Grenzen des zulässigen Bewegungsraums führen. In der Norm /DIN 09/ sind folgende sicherheitstechnische Anforderungen an die Steuerfunktionen der Krananlage gestellt:

- Stopp-Funktionen der Kategorie 0 und/oder Kategorie 1 und/oder Kategorie 2 müssen dort vorgesehen werden, wo sie aufgrund einer Risikobeurteilung und den funktionalen Erfordernissen des Hebezeuges erforderlich sind:
  - Stopp-Kategorie 0: Stillsetzen durch sofortiges Unterbrechen der Energiezufuhr zu den Antriebselementen des Hebezeuges.
  - Stopp-Kategorie 1: ein gesteuertes Stillsetzen, wobei die Energiezufuhr zu den Antriebselementen des Hebezeuges beibehalten wird, um das Stillsetzen zu erzielen. Die Energiezufuhr wird erst dann unterbrochen, wenn der Stillstand erreicht ist.

- Stopp-Kategorie 2: ein gesteuertes Stillsetzen, bei dem die Energiezufuhr zu den Antriebselementen des Hebezeuges beibehalten wird.

Die Gefährdungen durch den Betrieb der Krananlage und die entsprechende Schutzfunktionen wurden anhand generischer Informationen (u. a. Anforderungen aus Regeln und Standards) und Annahmen festgelegt. In der Studie /GÜN 03/ wurde auf folgende generelle Risiken beim Einsatz der Krananlage hingewiesen:

- Lastabstürze,
- Kollision eines Kranelementes mit einem Element der Umgebung, wobei unterschieden wird zwischen:
  - Kollisionen der Kranteile miteinander (z. B. zwischen dem Hub- und Fahrwerk),
  - Kollisionen des Krans oder der Last mit der Umgebung (z. B. Elemente der Gebäude, festpositionierte und temporäre Gegenstände innerhalb des Bewegungsraums),
  - Selbstzerstörung der Krananlage oder deren Teile (z. B. Getriebebruch, Zerstörung der Fahrwerke).

Die bei der Auswertung der spezifischen Betriebserfahrung gefundenen Fehlerfolgen lassen sich gut auf diese generellen Gefahren abbilden. Lediglich für die Fehlerfolge „nuklearspezifische Verriegelung unwirksam“ gibt es kein direktes Äquivalent, da sich /GÜN 03/ auf konventionelle Krananlagen bezieht.

Für die Spezifikation sicherheitsrelevanter Funktionen im Modell wurde der Bewegungsraum der Kranbrücke, der Hebeeinrichtung und der Laufkatze des Krans definiert, um Annahmen hinsichtlich der Festlegung von Fahr- und Hubgrenzen treffen zu können (siehe Abb. 3.2). Diese Grenzen des Bewegungsraumes wurden so festgelegt, dass die Hub- und Fahrwerke der Krananlage bei jeder Bewegung zum Stehen kommen, bevor eine Gefährdung durch einen Lastabsturz eintritt.

Es wurde zunächst angenommen, dass im Bewegungsraum keine weiteren Hindernisse außer Wände und Boden existieren, so als ob die Krananlage sich in einem leeren Raum bewegt. Aus Vereinfachungsgründen wird auch auf eine Modellierung der Größe der Traglast verzichtet. Die Last wird als ein Punkt-Modell betrachtet.

Anschließend wurden die Grenzwerte für die Bewegungen der Komponenten der Krananlage in dem spezifizierten Raum (siehe Abb. 3.2 , Länge XN-XS, Breite YW-YE, Höhe ZL-ZH) für die Modellierung der Kransteuerung festgelegt (siehe Tab. 3.2).

Tab. 3.2 Grenzwerte der verschiedenen Stopp-Funktionen

Kategorien der Stopp-Funktionen		**Kranbrücke**		**Laufkatze**		**Hubwerk**	
Nach DIN EN 60204-32	**KTA 3902**	**Grenzwert Nord**	**Grenzwert Süd**	**Grenzwert West**	**Grenzwert Ost**	**Grenzwert Unten**	**Grenzwert Oben**
2	Automatik (BELT)	XN-MIN1	XS-MIN1	YE-MIN1	YW-MIN1	ZH-MIN1	ZL-MIN1
1	Begrenzung (BELT)	XN-MIN2	XS-MIN2	YE-MIN2	YW-MIN2	ZH-MIN2	ZL-MIN2
0	Sicherheitsabschaltung (SILT)	XN-MIN3	XS-MIN3	YE-MIN3	YW-MIN3	ZH-MIN3	ZL-MIN3

3.2.3 Modell der Kransteuerung

Die Steuerung der Krananlage umfasst leittechnischen Einrichtungen zur Erfassung von Messwerten, zur Steuerung der Antriebe der Krananlage, zur Bedienung der Krananlage (u. a. Mensch-Maschine-Schnittstellen) und Hilfseinrichtungen, z. B.

- Instrumentierung / Messtechnik
    - Weggeber für Hubwerk und Fahrwerke,
    - Geschwindigkeitsmessung der Fahrwerke,
    - Lastmesseinrichtung für Hubwerk,
    - Aufsetzschalter und Stellungsüberwachung des Greifers,
    - Endlagenüberwachung des Hubwerks.
- Komponenten der Steuerung
    - Ein-/Ausgabebaugruppen für analoge und binäre (diskrete) Signale,

    - programmierbare Baugruppen der Signalverarbeitung (u. a. für Grenzwertbildung und -verarbeitung, logische Verknüpfungen),
    - Kopplungsbaugruppen (Signalinterface).
- Antriebssteuerung der Fahr- und Hubwerksmotoren
- Mensch-Maschine-Schnittstelle
    - Elemente für die manuelle Steuerung (z. B. Meisterschalter),
    - Anzeigeeinrichtungen der Beobachtungs- und Bediengeräte,
    - Testeinrichtungen.
- Stromversorgung der Leittechnik und der Antriebe.

Die Leittechnik zur Steuerung einer sicherheitsrelevanten Krananlage in einem Kernkraftwerk ist in eine Sicherheits- und eine Betriebssteuerung unterteilt und wird im weiteren als SILT und BELT bezeichnet. Die SILT ist vorgesehen, um die bei einem Auftreten von unzulässigen Betriebszuständen oder unzulässigen Überschreitungen von Begrenzungen (Wege, Geschwindigkeiten und Lasten oder deren Kombination) zu bewirken, dass die betreffenden Antriebe abgeschaltet werden und ein Anfahren der Antriebe verhindert wird. Das Abschalten eines Antriebs muss einschließen, dass die erforderlichen Bremsen wirksam werden. Die SILT muss von der BELT so unabhängig sein, dass bei bestimmungsgemäßem Betrieb, Fehlfunktionen oder Ausfällen der betrieblichen Steuerung die Funktion der Sicherheitssteuerung erhalten bleibt.

Hierbei sind folgende Vorgaben einzuhalten:

- Funktionen, die für den Betrieb des Hebezeugs erforderlich sind und nicht das Auftreten von unzulässigen Betriebszuständen oder unzulässige Überschreitungen von Begrenzungen überwachen, z. B. Fahrsteuerbefehle, sind in der betrieblichen Steuerung auszuführen.
- Die Sicherheitssteuerung überwacht die Einhaltung aller sicherheitstechnisch wichtigen Grenzwerte eines Hebezeugs und überführt das Hebezeug bei Auftreten von unzulässigen Betriebszuständen oder unzulässigen Überschreitungen von Begrenzungen in einen sicheren Zustand.

Die Funktionen der Sicherheitssteuerung (SILT) standen im Fokus der Entwicklung von Analysemethoden, weil für den Zuverlässigkeitsnachweis der SILT-Funktionen Anforderungen in der Norm DIN/IEC ISO 13849-1 und in der KTA 3902 festgelegt sind (vgl. Kapitel 2.1). Die erforderliche Zuverlässigkeit soll demzufolge durch Erfüllung sowohl deterministischer als auch probabilistischer Kriterien mittels geeigneter Analysemethoden nachgewiesen werden. Die modellbasierte Analyse der digitalen Kransteuerung wurde auf Basis eines Realisierungsbeispiels für die Steuerung des Hubwerks der Krananlage (siehe Abb. 3.3 aus der KTA 3902 /KTA 19a/) durchgeführt.

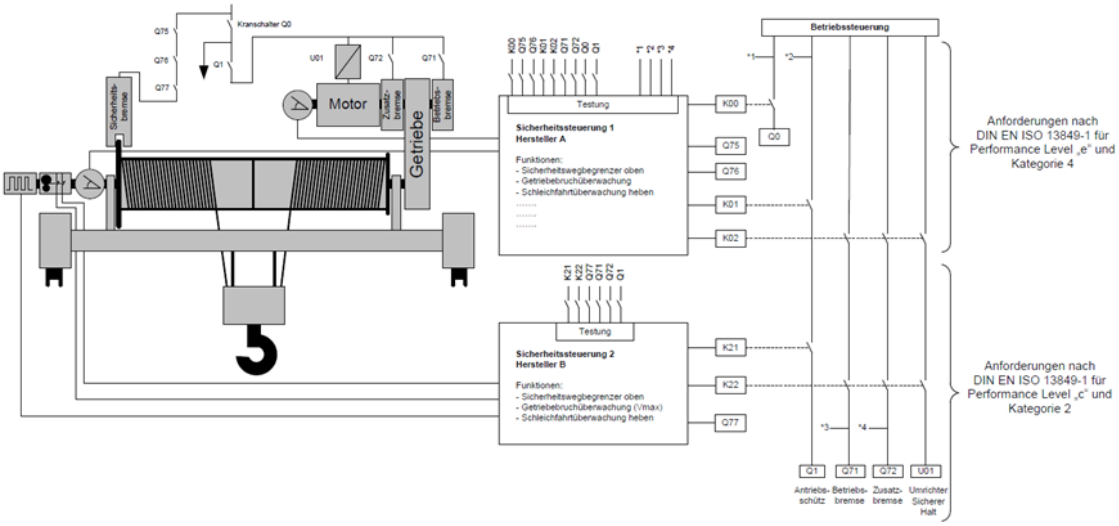

Abb. 3.3 Beispiel für die sicherheitsrelevanten Funktionen des Hubwerkes

Bei der Modellierung wurden zunächst nur die automatischen sicherheitsrelevanten Leittechnik-Funktionen (SILT- LEFU) der Krananlage spezifiziert, die zur Einhaltung der Fahr- und Lastbewegungsgrenzen (s. Tab. 3.2) erforderlich sind. Die evtl. vorhandenen mechanische Schutzeinrichtungen der Krananlage (u. a. die Rutschkupplungen, mechanischen Bremsen) werden bei der Modellierung der Kransteuerung nicht explizit berücksichtigt. Ihre Ausfälle können z. B. bei der Fehlerbaumanalyse als zusätzliche Basisereignisse (z. B. als Black-Box-Modell der Ausfälle) modelliert werden. Des Weiteren werden die betrieblichen Funktionen (u. a. Überlastungsschutz der Antriebe, Überwachung der Krananlage) nicht spezifiziert, weil hierzu ein detailliertes Modell der Krananlage erforderlich ist.

Für die Modellentwicklung der Kransteuerung wurden weitere grundsätzliche Annahmen getroffen:

- die Sicherheitssteuerungen (SILT) des Hubwerkes und der Fahrwerke (Kranbrücke und Laufkatze) werden voneinander getrennt durch verschiedene Hardware und unabhängig von der Betriebssteuerung ausgeführt,
- die Architektur der SILT wurde auf der Basis von Informationen zu einer SPS-Kransteuerung festgelegt. Die Anwendersoftware der SILT-Leittechnikfunktionen wurde ebenfalls in Anlehnung an die SPS-Software /SIE 09/ modelliert. Hierzu wurden Informationen zu fehlersicheren Baugruppen (Zentral- und Signalbaugruppen) aus der Siemens S7®-Produktfamilie SIMATIC S7-300 /SIE 13/ einbezogen,
- die auslösenden Ereignisse, die zur Anforderung von SILT-Funktionen führen können, werden bei den Analysen auf Basis generischer Informationen (u. a. Betriebserfahrungen mit Ereignissen mit Krananlagen und BE-Wechselbühnen in Kernkraftwerken, Literaturstudien, Regelwerksanforderungen) festgelegt.

Die Modellierung der SILT-Kransteuerung erfolgte durch Festlegung der typischen Merkmale bzw. Funktionen einer generischen digitalen Kransteuerung, u. a. redundante Signalverarbeitung, logische Verknüpfungen, Vorrangsteuerung. Des Weiteren wurden folgende Annahmen und Ansätze zum Aufbau (Leittechnik-Architektur) und zur Funktion der Hard- und Software der Kransteuerung getroffen:

- Black-Box-Modelle beschreiben das Verhalten der Ein- und Ausgangssignale einer Baugruppe (System, Teilsystem) und verwenden einen allgemeinen Modellansatz (u. a. regel- und wissensbasierte Modellierung, Analogiebetrachtungen) zur Evaluierung des möglichen Verhaltens der Baugruppe im Falle des Auftretens eines oder mehrerer Fehler. Zur Sicherstellung der Nachweisziele wurden konservative Annahmen hinsichtlich der Auswirkungen der Ausfälle getroffen.
- White-Box-Modelle stellen kausale Zusammenhänge innerhalb einer Baugruppe oder eines Systems dar. Die funktionalen Zusammenhänge wurden anhand vorhandener Informationen analytisch beschrieben und modelliert. Die Validierung der Modelle erfolgte mit Software-Werkzeugen der Fehlerbaum- und Simulationsanalyse. Hierzu zählen u. a. Sensitivitätsanalysen und dynamische Ablaufanalysen.
- Des Weiteren wurden Grey-Box-Modelle eingesetzt, die eine Mischform von Black-Box- und White-Box-Modellen darstellen. Typischerweise wurden diese Modelle für komplexe elektronische Komponenten /DIN 15b/ (auch als PLD-Programmable Logic

Device bezeichnet) eingesetzt, die eine Kombination von Eigenschaften besitzen, die sowohl für Hardware als auch für Software charakteristisch sind. Die PLD-Baugruppen werden zunehmend in der Antriebsteuerung und in der Instrumentierung eingesetzt, wobei typischerweise die Eigenschaften der Hardware als White-Box und die Funktionsweise der Software als Black-Box modelliert werden.

Im Vorhaben erfolgte die modellbasierte Vorgehensweise anhand weiterer Annahmen und des Erfahrungsrückflusses aus der Modellanalyse (z. B. FMEA, FTA, Simulationen) mit zunehmender Detaillierungstiefe schrittweise.

Im ersten Schritt wurde die Architektur der SILT-Steuerung der Kranbrücke (B-Bridge), des Katzfahrwerkes (T-Trolley) und des Hubwerkes (H-Hoist) anhand der Funktionspläne einheitlich festgelegt. Die Beschreibung der Architektur der SILT-Steuerungen erfolgt im Weiteren am Beispiel der Steuerung des Katzwerkes (SICF_T1/T2 – Safety Instrumentation and Control Trolley). Die SILT-Architektur besteht aus 2 gleichartigen Signalverarbeitungsredundanzen T1 und T2. In Abb. 3.4 ist der Funktionsplan der Katzsteuerung für die T1-Redundanz dargestellt. Die T2-Redundanz ist strukturell gleichartig aufgebaut und kann entweder identische oder unterschiedliche Hard- und Software enthalten. Diese Flexibilität in der Modellgestaltung ist erforderlich, um verschiedene Architektur-Varianten hinsichtlich Vorsorge gegen systematische Ausfälle in der Hard- und Software digitaler Leittechnik analysieren zu können.

