Weiterentwicklung der CAMIC-Methode zur sicherheitstechnischen Bewertung digitaler Leittechnik

GRS - 655

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Weiterentwicklung der CAMIC-Methode zur sicherheitstechnischen Bewertung digitaler Leittechnik

Abschlussbericht

Patrick Gebhardt
Christian Müller
Claudia Quester
Dagmar Sommer

November 2021

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) unter dem Förderkennzeichen RS1560 durchgeführt.

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

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

GRS - 655
ISBN 978-3-949088-46-9

Deskriptoren
CAMIC-Anwendung, CAMIC-Methode, Diversitätsmatrix, FMEA, FTA, Leittechnische Einrichtungen, PDCA

Kurzfassung

Dieses vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderte Forschungs- und Entwicklungsvorhaben RS1560 setzt die Entwicklungen des Vorhabens RS1525 (Neue Methoden zur Bewertung der Zuverlässigkeit fortschrittlicher Mensch-Maschine-Schnittstellen, digitaler leittechnischer Einrichtungen und personellorganisatorischer Einflüsse) fort. Im Vorhaben RS1525 wurde die Methode CAMIC (Cyclic Analytic Method for I&C) zur Bewertung PLD-basierter Leittechnik entwickelt. Die hierbei entwickelten Analysemethoden und Werkzeuge wurden im aktuellen Vorhaben weiter verbessert und auf die gesamte rechnerbasierte und programmierbare Leittechnik erweitert. Darüber hinaus wurde auch eine rechnergestützte CAMIC-Anwendung entwickelt, die den Nutzer durch die Bewertung mittels der CAMIC-Methode führt.

Für die Erweiterung der CAMIC-Methode auf die Bewertung der gesamten rechnerbasierten und programmierbaren Leittechnik wurden die vorhandenen Flussdiagramme modifiziert und erweitert, wodurch auch eine engere Benutzerführung erreicht und somit die Konsistenz und Genauigkeit von Bewertungen verbessert wurde.

Die erweiterte CAMIC-Methode wurde anschließend als rechnergestützte CAMIC-Anwendung umgesetzt. Als Grundlage für die CAMIC-Anwendung wurde Python verwendet. Python bietet den Vorteil, bereits entwickelte Pakete zu verwenden und somit den Aufwand für die Entwicklung zu minimieren. Die gesamte CAMIC-Methode inklusive der weiterentwickelten Flussdiagramme wurden in die CAMIC-Anwendung implementiert. Darüber hinaus ist es in der CAMIC-Anwendung möglich, eine Themensuche durchzuführen, neue Dokumente in der CAMIC-Anwendung hinzuzufügen, einen Bewertungsbogen im Word-Format zu erstellen und den Fortschritt der Bewertung unter dem eigenen Benutzerprofil zu speichern. Neben Python wurde für die Umsetzung einer individuellen Benutzerverwendung und Speicherung von Dateien eine MySQL-Datenbank angelegt.

Als letzter Schritt wurden sowohl die CAMIC-Methode als auch die CAMIC-Anwendung einer modellbasierten Erprobung unterzogen.

Inhaltsverzeichnis

1 Einleitung

Im BMWi-Vorhaben RS1525 (Bundesministerium für Wirtschaft und Energie) wurde der Bewertungsansatz CAMIC (Cyclic Analytic Method for Instrumentation and Control) zur Bewertung von PLD-basierten (Programmable Logic Device) leittechnischen Einrichtungen entwickelt /GRS 17/. Ziel dieses Vorhabens ist die Weiterentwicklung der CAMIC-Methode, dahingehend, dass neben der Bewertung einzelner, leittechnischer Einrichtungen auch die Bewertung komplexer rechnerbasierter oder programmierbarer Leittechniksysteme ermöglicht wird. Darüber hinaus soll der CAMIC-Ansatz rechnergestützt umgesetzt werden, um den Bewertungsprozess konsistent und jederzeit nachvollziehbar zu gestalten und zu dokumentieren.

Die Zielsetzung dieses Vorhabens war in 3 Teile gegliedert:

1. Weiterentwicklung der CAMIC-Methode zur sicherheitstechnischen Bewertung rechnerbasierter oder programmierbarer Leittechnik
2. Werkzeugentwicklung für die rechnergestützte Anwendung der CAMIC-Methode
3. Modellbasierte Erprobung der erweiterten Methode

Im ersten Teil des Vorhabens wurde die CAMIC-Methode auf die Bewertung komplexer, rechnerbasierter oder programmierbarer Leittechniksysteme erweitert. Zusätzlich wurde die Möglichkeit einer systematischen Themensuche in relevanten Regelwerken und Normen in die CAMIC-Methode integriert. Im zweiten Teil wurde Software entwickelt, die bei der Anwendung der CAMIC-Methode unterstützt und somit eine konsistente Analyse ermöglicht. Innerhalb der Software können relevante Dokumente mit dem Projekt verknüpft werden und die Analyse wird dokumentiert. Dadurch wird eine Reproduzierbarkeit der Analyse sichergestellt. Im letzten Teil des Vorhabens erfolgte eine modellbasierte Erprobung der erweiterten CAMIC-Methode, wofür mehrere verschiedene Szenarien entwickelt und bearbeitet wurden (siehe Kapitel 5).

2 Hintergrundinformationen

2.1 Definition von Begriffen

Leittechnik-Funktion bzw. leittechnische Funktion (LT-Funktion):

Funktion zum Messen, Steuern, Regeln, Überwachen, Aufzeichnen und Schützen eines Prozesses oder einer Einrichtung /KTA 15/.

Leittechnik-System bzw. leittechnisches System (LT-System):

Auf elektrischer und/oder elektronischer und/oder programmierbarer elektronischer Technologie beruhendes System, das sowohl leittechnische Funktionen als auch auf sich selbst bezogene Dienstleistungs- und Überwachungsfunktionen ausführt /DIN 13/.

Leittechnische Architektur (LT-Architektur):

Organisatorische Struktur von leittechnischen Systemen der Anlage, die sicherheitstechnische Bedeutung haben (siehe auch leittechnisches System) /DIN 13/.

Leittechnische Einrichtung (LTE):

Leittechnische Einrichtungen sind Geräte (u. a. einzelne oder mehrere zusammenwirkende Baugruppen eines LT-Systems) zur Ausführung von LT-Funktionen. LTE umfassen sowohl automatische Einrichtungen als auch die Einrichtungen zur Prozessführung durch einen Operator in Anlehnung an /KTA 15/.

Geräte / Baugruppe:

Ein oder mehrere Teile eines Systems. Ein Gerät ist ein einzelnes, definierbares (und üblicherweise ausbaubares) Teil eines Systems /DIN 13/. Anordnung von Komponenten/Bauelementen (Bausteinen), durch die eine bestimmte Funktion ausgeführt wird. *Hinweis*: Geräte bestehen aus Hardware und ggf. Software. Eine LT-Baugruppe ist ein austauschbares Gerät mit standardisierter Schnittstelle /KTA 15/.

- **Gerät, nichtprogrammierbar:** Gerät bestehend aus diskreten, nichtprogrammierbaren Bauelementen. /KTA 15/

- **Gerät, programmierbar:** Gerät bestehend aus mindestens einem programmierbaren Bauelement. Hinweis: Zu den programmierbaren Bauelementen zählen z. B. FPGAs, PLDs und ASICs. /KTA 15/
- **Gerät, rechnerbasiert:** Gerät bestehend aus mindestens einem Prozessor. Hinweis: Die Gerätefunktion ist im Speicher hinterlegt. /KTA 15/

Anregeebene, Logikebene, Steuerebene:

Diese Begriffe dienen der Beschreibung des funktionellen Aufbaus von LTE und werden hier gemäß Abb. 2.1 verwendet.

Signalpfad:

Reicht hier von der Anregeebene, über die Logikebene bis hin zur Steuerebene.

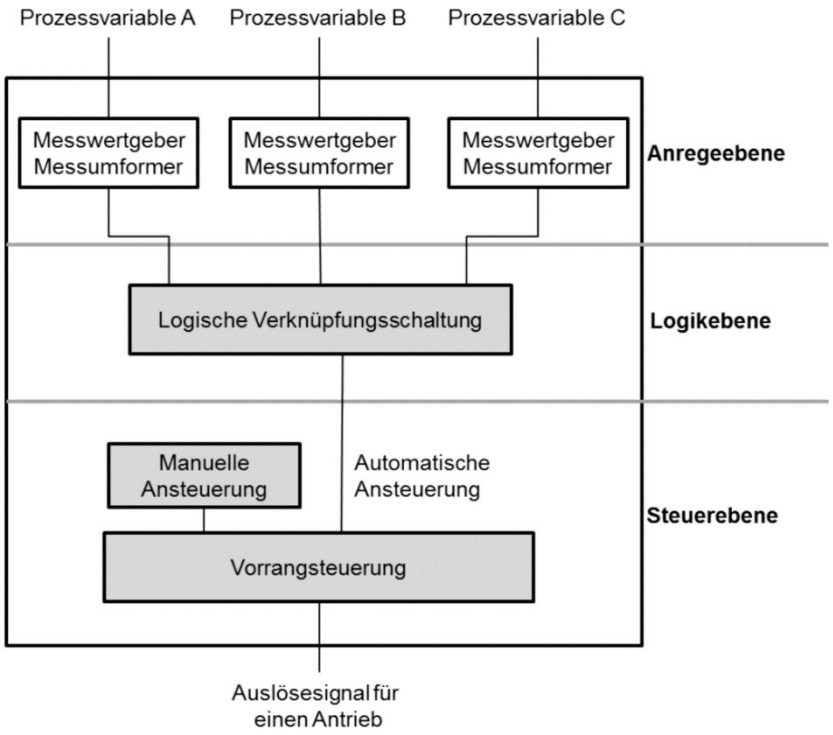


Abb. 2.1 Aufbau der Signalverarbeitung zur Steuerung sicherheitstechnisch wichtiger Antriebe /GRS 17/

Vorrangsteuerung:

Die Vorrangsteuerung ist eine Steuereinrichtung, die den Vorrang eines Steuersignals vor einem oder mehreren anderen bewirkt /KTA 15/.

Redundanz:

Die Redundanz ist das Vorhandensein von mehr funktionsbereiten Einrichtungen, als zur Erfüllung der vorgesehenen Funktion notwendig ist /KTA 15/.

Diversität / Diversitäre LTE:

Vorhandensein von zwei oder mehr funktionsbereiten Einrichtungen zur Erfüllung der vorgesehenen Funktion, die physikalisch oder technisch verschiedenartig ausgelegt sind /KTA 15/. Vorhandensein von zwei oder mehr redundanten Systemen oder Komponenten, um eine bestimmte Funktion durchzuführen, wobei die verschiedenen Systeme oder Komponenten derartig unterschiedliche Eigenschaften haben, dass die Möglichkeit von Versagen aufgrund gemeinsamer Ursache verringert wird /DIN 13/.

Fehlzustandsart (failure mode):

Ein failure mode (Fehlzustand) bezeichnet den Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist. Ein Fehlzustand ist oft das Ergebnis eines Ausfalls der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein /DIN 06/.

Fehlzustandsauswirkung (failure effect):

Eine Ausfallauswirkung bezeichnet die Folge einer Ausfallart hinsichtlich des Betriebs, der Funktion oder des Zustands einer Einheit /DIN 06/. Es wird zwischen lokalen und globalen Fehlzustandsauswirkungen unterschieden, wobei mit „lokalen Fehlzustandsauswirkungen“ in diesem Dokument Fehlzustandsauswirkungen auf die betrachtete LTE an sich sowie auf das LT-System, in welchem diese vorgesehen ist, bezeichnet werden. Der Begriff „globale Fehlzustandsauswirkungen“ (end effects) bezieht sich hier auf Fehlzustandsauswirkungen auf die LT-Funktion oder die LT-Funktionen, die von dem betroffenen LT-System unter Beteiligung der vorgesehenen LTE ausgeführt werden.

Versagen aufgrund gemeinsamer Ursache; GVA (gemeinsam verursachter Ausfall, engl. CCF - common cause failure):

Versagen infolge eines oder mehrerer Ereignisse, das/die ein koinzidentes Versagen in zwei oder mehreren eigenständigen Kanälen eines mehrkanaligen Systems oder in

verschiedenen Systemen verursacht/verursachen, sodass es zu einem Versagen des Systems/der Systeme kommt. Abhängig von den Umständen kann CCF auf Systemebene oder auf Ebene von Systemen betrachtet werden, die eine Sicherheitsgruppe darstellen /DIN 13/.

2.2 Bewertung rechnerbasierter und programmierbarer Leittechnik

Auch in der Kerntechnik werden immer mehr Systeme und Komponenten der Leittechnik rechnerbasiert oder programmierbar ausgeführt. Diese Digitalisierung der Leittechnik erfordert eine genaue Analyse und Bewertung der hierdurch erreichten Zustandsänderung. Erst wenn die geplante Digitalisierung einen deutlichen Mehrwert für das System bringt, sollte mit der Umsetzung begonnen werden. Viele Bewertungsmethoden für rechnerbasierte oder programmierbare leittechnische Systeme und Komponenten sind aber noch unzureichend und müssen konsistenter gestaltet werden. Daher befasst sich die GRS unter anderem damit, geeignete Methoden für die Bewertung rechnerbasierter oder programmierbarer leittechnischer Komponenten zu entwickeln. Basierend auf der langen Erfahrung der GRS im Bereich der Kerntechnik und der Synergie mehrerer Fachgebiete werden in diesem Vorhaben bekannte Methoden auf die rechnerbasierter oder programmierbarer Leittechnik erweitert.

2.3 Sachstand zur CAMIC-Methode

In dem BMWi-Vorhaben RS1525 /GRS 17/ wurde ein systematischer Ansatz zur sicherheitstechnischen Bewertung von PLD-basierter Leittechnik entwickelt. Die im Rahmen des genannten Vorhabens entwickelte CAMIC-Methode basiert dabei auf den Grundsätzen des PDCA-Zyklus (PLAN-DO-CHECK-ACT) /DIN 08/ und kann für unterschiedliche Zielstellungen eingesetzt werden. Hierzu zählen auch die Bewertung einer geplanten leittechnischen Architektur oder die Bewertung von vorgesehenen Änderungen an einer bestehenden leittechnischen Architektur.

2.3.1 PDCA-Zyklus

Dieser Prozess beinhaltet alle Schritte von der Planung und Vorbereitung der Bewertung mit Analyse der leittechnischen Einrichtung (LTE) innerhalb der geplanten leittechnischen Architektur (LT-Architektur) (Prozessschritt PLAN) über die Bewertung der vorgesehenen Änderungen an der bestehenden leittechnischen Architektur oder der

geplanten LT-Architektur im Hinblick auf mögliche Auswirkungen auf leittechnische Systeme und die Ausführung leittechnischer Funktionen (Prozessschritt DO) und einem Abgleich mit den Anforderungen an die leittechnische Architektur sowie bei Bedarf mit zusätzlichen Anforderungen an den konkret geplanten Austausch von Systemen und Komponenten (Prozessschritt CHECK) bis hin zum Einfließen der gewonnenen Erkenntnisse in die Planungen des Einsatzes der LTE (Prozessschritt ACT) und ggf. einer Wiederholung des gesamten Prozesses nach einer Anpassung der Planungen für die vorgesehene bzw. geänderte leittechnische Architektur (Abb. 2.2).

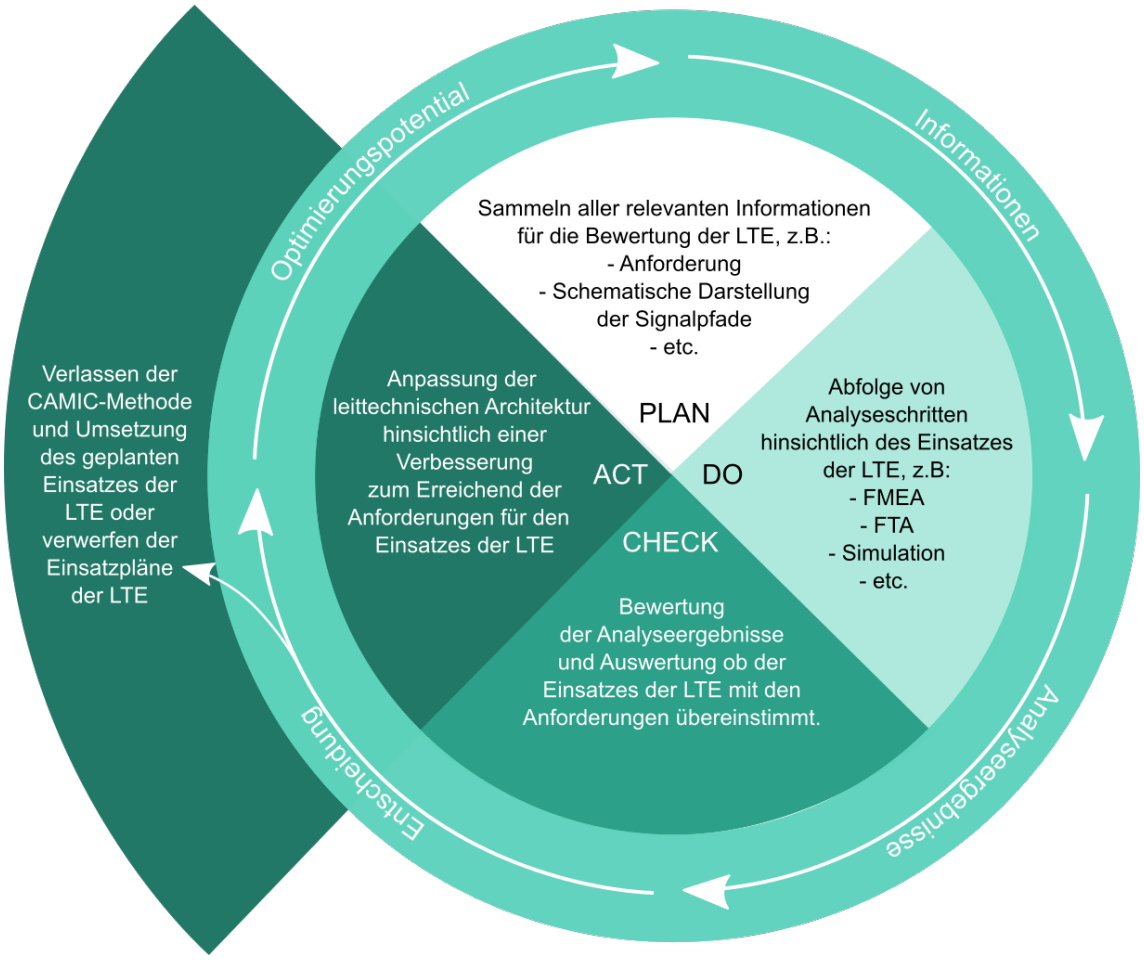


Abb. 2.2 Beispiel der Vorgehensweise für die Bewertung des vorgesehenen Einsatzes von LTE mit der CAMIC-Methode

Die CAMIC-Methode umfasst folgende Prozessschritte:

PLAN

Hier erfolgt die Planung der Bewertung mit Zusammenstellung aller für die Bewertung relevanten Dokumente und Informationen. Der Prozess der Bewertung einer geplanten leittechnischen Architektur oder der Bewertung von vorgesehenen Änderungen an einer bestehenden leittechnischen Architektur umfasst nicht die Planung der leittechnischen Architektur an sich, sondern setzt diese Planung voraus. Eine Berücksichtigung von Änderungen an dieser Planung ist im Rahmen des Bewertungsprozesses möglich. Im Prozessschritt – PLAN – der CAMIC-Methode werden alle relevanten Informationen für die Analyse des Einsatzes der LTE im LT-System gesammelt. Für eine solche Bewertung sind typischerweise zwei Arten von Informationen grundlegend. Zum einen handelt es sich dabei um technische Informationen über die leittechnische Architektur und die für die Bewertung relevanten leittechnischen Systeme und Komponenten. Zum anderen handelt es sich um Anforderungen an die leittechnische Architektur und die eingesetzten leittechnischen Systeme und Komponenten. Diese Anforderungen umfassen mindestens alle relevanten Anforderungen aus dem nationalen und internationalen Regelwerk, können aber durch weitere Anforderungen wie beispielsweise Kundenanforderungen ergänzt werden. Ein mögliches Projekt für die Verwendung der CAMIC-Methode wäre zum Beispiel der Austausch einer bislang programmierbaren ausgeführten leittechnischen Komponente durch eine komplexe, rechnerbasierte Komponente unter Einhaltung aller relevanten Regelwerksanforderungen und der zusätzlichen Anforderung, dass der Austausch der Komponente die Zuverlässigkeit einer ausgewählten leittechnischen Funktion erfüllt, indem ein bislang bestehendes CCF-Potential beseitigt wird.

DO

Auf Grundlage der gesammelten Informationen kann mit dem darauffolgenden Prozessschritt – DO – die eigentliche Analyse erfolgen. Je nach Auslegung der komplexen rechnerbasierten oder programmierbaren leittechnischen Komponente oder abhängig von der eigentlichen Fragestellung der Bewertung kann eine unterschiedliche Abfolge von Analyseschritten erfolgen. Dabei können unterschiedliche Analysewerkzeuge, wie FMEA (failure mode and effects analysis), FTA (fault tree analysis), CCF-Analyse oder Simulationen, in den einzelnen Analyseschritten angewendet und ausgewertet werden. Im hier entwickelten Bewertungsansatz ist diese Abfolge von Analyseschritten zu Beginn der Analyse noch nicht im Einzelnen vorgegeben, sondern wird unter Berücksichtigung

von Zwischenergebnissen durch Entscheidungskriterien festgelegt. Dieser Teil der Analyse liefert eine Aussage über die möglichen (negativen) Auswirkungen eines Fehlzustandes der LTE bei vorgesehenem Einsatz innerhalb des LT-Systems.

CHECK

Im vorletzten Prozessschritt – CHECK – wird das Ergebnis der Analyse mit den gesammelten Informationen aus – PLAN – abgeglichen. Dabei wird untersucht ob die geplanten Änderungen an der leittechnischen Architektur oder die vorgesehene leittechnische Architektur allen relevanten Anforderungen entsprechen und ob die in – DO – ermittelten Auswirkungen der vorgesehenen Änderungen an der leittechnischen Architektur bzw. des Einsatzes der LTE auf die leittechnischen Funktionen vertretbar sind.