- Modellierung der Hardware (siehe Abb. 3.4)
  - Die digitalen Eingänge (u. a. von Wege- und Endschaltern) werden über die Binäreingabebaugruppe (DIM – Digital Input Module) erfasst. Die Überwachung der Wege- bzw. Endschalter (A1, A2, B1 und B2) erfolgt durch die Öffner- und Schließer-Relaiskontakte.
  - Die analogen Eingangssignale (z. B. von Steuerschalter MT, Geschwindigkeitssensor VT) werden über die Analogeingabebaugruppe (AIM – Analog Input Module) eingelesen und auf ihre Plausibilität (u. a. Verletzung des zulässigen Messbereiches) überprüft.
  - Die binären Signale der Antriebssteuerung (u. a. Stromversorgung EIN/AUS, Bremsen EIN/AUS) werden über die Binärausgabebaugruppe (DOM Digital Output Module) an die Schaltanlage ausgegeben.

- Die Signalverarbeitung erfolgt in der Prozessor Baugruppe CPU durch die Anwendersoftware. In der Anwendersoftware sind die SILT-Funktionen (LEFU/ICF) durch logische Verknüpfungen (z. B. Boolean Logik: AND, OR), Grenzwertgeber und Schaltlogiken (z. B. RS-Flip-Flops) implementiert.

- Die Kopplungsbaugruppen (u. a. Leistungsschütze, Entkopplungsmodule), Messeinrichtungen (u. a. Sensoren, Wege- und Endschalter) und Bedienelemente (u. a. Master- und Schlüsselschalter) der Kransteuerung werden als Black-Box-Module bei der Modellierung und Analyse berücksichtigt.

- Modellierung der Software (siehe Abb. 3.4)

  - Die Betriebssoftware der CPU-Baugruppen der Kransteuerung wird nicht explizit modelliert. Wenn der Einfluss systematischer Ausfälle (GVA) durch die Fehlfunktion identischer Betriebssoftware untersucht werden soll, sollte dies durch konservative Annahmen zum GVA entsprechender Hardware abgedeckt werden.

  - Die Anwendersoftware der SILT wird in Anlehnung an die STEP7-Programmierung mit graphischer Verschaltung von vordefinierten Bausteinen modelliert.

  - Bei der Modellierung können prinzipiell fehlererkennende und fehlerbeherrschende Maßnahmen in der Hard- und Software je nach Bedarf (z. B. Architekturvarianten mit Signalvalidierungen) berücksichtigt werden (u. a. automatische Diagnose-Funktionen wie zyklische Überprüfungen, Einschalt- und Anfahrtests usw.). Im Vorhaben wurde zunächst der konservative Ansatz verfolgt, dass diese Maßnahmen (fault-tolerant measures) weitgehend unberücksichtigt bleiben. Sie sollen bei einer möglichen zukünftigen Weiterentwicklung der modellbasierten Analyse von Kransteuerungen auf der Basis einer realen Kransteuerung modelliert werden.

- Modellierte Funktionen (siehe Abb. 3.4)

  - Die Mensch-Maschine-Schnittstelle dient im Wesentlichen der Anzeige von ausgewählten Daten und Betriebszuständen der Anlage und wird im Modell nicht explizit berücksichtigt. Das Katzwerk (M Trolley) wird durch die Freigabe (ET-Schalter) und die Betätigung des Steuerschalters (MT-1) in Bewegung gesetzt.

- Beim Verletzen von Fahrbereichsgrenzen (SICF_T1(2)-1, 2, 3, 4, 5) oder beim Überschreiten des Geschwindigkeitsgrenzwertes (SICF_T1(2)-6) erfolgt die Abschaltung der Stromversorgung der Antriebe des Katzwerkes und die Auslösung der Bremsfunktion (Brake T1-5).
- Die Auslösung der SILT-Schutzfunktionen SICF_T1(2)-1, -2, -3, -4, -5 erfolgt nach dem Ruhestromprinzip und der Schutzfunktion SICF_T1(2)-6 nach dem Arbeitsstromprinzip.
- Die sicherheitsgerichtete (fail-safe) Funktion der SILT-Steuerung wird in den zwei Redundanzen T1 und T2 unabhängig ausgelöst, wobei jede Einzelanregung zum Abschalten der Stromversorgung oder zum Abbremsen des Antriebes führen soll.

Die SILT-Funktionen der Steuerung der Kranbrücke und des Hubwerkes unterscheiden sich von den SILT-Funktionen des Katzwerks SICF-T hinsichtlich der Eingangssignale, Anregekriterien (u. a. Grenzwerte) und in der Art manueller Betätigung (u. a. in der Freigabe- und Masterschalter-Konfiguration). Die Hardware-Architektur der SILT-Funktionen der Kranbrücke (SICF-B-1 und B-2) und des Hubwerks (SICF H-1 und H-2) bestehen ebenso wie die SILT-Funktionen des Katzwerks (SICF T-1 und T-2) jeweils aus zwei Redundanzen und sind somit praktisch identisch ausgeführt.

In Tab. 3.3 sind die wesentlichen Angaben und Parameter zu den modellierten SILT-Funktionen der Kransteuerung zusammengefasst. Die detaillierten Unterlagen zu den o. g. Modellen sind in der Projektdokumentation (Funktionsblockdiagramme / MS Visio, Konfigurationsdaten / MS Excel) abgelegt. Die Modelle sind so gestaltet, dass sie bei Bedarf für eine reale Steuerung der Krananlage hinsichtlich der eingesetzten Hard- und Software und deren Architektur mit relativ geringem Aufwand angepasst werden können.

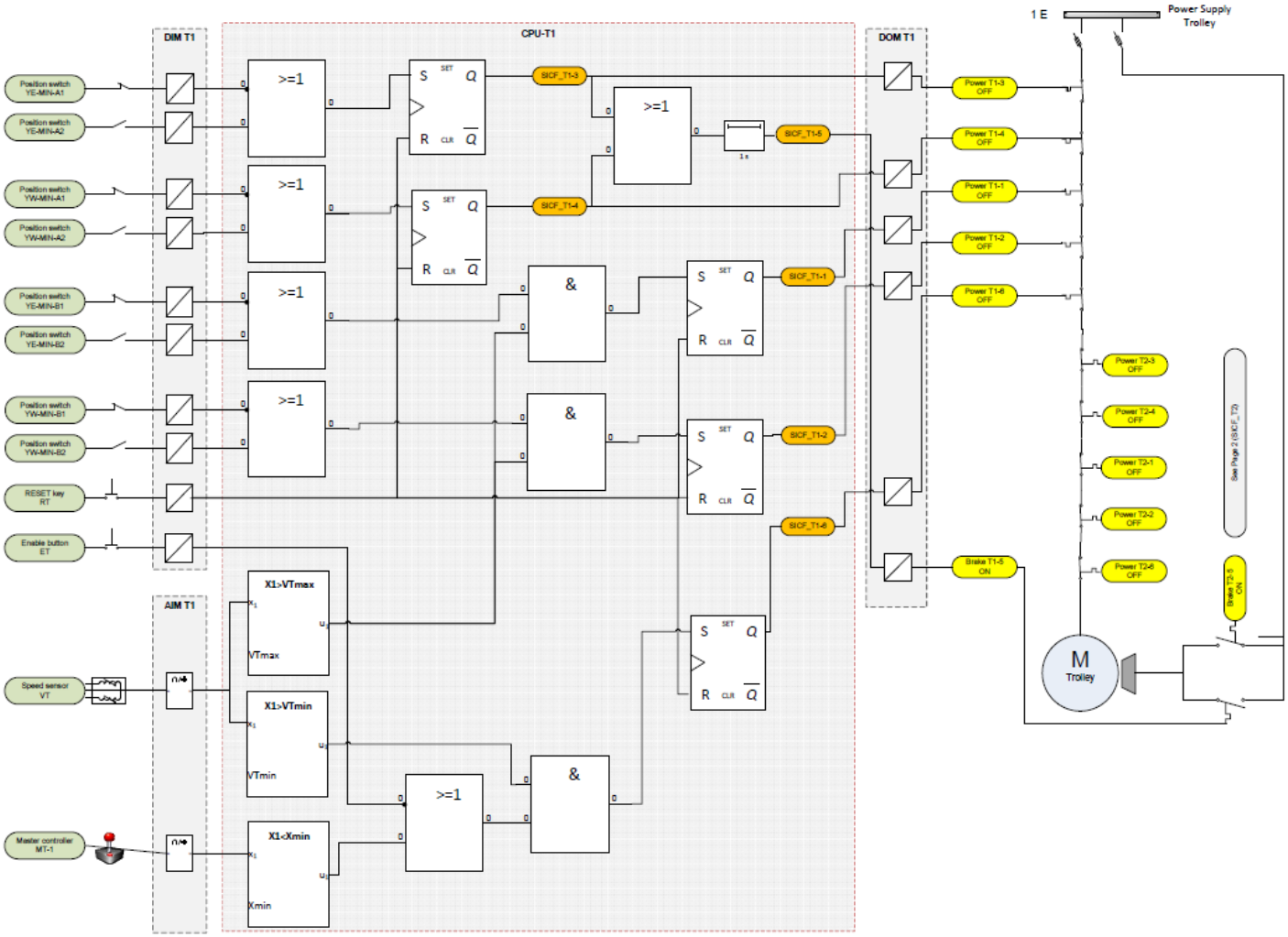

Abb. 3.4 Funktionsblockdiagramm der SILT-Steuerung des Katzwerkes des Krananlagemodells

Tab. 3.3 Zusammenstellung wichtiger Parameter der modellierten Kransteuerung

SILT-Funktion (SICF)	Antrieb	Anregekriterien	Sensor/Parameter Typ 1	Sensor/Parameter Typ 2	Anregung
T1(2)-1	Katzwerk	Geschwindigkeit > VTmax UND Wegendschalter YE-MINB	ODER-Verknüpfung aus 2 binären Wegendschaltersignale YE-MIN-B1, YE-MIN-B2	analoges Signal der Geschwindigkeitsmessung über Drehgeber VT	Abschaltung der Stromversorgung der Katz-Antriebe
T1(2)-2	Katzwerk	Geschwindigkeit > VTmax UND Wegendschalter YW-MINB	ODER-Verknüpfung aus 2 binären Wegendschaltersignale YW-MIN-B1, YW-MIN-B3	analoges Signal der Geschwindigkeitsmessung über Drehgeber VT	Abschaltung der Stromversorgung der Katz-Antriebe
T1(2)-3	Katzwerk	Überschreitung der Fahrgrenze links YE-MIN-A	binäres Endschaltersignal YE-MIN-A1	binäres Endschaltersignal YE-MIN-A2	Abschaltung der Stromversorgung der Katz-Antriebe
T1(2)-4	Katzwerk	Überschreitung der Fahrgrenze rechts YW-MIN-A	binäres Endschaltersignal YW-MIN-A1	binäres Endschaltersignal YW-MIN-A2	Abschaltung der Stromversorgung der Katz-Antriebe
T1(2)-5	Katzwerk	Auslösung von SICF_TR-3 oder SICF_TR-4	binäres Signal SICF_TR-3	binäres Signal SICF_TR-4	Auslösung der Katzwerk-Bremsen
T1(2)-6	Katzwerk	Verhinderung der unerwarteten Bewegung des Katzwerkes	ODER-Verknüpfung aus 1 analogem Signal des Meisterschalters MT < 1 % oder kein Signal von Freigabeschalter ET	analoges Signal der Geschwindigkeitsmessung über Drehgeber VT	Abschaltung der Stromversorgung der Katz-Antriebe
B1(2)-1	Brücke	Geschwindigkeit > VBmax UND Wegendschalter XN-MINB	ODER-Verknüpfung aus 2 binären Wegendschaltersignale XN-MIN-B1, XN-MIN-B2	analoges Signal der Geschwindigkeitsmessung über Drehgeber VB	Abschaltung der Stromversorgung der Kranbrücke-Antriebe
B1(2)-2	Brücke	Geschwindigkeit > VBmax UND Wegendschalter XS-MINB	ODER-Verknüpfung aus 2 binären Wegendschaltersignale XS-MIN-B1, XS-MIN-B2	analoges Signal der Geschwindigkeitsmessung über Drehgeber VB	Abschaltung der Stromversorgung der Kranbrücke-Antriebe
B1(2)-3	Brücke	Überschreitung der Fahrgrenze hinten XN-MIN-A	binäres Endschaltersignal XN-MIN-A1	binäres Endschaltersignal XN-MIN-A2	Abschaltung der Stromversorgung der Kranbrücke-Antriebe
B1(2)-4	Brücke	Überschreitung der Fahrgrenze vorn XS-MIN-A	binäres Endschaltersignal XS-MIN-A2	binäres Endschaltersignal XS-MIN-A3	Abschaltung der Stromversorgung der Kranbrücke-Antriebe
B1(2)-5	Brücke	Auslösung von SICF_BR-3 oder SICF_BR-4	binäres Signal SICF_BR-3	binäres Signal SICF_BR-4	Auslösung der Kranbrücke-Bremsen

SILT-Funktion (SICF)	Antrieb	Anregekriterien	Sensor/Parameter Typ 1	Sensor/Parameter Typ 2	Anregung
B1(2)-6	Brücke	Verhinderung der unerwarteten Bewegung der Kranbrücke	ODER-Verknüpfung aus 1 analogem Signal des Meisterschalters MB < 1 % oder kein Signal von Freigabeschalter EB	analoges Signal der Geschwindigkeitsmessung über Drehgeber VB	Abschaltung der Stromversorgung der Kranbrücke-Antriebe
H1(2)-1	Hubwerk	Hub-Geschwindigkeit > VHmax UND Wegendschalter ZH-MIN-B	ODER-Verknüpfung aus 2 binären Wegendschaltersignalen ZH-MIN-B1, ZH-MIN-B2	analoges Signal der Geschwindigkeitsmessung über Drehgeber VH	Abschaltung der Stromversorgung der Hubwerk-Antriebe
H1(2)-2	Hubwerk	Hub-Geschwindigkeit > VHmax UND Wegendschalter ZL-MIN-B	ODER-Verknüpfung aus 2 binären Wegendschaltersignalen ZL-MIN-B1, ZL-MIN-B2	analoges Signal der Geschwindigkeitsmessung über Drehgeber VH	Abschaltung der Stromversorgung der Hubwerk-Antriebe
H1(2)-3	Hubwerk	Überschreitung der Wegbegrenzung heben ZH-MIN-A	2 binäre Endschaltersignale ZH-MIN-A1 and -A2 (1oo2)	keine	Abschaltung der Stromversorgung der Hubwerk-Antriebe
H1(2)-4	Hubwerk	Überschreitung der Wegbegrenzung senken ZL-MIN-A	2 binäre Endschaltersignale ZL-MIN-A1 and -A2 (1oo2)	keine	Abschaltung der Stromversorgung der Hubwerk-Antriebe
H1(2)-5	Hubwerk	Auslösung von SICF_HR-3 oder SICF_HR-4	binäres Signal SICF_HR-3	binäres Signal SICF_HR-4	Auslösung der Hubwerk-Bremsen
H1(2)-6	Hubwerk	Überschreitung der Betriebslast (Fmax>110 %)	analoges Signal von Lastmessbolzen F1	analoges Signal von Lastmessbolzen F2	Abschaltung der Stromversorgung der Hubwerk-Antriebe
H1(2)-7	Hubwerk	Verhinderung der unerwarteten Bewegung des Hubwerkes	ODER-Verknüpfung aus 1 analogem Signal des Meisterschalters MH < 1 % oder kein Signal vom Freigabeschalter EH	analoges Signal der Geschwindigkeitsmessung über Drehgeber VH	Abschaltung der Stromversorgung der Hubwerk-Antriebe
H1(2)-8	Hubwerk	Lastmessungsgrenzwert (Fmin>1 %)	analoges Signal von Lastmessbolzen F1	analoges Signal von Lastmessbolzen F2	Verriegelung des Öffnens des Greifers

3.3 Modellbasierte Analysen der Kransteuerung

3.3.1 Fehlermode- und Ausfalleffektanalyse (FMEA) der Kransteuerung

Im Abschnitt 3.1.1 wurde bereits darauf hingewiesen, dass die Hauptaufgabe der FMEA-Analyse ist, die Ursachen und Auswirkungen von potenziellen Fehlern in einer Komponente oder einem System analytisch zu ermitteln. Demnach wurden im ersten Schritt systematisch die Einzelausfälle leittechnischer Komponenten (u. a. Sensor/Geber, Ein- und Ausgabebaugruppen, Verarbeitungslogik der Signale) der modellierten Kransteuerung (siehe Abschnitt 3.2) analysiert und deren Auswirkungen ermittelt.