ACT

Sind alle Anforderungen erfüllt, kann im Prozessschritt – ACT – der Zyklus verlassen werden und anschließend können die geplanten Änderungen an der leittechnischen Architektur (z. B. der Einbau oder Austausch einer komplexen rechnerbasierten oder programmierbaren leittechnischen Komponente) erfolgen. Ist mindestens eine Anforderung nicht erfüllt, bleiben zwei Optionen. Entweder kann (innerhalb des Prozesses, der für die tatsächlichen Änderungen verantwortlich ist, und damit außerhalb des CAMIC-Bewertungsprozesses) eine Entscheidung getroffen werden, die letztlich entweder zu Änderungen an Planungen für die vorgesehene leittechnische Architektur oder zu Änderungen an den zu erfüllenden Anforderungen führt. Dann kann auf Basis der geänderten Planungen oder der geänderten Anforderungen erneut eine Bewertung mit der CAMIC-Methode (weiterer Durchlauf des PDCA-Zyklus) durchgeführt werden oder die Pläne für den Einsatz der LTE können verworfen und der Zyklus daher verlassen werden.

2.3.2 Bewertungsmethode

Für die Bewertungsmethode des Vorgängervorhabens RS1525 /GRS 17/ wurden verschiedene Begriffe und Elemente der Flussdiagramme zusammengetragen und definiert. Im Folgenden werden diese Begriffe und Elemente erneut aufgegriffen und gegebenenfalls im Bezug zu diesem aktuellen Vorhaben erweitert.

2.3.3 Analysewerkzeuge

Bei der Bewertung für den Einsatz einer LTE in rechnerbasierter oder programmierbarer Leittechnik werden viele Fragen aufgeworfen. Für die Beantwortung dieser Fragen gibt es, je nach Fragestellung, unterschiedliche Ansätze.

- Welche Fehlermöglichkeiten bzw. Fehlzustandsarten der LTE sind möglich und welche Auswirkungen ergeben sich daraus auf die Funktionsfähigkeit der LTE?
  - Analyse der Ausfallmöglichkeiten einer einzelnen LTE; Generische Auswertung für eine einzelne LTE.
- Wie verhalten sich das LT-System, in dem die LTE verbaut ist, und die LT-Funktion, welche dieses LT-System ausführt, wenn es zu Fehlzuständen der LTE kommt?
  - Bewertung der Ausfallmöglichkeiten eines LT-Systems oder einer LT-Funktion aufgrund von Fehlzuständen einer einzelnen LTE.
- Eine bestimmte Fehlfunktion der LTE an sich, des LT-Systems, in dem diese verbaut ist, oder der LT-Funktion, welche dieses LT-System ausführt, soll vermieden werden. Welche Fehlzustandsarten der LTE können zu dieser Fehlfunktion führen?
  - Analyse der möglichen Pfade, die zu einer ausgewählten Fehlfunktion führen können.
- Wie hoch ist die Wahrscheinlichkeit, dass es zu ausgewählten Fehlfunktionen der LTE kommt?
  - Analyse der Ausfallraten der LTE bzgl. einer ausgewählten Fehlfunktion.
- Ist ein GVA zweier vorgegebener Typen LTE möglich?
  - Bewertung der Diversität zweier vorgegebener Komponenten.

Für die Beantwortung der Frage nach einer einzelnen LTE reicht die Analyse hinsichtlich einer FMEA oder FTA (Abschnitt 2.3.3.1 und 2.3.3.2) meist aus. Bei der Verwendung von LTE in Kombination mit rechnerbasierter oder programmierbarer Leittechnik eines Kernkraftwerks muss eine deutlich umfangreichere Analyse angewandt werden. Um eine Bewertung und Abschätzung des Einsatzes von LTE in rechnerbasierter oder programmierbarer Leittechnik zu ermöglichen, sollten mehrere Analysewerkzeuge aufeinander aufbauend angewendet werden. Eine solche Kombination verschiedener Analysewerkzeuge führt bei fast allen Fragestellungen zu einer deutlichen Verfeinerung des

Bewertungsergebnisses. Der im Rahmen dieses Vorgängervorhabens RS1525 /GRS 17/ entwickelte CAMIC-Bewertungsansatz kombiniert deshalb unter anderem die folgenden Analysewerkzeuge.

2.3.3.1 FMEA – Fehlzustandsart- und -auswirkungsanalyse

Die FMEA /DIN 06/, zu Deutsch *Fehlzustandsart- und -auswirkungsanalyse*, ist eine Analysemethode zur qualitativen Sicherheits- und Zuverlässigkeitsanalyse technischer Einrichtungen und Systeme oder zur Bewertung von Prozessen /WER 11/. In der Sicherheitstechnik wird die FMEA vor allem zur Analyse von Fehlern sowie deren Erkennung, Vermeidung und Auswirkungen verwendet. 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. Darüber hinaus kann die FMEA auf verschiedenen 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. Mit Fortschreiten der Analyse können, die auf niedrigerer Ebene festgestellten Ausfallauswirkungen auf höherer Ebene Ausfallarten bedingen. Die Ausfallarten auf niedrigerer Ebene können zu Ausfallursachen auf höherer Ebene werden und so weiter.

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.

In der Kerntechnik wurde die FMEA-Methode bereits in der Vergangenheit für die Bewertung analoger Sicherheitsleittechnik eingesetzt. In der aktuellen Version der kerntechnischen Regel KTA 3501 /KTA 15/ wird gefordert:

- „Bei Einsatz von rechnerbasierten oder programmierbaren Geräten sind im Rahmen einer Fehlermöglichkeits- und Einflussanalyse auf Systemebene die Auswirkungen auf die Anlage bei aktiven und passiven Fehlern der Komponenten darzustellen."

- „Ausfälle, die zu nicht sicherheitsgerichteten Maßnahmen und kritischen Anlagenzuständen führen können, sind zu ermitteln und hierfür geeignete Maßnahmen zur Fehlerbeherrschung vorzusehen. Das Verhalten der Ausgangssignale beim Auftreten von Fehlern ist zu spezifizieren."

Die typische FMEA-Vorgehensweise umfasst folgende Arbeitsschritte:

- **Planung**:
  - Bestimmung der Zielsetzung und des Umfangs der Analyse,
  - Ermittlung und Festlegung von Grenzen, Schnittstellen und Randbedingungen der Analyse,
  - Definition von Entscheidungskriterien für die Behandlung von Ausfallarten,
  - Festlegungen zum Analyseansatz (u. a. induktiv oder deduktiv, Detaillierungsgrad, Form der Dokumentation),
  - Zerlegung der Betrachtungseinheit in geeignete Elemente (Funktionsblöcke).
- **Durchführung**:
  - Bestimmung von Funktionen und Leistungsmerkmalen der Betrachtungseinheiten,
  - Analytische Identifikation von Fehlzustandsarten (u. a. mögliche Ausfallarten und ggf. mögliche Fehler- und Ausfallursachen),
  - Bestimmung von lokalen und weiteren möglichen Auswirkungen (z. B. Funktionsverlust auf der nächsthöheren Ebene oder höhergelegenen Ebenen),
  - Identifikation von Fehlererkennungsmethoden (z. B. selbstmeldende Ausfälle, Online-Fehlerdiagnose, Prüfungen).
- **Ergebnisdokumentation**:
  - Beschreibung des analysierten Systems (u. a. Funktionsbeschreibung, Block bzw. Funktionsdiagramme),
  - getroffene Annahmen und Anwendungsbereich,

- detaillierte und nachvollziehbare Zusammenfassung der Analyse in einer geeigneten Form (z. B. FMEA-Tabelle mit Fehlzustandsarten, Auswirkungen, Fehlererkennung, siehe beispielsweise Worksheet in /DIN 06/).

Als Grundlage für FMEA in rechnerbasierter oder programmierbarer Leittechnik kerntechnischer Anlagen dient zum Beispiel ein Funktionsplan.

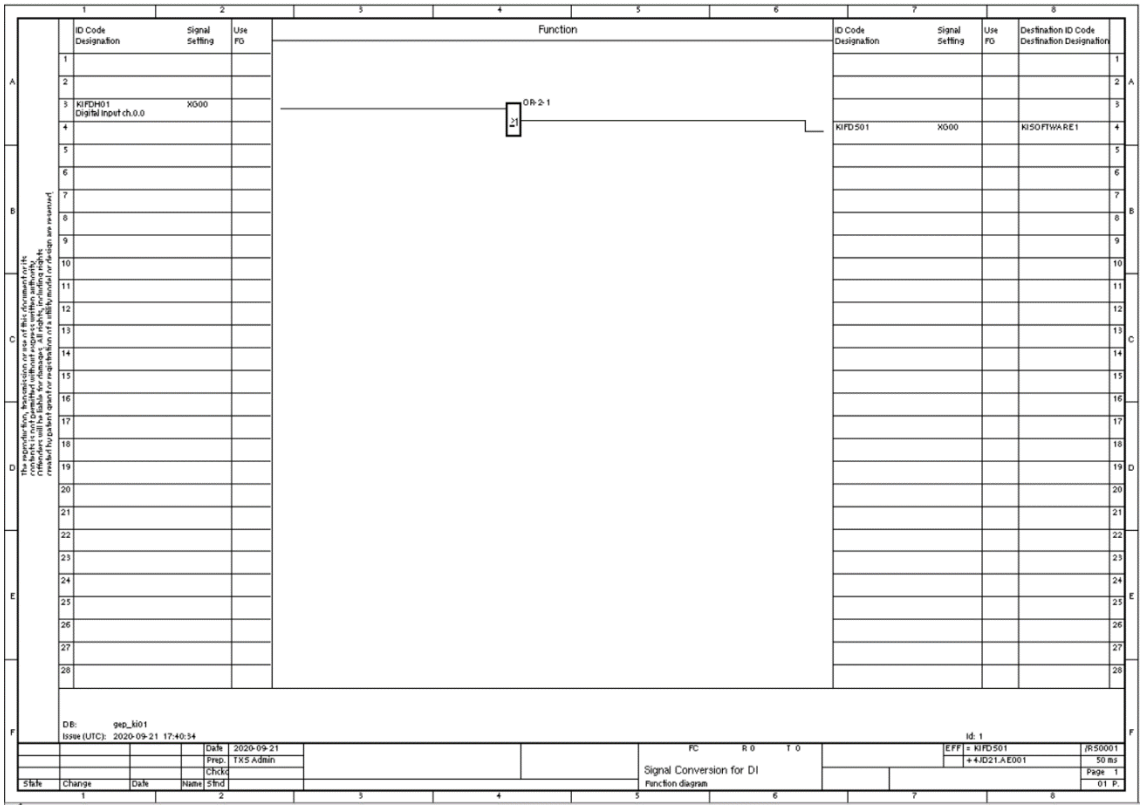


Abb. 2.3 Beispielhafter, einfacher Funktionsplan in welchem ein Eingangssignal nur weitergeleitet wird. In diesem Fall kann das Ausgangssignal des LTE nur zwei Zustände haben. Entweder es sendet ein Ausgangssignal oder es sendet kein Ausgangssignal

Anhand dieses Funktionsplans (Abb. 2.3) wird eine Analyse der betroffenen Komponenten und Signalpfade durchgeführt. Dabei muss gegebenenfalls auch der Ausgangszustand des Systems berücksichtigt werden. Die FMEA wird auf der Basis einer relativ einfachen Analysematrix (z. B. orthogonale FMEA-Tabelle) aufgebaut, in der die Ursache und die Auswirkung in einem direkten Zusammenhang dargestellt werden. Als erstes Beispiel betrachten wir eine LTE, welche aus einem Sender (DI) und einem Empfänger (DO) besteht. Der Sender leitet ein Signal an den Empfänger weiter. Außerdem soll die Annahme getroffen werden, dass der Sender im Fehlzustand das Signal „0“ an den

Empfänger ausgibt. Um jetzt das anstehende Signal am Empfänger zu ermitteln, wird alles in einer Tabelle (Tab. 2.1) zusammengefasst.