Die Ausfälle wurden zunächst auf der Basis der Black-Box-Betrachtung der modellierten Baugruppen (siehe Abb. 3.4 für SILT-Funktionen des Katzwerks) analysiert, wobei die hierzu erforderlichen Annahmen auf der Basis von Festlegungen in Tab. 3.3 und der in der FMEA-Tab. 3.4 enthaltenen Funktionsbeschreibungen der Komponenten getroffen wurden. Um eine Bewertung potenzieller Fehlzustandsarten und Fehlzustandsauswirkungen auf Modellbasis zu ermöglichen, wurden weitere Annahmen hinsichtlich der internen und externen Signalverarbeitung (Grey-Box-Modell) getroffen. Dies betrifft insbesondere die Fehlererkennung (z. B. Fehlerdefinition als selbstmeldend oder erkennbar bei der Prüfung). Hierzu wurden die entsprechenden Regelwerksanforderungen bezüglich der Fehlererkennung als umgesetzt angenommen.

In Tab. 3.4 werden die Ergebnisse des ersten Schrittes der modellbasierten FMEA (Black-Box-Betrachtung) für die SILT-Steuerung des Katzwerks gezeigt, wobei die potenziellen Ausfälle der Bauteile einer Baugruppe im Zusammenhang mit den möglichen Auswirkungen dargestellt wurden. Die in der FMEA ermittelten Fehlerausfallarten der Baugruppen (Failure Modes) wurden in den nachfolgenden Analyseschritten als Basiselemente der Fehlerbaumanalyse oder Funktionsblöcke in der Simulationsanalyse eingesetzt, wobei auch die Ergebnisse der FMEA zusätzlich evaluiert und ggf. angepasst wurden. Naturgemäß sind die Ergebnisse einer FMEA, die auf einer Black-Box-Betrachtung aufgebaut ist, mit vielen Unsicherheiten behaftet, dennoch bietet diese Vorgehensweise eine gute Basis für eine zukünftige Validierung der Modelle einer Kransteuerung anhand detaillierterer Dokumente zum Aufbau und zur Funktion von deren Baugruppen und ebenso zur Prüfung und Handhabung der Kransteuerung anhand von Betriebsvorschriften.

Tab. 3.4 Ergebnistabelle der FMEA der SILT-Steuerung des Katzwerks

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
1	FBO	YE-MIN-A1	Endschalter	Öffner-Kontakt	öffnet nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-3	Prüfung
2	FBO	YE-MIN-A1	Endschalter	Öffner-Kontakt	fehlerhaft geöffnet	Fehlanregung	Fehlanregung SICF_TR1-3	selbstmeldend
3	FBC	YE-MIN-A2	Endschalter	Schließer-Kontakt	schließt nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-3	Prüfung
4	FBC	YE-MIN-A2	Endschalter	Schließer-Kontakt	fehlerhaft geschlossen	Fehlanregung	Fehlanregung SICF_TR1-3	selbstmeldend
5	FBO	YW-MIN-A1	Endschalter	Öffner-Kontakt	öffnet nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-4	Prüfung
6	FBO	YW-MIN-A1	Endschalter	Öffner-Kontakt	fehlerhaft geöffnet	Fehlanregung	Fehlanregung SICF_TR1-4	selbstmeldend
7	FBC	YW-MIN-A2	Endschalter	Schließer-Kontakt	schließt nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-4	Prüfung
8	FBC	YW-MIN-A2	Endschalter	Schließer-Kontakt	fehlerhaft geschlossen	Fehlanregung	Fehlanregung SICF_TR1-4	selbstmeldend

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
9	FBO	YE-MIN-B1	Wegschalter	Öffner-Kontakt	öffnet nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-1	Prüfung
10	FBO	YE-MIN-B1	Wegschalter	Öffner-Kontakt	fehlerhaft geöffnet	Fehlanregung	Fehlanregung SICF_TR1-1	selbstmeldend
11	FBC	YE-MIN-B2	Wegschalter	Schließer-Kontakt	schließt nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-1	Prüfung
12	FBC	YE-MIN-B2	Wegschalter	Schließer-Kontakt	fehlerhaft geschlossen	Fehlanregung	Fehlanregung SICF_TR1-1	selbstmeldend
13	FBO	YW-MIN-B1	Wegschalter	Öffner-Kontakt	öffnet nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-2	Prüfung
14	FBO	YW-MIN-B1	Wegschalter	Öffner-Kontakt	fehlerhaft geöffnet	Fehlanregung	Fehlanregung SICF_TR1-2	selbstmeldend
15	FBC	YW-MIN-B2	Wegschalter	Schließer-Kontakt	schließt nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-2	Prüfung
16	FBC	YW-MIN-B2	Wegschalter	Schließer-Kontakt	fehlerhaft geschlossen	Fehlanregung	Fehlanregung SICF_TR1-2	selbstmeldend
17	FBC	RT	Reset-Taste	Schließer-Kontakt	schließt nicht	Ausfall bei Anforderung	Ausfall der Rücksetzung der Anregung	Prüfung

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
18	FBCS	RT	Reset-Taste	Schließer-Kontakt	fehlerhaft geschlossen	Ausfall bei Anforderung	Deaktivierung aller Funktionen von SICF-TR1	Prüfung
19	FBC	ET	Freigabe-Taste	Schließer-Kontakt	schließt nicht	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-2	Prüfung
20	FBCS	ET	Freigabe-Taste	Schließer-Kontakt	fehlerhaft geschlossen	Fehlanregung	Fehlanregung der Katzbewegung	selbstmeldend
21	FAH	VT	Geschwindigkeitssensor	Analogsignal	Signal zu hoch	Ausfall bei Anforderung	keine Sicherheitsrelevanz	Prüfung
22	FAL	VT	Geschwindigkeitssensor	Analogsignal	Signal zu niedrig	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1-1	Prüfung
23	FAI	VT	Geschwindigkeitssensor	Analogsignal	Invarianter Wert	Ausfall bei Anforderung	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
24	FAH	MT	Meister-Schalter	Analoges Steuerungssignal	Signal zu hoch	nicht anwendbar	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden
25	FAL	MT	Meister-Schalter	Analoges Steuerungssignal	Signal zu niedrig	nicht anwendbar	sollte im spezifizierten Anforderungsfall analysiert werden	Prüfung oder beim manuellen Fahren
26	FAI	MT	Meister-Schalter	Analoges Steuerungssignal	Invarianter Wert	nicht anwendbar	sollte im spezifizierten Anforderungsfall analysiert werden	Prüfung oder beim manuellen Fahren
27	FDHall	DIM-TR1	Digitalsignal-Eingabe-Baugruppe, 16 Kanäle	Entkopplung und Erfassung binärer Signale	feste "1" auf allen Kanälen	Fehlanregung	Fehlanregung SICF_TR1	selbstmeldend
28	FDLall	DIM-TR1	Digitalsignal-Eingabe-Baugruppe, 16 Kanäle	Entkopplung und Erfassung binärer Signale	feste "0" auf allen Kanälen	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1	Prüfung
29	FDHone	DIM-01-TR1	Digitalsignal-Eingabe-Baugruppe, 1 Kanal	Entkopplung und Erfassung binärer Signale	feste "1" auf einem Kanal	Fehlanregung	Fehlanregung SICF_TR1	selbstmeldend

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
30	FDLone	DIM-01-TR1	Digitalsignal-Eingabe-Baugruppe, 1 Kanal	Entkopplung und Erfassung binärer Signale	feste "0" auf einem Kanal	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1	Prüfung
31	FAHall	AIM-TR1	Analogsignal-Eingabe-Baugruppe, 16 Kanäle	Entkopplung und Erfassung analoger Signale	Signal zu hoch auf allen Kanälen	siehe Ausfallart von MT und VT	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden
32	FALall	AIM-TR1	Analogsignal-Eingabe-Baugruppe, 16 Kanäle	Entkopplung und Erfassung analoger Signale	Signal zu niedrig auf allen Kanälen	siehe Ausfallart von MT und VT	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden
33	FAIall	AIM-TR1	Analogsignal-Eingabe-Baugruppe, 16 Kanäle	Entkopplung und Erfassung analoger Signale	Invarianter Wert (alle Kanäle)	siehe Ausfallart von MT und VT	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
34	FAHone	AIM-01-TR1	Analogsignal-Eingabe-Baugruppe, 1 Kanal	Entkopplung und Erfassung analoger Signale	Signal zu hoch	siehe Ausfallart von MT und VT	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden
35	FALone	AIM-01-TR1	Analogsignal-Eingabe-Baugruppe, 1 Kanal	Entkopplung und Erfassung analoger Signale	Signal zu niedrig	siehe Ausfallart von MT und VT	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden
36	FAIone	AIM-01-TR1	Analogsignal-Eingabe-Baugruppe, 1 Kanal	Entkopplung und Erfassung analoger Signale	Invarianter Wert	siehe Ausfallart von MT und VT	sollte im spezifizierten Anforderungsfall analysiert werden	sollte im spezifizierten Anforderungsfall analysiert werden
37	FDHall	DOM-TR1	Digitalsignal-Ausgabe-Baugruppe, 16 Kanäle	Entkopplung und Ausgabe binärer Signale	feste "1" auf allen Kanälen	Fehlanregung	Fehlanregung all SICF_TR1	selbstmeldend
38	FDLall	DOM-TR1	Digitalsignal-Ausgabe-Baugruppe, 16 Kanäle	Entkopplung und Ausgabe binärer Signale	feste "0" auf allen Kanälen	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1	Prüfung

lfd. Nr.	FMEA-Code	Bauteil	Funktion Baugruppe	Funktion Bauteil	Ausfallart Bauteil, Signal	Fehlertyp	Auswirkung übergeordnete Funktion	Erkennung
39	FDHone	DOM-01-TR1	Digitalsignal-Ausgabe-Baugruppe, 1 Kanal	Entkopplung und Ausgabe binärer Signale	feste "1" auf einem Kanal	Fehlanregung	Fehlanregung SICF_TR1	selbstmeldend
40	FDLone	DOM-01-TR1	Digitalsignal-Ausgabe-Baugruppe, 1 Kanal	Entkopplung und Ausgabe binärer Signale	feste "0" auf einem Kanal	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1	Prüfung
41	FPMall	CPU-TR1	Prozessor-Baugruppe	Digitale Signalverarbeitung	Ausfall der DOM-Baugruppe (alle Signale)	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1	Prüfung
42	FPMall	CPU-TR1	Prozessor-Baugruppe	Digitale Signalverarbeitung	Ausfall der DOM-Baugruppe (alle Signale)	Fehlanregung	Fehlanregung SICF_TR1	selbstmeldend
43	FPMone	CPU-TR1	Prozessor-Baugruppe	Digitale Signalverarbeitung	Ausfall der DOM-Baugruppe (ein Signal)	Ausfall bei Anforderung	Ausfall der Anregung SICF_TR1	Prüfung
44	FPMone	CPU-TR1	Prozessor-Baugruppe	Digitale Signalverarbeitung	Ausfall der DOM-Baugruppe (ein Signal)	Fehlanregung	Fehlanregung SICF_TR1	selbstmeldend

3.3.2 Fehlerbaummodellierung und -analyse der Kransteuerung

Die Erkenntnisse aus der Modellierung (siehe Abschnitt 3.2) und aus der modellbasierten FMEA der Kransteuerung (siehe Abschnitt 3.3.1) haben gezeigt, dass die Analyse eines Teiles der Kransteuerung für die Methodenentwicklung ausreichend ist, da sich die leittechnischen Architekturen der Steuerung von Katzwerk und Hubwerk gleichen, und der weitere Aufwand zur Modellierung und Analyse eines symmetrischen und aus identischen Modulen aufgebauten Modells der Kransteuerung keine weiteren Erkenntnisse bringt. Für die Fehlerbaumanalyse wurde deshalb beispielhaft das Modell der Steuerung der Laufkatze herangezogen und als Ereignis ein Lastabsturz durch einen Fehler der Laufkatze ausgewählt.

- Ereignisablauf

Für den Ereignisablauf wird angenommen, dass das Katzwerk spontan, z. B. durch eine Fehlfunktion der betrieblichen Leittechnik, in Richtung der Ostseite des Gebäudes (E) mit maximaler Geschwindigkeit in Bewegung gesetzt wird. Nur unter der Voraussetzung, dass solch ein Ereignis vorliegt, kann es überhaupt zu einem Lastabsturz durch das Versagen der Schutzeinrichtungen der Katze kommen (falls die gestaffelten Schutzfunktionen gerade dann versagen).

- Hypothesen und Annahmen zur Fehlerbaummodellierung

Die Fehlerbaumanalyse soll umfassende und nachvollziehbare Aussagen zu sicherheitsrelevanten Funktionen im Anforderungsfall liefern.

Der ungestörte Ablauf des untersuchten Fahrvorgangs setzt voraus, dass beim Verfahren der Katze in Richtung Osten drei gestaffelte Leittechnik-Funktionen (LEFU) durch eine automatische Anregung bei Erreichen der gestaffelten Fahrbereichsgrenzwerte einen Lastabsturz verhindern sollen.

Tab. 3.5 Leittechnik-Funktionen und Fahrbereichsgrenzen des Katzfahrwerks

Leittechnik-Funktion	**Fahrbereichsgrenzen in Ost-Richtung YE**
Sicherheitsleittechnik SILT: SICF-T1	YE-MIN-A
Begrenzung - Betriebsleittechnik BELT: LICF	YE-MIN-B
Automatische Steuerung - Betriebsleittechnik BELT: OICF	YE-MIN-C

Eine Verletzung des OICF-Grenzwertes YE-MIN-C führt noch zu keiner Auslösung automatischer Maßnahmen, es erfolgt aber eine Meldung an den Leitstand. Damit es überhaupt zu einem weiteren Fehler kommen kann, muss also diese Meldung gestört sein oder vom Bediener ignoriert werden. Danach greift zunächst der LICF-Grenzwert YE-MIN-B und die BELT schaltet die Antriebe ab. Falls diese Maßnahme nicht wirksam wird und der Grenzwert YE-MIN-A erreicht greift die SILT ein.

Zunächst wurde ein sehr vereinfachtes Modell der Betriebsleittechnik (OICF), siehe Abb. 3.5 (Teil 1) und Abb. 3.6 (Teil 2) erstellt. In Abb. 3.5 (Teil 1) wird der Teil des Modells gezeigt, in dem die Fahrbefehle des Katzwerks generiert werden. Das Modell berücksichtigt nicht die Verriegelungen (z. B. Blockierung von gegensätzlichen Befehlen) und Meldungen an die Mensch-Maschine-Schnittstelle der Krananlage.