Tab. 2.1 FMEA mit dem einfachen Fall, dass das Eingangssignal nur weitergeleitet werden muss

Soll	**Di-Err**	**DI**	**DO**
1	O.K.	1	1
1	Err.	0	0
0	O.K.	0	0
0	Err.	0	0

In diesem Fall kann das Ausgangssignal der LTE nur zwei Zustände annehmen: Entweder die LTE sendet ein Signal oder sie sendet kein Signal. Wir gehen hier davon aus, dass das Eingangssignal dauerhaft anstehen soll und die LTE dazu dient, dies zu überprüfen und bei Ausfall des Eingangssignals einen Fehlzustand anzunehmen. Die LTE entspricht in diesem Fall also einer 1v1-Auswahlschaltung.

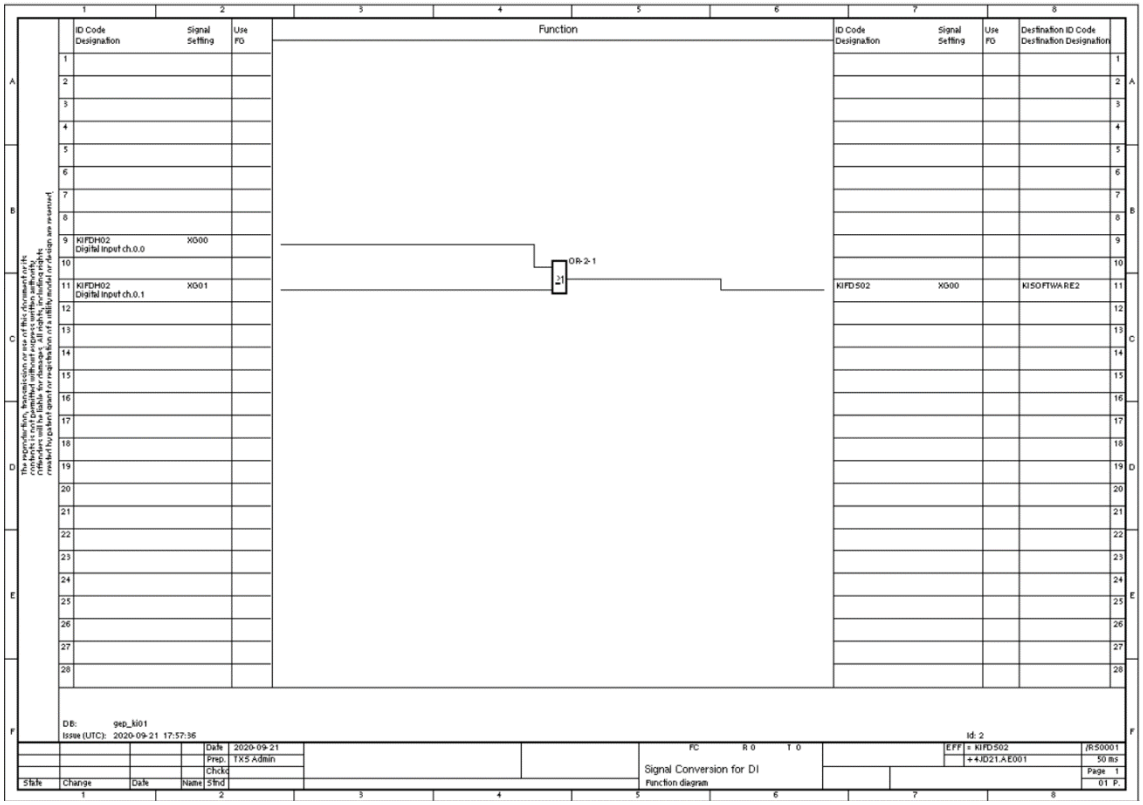


Abb. 2.4 Funktionsdiagramm mit erweitertem Fall, dass zwei Eingangssignale überprüft werden. In diesem Fall wird das Ausgangssignal nur dann nicht weitergeleitet, wenn beide Eingangssignale ausfallen

Als zweites Beispiel betrachten wir jetzt einen zweifach redundanten Aufbau. Hier wird das Signal nur dann nicht weitergeleitet, wenn beide Eingangssignale ausfallen (beispielsweise, weil die entsprechenden Sender defekt sind) (Abb. 2.4). In diesem Beispiel repräsentiert die LTE also eine 1v2-Auswahlschaltung.

Eine FMEA der Signalübertragung sieht in diesem Fall wie folgt aus:

Tab. 2.2 FMEA des erweiterten Falls, dass zwei Eingangssignale überpüft werden und zwar in dem Sinn, dass das Ausgangssignal 1 annimmt, sobald eines der beiden Eingangssignale 1 ist

Soll	DI1-Err	DI2-Err	DI1	DI2	DO
1	O.K.	O.K.	1	1	1
1	Err.	O.K.	0	1	1
1	O.K.	Err.	1	0	1
1	Err.	Err.	0	0	0
0	O.K.	O.K.	0	0	0
0	Err.	O.K.	0	0	0
0	O.K.	Err.	0	0	0
0	Err.	Err.	0	0	0

Die Ergebnisse einer FMEA sollen helfen, alle sicherheitsrelevanten Aspekte (u. a. potenzielle Gefährdungen, Fehlervorbeugung und -beherrschung) einer komplexen LT-Einrichtung zu ermitteln und können als Grundlage für weiterführende Analysen benutzt werden, u. a. für

- Zuverlässigkeitsanalyse,
- Verfügbarkeitsanalyse,
- Bewertung der Instandhaltung.

Die Effektivität einer FMEA kann zudem durch Kombination mit anderen Analysemethoden erhöht werden, z. B.

- Fehlzustandsbaumanalyse der Auswirkungen der ermittelten Einzelfehler (Fehlzustandsarten) und deren Kombinationen,
- GVA-Analyse der potenziellen GVA-Kandidaten (Fehlzustandsarten) auf Systemebene,
- Markov-Analyse der Erkennung und Reparatur von ermittelten Fehlzustandsarten.

Die o. g. Eigenschaften der FMEA-Methode verdeutlichen, dass diese Methode für unterschiedliche Fehlzustandsart- und Auswirkungsanalysen von LTE und Systemen mit dem entwickelten CAMIC-Bewertungsansatz verwendet werden kann.

2.3.3.2 FTA – Fehlzustandsbaumanalyse

Eine weitere Analysemethode ist die FTA (Fault Tree Analysis), zu Deutsch Fehlzustandsbaumanalyse genannt /DIN 07/. Diese dient dazu, eine Vorhersage über die Zuverlässigkeit eines Systems zu treffen. Dazu wird systematisch die Abhängigkeit zwischen Ausfall des Systems und dem Ausfall seiner Komponenten betrachtet. Anschließend wird die Wahrscheinlichkeit für den Ausfall des Systems berechnet /BFS 05/. Die Berechnung 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 (Primär- oder Basisereignisse) besonders hervorzuheben, die zum festgelegten Hauptereignis führen können. Die leittechnischen Komponenten des Systems werden über logische Verknüpfungen entlang der Signalpfade miteinander verbunden (Abb. 2.5). Die verwendeten Symbole der Fehlerbaumanalyse entsprechen dem festgelegten IEC Standard /DIN 07/.

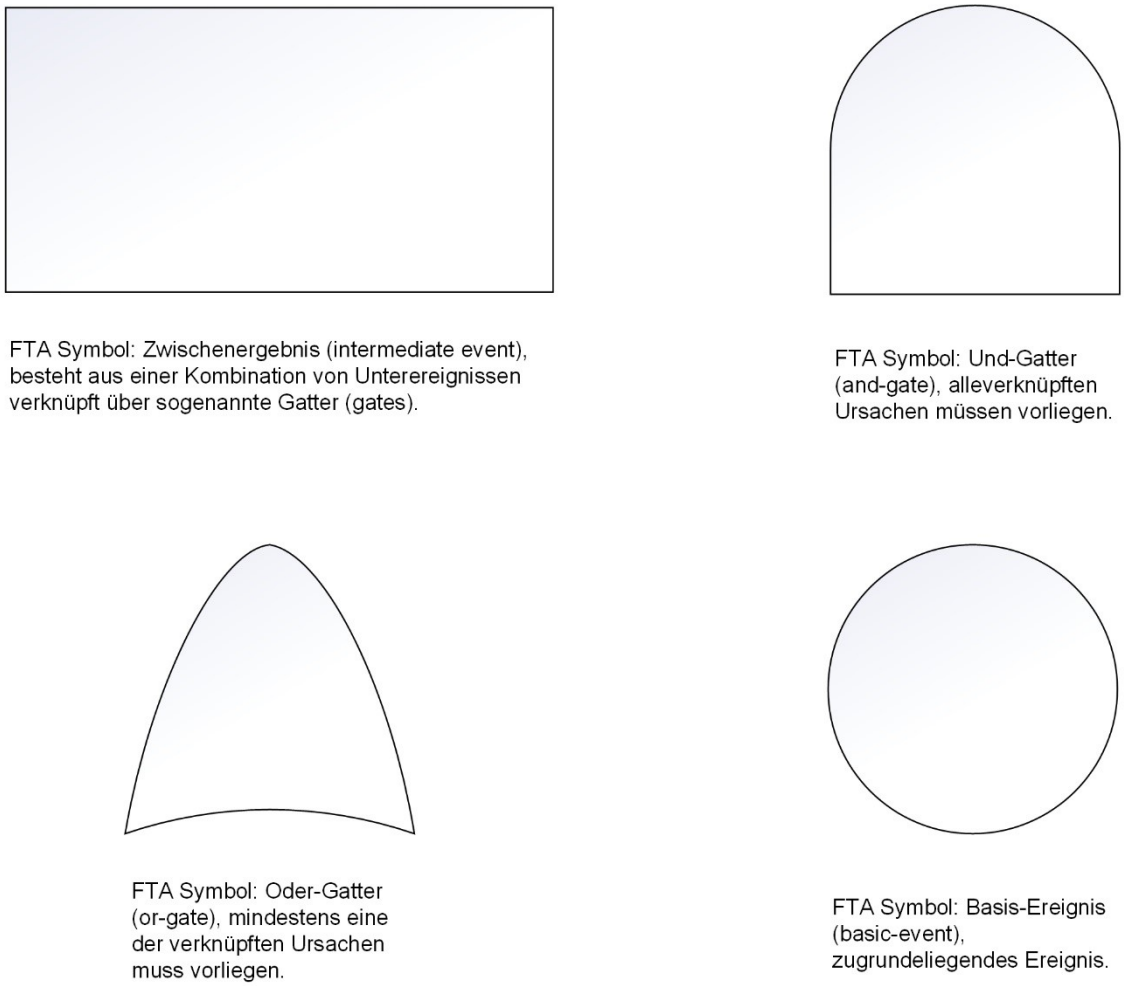


Abb. 2.5 Übersicht einiger FTA Symbole, /DIN 07/

Die Analyse kann qualitativer oder quantitativer Natur sein. Sind die Wahrscheinlichkeiten der Primärereignisse bekannt, können die Eintrittswahrscheinlichkeiten des Hauptereignisses sowie aller Zwischenereignisse im Rahmen einer quantitativen Analyse berechnet werden /DIN 07/.

Die Fehlzustandsbaumanalyse kann dabei helfen, kritische Komponenten (genauer deren Fehlzustandsarten) bzw. Kombinationen von Ausfällen (Minimalschnitte) zu ermitteln und bei Verfügbarkeit von Zuverlässigkeitskenndaten (z. B. Ausfallraten) die Eintrittswahrscheinlichkeiten der Top-Ereignisse (z. B. Ausfall einer Systemfunktion) zu quantifizieren.

Der Zweck der Fehlzustandsbaumanalyse ist demnach die Ermittlung der logischen Verknüpfungen von Komponenten- oder Teilsystemausfällen, die zu einem unerwünschten Ereignis führen. In der Regel entsprechen die Fehlzustandsarten der FMEA-Analyse den Primärereignissen der Fehlzustandsbaumanalyse. Ebenso lässt sich das Hauptereignis

der Fehlzustandsbaumanalyse innerhalb einer FMEA als (globale) Fehlzustandsauswirkung ermitteln. Ziele sind die systematische Identifizierung aller möglichen Ausfallkombinationen (Ursachen, Kombinationen von Fehlzustandsarten), die zu einem vorgegebenen unerwünschten Ereignis führen, sowie die Ermittlung von Zuverlässigkeitskenngrößen, wie z. B. Eintrittshäufigkeiten der Ausfallkombinationen, Eintrittshäufigkeit des unerwünschten Ereignisses oder Nichtverfügbarkeit des Systems bei Anforderung /DIN 81/.

Die Fehlzustandsbaumanalyse wird mit Hilfe von Modellierungs- und Analysewerkzeugen (z. B. RiskSpectrum® -Software) durchgeführt, wobei die Ursachen (i. d. R. die Ausfallwahrscheinlichkeiten bzw. Fehlzustandsarten von Systemkomponenten) und die Auswirkungen in einem Fehlzustandsbaummodell grafisch dargestellt werden. Die Ergebnisse (z. B. Minimalschnitte) werden automatisch durch die Software ermittelt.

Die Fehlzustandsbaumanalyse kann auch bei Systemen eingesetzt werden, die aus verschiedenen Teilen (mechanische und elektrische Komponenten, Leittechnik, Personalhandlungen) bestehen und die in gegenseitiger Wechselbeziehung stehen, welche nicht in einfacher Weise mittels anderer Verfahren modelliert werden können /DIN 07/.

Die Fehlzustandsbaumanalyse umfasst:

- **Analyse des zu untersuchenden Systems oder der Systemfunktion**
  - Zur Untersuchung der Systemfunktion genügt es, das technische System als Black Box zu betrachten, die über Ein- und Ausgaben verfügt.
  - Die Ein- und Ausgaben sowie die Leistungsziele der Systemfunktionen und zulässigen Abweichungen sind zu untersuchen. Dabei müssen neben den Umgebungsbedingungen auch Hilfsquellen wie die Energie- und Medienversorgung, das Zusammenwirken der Komponenten zur Erzeugung der Systemfunktion und die Reaktion des Systems auf Ausfälle innerhalb des Systems oder der Hilfsquellen berücksichtigt werden.
  - Identifizierung der einzelnen Komponenten des Systems und deren Fehlzustandsarten.
  - Festlegung des unerwünschten Ereignisses und der Ausfallkriterien.
  - Festlegung der zu betrachtenden Zeitintervalle.

- **Fehlzustandsbaummodellierung**
  - Aus der Festlegung des unerwünschten Ereignisses sind die Ausfallarten der Komponenten abzuleiten, die bei der Aufstellung des Fehlzustandsbaums zu berücksichtigen sind,
  - Festlegung des Anwendungsbereichs und des Untersuchungsziels des Fehlzustandsbaums,
  - Festlegung der Grenzen des Systems und des zu untersuchenden Objekts und der Analysetiefe und Randbedingungen,
  - Zusammenstellung der Kenngrößen der Eingänge in den Fehlzustandsbaum wie Ausfallraten, Ausfallzeiten, Testintervalle und Nichtverfügbarkeiten,
  - Fehlzustandsbaummodellierung ist ein iterativer Prozess und endet, wenn Basisereignisse (Blätter des Fehlzustandsbaums) keine funktionellen Abhängigkeiten mehr haben.
- **Auswertung des Fehlzustandsbaums**
  - Quantifizierung von Risiken, Komponenten, Abhängigkeiten, die maßgebend zum unerwünschten Ereignis beitragen,
  - Die Ausfallkombinationen werden durch die Minimalschnitte beschrieben,
  - Analyse der Unverfügbarkeit der Komponenten,
  - Sensitivitätsanalysen: mit der Sensitivitätsanalyse wird bestimmt, wie empfindlich die Ergebnisse gegenüber Randbedingungen und Annahmen sind,
  - Importanz-Analysen: damit wird festgestellt, welche Ergebnisse am empfindlichsten gegenüber den mit den relevanten Modellparametern verbundenen Unsicherheiten sind.

Im Rahmen der CAMIC-Methode ist der Einsatz der Fehlzustandsbaummodellierung und -analyse (FTA) vorgesehen, wenn die Fehlzustandsart- und Auswirkungsanalyse (FMEA) an Grenzen bei der Ermittlung potenzieller Auswirkungen stößt oder eine Analyse der Kombinationen von Ausfallarten erforderlich ist.

2.3.3.3 Matrix der Diversitätsmerkmale

Als weiteres Analysewerkzeug bei der Bewertung rechnerbasierter oder programmierbarer Leittechnik wird die von der GRS im Rahmen des BMU-Vorhabens 3611R01355 entwickelte Matrix zur Bewertung der Diversitätsmerkmale leittechnischer Komponenten herangezogen /GRS 15a/. Bei der Entwicklung dieser Matrix wurden zwei wesentliche Ziele verfolgt:

- Betrachtung relevanter Aspekte des Lebenszyklus von der Formulierung der Anforderungen über Entwicklung und Herstellung bis hin zu Betrieb und Instandhaltung bei der Definition und der Erarbeitung von Diversitätsmerkmalen,
- Herstellung des Anwendungsbezugs dieser Diversitätsmerkmale über ihre Anwendbarkeit auf einzelne Baugruppen, Redundanzen eines LT-Systems oder ganze LT-Systeme.

Die Matrix der Diversitätsmerkmale basiert einerseits auf einer generischen Darstellung eines LT-Systems, welche sowohl die für die Ausführung der LT-Funktionen wichtigen Bestandteile des LT-Systems als auch weitere technische Aspekte des LT-Systems, die nicht direkt der Ausführung der LT-Funktionen dienen, abdeckt (Spalten der Matrix). Andererseits enthält sie diejenigen Diversitätsmerkmale, welche die für die Beurteilung der Diversität relevanten Aspekte des Lebenszyklus dieses generischen Leittechniksystems umfassen. Die Matrix der Diversitätsmerkmale an sich verknüpft in Abhängigkeit von den betrachteten Baugruppen, Komponenten oder LT-Systemen die Bestandteile des generischen LT-Systems mit den Diversitätsmerkmalen. Sie gibt Aufschluss darüber, welche Diversitätsmerkmale für das Vorliegen von Diversität in einem bestimmten Bestandteil eines Leittechniksystems relevant sind. Der erste Schritt bei der Anwendung dieser Matrix im Rahmen der Bewertung von Diversität ist die Anpassung der Matrix an den vorliegenden Bewertungsgegenstand, die konkrete LT-Architektur und die zugrunde gelegte Fragestellung bei der Bewertung. Dies geschieht durch Festlegung der relevanten Diversitätsmerkmale und zutreffenden Aspekte des zugrunde gelegten generischen LT-Systems und anschließende Streichung der für die Bewertung der konkreten Fragestellung nicht relevanten Zeilen und Spalten der Matrix. Die auf die konkrete Fragestellung angepasste Diversitätsmatrix ist daher immer eine Teilmatrix der vollständigen Diversitätsmatrix. Im Rahmen der CAMIC-Methode für LTE wird die Matrix der Diversitätsmerkmale aufbauend auf eine FMEA oder FTA für Diversitätsbetrachtungen im Rahmen der GVA-Analyse eingesetzt.

2.4 Sachstand in der Softwareentwicklung

2.4.1 Python

Aufgrund der Flexibilität und des Umfangs der Module wurde für die CAMIC-Anwendung die Programmiersprache Python /PSF 21/ gewählt.

Python wurde Anfang der 1990er Jahre von dem niederländischen Softwareentwickler Guido van Rossum entwickelt. Heute zählt Python zu den wichtigsten wissenschaftlichen Programmiersprachen weltweit. Angewendet wird Python unter anderem von Google, DLR (Deutsche Luft- und Raumfahrtbehörde) und der NASA. Ziel von Python war es, eine leicht lesbare Programmiersprache zu entwickeln. Daher wird bei Programmblöcken, wie zum Beispiel Schleifen, auf geschweifte Klammern verzichtet. Stattdessen wird der komplette Programmblock eingerückt.

Als objektorientierte Programmiersprache liegt der weitere Vorteil in der Definition von Klassen innerhalb Pythons. Damit werden unnötige Wiederholungen von Codeblöcken vermieden. Alternativ werden Instanzen von Klassenobjekten mit den benötigten Methoden erzeugt. Außerdem handelt es sich bei Python um eine frei verfügbare Programmiersprache. Das bringt den Vorteil, dass mittlerweile sehr viele nützliche Pakete für Python entwickelt wurden. Für die wissenschaftliche Analyse stehen zum Beispiel das Mathematikpaket – NumPy /NUM 21/, das Plotpaket – Matplotlib /MAT 21/ oder das Tabellenpaket – panda /PAN 21/, zur freien Verfügung.

Neben der Vielzahl an Analysewerkzeugen, die die Analyse in Python sehr effizient machen, bietet Python außerdem diverse Schnittstellen. So können in Python Schnittstellen zu Ausgabegeräten und zu unterschiedlichen Datenbanken definiert werden. Für die CAMIC-Anwendung ist die Anbindung an eine Datenbank zum Ablegen von Dokumenten und zum Speichern von Fortschritten unverzichtbar. Ebenso unverzichtbar für die CAMIC-Anwendung ist die Benutzeroberfläche (GUI – Graphical User Interface). Python bietet auch hier mehrere Möglichkeiten eine GUI zu realisieren. Für den Einstieg in die Entwicklung einer Benutzeroberfläche wurde Tkinter /TKI 21/ gewählt. Tkinter bietet genügend Flexibilität zur Realisierung der Designvorgaben und eine einfache Integration der CAMIC-Methode.