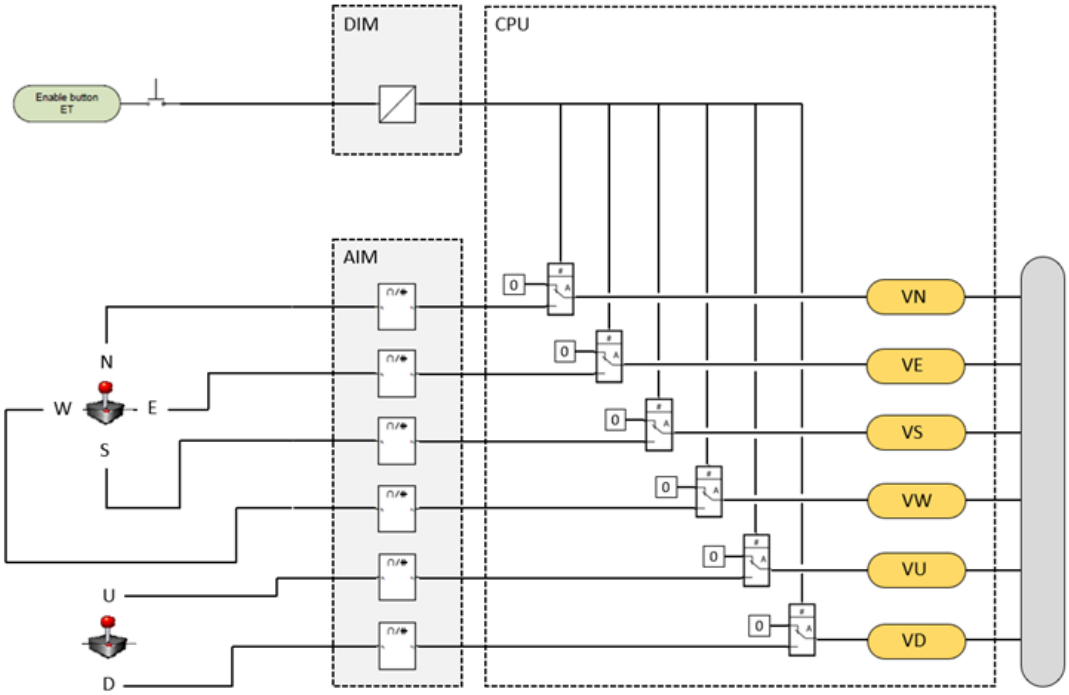

Abb. 3.5 Modell der Betriebsleittechnik-Funktionen OICF (Teil 1)

In Abb. 3.5 ist die Generierung von Fahrbefehlen mit unterschiedlichen Geschwindigkeiten in alle Bewegungsrichtungen der Krananlage (VN-Nord, VE-Ost, VS-Süd, VW-West, VU-Oben, VD-Unten) dargestellt. Hierzu soll der entsprechende Joystick (W-E-Richtung für das Katzwerk) sowie der Freigabe-Knopf (ET) betätigt werden. Der Freigabe-Knopf (ET) wird nur in den LEFUs der betrieblichen Leittechnik bei der Generierung der Fahrbefehle berücksichtigt. Die Joystick-Eingaben laufen über die analogen Eingabebaugruppen (AIM – Analog Input Module). Die Betätigung des Freigabe-Knopfs läuft über eine digitale Eingabebaugruppe (DIM – Digital Input Module). Beide werden dann auf der CPU-Baugruppe verarbeitet.

Des Weiteren werden für die betrieblichen Grenzwerte in der betrieblichen Leittechnik (OICF) Meldungen generiert und ein Signal („Fahrbefehl“) für die Weiterverwendung in der SILT erzeugt (Teil 2 des Modells der Betriebsleittechnikfunktionen, siehe Abb. 3.6).

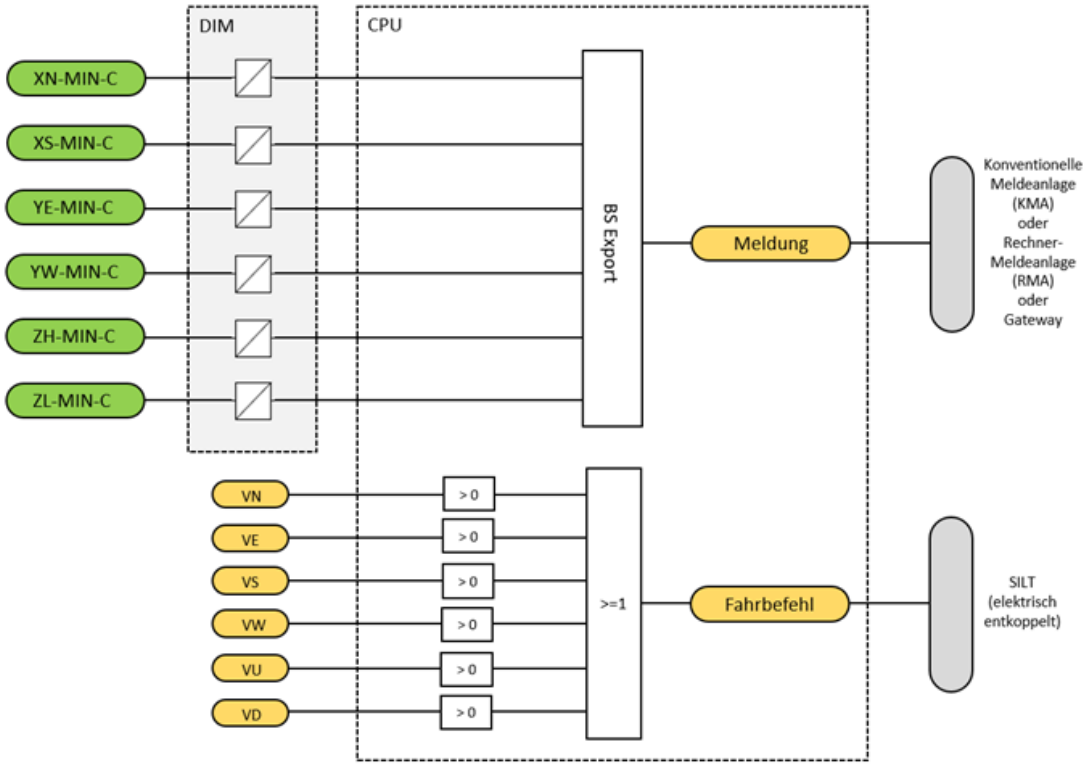

Abb. 3.6 Modell der Betriebsleittechnik-Funktionen OICF (Teil 2)

Die Sicherheits-Leittechnikfunktionen (SILT-Funktionen) der Kransteuerung wurden auf der Basis des Funktionsblockdiagramms im Abschnitt 3.2.3 (Abb. 3.4) für die Fehlerbaummodellierung erstellt. In Abb. 3.7 ist exemplarisch die SILT-Funktion SICF-T1-6 für das Katzwerk in einer der beiden Redundanzen dargestellt. Die Auslösung der Funktion SICF_T1-6 erfolgt, wenn mehr als eine Sekunde kein Fahrbefehl mehr ansteht und die Geschwindigkeit des Katzwerks aber immer noch größer als VTmin ist. Sie schaltet die Antriebe ab. Man beachte, dass der untere Eingang in das UND negiert ist und das verwendete Zeitglied eine Abfallverzögerung (OFFDELAY) von 1 s darstellt. Außerdem wurde der Flipflop-Baustein (wie auch alle anderen Flipflops im Funktionsplan) als RESET-dominant gekennzeichnet und modelliert. Wie in der Gesamtübersicht der sicherheitstechnischen Funktionen des Katzwerks (SICF, Abb. 3.8) ersichtlich, können sämtliche angeregte Funktionen (SICF_T1-1 bis SICF_T1-6) über einen gemeinsamen RESET-Schlüsselschalter (RT) gelöscht werden. Während des RESET-Vorgangs ist die gesamte SILT deaktiviert.

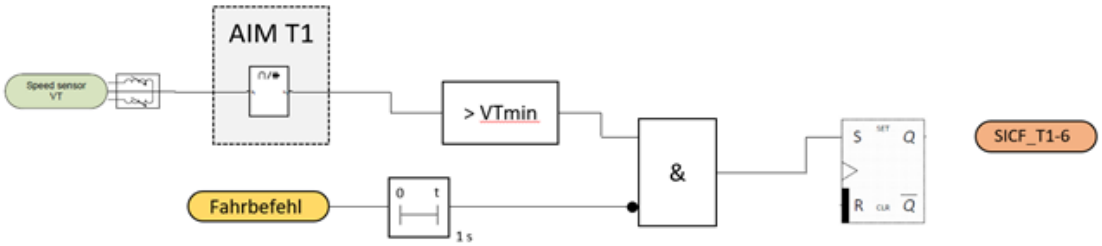

Abb. 3.7 Auslösung der SICF-T6 Funktion im Modell

Bei den Funktionen SICF_T1-1 und SICF_T1-2 handelt es sich um Sicherheitsfunktionen, die bei Erreichen des ersten Wegendschalters (T1-1 für den östlichen, T1-2 für den westlichen) der Sicherheitssteuerung und gleichzeitigem Vorliegen einer Geschwindigkeit größer als der Grenzwert VTmax (was bedeutet, dass die Bremsung nicht ordnungsgemäß eingeleitet wurde) die Antriebe abschalten. Die Funktionen SICF_T1-3 und SICF_T1-5 schalten bei Erreichen des zweiten Wegendschalters (T1-3 für den östlichen, T1-4 für den westlichen) der Sicherheitssteuerung die Antriebe ab und über SICF_T1-5 wird gleichzeitig die Sicherheitsbremse eingelegt.

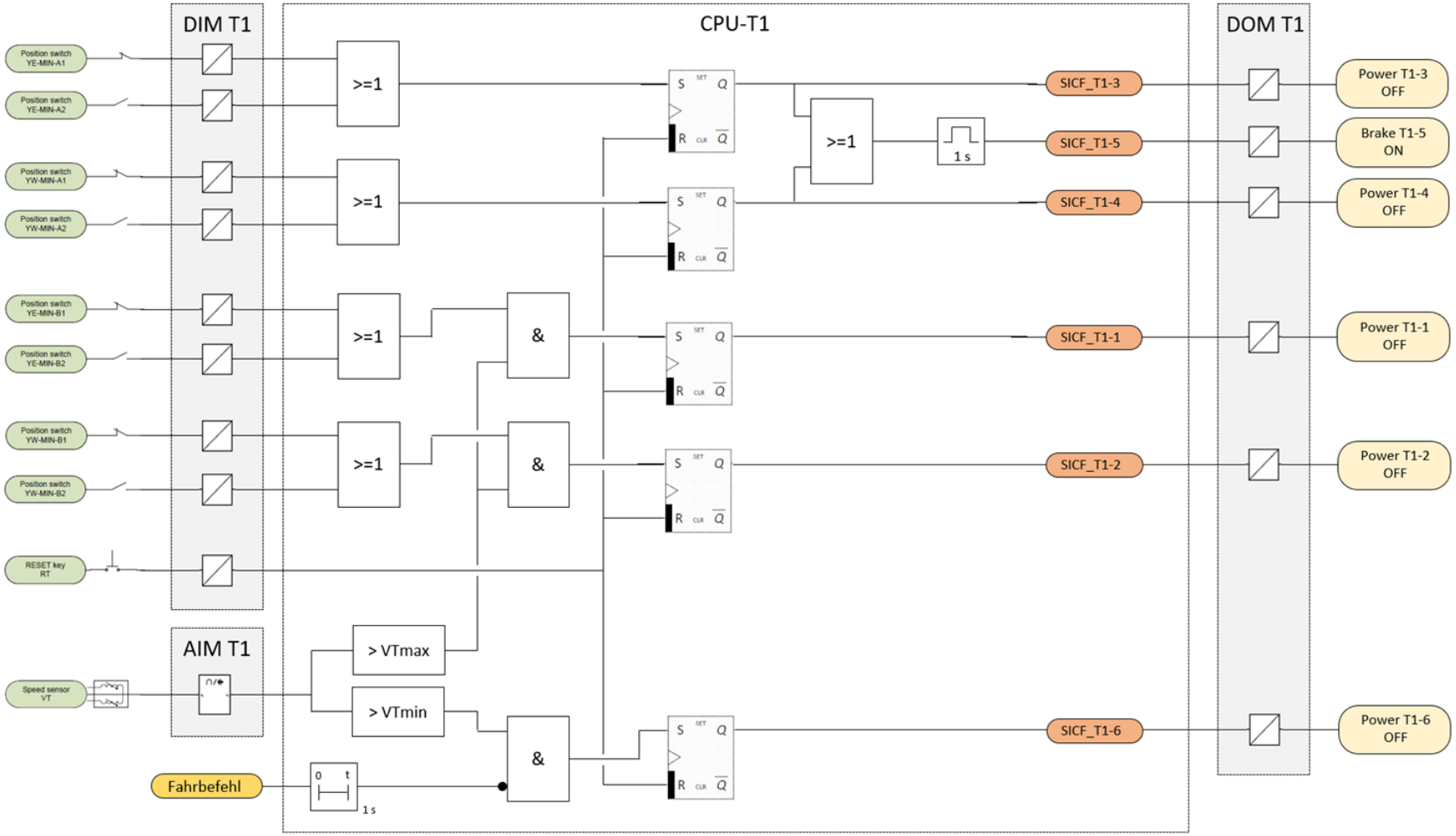

Abb. 3.8 Modell der SILT-Funktionen des Katzwerks SICF

Die Auslösung der Bremsfunktion SICF_T1-5 erfolgt nach Verletzung einer der beiden Grenzwerte YE-MIN-A oder YW-MIN-A, wobei das Auslösesignal auf 1 Sekunde begrenzt wird.

Die Quantifizierung der Fehlerbaumanalyse erfolgte auf Basis generischer Informationen und ingenieurtechnischer Schätzungen. Ziel der ingenieurtechnischen Einschätzung war es Zahlen in plausiblen Größenordnungen zur Erprobung der Methode abzuschätzen. Die folgenden Zahlen müssten daher bei der Bestimmung der Zuverlässigkeit einer realen Krananlage durch eine Auswertung der Zuverlässigkeit der jeweiligen kranspezifischen Einzelkomponenten und Bauteile ersetzt bzw. ergänzt werden.

Die Zuverlässigkeit der Sicherheitsbremsen (einschließlich der Ansteuerung) der Krane (nach KTA 3902 4.3) wurde wie folgt eingeschätzt:

- Kumulierte Betriebszeit ≈ 1.373 Jahre, bei ≈1 Funktionsausfall:
  - λ (Si.-Bremse) = 1/1.373 Jahre = 0,73 x 10E-3/Jahr = 0,83 x 10E-7/h
- Nichtverfügbarkeit der Sicherheitsbremse (Prüfintervall t = 1 Jahr):
  - q (Si.-Bremse / t = 1a) = 0,83 x 10E-7/h x 8670h = 0,73 x 10E-3

Des Weiteren wurden auch Daten aus dem PSA Datenband /BFS 05b/ für leittechnischen Komponenten und aus weiteren Forschungsvorhaben der GRS zur Analyse digitaler Leittechnik /PIL 10/ zur Abschätzung plausibler Daten herangezogen. Die wesentlichen hieraus abgeleiteten Parameter sind in Tab. 3.6 zusammengefasst.