2.4.2 MySQL

Ein Satz zur Verwendung von MySQL in CAMIC

MySQL /MYS 21/ ist eine der verbreitetsten Datenbankstrukturen weltweit. Die Datenbank MySQL wurde 1994 von der Firma MySQL AB entwickelt. Weltweit wird MySQL unter anderem von Facebook oder YouTube eingesetzt. Die in MySQL eingesetzte Datenbanksprache ist SQL (Structured Query Language) und dient der einfachen Abfrage der Informationen aus der Datenbank. Semantisch ist die Sprache SQL an die englische Sprache angelehnt, was eine Verwendung der SQL-Abfragen intuitiv gestaltet.

2.5 Sachstand zur sicherheitstechnischen Bewertung von rechnerbasierter und programmierbarer Leittechnik

Die GRS hat bereits viele Erfahrungen auf dem Gebiet der sicherheitstechnischen Bewertung von rechnerbasierter und programmierbarer Leittechnik gesammelt. Im Folgenden wird eine Auswahl der durchgeführten Arbeiten vorgestellt:

- **Abgeschlossene Arbeiten**
  - **Aufstellung von Kriterien zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken**: In diesem Vorhaben wurde eine Diversitätsmatrix entwickelt, die bei der Bewertung der Diversität von programmierbaren und rechnerbasierten leittechnischen Komponenten und Systemen als Grundlage eingesetzt werden kann. /GRS 15a/
  - **Entwicklung und Einsatz von Analysemethoden zur Beurteilung softwarebasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken:** In diesem Vorhaben wurde auf Basis von Betriebserfahrung unterhalb der Meldeschwelle aus verschiedenen deutschen Kernkraftwerken das Ausfallverhalten von programmierbaren und rechnerbasierten leittechnischen Einrichtungen untersucht. /GRS 15b/
  - **Zuverlässigkeitsbewertung unter neuen Anforderungen an Sicherheitsleittechnik in Kernkraftwerken: Analysen der Anwendungspraxis:** In diesem Vorhaben wurden die Bewertungsmaßstäbe für rechnerbasierte oder programmierbare Baugruppen und Systeme, die für eine Anwendung im nuklearen Bereich vorgesehen sind, weiterentwickelt. Im Fokus standen dabei neben

konkreten Anforderungen an die Softwareentwicklung und den Softwarelebenszyklus die Prozesse und Methoden der Qualifizierung und der Bewertung der Systemzuverlässigkeit sowie die Anwendbarkeit von Software-Metriken. /GRS 16/

- **Neue Methoden zur Bewertung der Zuverlässigkeit fortschrittlicher Mensch-Maschine-Schnittstellen digitaler leittechnischer Einrichtungen und personell-organisatorischer Einflüsse:** In diesem Vorhaben verfolgte die GRS das Ziel, methodische Ansätze und Werkzeuge für Sicherheitsanalysen in der Kerntechnik weiterzuentwickeln. In einem Teilvorhaben wurde die CAMIC-Methode zur Bewertung der Sicherheit- und Zuverlässigkeit digitaler Leittechnik entwickelt, die auf der Basis von PLD-Technologien (Programmable Logic Devices) aufgebaut ist. /GRS 17/

- **Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik**: Im Rahmen dieses Vorhabens wurden umfangreiche Arbeiten zur Modellierung von unterschiedlichen Architekturen rechnerbasierter und programmierbarer Leittechniksysteme mittels Fehlerbaum-Methoden und Markov-Prozessen durchgeführt. Mit Hilfe der durchgeführten Modellierung wurden mittels Sensititvitätsanalysen der Einfluss verschiedener Parameter der Leittechnikarchitekturen auf deren Zuverlässigkeit untersucht. /GRS 18/

- **Erforschung von Ausbreitungswegen von Softwarefehlern in softwarebasierter Leittechnik in Kernkraftwerken**: Der Schwerpunkt dieses Vorhabens lag darin, die Auswirkungen und die Ausbreitung von Softwarefehlern innerhalb von softwarebasierten Leittechniksystemen systematisch zu untersuchen. /GRS 20a/

- **Diversitätsbewertung von komplexen elektronischen Komponenten für den Einsatz in sicherheitstechnisch wichtigen Einrichtungen in Kernkraftwerken**: In diesem Vorhaben wurden auf Basis der im vorgenannten Vorhaben entwickelten Diversitätsmatrix Diversitätsmerkmale speziell für die Bewertung komplexer elektronischer Komponenten für sicherheitstechnisch wichtige Anwendungen erarbeitet. /GRS 20b/

- **Forschungsarbeiten zur Entwicklung einer Bewertungsgrundlage für rechnerbasierte und programmierbare Leittechniksysteme in kerntechnischen Anlagen und Erforschung des Weiterentwicklungsbedarfs der dazugehörigen Anforderungen in der Leittechnik:** In diesem Vorhaben wurden die Grundlagen zur Bewertung programmierbarer oder rechnerbasierter Sicherheitsleittechnik („digitale Leittechnik“ – DI&C) unter Berücksichtigung der internationalen Erfahrungen erweitert und überarbeitet. /GRS 21a/

- **Laufende Arbeiten**

  - **Analyse der Fehlerausbreitung in der Netzwerkkommunikation digitaler Leittechniksysteme mit Hilfe eines Testsystems:** Die Signalverarbeitung digitaler Leittechnik nutzt sowohl für die interne als auch für die externe Kommunikation unterschiedliche Netzwerktechnologien und -topologien, deren Zuverlässigkeits- und Sicherheitsbewertung im Vordergrund dieses Vorhabens steht.

3 Weiterentwicklung der CAMIC-Methode zur sicherheitstechnischen Bewertung rechnerbasierter oder programmierbarer Leittechnik

Die im BMWi-Vorhaben RS1525 entwickelte CAMIC-Methode wurde nur für ausgewählte, PLD-basierte leittechnische Einrichtungen entwickelt. In diesem Arbeitspaket erfolgte die Erweiterung der CAMIC-Methode auf ein breiteres Spektrum an Anwendungsfällen. Die Erweiterung zielt auf die Bewertung komplexer rechnerbasierter oder programmierbarer Leittechniksysteme und -komponenten, wobei die beiden Aspekte der Fehlervermeidung und der Fehlerbeherrschung Berücksichtigung fanden.

Wesentlich bei der Bewertung von sicherheitstechnisch wichtigen Einrichtungen sind die Anforderungen aus den jeweils anzuwendenden Regelwerken und Normen. Daher wurde die CAMIC-Methode, um die Möglichkeit systematischer Themensuchen in relevanten Dokumenten erweitert. Es ist jetzt möglich, zu festgelegten Themen Selektion und Ausgabe von Anforderungen durchzuführen.

3.1 Weiterentwicklung der Bewertungsmethodik

Im ersten Prozessschritt erfolgte die Spezifikation der mittels der CAMIC-Methode zu betrachtenden Fragestellungen:

- Betrachtung neuer Leittechniksysteme,
- Bewertung von Umrüstmaßnahmen,
- Austausch einzelner leittechnischer Einrichtungen in einem bestehenden System.

Auf dieser Basis wurde die Entwicklung und Beschreibung der CAMIC-Methode für die genannten Anwendungsfälle durchgeführt. Hierzu wurden sämtliche Prozessschritte der CAMIC-Methode (PLAN, DO, CHECK, ACT) so angepasst und erweitert, dass anschließend für diese Anwendungsfälle Entscheidungskriterien, Analyseschritte und -werkzeuge, einschließlich konsistenter Verknüpfungen zwischen den Arbeitsschritten, zur Verfügung stehen.

In diesem Zuge wurde auch das gesamte CAMIC-Flussdiagramm erweitert. Dazu wurden Teildiagramme für die neuen Anwendungsfälle erstellt.

Da die rechnergestützte CAMIC-Anwendung den gesamten Anwendungsbereich von CAMIC abdeckt, wurde außerdem die erweiterte CAMIC-Methode vollständig in der CAMIC-Anwendung realisiert. Die Entwicklung der CAMIC-Anwendung wurde im Rahmen des Arbeitspakets – Werkzeugentwicklung für die rechnergestützte Anwendung der CAMIC-Methode – umgesetzt.

Für die Weiterentwicklung der CAMIC-Methode wurden die zusätzlich im Rahmen von CAMIC zu betrachtenden Fragestellungen spezifiziert sowie Weiterentwicklungsbedarf bei den bisher durch CAMIC abgedeckten Fragestellungen identifiziert. Die CAMIC-Methode wurde dahingehend erweitert, dass sie nicht nur die Bewertung einzelner leittechnischer Einrichtungen wie z. B. Baugruppen der Antriebssteuerung oder der Messwerterfassung, sondern auch die Bewertung komplexer rechnerbasierter oder programmierbarer Leittechniksysteme wie z. B. Schutzsysteme oder Begrenzungen in den Reaktoranlagen hinsichtlich Fehlervermeidung und Fehlerbeherrschung ermöglicht. Die Abfragen, Anforderungen und Entscheidungskriterien der CAMIC-Methode, die aus einer Vielzahl von Tabellen, Abfragen, Entscheidungskriterien, Erläuterungen und Flussdiagrammen bestehen, wurden bis zur in diesem Vorhaben durchgeführten Weiterentwicklung manuell ausgewertet. Für die Weiterentwicklung wurden zunächst die Elemente der Flussdiagramme angepasst. Darauffolgend wurden die Prozessschritte des PDCA-Zyklus anhand der geänderten Elemente des Flussdiagramms überarbeitet. Im Folgenden werden die neuen Flussdiagramme der CAMIC-Methode vorgestellt.

3.1.1 Definition von Elementen der Flussdiagramme

Das Hauptziel der Bewertungsmethode ist die Antwort auf die Frage, ob der Einbau/Austausch einer LTE den Anforderungen entspricht. Als Bewertungsansatz wurde eine schematische Darstellung der Vorgehensweise in Form eines Analyse-Ablaufplans (Flussdiagramms) erstellt. Die Erstellung der Analyse-Ablaufpläne wurde nach DIN 66001 /DIN 84/ durchgeführt. Im Vergleich zum Vorgängervorhaben wurden einige Elemente des Flussdiagramms erweitert, um so ein nachvollziehbares Vorgehen der Bewertungsmethode zu gewährleisten. Um das Flussdiagramm optimal in der rechnergestützten Anwendung umsetzen zu können, wurden Schleifen durch Entscheidungskriterien ersetzt, die unterschiedlichen Haltepunkte wurden direkt in das Zwischenergebnis implementiert und die Eingangsinformationen fließen direkt in die Analyse mit ein. In den Abb. 3.1 bis Abb. 3.6 sind die alle Elemente des Flussdiagramms dargestellt.

Abb. 3.1 Flussdiagrammelement: **Analyseschritt**

Analyseschritt: In dem Analyseschritt können verschiedene Analysemethoden angewendet oder Informationen zusammengetragen werden.