Tab. 3.6 Generische Zuverlässigkeitsgrößen für die Fehlerbaumelemente

Lfd. Nr.	Modul	Ausfallarten	Ausfallwahrscheinlichkeit (Anforderungsdauer 1 Jahr)
1	Endlagenschalter (Stop Position Switch)	Öffnet/Schließt nicht	1.10 E-03
2	Wegeschalter (Position Switch)	Öffnet/Schließt nicht	6.00 E-03
3	Freigabe-Schalter (Enable Button)	Öffnet/Schließt nicht	6.00 E-03
4	Geschwindigkeitssensor (Speed Sensor)	Ausfall Richtung Null/Vollausschlag	1.00 E-03
5	Hauptregler/Meisterschalter (Master Controller)	Ausfall Richtung Null/Vollausschlag	1.00 E-01
6	Digitale Eingabebaugruppe (Digital Input Module (DIM) for 16 Signals)	Ausfall aller Signale auf “1" oder “0”	2.40 E-03
7	Analoge Eingabebaugruppe (Analog Input Module (AIM) (one Channel))	Ausfall aller Signale auf “Null" oder “Vollausschlag”	2.40 E-03
8	Digitale Ausgabebaugruppe Digital Ouput Module (DOM) for 16 Signals	Ausfall aller Signale auf “1" oder “0”	2.0 E-03
9	Prozessor-Baugruppe (Processing Unit (PU))	Ausfall der DOM (alle Signale)	2.40 E-03
10	Relais	Öffnet/Schließt nicht	CCF: Kopplungsmodell /BFS 05b/
11	Anwendungssoftware (LEFU) (Application Software)	Ausfall der PU (SICFn)	CCF: β-Faktor-Modell

Auf Grundlage der Funktionspläne (Abb. 3.5 bis Abb. 3.8) und der o. g. Annahmen wurden für ein Top-Ereignis („Lastabsturz“) die entsprechenden Fehlerbäume erstellt. Auszüge aus diesem Fehlerbaummodell sind in den Abb. 3.9ff. dargestellt, um dessen Erstellung exemplarisch nachvollziehbar darzustellen.

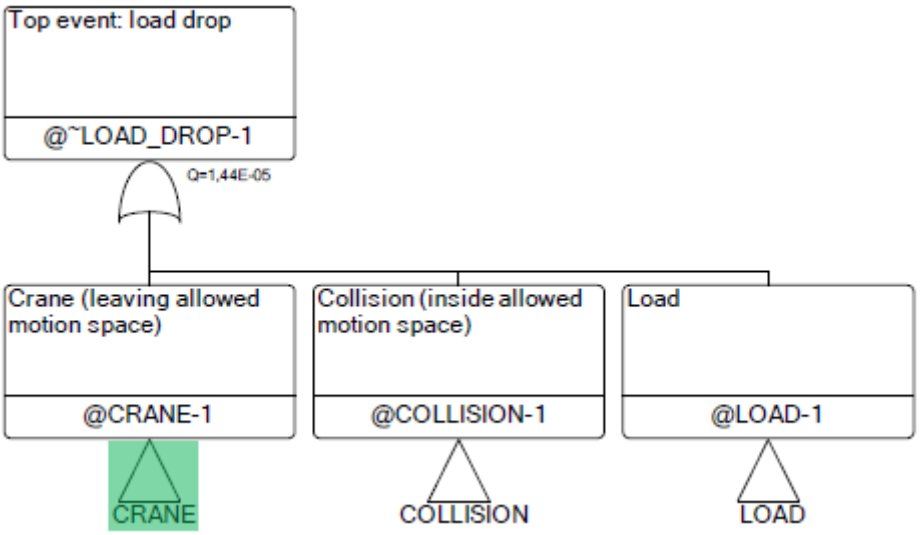

Abb. 3.9 Top-Ereignis im Fehlerbaummodell zum Lastabsturz.

Exemplarisch ist die Fortsetzung des grün markierten Zweigs in der nachfolgenden Abb. dargestellt.

Ein Lastabsturz kann durch das Verlassen des erlaubten Bewegungsraums, durch Kollisionen innerhalb des erlaubten Bewegungsraums oder durch die Last selbst (z. B. durch Überlast) verursacht werden. Abb. 3.10 zeigt, dass das Verlassen des erlaubten Bewegungsraums durch die Brücke („Bridge“), das Katzwerk („Trolley“) oder das Hubwerk („Hoist“) verursacht werden kann.

Wie exemplarisch für das Katzwerk in Abb. 3.11 dargestellt, kann der erlaubte Bewegungsraum jeweils nur in bestimmten Richtungen verlassen werden (hier östlich „E“ oder westlich „W“). Hierzu muss jedoch gerade eine Bewegung in der entsprechenden Richtung stattfinden („Moving E“ bzw. „Moving W“) und gleichzeitig müssen die entsprechenden Sicherheitsabschaltungen versagen („No Power [...] OFF“).

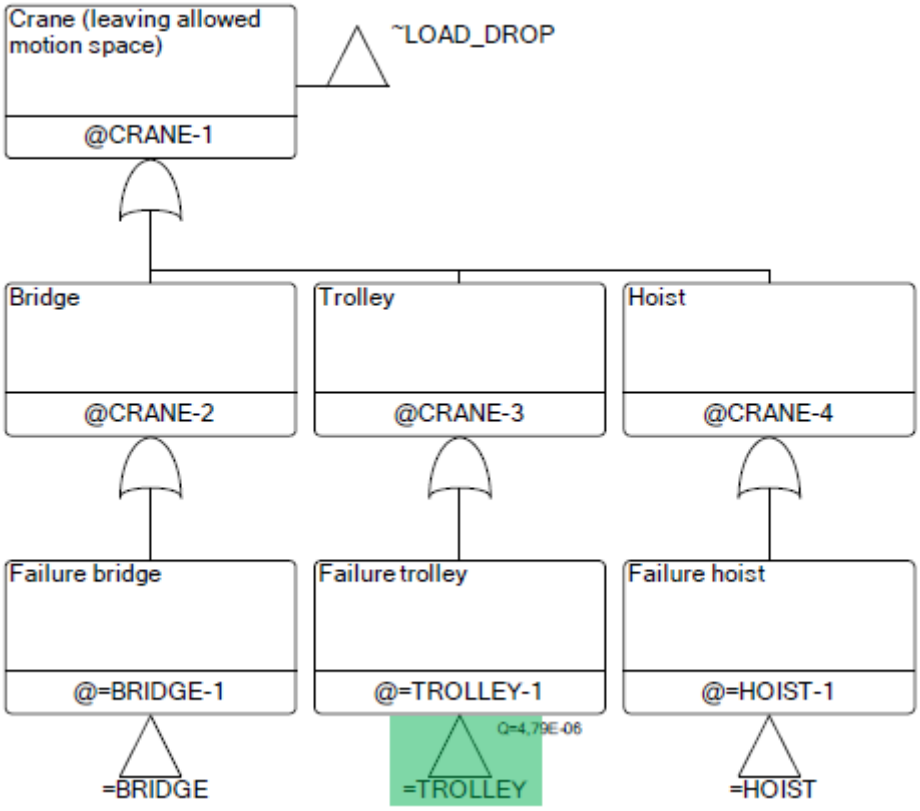

Abb. 3.10 Fortsetzung des Fehlerbaums aus Abb. 3.9: Verlassen des erlaubten Bewegungsraums durch Brücke, Katze oder Hubwerk

Exemplarisch ist die Fortsetzung des grün markierten Zweigs in der nachfolgenden Abb. dargestellt.

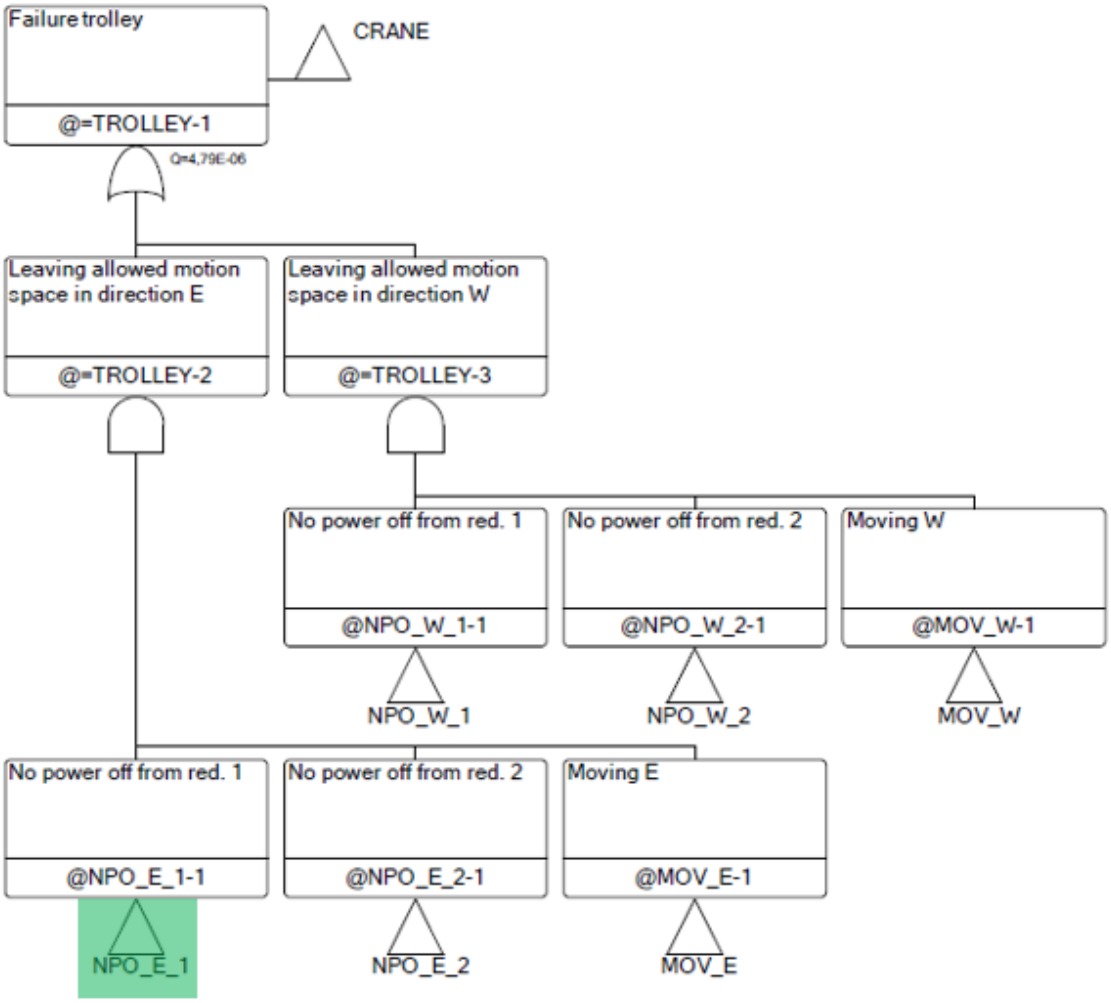

Abb. 3.11 Fortsetzung des Fehlerbaums aus Abb. 3.10: Das Katzwerk („Trolley“) kann den erlaubten Bewegungsraum („allowed motion space“) in östlicher („E“) oder westlicher („W“) Richtung verlassen.

Repräsentativ wird eine Ursache („No power off from red. 1“, grün markiert) in der nachfolgenden Abbildung detaillierter dargestellt.

Abb. 3.12 und Abb. 3.13 zeigen exemplarisch weitere Details des Fehlerbaummodells zum Lastabsturz (Abb. 3.12 ist die Fortsetzung des grün markierten Zweigs in Abb. 3.11, Abb. 3.13 wiederum ist die Fortsetzung des grün markierten Zweigs in Abb. 3.12).

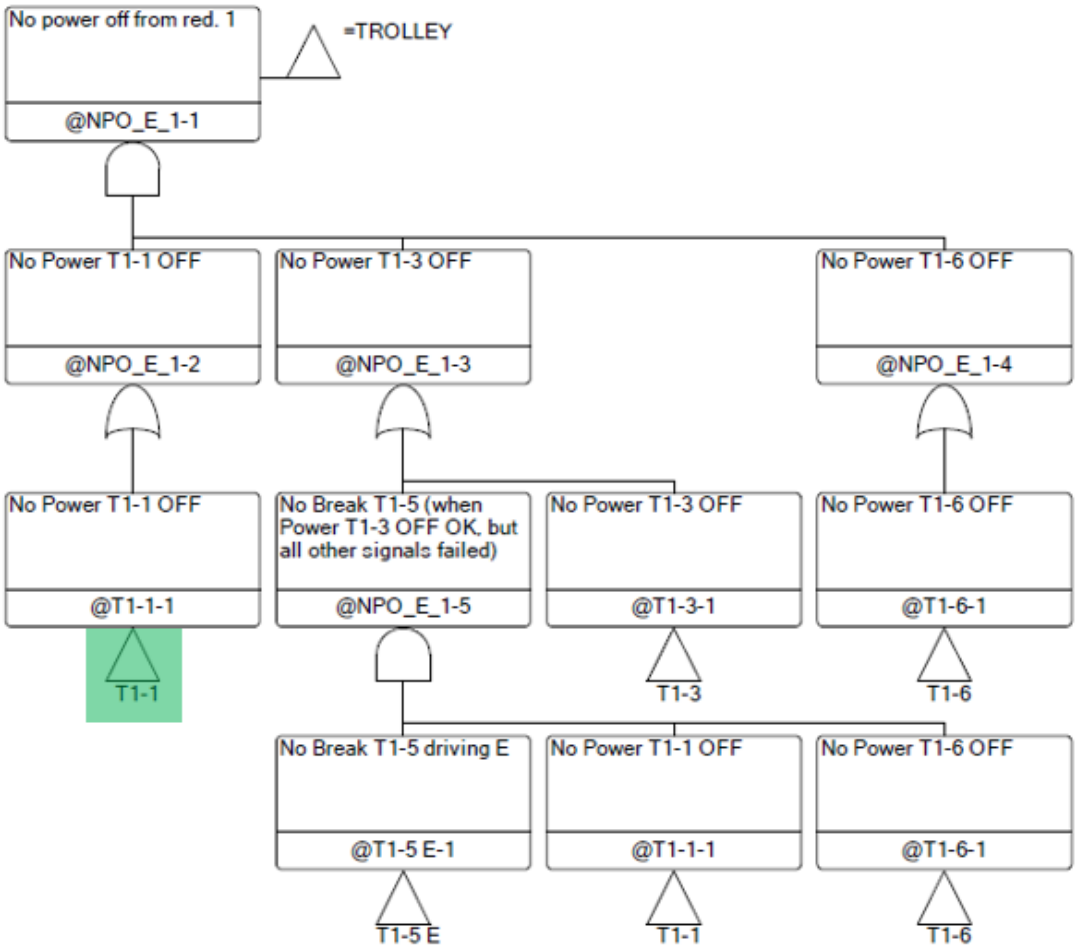

Abb. 3.12 Fortsetzung des Fehlerbaums aus Abb. 3.11: Die Nichtabschaltung des Katzwerks („Trolley“) durch die Redundanz 1 („No power off from red. 1“) bei einer ungewollten Bewegung in östlicher Richtung.

Exemplarisch zeigt die nachfolgende Abbildung den grün markierten Zweig.

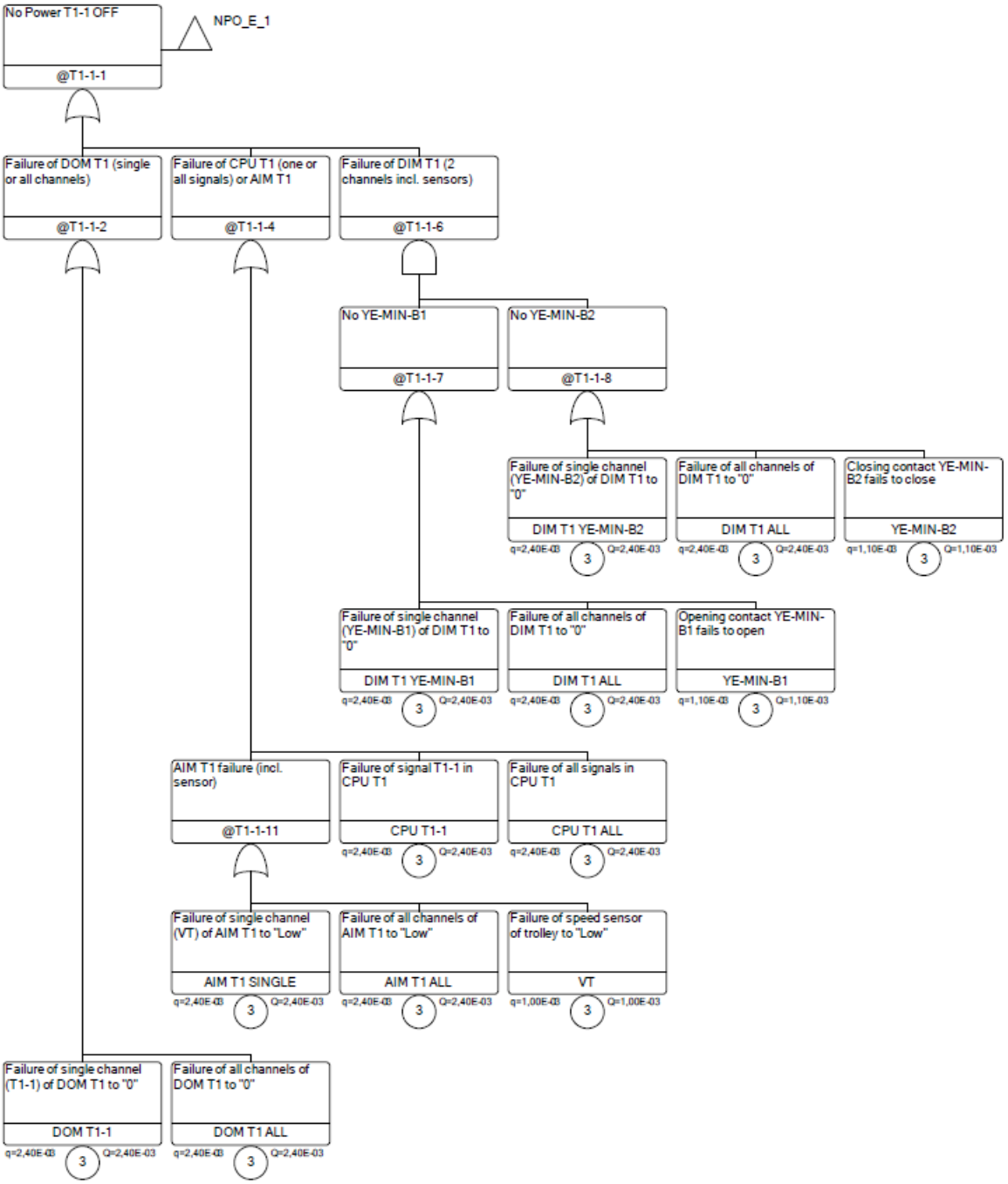

Abb. 3.13 Fortsetzung des Fehlerbaummodells zum „Lastabsturz“, die die Ursachen für das Versagen des Signals „T1-1“ aus Abb. 3.12 darstellt

Das in den vorangegangenen Abbildungen auszugsweise dargestellte Gesamtfehlerbaummodell zum Lastabsturz erlaubt, im Gegensatz zur FMEA, auch quantitative Aussagen hinsichtlich der Fehlerkombinationen, die zum Eintritt des Top-Ereignisses beitragen (die sogenannten Minimalschnitte bzw. Minimal Cut Sets (MCS)). Im vorliegenden Fall gibt es z. B. für das Katzwerk 16.471 Minimalschnitte, welche zu einem Lastabsturz führen. Von diesen tragen allerdings bereits die ersten acht Minimalschnitte den größten

Teil zur Gesamteintrittswahrscheinlichkeit eines Lastabsturzes bei (siehe Tab. 3.7). Jeder der acht MCS trägt 12,28 % der Gesamteintrittswahrscheinlichkeit eines Lastabsturzes verursacht durch das Katzwerk bei.

Tab. 3.7 Die ersten 8 von insgesamt 16.471 Minimalschnitten allein für das Katzwerk, die zu einem Lastabsturz führen

Nr.	Wskt.	%	Ereignis 1	Ereignis 2	Ereignis 3
1	5,76 E-07	12,28	CCF[4] CPU[5] T1[6] ALL	CCF DOM[7] T2[8] ALL[9]	Unbeabsichtigte[10] Bewegung in Richtung Osten
2	5,76 E-07	12,28	CCF CPU T1 ALL	CCF DOM T2 ALL	Unbeabsichtigte Bewegung in Richtung Westen
3	5,76 E-07	12,28	CCF CPU T1 ALL	CCF CPU T2 ALL	Unbeabsichtigte Bewegung in Richtung Westen
4	5,76 E-07	12,28	CCF DOM T1 ALL	CCF DOM T2 ALL	Unbeabsichtigte Bewegung in Richtung Osten
5	5,76 E-07	12,28	CCF CPU T1 ALL	CCF CPU T2 ALL	Unbeabsichtigte Bewegung in Richtung Osten
6	5,76 E-07	12,28	CCF DOM T1 ALL	CCF DOM T2 ALL	Unbeabsichtigte Bewegung in Richtung Westen
7	5,76 E-07	12,28	CCF CPU T2 ALL	CCF DOM T1 ALL	Unbeabsichtigte Bewegung in Richtung Westen
8	5,76 E-07	12,28	CCF CPU T2 ALL	CCF DOM T1 ALL	Unbeabsichtigte Bewegung in Richtung Osten

Erwartungsgemäß kommen die Hauptbeiträge zur Eintrittswahrscheinlichkeit eines Lastabsturzes von gemeinsam verursachten Ausfällen (GVA). Im Falle des Katzwerks konkret GVA der Prozessormodule und der digitalen Ausgangskarten, jeweils gleichzeitig mit ungewollten Bewegungen in die eine oder andere mögliche Richtung.

[4] CCF: Gemeinsam Verursachter Ausfall (GVA) (engl. Common Cause Failure)

[5] CPU: Processor Module (vgl. Abb. 3.8)

[6] T1: Katzwerk („Trolley“) Redundanz 1

[7] DOM: Digital Out Module (vgl. Abb. 3.8)

[8] T2: Katzwerk („Trolley“) Redundanz 2

[9] ALL: Alle Signale, d.h. 2v2-CCF

[10] oder versehentliche

Unter der Annahme der generischen Zuverlässigkeitskenngrößen in Tab. 3.6 ergibt sich eine Gesamteintrittswahrscheinlichkeit für Lastabstürze von $1{,}44 \cdot 10^{-5}$ pro Jahr, die sich ursächlich auf Brücke, Katzwerk und Hubwerk gleichermaßen verteilen.

3.3.3 Simulationsanalyse

3.3.3.1 Simulationsmodell

Die in Kapitel 3.2.3 beschriebenen leittechnische Sicherheitsfunktionen der Kransteuerung (SILT Katzwerk: SICF_T1(2)) wurden mittels der Matlab/Simulink-Software nachgebildet. Diese Implementierung erlaubt es, die Logik des Systems eingehend zu prüfen und Fehleranalysen durchzuführen.

Die Modellierung erfolgte auf der Basis des Funktionsblockdiagramms in Abb. 3.4, wobei hierzu ein entsprechendes Simulink-Modell (siehe Abb. 3.14) erstellt wurde. In dem Simulink-Modell wurden die Funktionalitäten abgebildet, die von den Eingangssignalen (Positionssignale, Geschwindigkeitsmessung, Reset- und Enable-Signale, Master-Controller-Signal) zu den daraus berechneten Steuersignalen (Bremse Aktivieren, Energieversorgung abschalten) führen.

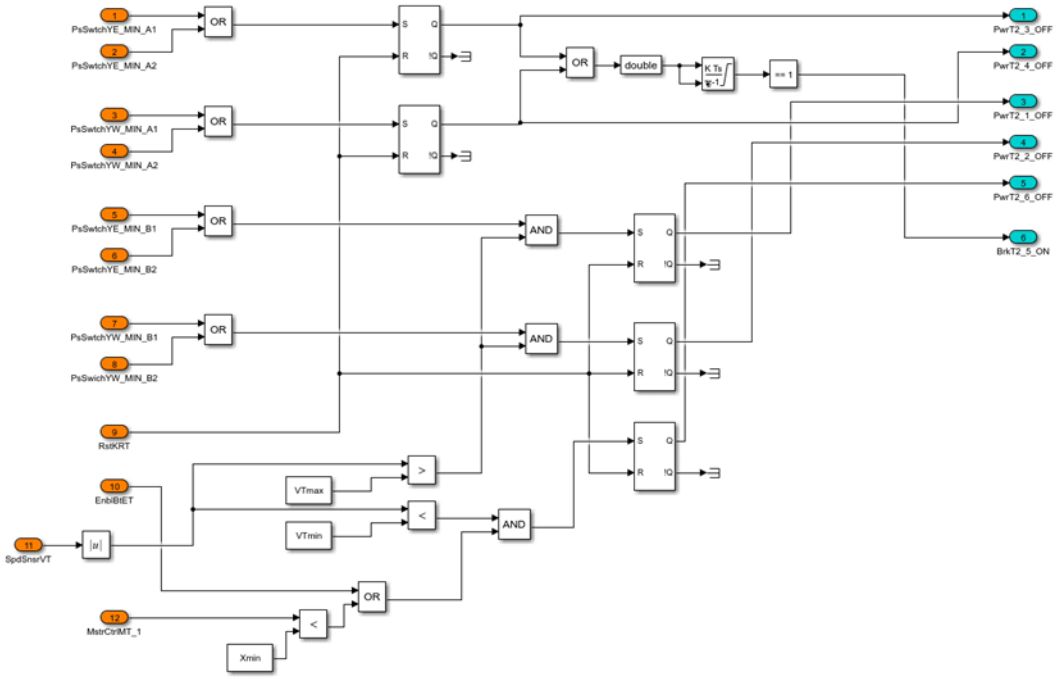

Abb. 3.14 Simulink-Modell der SILT-Steuerung des Katzwerks

3.3.3.2 Simulationsanalysen

Das Simulink-Modell der Kransteuerung erlaubt die modellierte Funktion durch eine Simulation zu testen. Hierzu wurden exemplarisch Simulationen für zwei verschiedene Szenarien durchgeführt. Motiviert wurden die Szenarien durch nachfolgend dargestellte Überlegungen (siehe hierzu Abb. 3.15).

Das Katzwerk der Krananlage bewegt sich entlang einer Laufschiene in eine Richtung (z. B. Ost-Wand). An zwei Positionen der Laufschiene sind jeweils zwei (redundante) Schalter angebracht, die das Überfahren dieser Position signalisieren. Zusätzlich wird die Geschwindigkeit der Laufkatze des Krans gemessen. Es werden zwei Szenarien beschrieben, bei denen je nach Position und Geschwindigkeit des Krans Maßnahmen ausgelöst werden sollen:

- Szenario 1: wird die **erste Position** überfahren **und die Geschwindigkeit** überschreitet einen SILT-Grenzwert, dann wird die Energieversorgung des Antriebes des Katzwerks abgeschaltet.
- Szenario 2: wird die zweite Position überfahren, dann wird der Antrieb abgeschaltet **und** die Bremsen des Katzwerks werden aktiviert.

Für die o. g. Fälle sollte ermittelt werden, ob die entsprechenden Maßnahmen (Aktivierung der Bremsen, Abschalten der Energieversorgung) noch ausgeführt werden, wenn bestimmte Signale (die der Geschwindigkeitsmessung und der Positionsschalter) ausfallen.

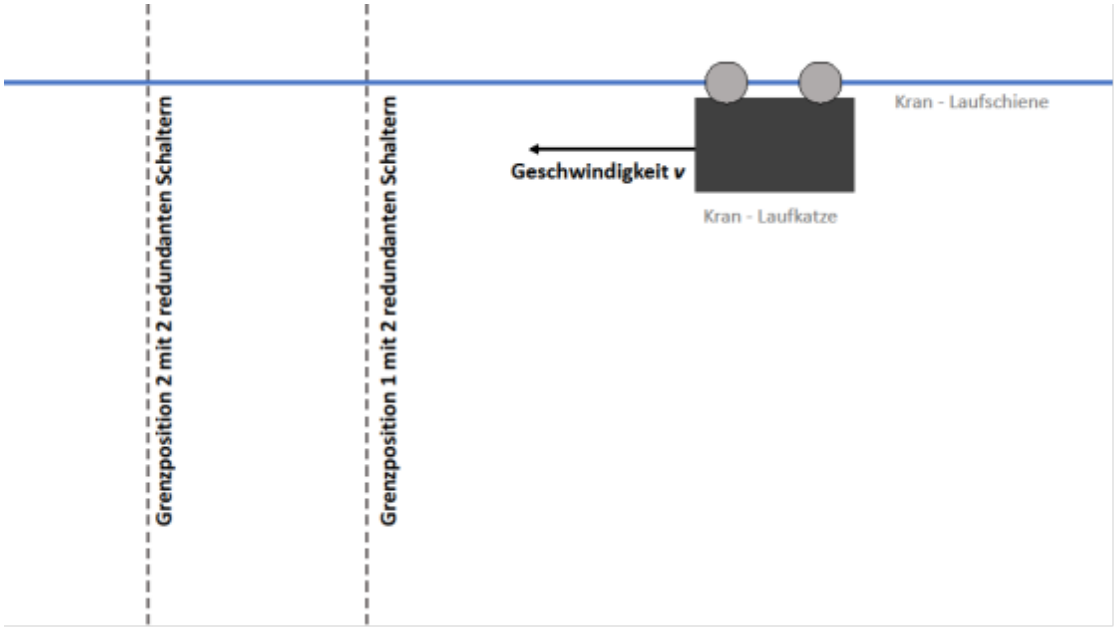

Abb. 3.15 Darstellung der Ausgangssituation für die Simulationen

Im ersten Szenario wird angenommen, dass die erste Grenzposition mit erhöhter Geschwindigkeit überfahren wird. Im Normalfall sollten beide Positionsschalter an dieser Position auslösen und die erhöhte Geschwindigkeit sollte gemessen werden. Infolge dessen sollte die Abschaltung der Energieversorgung ausgelöst werden. Ein Ausfall der beiden Positionsschalter wird dahingehend mit Nichtauslösen derselben beschrieben, ein Ausfall des Geschwindigkeitssensors mit der Angabe einer zu niedrigen Geschwindigkeit.

In Tab. 3.7 sind die Ergebnisse der Simulation in folgender Weise codiert:

- Eine 1 bei den Positionsschaltern bedeutet ein Auslösen, eine 0 ein Nicht-Auslösen,
- Eine 1 bei der Geschwindigkeitsmessung bedeutet ein Überschreiten des Grenzwertes, eine 0 einen zulässigen Wert,
- Eine 1 bei Abschaltung des Antriebs bedeutet eine Auslösung derselben, eine 0 ein Nicht-Auslösen

Tab. 3.8 Ergebnisse der Simulation des ersten Szenarios

Positionsschalter 1	Positionsschalter 2	Geschwindigkeits-messung	Abschaltung des Antriebes
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	0
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	1

Die Simulation im ersten Szenario zeigt, dass solange eines der beiden Positionssignale und das Geschwindigkeitssignal korrekt sind, wird die erforderliche Sicherheitsfunktion ausgelöst. Der Ausfall entweder beider Positionssignale oder des Geschwindigkeitssignals führen zu einem Nicht-Auslösen der Sicherheitsfunktion.