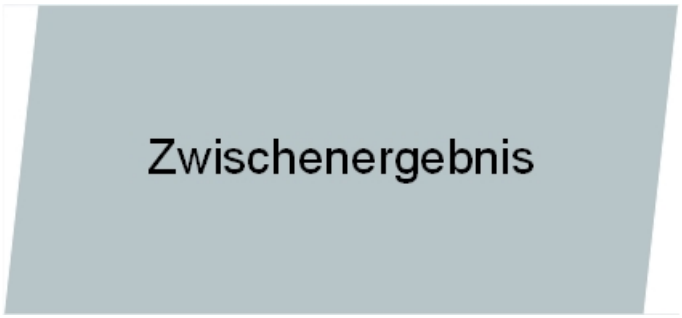


Abb. 3.2 Flussdiagrammelement: **Zwischenergebnis**

Zwischenergebnis: Bei Zwischenergebnissen handelt es sich um die Ergebnisse einer zuvor durchgeführten Analyse. Das Zwischenergebnis wird entweder für eine weitere Analyse oder für die Bewertung eines darauffolgenden Entscheidungskriteriums benötigt. Bei einigen Zwischenergebnissen könnte sich entscheiden lassen, ob ein nachgeordnetes Entscheidungskriterium erfüllt ist oder nicht.

Abb. 3.3 Flussdiagrammelement: **Projektabschluss**

Projektabschluss: Dieses Element wird ausschließlich im Prozessschritt ACT verwendet. Bei positiven Projektabschluss erfolgt eine Umsetzung der Planung des Einbaus der LTE. Bei negativem Projektabschluss wird die Planung des Einbaus der LTE verworfen.

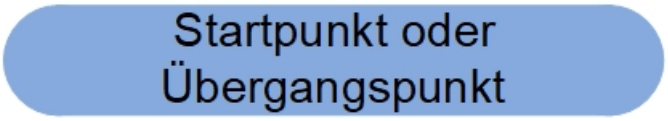


Abb. 3.4 Flussdiagrammelement: **Startpunkt oder Übergangspunkt**

Startpunkt oder Übergangspunkt: Der Startpunkt wird am Anfang der Bewertung oder der Prozessschritte des PDCA-Zyklus verwendet. Der Übergangspunkt wird am Ende eines Prozessschrittes des PDCA-Zyklus angewendet, um zu signalisieren, dass die Bewertung im nächsten Prozessschritt fortgesetzt wird.

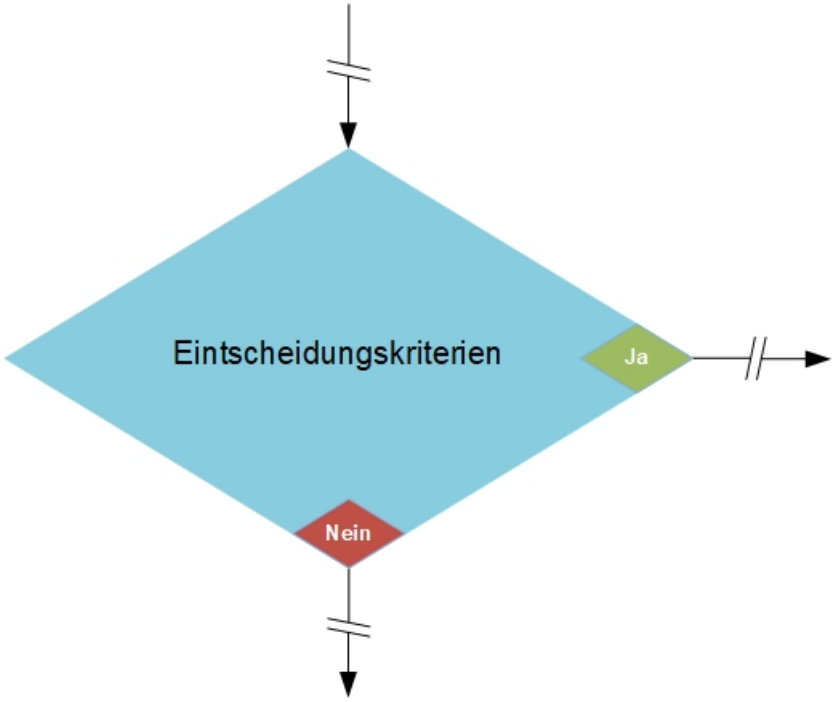


Abb. 3.5 Flussdiagrammelement: **Entscheidungskriterium**

Entscheidungskriterien: Die Erfüllung von Entscheidungskriterien wird anhand von Eingangsinformationen oder bei vorausgehenden Analyseschritten ermittelten Zwischenergebnissen bewertet. Die Entscheidungskriterien sind als Fragen formuliert. Die Antworten auf diese Fragen bestimmen schrittweise die genaue Abfolge der Analyseschritte. Hierbei ist anzumerken, dass jede Änderung am geplanten Einsatz der LTE gegenüber einem vorherigen Durchlaufen des PDCA-Zyklus diese Abfolge ändern kann.

Abb. 3.6 Flussdiagrammelement: **Verknüpfungen**

Verknüpfungen zu anderen / von anderen Flussdiagrammen: Die Verknüpfung ermöglicht eine Flexibilität in der Analyse. Es können die unterschiedlichen Vorgehensweisen innerhalb eines PDCA-Prozessschritts miteinander verbunden werden.

3.1.2 CAMIC-Prozessschritt: PLAN

Im Prozessschritt PLAN erfolgte bisher das Zusammentragen aller für die Analyse relevanten allgemeinen Informationen hinsichtlich des geplanten Einsatzes von PLD-LTE in den LT-Systemen sowie aller Anforderungen, denen diese LT-Systeme und die PLD-LTE an sich genügen müssen /GRS 17/. Dies erfolgte jedoch ohne Konsistenzprüfungen. Die wichtigsten Informationen für diesen Prozessschritt konnten bisher auf die folgenden drei Kategorien aufgeteilt werden:

1. Welche PLD-LTE soll betrachtet werden (Projektschlüsselfragen)
2. Wo soll die PLD-LTE eingesetzt werden (Architektur)
3. Welche Anforderungen gibt es für den Einsatz der PLD-LTE (Normen und Anforderungen)

Benötigt wurden dazu Informationen zum geplanten Einsatz der PLD-LTE zur Einschätzung der Anzahl und Typen der PLD-LTE im geplanten Projekt, die schematische Darstellung der Signalpfade für die vom Einsatz der PLD-LTE betroffenen LT-Funktionen zum Bestimmen der Position innerhalb der leittechnischen Signalpfade und Sicherheitsspezifikationen, Anforderungen aus dem Regelwerk und Sicherheitsanalysen, zur Zusammenstellung der Anforderungen an die LT-Einrichtung.

Diese bisherige Vorgehensweise des Prozessschritts PLAN ist in Abb. 3.7 dargestellt.

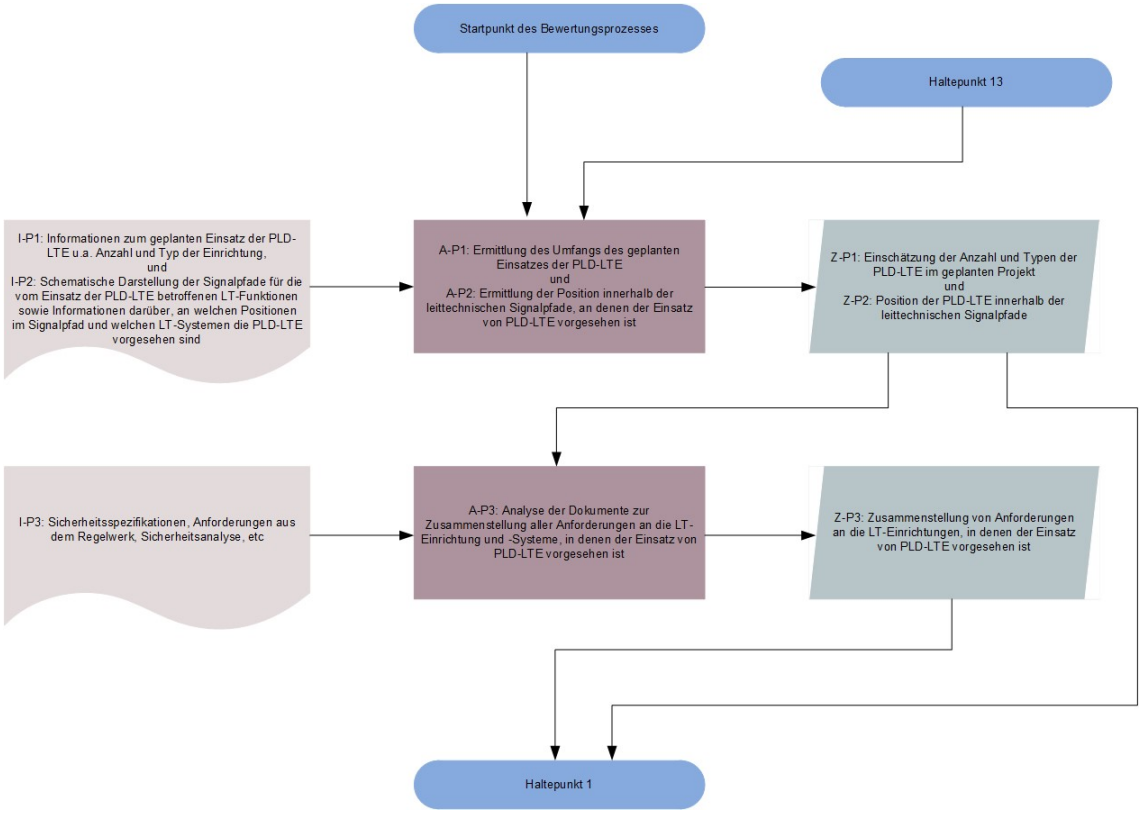


Abb. 3.7 Analyse-Ablaufplan P-1 - Vorgehensweise im Prozessschritt PLAN /GRS 17/

Im Rahmen dieses Projekts wurde der Prozessschritt PLAN dahingehend erweitert, dass er nun zum einen auf beliebige LTE anwendbar ist und er zum anderen nun eine deutlich detailliertere Vorgehensweise umfasst. Diese ist jetzt durch eine verstärkte Benutzerführung darauf ausgerichtet, auf Basis der jeweiligen Fragestellung der Bewertung die Analyseschritte in den folgenden Prozessschritten zielgerichtet vorzubereiten.

Die Vorbereitung der Analyse erfolgt jetzt in sieben Teilschritten.

1. Projektschlüsselfragen (A-c002-e000)
2. Technische Informationen (A-c003-e000)
3. Leittechnische Architektur (A-c004-e000)
4. Leittechnische Funktionen (A-c005-e000)
5. Funktionsspezifische Informationen (A-c006-e000)
6. Normen und Anforderungen (A-c007-e000)
7. Themensuche (A-c008-e000)

Im direkten Vergleich mit dem ursprünglichen Prozessschritt PLAN wurde die CAMIC-Methode um weitere technische und um funktionsspezifische Informationen ergänzt. Darüber hinaus wurde PLAN um eine Themensuche auf projektbezogene Dokumente erweitert. Die Abb. 3.8 und Abb. 3.9 stellen den erweiterten Prozessschritt PLAN inklusive der Erläuterungen dar.