Im zweiten Szenario wird das Überfahren der zweiten Grenzposition angenommen. Im Normalfall sollten beide Positionsschalter auslösen, die Bremse aktiviert und die Energieversorgung abgeschaltet werden. Die Ergebnisse für Szenario 2 sind in Tab. 3.8 analog zu den Ergebnissen aus dem ersten Szenario mit identischer Codierung zusammengefasst.

Tab. 3.9 Ergebnisse der Simulation des zweiten Szenarios

Positionsschalter 1	Positionsschalter 2	Aktivierung der Motor-Bremse	Abschaltung des Antriebes
0	0	0	0
1	0	1	1
0	1	1	1
1	1	1	1

Die Simulation im zweiten Szenario zeigt, dass solange eines der beiden Positionssignale korrekt die erforderliche Funktion auslöst, werden die Sicherheitsmaßnahmen eingeleitet.

Auf der Basis von durchgeführten Simulationen einer leittechnischen Funktion der Kransteuerung können bereits erste Schlussfolgerungen zu den Auswirkungen von Einzelfehlern oder deren Kombinationen gezogen werden, z. B. bei fehlerhaften Positionssensoren wird die Bremse nicht ausgelöst und damit die Geschwindigkeit nicht reduziert.

Die Auswirkungen eines solchen Ablaufs müssen dann durch Erweiterung der Modellierung und weitere Analysen untersucht werden.

3.3.3.3 Erweiterung der Simulation

Die in den vorigen Abschnitten beschriebene Simulation einer SILT-Funktion der Kransteuerung bildet nur einen Teil der gesamten Krananlage ab, so gehören z. B. zum Gesamtsystem der Kransteuerung außerdem andere Funktionen (Software- und Hardware der Betriebsleitechnik, siehe auch Kapitel 3.2.3). In der Simulation ließen sich u. a. die Kransteuerung und -regelung, die Sensoren, das physische Kransystem mit Motoren, die Laufräder, die Umgebung des Krans und die Mensch-Maschine-Schnittstelle miteinander koppeln. All diese zusätzlichen Elemente der Simulation könnte man, je nach Anforderungsfall, prinzipiell mit unterschiedlichen Werkzeugen, in verschiedenen Detailgraden realisieren. Hierzu müssen u. a. zusätzliche Simulationsmodelle erstellt werden, die die dynamischen Abläufe der Bewegungen des Kranes bzw. die Strukturmechanik von Auswirkungen von Kollisionen und Aufprällen der Krananlage und der Lasten berücksichtigen.

Ein Beispiel für die Kopplung dieser verschiedenen Modell-Domänen wäre z. B. die Simulation der Bewegung eines Krans, dessen Steuerung durch die Leittechnik bestimmt wird, um damit die Ausgangssituation eines Aufpralls (Geschwindigkeit und Orientierung des bewegten Objektes) für eine strukturmechanische Simulation zu liefern. Im Folgenden wird der Beitrag von verschiedenen Simulationsdomänen beschrieben.

- Simulation der Bewegungsdynamik

Die Simulation der Bewegungen des Kran-Last-Systems kann Aufschluss darüber geben, ob in einer bestimmten Raumkonfiguration ein Zusammenstoß möglich ist, oder mit welcher Geschwindigkeit Zusammenstöße zu erwarten sind. Hierfür können Bewegungsgleichungen für das Kransystem aufgestellt und numerisch gelöst werden. Je nach Detailgrad sind hier auch Echtzeitsimulationen mit gleichzeitiger Visualisierung möglich. Dies ermöglicht z. B. auch das Prüfen des Verhaltens von Sicherheitsfunktionen der Leittechnik bei Steuerung des Systems durch einen Benutzer (z. B. über eine grafische Bedienoberfläche (GUI) oder eine andere Eingabemethode, wie z. B. einen Joystick). Je nach Anwendungsfall sollte hierbei der Detailgrad der Simulation genau festgelegt werden, zum Beispiel, ob die Last als Punktmasse, oder ausgedehnter Körper betrachtet wird, oder ob die Visualisierung in zwei oder drei Dimensionen notwendig ist.

- Simulation der leittechnischen Funktionen

Die leittechnischen Funktionen (z. B. Sicherheitsfunktionen, wie die automatische Abschaltung und die Auslösung von Bremsen bei Überfahren einer Grenzposition, oder die Antriebsregelung der Krananlage) können simuliert und in die Simulation der Bewegung der gesamten Krananlage integriert werden. Somit kann auch das Gesamtverhalten der Krananlage beim Ausfall verschiedener Funktionalitäten (Sensor/Verarbeitungsfehler) getestet und mögliche Auswirkungen können bewertet werden.

- Simulation von Kollisionen und Aufschlägen

Zur Erweiterung der Simulation für die Analyse von Zusammenstößen einer Last mit einem Hindernis, oder des Aufschlags einer Last auf dem Boden, müssen numerische Verfahren zur strukturdynamischen Simulation (z. B. FEM-Simulation) zu Rate gezogen werden. Die dazu üblicherweise verwendeten ressourcenintensiven Verfahren erschweren eine realitätsgetreue Simulation in Echtzeit und somit auch eine direkte Kopplung mit der oben beschriebenen Simulation der Bewegungsdynamik. Eine vorhergehende Simulation des Bewegungsvorgangs des Krans ist aber trotzdem sinnvoll verwertbar, insofern dadurch die Randbedingungen (z. B. Aufprallgeschwindigkeit) für die strukturdynamische Simulation festgelegt werden können.

- Beispiel für eine 2-D Simulation der Bewegungsdynamik des Katzwerks

Beispielhaft wurde ein zweidimensionales Modell entwickelt der Bewegungsdynamik des Katzwerks und dessen Zustand in einer GUI visualisiert. Damit wurde eine Simulationsumgebung geschaffen, die es erlaubt, die oben beschriebene leittechnische Sicherheitsfunktion mit komplexen Abläufen der Eingangssignale zu prüfen. Hierzu wurde ein Ansatz aus der Dissertation /BUN 04/ verwendet.

Das zugrundeliegende physikalische Modell /BUN 04/ wird durch den folgenden Satz von Gleichungen beschrieben:

$$\begin{aligned} A\ddot{s} - B\ddot{\varphi} &= F(t) \\ -B\ddot{s} + C\,\ddot{\varphi} + D\varphi &= 0 \end{aligned} \tag{3.1}$$

Wobei s die Position der Laufkatze und φ der Auslenkungswinkel der Last ist. Die Bedeutungen der Konstanten A, B, C, D, sowie deren Berechnung aus den physikalischen Parametern des Systems lassen sich /BUN 04/ entnehmen. Sie ergeben sich aus den

jeweiligen Lagrange-Gleichungen des Gesamtsystems unter Verwendung der generalisierten Koordinaten s und φ. Die Konstanten sind abhängig von den Abmessungen und der Art der Hubseilführung des zu simulierenden Krans und den Massen der einzelnen Komponenten. In die Berechnung von A, B, C und D können außerdem u. a. Größen wie die Seillängen, der Abstand der Anschlagpunkte zum Schwerpunkt der Last, der Abstand der Anschlagpunkte zueinander (sowohl an der Last als auch am Kran) und das Trägheitsmoment der Last eingehen.

Zusätzlich wird eine der Bewegungsrichtung der Laufkatze entgegengerichtete Kraft berücksichtigt, die die Gleitreibung der Laufkatze abbilden kann und auch zur Simulation des Bremsvorganges verwendet wird. Das Modell beinhaltet die Kleinwinkelnäherung ($\sin\alpha \approx \alpha$) für Pendelschwingungen und ist dadurch nur für kleine Auslenkungen und langsame Schwingungen der Last gültig. Die obigen Gleichungen wurden für die Simulation in einer diskretisierten Form in ein Simulink-Modell übertragen, das Modell ist in Abb. 3.16 dargestellt.

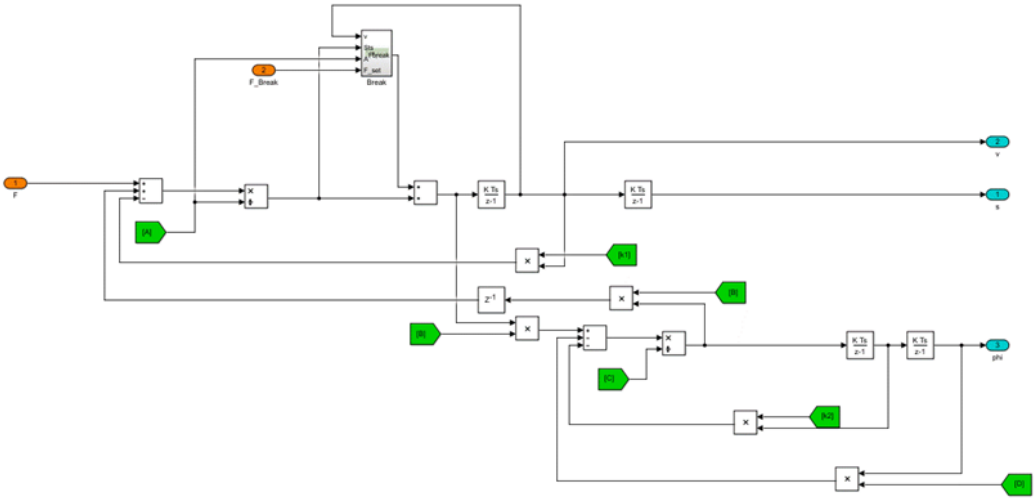

Abb. 3.16 Simulink-Modell der Bewegung einer Krananlage

Die Darstellung des Systemzustandes und die Steuerung des Systems erfolgen über eine grafische Benutzeroberfläche (siehe Abb. 3.17).

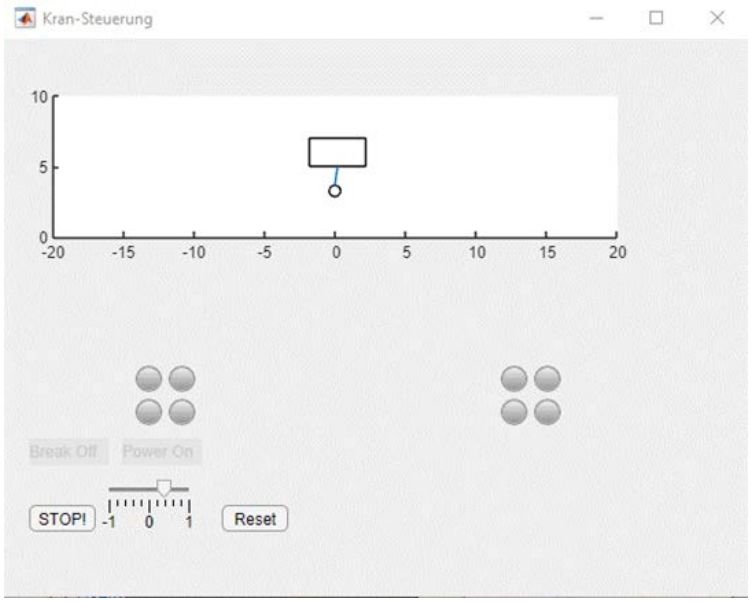

Abb. 3.17 Graphische Benutzeroberfläche und Visualisierung der Simulation des Katzwerks

Die hier vorgestellte Modellerweiterung ermöglicht, eine beschleunigende Kraft an die Laufkatze anzulegen, den Bremsvorgang einzuleiten und die Bewegung, nach Auslösung der Bremse oder Abschaltung des Motors, wieder freizugeben. Zusätzlich zu einer vereinfachten Darstellung der Laufkatze und der schwingenden Last werden außerdem das Auslösen der Positionssensoren, sowie das das Auslösen der Bremsen und das Abschalten des Antriebs der Laufkatze dargestellt. Hiermit wurde beispielhaft anhand eines zweidimensionalen Modells der Bewegungsdynamik des Katzwerks gezeigt wie die Modellierung der Kransteuerung zukünftig um weitere Aspekte erweitert werden kann. Ein ähnliches Vorgehen könnte auch für Bewegungen des Hubwerks und der Kranbrücke gewählt werden.

4 Zusammenfassung und Ausblick

Ziel des Vorhabens 4717R01361 „Erforschung eines Ansatzes zur Systemvalidierung der sicherheitstechnischen Funktion von softwarebasierten Kransteuerungen“ war es eine modellbasierte Vorgehensweise zur Analyse digitaler Kransteuerungen zu entwickeln und zu erproben, die es ermöglicht die korrekte Umsetzung der Sicherheitsfunktionen im Steuerungssystem eines Kranes zu validieren.

Hierzu wurde in einem ersten Arbeitspaket das anzuwendende Regelwerk zusammengestellt, die verwendete Technik und die typischen Einsatzbereiche erfasst und die vorliegende spezifische Betriebserfahrung ausgewertet.

Bei den für die Auslegung der Steuerung von Hebezeugen in Kernkraftwerken zentralen Regelwerken handelt es sich um die KTA-Regeln 3902 und 3903, welche konkrete Anforderungen an die Ausführung von anwendungsspezifischen Schutzfunktionen stellen. Den einzelnen Schutzfunktionen werden dort Performance Level zugewiesen, wie sie in DIN ISO 13849-1 definiert werden. DIN ISO 13849-1 enthält auch genauere Hinweise zur Konzeptionierung von Steuerungen und zur Berechnung der Performance Level abhängig von Zuverlässigkeitskenngrößen. Alternativ können Safety Integrity Level nach DIN EN 61508 verwendet werden. Deterministische Vorgaben zur Auslegung der elektrischen Schutzeinrichtungen finden sich in DIN EN 60204-32.

Typische Hebezeuge in deutschen Kernkraftwerken, an die erhöhte Anforderungen im Sinne der KTA 3902 gestellt werden, sind neben den Reaktorgebäudekranen, die Halbportalkrane im Außenbereich von Druckwasserreaktoren und in einigen Fällen die Krane im Zwischenlager. Die Anzahl der Hebezeuge mit zusätzlichen Anforderungen im Sinne der KTA 3902 ist größer. Zu nennen sind in Druckwasserreaktoren die Konsolkrane im Reaktorgebäude und in Siedewasserreaktoren die Schwenkkrane, die in etwa vergleichbare Aufgaben beim Brennelementtransport erfüllen. Dazu kommen die Krane im Lager für unbestrahlte Brennelemente. Anlagenspezifisch kommen außerdem eine gewisse Anzahl an weiteren Hebezeugen dazu, die in der Behandlung radioaktiver Abfälle oder für den Transport größerer oder kontaminierter Komponenten im Kontrollbereich eingesetzt werden. Lastaufnahme- und Anschlagmittel werden abhängig von der zu transportierenden Last und der entsprechenden Umgebung eingestuft. Für die Brennelementlademaschinen werden in KTA 3902 gesonderte Anforderungen spezifiziert. Die Reaktorgebäudekrane, die Brennelementlademaschinen, die Zwischenlagerkrane und die Hebezeuge, die bei der Behandlung radioaktiver Abfälle eingesetzt werden, können

generell als rückbaurelevant eingestuft werden. Für die übrigen Hebezeuge ist diese Einstufung abhängig vom anlagenspezifischen Rückbaukonzept.

Zur Auswertung der spezifischen Betriebserfahrung wurden Ereignisse aus Kernkraftwerken aus der GRS-eigenen Datenbank VERA ergänzt durch ausgewählte Ereignisse aus anderen kerntechnischen Anlagen und internationale Ereignisse aus der IRS-Datenbank der IAEA untersucht. Für den Auswertezeitraum zwischen dem 01.01.2000 und dem 31.05.2017 wurden insgesamt 135 Ereignisse mit Fehlern/Fehlfunktionen an Hebezeugen verteilt auf 111 Ereignismeldungen gefunden. Diese Ereignisse wurden hinsichtlich ihrer Fehlerfolge, der fehlerverursachenden Einrichtung, der Fehlerart und der Frage, ob die Steuerung bei dem Fehler eine Rolle spielte, kategorisiert und gruppiert. Beobachtete Fehlerfolgen waren Lastabstürze, Kollisionen mit einem Umgebungselement, ungeplante Verbindungen zwischen Hebezeug und Last (Kollisionen oder ungeplante Hebevorgänge), Selbstschädigungen und unwirksame nuklearspezifische Verriegelungen (u. a. Strahlenschutz oder Kritikalitätssicherheit).

Die Fehler, bei denen die Steuerung des Hebezeugs eine Rolle spielte, wurden dann detaillierter ausgewertet. Es zeigte sich, dass Fehler in der Steuerung selten zu Lastabstürzen, aber häufig zu Selbstzerstörungen und Kollisionen mit Umgebungselementen führen. Im Hinblick auf die Fehlerart handelte es sich verhältnismäßig selten um Bedienfehler, dafür verhältnismäßig häufig um Auslegungsfehler. Die Fehler ließen sich in vier weitere Untergruppen gliedern: 1. Komponentenausfälle, bei denen einzelne (in wenigen Fällen: mehrere) Komponenten der Steuerung (Hardware) ausgefallen waren. 2. Programmierfehler, bei denen die Software der Steuerung Logik- oder Rechenfehler enthielt 3. Parametrierfehler, bei denen Variablen in der Software der Steuerung mit unzulässigen Werten besetzt wurden und 4. Spezifikationsfehler, bei denen notwendige Sicherheitsfunktion nicht oder nicht mit der spezifizierten Zuverlässigkeit umgesetzt waren.

In einem zweiten Arbeitspaket wurde eine modellbasierte Vorgehensweise zur Analyse digitaler Kransteuerung entwickelt und erprobt. Die Vorauswahl der Analysemethoden erfolgte auf der Basis der in der GRS bereits gesammelten Erfahrungen auf dem Gebiet deterministischer und probabilistischer Analysen digitaler Leittechnik in Kernkraftwerken. Anschließend wurde ein vereinfachtes Modell einer Krananlage (u. a. Bewegungsraum, Annahmen zu Bewegung der Anlage und Lasten) und der Kransteuerung auf der Grundlage eines Konzepts der modellbasierten Analyse entwickelt.

Die Entwicklung und Erprobung der Analysemethoden der modellierten Kransteuerung erfolgte in drei Schritten:

- Modellbasierte Fehlerausfallart- und Auswirkungsanalyse (FMEA– Failure Mode and Effects Analysis),
- Fehlerbaummodellierung und -analyse,
- Entwicklung und Analyse einer simulierten Kransteuerung.

Für die o. g. eingesetzten Methoden konnte ihre Eignung für eine modellbasierte Analyse potenzieller Ausfälle leittechnischer Komponenten der Steuerung grundsätzlich demonstriert werden. Die FMEA kann dazu beitragen, auf der Basis von getroffenen Annahmen die Auswirkungen potenzieller Einzelfehler auf die Funktion der modellierten Kransteuerung und/oder Kandidaten für systematische Ausfälle (Gemeinsam Verursachter Ausfall, GVA) zu ermitteln. Dennoch wurde bereits bei der Modellierung der Kransteuerung festgestellt, dass für die Durchführung einer verlässlichen FMEA viele Detailinformationen zum Aufbau und zur Funktion sowohl einzelner Komponenten als auch des gesamten Systems der Krananlage erforderlich sind. Hierzu gehören u. a. Angaben zum Betrieb (u. a. Lasten, Fahrgeschwindigkeiten, Betriebs- bzw. Arbeitsanweisungen) und zu Prüfungen der Krananlage und deren Steuerung (inklusive Mensch-Maschine-Schnittstelle), zur Überwachung der Krananlage und zu Zuverlässigkeitskenndaten von Herstellern oder aus der Betriebserfahrung. Diese Feststellungen gelten ebenfalls für die Fehlerbaum- und Simulationsanalysen.

Die Fehlerbaumanalysen lieferten im Wesentlichen die Ausfallkombinationen von SILT-Komponenten, die zum Lastabsturz führen können. Bei der Fehlerbaummodellierung wurden Ergebnisse der modellbasierten FMEA, als Basiselemente eingesetzt und die Quantifizierung erfolgte auf Basis von Schätzungen. Die Sensitivitäts- und Minimalschnittanalysen der im Vorhaben durchgeführten Fehlerbaumanalyse ist für die modellbasierten Analysen besonders wichtig, weil damit auch die Modellunsicherheiten erkannt und reduziert werden können. Die Simulationsanalysen bieten wesentliche Erweiterungen für Analysen dynamischer Abläufe bei Bewegungen der Krananlage und zur Validierung der FMEA und Fehlerbaumanalysen.

Des Weiteren wurde bei statischen Fehlerbaumanalysen und dynamischen Simulationsanalysen erkannt, dass für die Bewertung der Wirksamkeit einzelner Funktionen der

Kransteuerung eine konsistente, umfassende Modellierung der Krananlage, des Bewegungsraums und der zu bewegenden Lasten erforderlich ist. Nur damit können auch die potenziellen Gefährdungen und ggf. das Schadensausmaß aussagefähig abgeschätzt werden. Bei dem im Vorhaben erreichten Stand der Modellentwicklung der Krananlage ist diese Abschätzung praktisch noch nicht möglich.

Eine weitere Verbesserung der Aussagefähigkeit der modellbasierten Fehlerbaum- und Simulationsanalyse kann durch Berücksichtigung der betrieblichen Funktionen der Kransteuerung und der mechanischen Sicherungseinrichtungen bei der Modellierung der Krananlage und -steuerung erreicht werden. Damit kann auch das gestaffelte Sicherheitskonzept einer Krananlage umfassend und nachvollziehbar bewertet werden.

Abschließend ist anzumerken, dass eine mögliche Weiterentwicklung der modellbasierten Analysen der Kransteuerung eine Vorgehensweise zur Validierung- und Verifizierung der Modelle zur Reduzierung der Unsicherheiten der Ergebnisse modellbasierter Analysen beinhalten sollte.

Literaturverzeichnis

/BFS 05a/ Facharbeitskreis probabilistische Sicherheitsanalyse für Kernkraftwerke (FAK): Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand August 2005, BfS-SCHR-37/05, Salzgitter, Oktober 2005

/BFS 05b/ Facharbeitskreis probabilistische Sicherheitsanalyse für Kernkraftwerke (FAK): Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-38/05, Salzgitter, Oktober 2005

/BGV 96/ Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit BG-Vorschrift D8 „Unfallverhütungsvorschrift Winden, Hub- und Zuggeräte“; Fassung vom April 1996; Maschinenbau- und Metall-Berufsgenossenschaft, April 1996

/BGV 01/ Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit BG-Vorschrift D6 „Unfallverhütungsvorschrift Krane“; Fassung vom April 2001; Maschinenbau- und Metall-Berufsgenossenschaft, April 2001

/BUN 04/ Buntoro Sandhy Margono
Optimierung von Bewegungsabläufen mit schwingungsfreien Endpositionen zur Verkürzung der Arbeitszyklen von Container-Schnellumschlaganlagen
Dissertation, Universität Duisburg-Essen, 2004

/DGU 97/ DGUV Vorschrift 3 „Unfallverhütungsvorschrift Elektrische Anlagen und Betriebsmittel“; Fassung vom 1. Januar 1997; Deutsche Gesetzliche Unfallversicherung; Januar 1997

/DGU 00/ DGUV Vorschrift 55 „Unfallverhütungsvorschrift Winden, Hub- und Zuggeräte“; Fassung vom Oktober 2000; Deutsche Gesetzliche Unfallversicherung; Oktober 2000

/DGU 01/ DGUV Vorschrift 53 „Unfallverhütungsvorschrift Krane“; Fassung vom Juli 2001; Deutsche Gesetzliche Unfallversicherung; Juli 2001

/DGU 08/ DGUV Regel 100-500 „Betreiben von Arbeitsmitteln“ Kapitel 2.8 Betreiben von Lastaufnahmeeinrichtungen im Hebezeugbetrieb; Fassung vom April 2008; Deutsche Gesetzliche Unfallversicherung; April 2008

/DGU 12/ DGUV Grundsatz 309-001 „Prüfung von Kranen“; Fassung vom August 2012; Deutsche Gesetzliche Unfallversicherung; August 2012

/DIN 06a/ DIN EN 60812 „Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)“; Deutsche Fassung EN 60812:2006; Deutsches Institut für Normung; November 2006

/DIN 06b/ DIN EN 61078 „Techniken für die Analyse der Zuverlässigkeit – Zuverlässigkeitsblockdiagramm und Bool’sche Verfahren“; Deutsche Fassung EN 61078:2006-10; Deutsches Institut für Normung; November 2006

/DIN 07a/ DIN EN 14492-2 „Krane – Kraftgetriebene Winden und Hubwerke – Teil 2: Kraftgetriebene Hubwerke“; Deutsche Fassung EN 14492-2:2006; Deutsches Institut für Normung; April 2007

/DIN 07b/ DIN IEC 61025 „Fehlzustandsbaumanalyse“; Deutsche Fassung EN 61025:2007; Deutsches Institut für Normung; August 2007

/DIN 07c/ DIN EN 61165 „Anwendung des Markoff-Verfahrens“; Deutsche Fassung EN 61165:2006; Deutsches Institut für Normung; Februar 2007

/DIN 09/ DIN EN 60204-32 „Sicherheit von Maschinen – Teil 32: Anforderungen für Hebezeuge“; Deutsche Fassung EN 60204-32:2008; Deutsches Institut für Normung; März 2009

/DIN 10/ DIN EN 62138 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C“; Deutsche Fassung EN 62138:2009; Deutsches Institut für Normung; März 2010

/DIN 11a/ DIN EN 61508-1 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen“; Deutsche Fassung EN 61508-1:2010; Deutsches Institut für Normung; Februar 2011

/DIN 11b/ DIN EN 61508-2 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme“; Deutsche Fassung EN 61508-2:2010; Deutsches Institut für Normung; Februar 2011

/DIN 11c/ DIN EN 61508-3 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software“; Deutsche Fassung EN 61508-3:2010; Deutsches Institut für Normung; Februar 2011

/DIN 11d/ DIN EN 61508-5 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)“; Deutsche Fassung EN 61508-5:2010; Deutsches Institut für Normung; Februar 2011

/DIN 11e/ DIN EN 61508-6 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3“; Deutsche Fassung EN 61508-6:2010; Deutsches Institut für Normung; Februar 2011

/DIN 11f/ DIN EN 61508-7 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Überblick über Verfahren und Maßnahmen“; Deutsche Fassung EN 61508-6:2010; Deutsches Institut für Normung; Februar 2011

/DIN 13a/ DIN EN 61513 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“; Deutsche Fassung EN 61513:2013; Deutsches Institut für Normung; September 2013

/DIN 13b/ DIN EN 61131-6„Speicherprogrammierbare Steuerungen – Teil 6: funktionale Sicherheit“; Deutsche Fassung EN 61131-6:2012; Deutsches Institut für Normung; Oktober 2013

/DIN 15a/ DIN EN 60812 Entwurf „Fehlzustandsart- und -auswirkungsanalyse (FMEA)“; Entwurfsversion vom 03. Juli 2015; Deutsches Institut für Normung; August 2015

/DIN 15b/ DIN EN 62566 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen“; Deutsche Fassung EN52566:2015-02; Deutsches Institut für Normung; Februar 2015

/DIN 16a/ DIN ISO 13849-1 „Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze“; Deutsche Fassung EN ISO 13849-1:2015; Deutsches Institut für Normung; Juni 2016

/DIN 16b/ DIN EN 62061 „Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“; Deutsche Fassung EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015; Deutsches Institut für Normung; Mai 2016

/DIN 17/ DIN EN 61800-5-2 „Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit“; Deutsche Fassung EN 61800-5-2:2017; Deutsches Institut für Normung; November 2017

/DIN 18/ DIN EN 13135 „Krane — Sicherheit — Konstruktion — Anforderungen an die Ausrüstungen“; Deutsche Fassung EN 13135:2013+A1:2018; Deutsches Institut für Normung; August 2018

/GRS 12/ GRS gGmbH
Entwicklung einer Methode zur einheitlichen Durchführung von Sensitivitätsstudien im Rahmen von PSA
GRS-A-3675, September 2012

/GRS 15a/ GRS gGmbH;
Entwicklung eines Ansatzes zur Analyse der Netzwerktechnologien in sicherheitsrelevanten Leittechniksystemen hinsichtlich Verbreitung und Auswirkung postulierter Fehler; GRS-377; ISBN 978-3-944161-58-7, Juni 2015

/GRS 15b/ GRS gGmbH;
Fortschrittliche Methoden und Werkzeuge für probabilistische Sicherheitsanalysen; GRS-A-3742; Juli 2015

/GRS 17/ GRS gGmbH;
Zuverlässigkeitsbewertung digitaler leittechnischer Einrichtungen; GRS-A-3890; August 2017

/GÜN 03/ Günthner W.A., Schubert I.
Sicherheitsleitlinien für automatisierte Krananlagen im personenzugänglichen Umfeld
Forschungsbericht zum BMWi-Vorhaben (Projekt-Nr. 12932 N/1), Technische Universität München, Boltzmannstrasse 15, 85748 Garching bei München, 4.11.2003

/HSU 97/ Mei-Chen Hsueh, Timothy K. Tsai, and Ravishankar K. Iyer
Fault Injection Techniques and Tools
IEEE Press 1997, University of Illinois at Urbana-Champaign, April 1997.

/KOO 12/ Maha Kooli, Giorgio Di Natale
A Survey on Simulation-Based Fault Injection Tools for Complex Systems
DTIS: Design and Technology of Integrated Systems in Nanoscale Era, May 2014, Santorini, Greece. 0.1109/DTIS.2014.6850649, hal-0107547

/KTA 19a/ KTA 3902 Auslegung von Hebezeugen in Kernkraftwerken; Fassung 2019-11 (Änderungsentwurf Gründruck); http://www.kta-gs.de/d/regeln/3900/3902_re_2019_11.pdf; abgerufen am 11.02.2020

/KTA 19b/ KTA 3903 Prüfung und Betrieb von Hebezeugen in Kernkraftwerken; Fassung 2019-11 (Änderungsentwurf Gründruck); http://www.kta-gs.de/d/regeln/3900/3903_re_2019_11.pdf; abgerufen am 11.02.2020

/NEA 12/ NEA/CSNI OECD
Use and Development of Probabilistic Safety Assessment;
NEA/CSNI/R(2012)11; December 2012

/NEA 15/ NEA/CSNI OECD
Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis, Nuclear Safety
NEA/CSNI/R(2014)16, February 2015

/PIL 04/ Piljugin, E
Anpassung und Erprobung von Methoden zur probabilistischen Bewertung digitaler Leittechnik.
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A 3258, 01.12.2004

/PIL 10/ Piljugin, E., Herb, J.
Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-A-3550, Garching, August 2010.

/SCA 12/ Scandpower AB
RiskSpectrum Analysis Tools
Theory Manual, Version 3.2.1, © Scandpower AB 1984 – 2012

/SIE 09/ Siemens AG
SIMATIC. Industrie Software S7 F/FH Systems - Projektieren und Programmieren.
Programmier- und Bedienhandbuch, A5E00048979-06, Siemens AG Industry Sector, Postfach 48 48, 90026 NÜRNBERG, 05/2009

/SIE 13/ Siemens AG
SIMATIC. Automatisierungssystem S7-300. Baugruppendaten.
Gerätehandbuch, A5E00105504-08, Siemens AG Industry Sector, Postfach 48 48, 90026 NÜRNBERG, 02/2013

Abbildungsverzeichnis

Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-947685-45-5