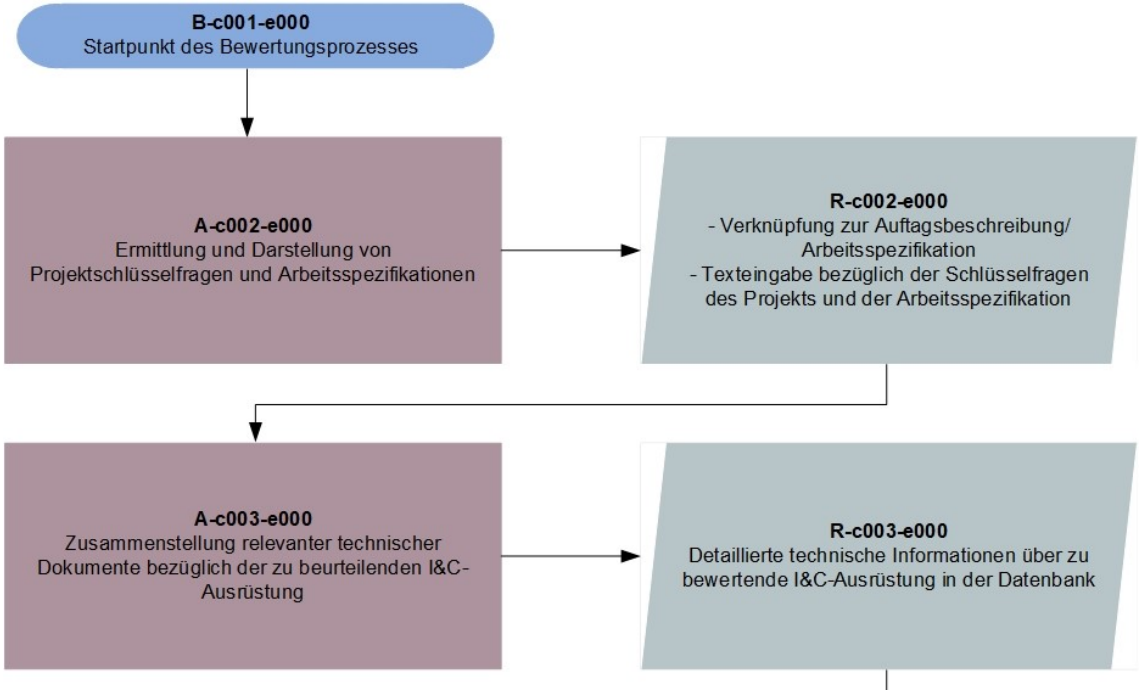


Abb. 3.8 Neue Vorgehensweise des Bewertungssatzes im Prozessschritt PLAN, Bild 1

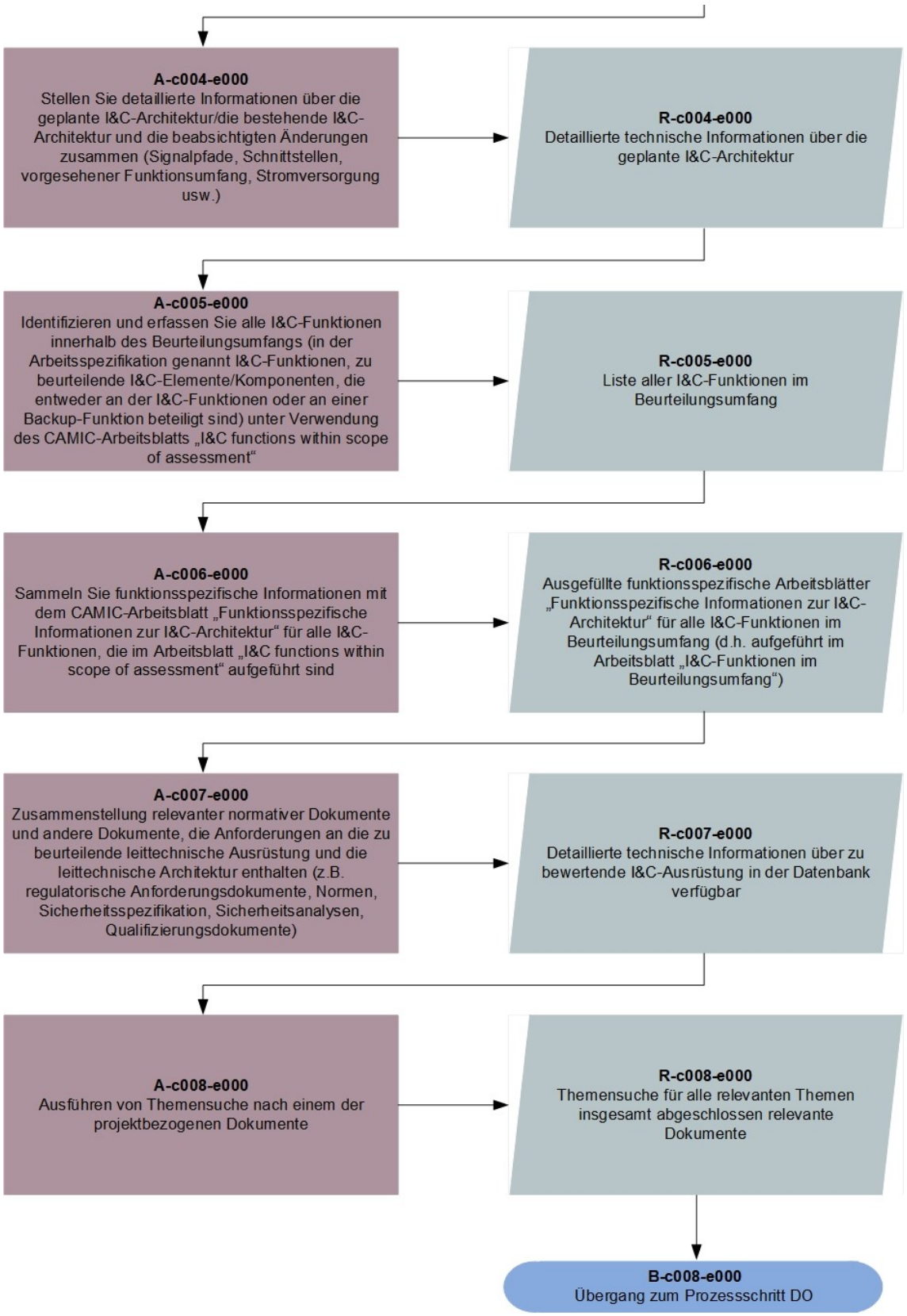


Abb. 3.9 Neue Vorgehensweise im Prozessschritt PLAN, Bild 2

Projektschlüsselfragen - (A-c002-e000)

Für jede Bewertung mit CAMIC ist es wichtig, sich mit den Auftraggebern klar über die Schlüsselfragen des Projekts und die Formulierung der Arbeitsspezifikation zu einigen, da sich der CAMIC-Workflow (d. h. Art und Reihenfolge der Analyseschritte) teilweise an die Schlüsselfragen der Bewertung aufgrund der Datenlage und der getroffenen Entscheidungen anpasst.

Zu den erwarteten Zwischenergebnissen, die sich aus den aufwendigen Analyseschritten ergeben, gehören Beschreibungen der Projekt-Schlüsselfragen und der Arbeitsspezifikation sowie Links zu den entsprechenden Dokumenten.

Technische Informationen - (A-c003-e000)

Aus der Arbeitsspezifikation geht klar hervor, ob die Bewertung der leittechnischen Einrichtung direkt oder indirekt Teil der hier angestrebten Bewertung mit CAMIC ist.

Daher ist die Zusammenstellung von technischen Informationen wie Systembeschreibungen, technischen Handbüchern, Datenblättern, Qualifizierungsunterlagen usw. unerlässlich. Dieser Analyseschritt wird bei der rechnergestützten CAMIC-Anwendung erleichtert durch den Import solcher Dokumente in die CAMIC-Datenbank als Grundlage für die spätere Bewertung im Prozessschritt DO oder - falls ein Dokument selbst eingeschränkt verfügbar oder vertraulich ist oder dem Geheimschutz unterliegt - die Eingabe der entsprechenden Dokumentdaten.

Zu den erwarteten Zwischenergebnissen, wie sie durch aufwendige Analyseschritte erzielt werden, gehört die Zusammenstellung ausreichender technischer Informationen über die zu bewertende leittechnische Einrichtung bzw. die Rolle, die sie bei der Bewertung in der CAMIC-Datenbank spielen soll.

Leittechnische Architektur - (A-c004-e000)

Nach der Zusammenstellung der technischen Dokumentation der zu bewertenden Leittechniksysteme und -komponenten ist es unerlässlich, detaillierte Informationen sowohl über die bestehende leittechnische Architektur als auch über die geplante leittechnische Architektur zusammenzustellen. Zu diesen Detailinformationen gehören Informationen über Signalwege, Schnittstellen, vorgesehenen Funktionsumfang, Stromversorgung usw. Bei Neubau-Anlagen ist mindestens die Zusammenstellung von Informationen über

die geplante leittechnische Architektur erforderlich, je nach Fragestellung können hier aber auch weitergehende Informationen notwendig sein.

Auch dieser Analyseschritt wird bei der rechnergestützten CAMIC-Anwendung durch den Import von Dokumenten erleichtert, die diese Informationen bereitstellen, in die CAMIC-Datenbank als Grundlage für die spätere Bewertung im Prozessschritt DO oder - falls ein Dokument selbst eingeschränkt oder vertraulich ist - die Eingabe der entsprechenden Dokumentdaten. Erwartete Zwischenergebnisse, wie sie durch aufwendige Analyseschritte erzielt werden, umfassen eine Zusammenstellung von ausreichenden Informationen über die bestehende und beabsichtigte leittechnische Architektur, die in der CAMIC-Datenbank bewertet werden oder bei der Bewertung eine Rolle spielen sollen.

Leittechnische Funktionen - (A-c005-e000)

Die Bewertung von Leittechniksystemen oder leittechnischen Einrichtungen mit der CAMIC-Methodik umfasst bei den meisten zugrundeliegenden Fragestellungen auch die Abschätzung der Folgen des geplanten Austauschs für alle beteiligten Leittechnikfunktionen. Daher ist es notwendig, alle leittechnischen Funktionen im Rahmen der Bewertung zu identifizieren und einzubeziehen. Ausführliche Analyseschritte berücksichtigen drei verschiedene Quellen für relevante Informationen über potenziell betroffene leittechnische Funktionen:

1. Leittechnische Funktionen, die in der Arbeitsspezifikation explizit genannt werden,
2. Leittechnische Funktionen, die in der Arbeitsspezifikation indirekt über zu bewertende leittechnische Einrichtungen/Komponenten spezifiziert werden (d. h. jede leittechnische Funktion, die eine solche leittechnische Einrichtung/Komponente beinhaltet, sowie jede leittechnische Funktion, die als Backup-Funktion für eine der identifizierten leittechnische Funktionen dient),
3. Leittechnische Funktionen, die direkt vom Benutzer spezifiziert werden.

Ein im Rahmen der Erweiterung der CAMIC-Methode erstelltes CAMIC-Arbeitsblatt "I&C functions within scope of assessment" hilft bei der Zusammenstellung dieser Informationen. Dieses Arbeitsblatt wird direkt aus der CAMIC-Anwendung heraus aufgerufen. Informationen aus allen drei Quellen werden auf die gleiche Weise zusammengestellt, um vergleichbare Zwischenergebnisse zu gewährleisten. Erwartete Zwischenergebnisse, wie sie sich aus aufwendigen Analyseschritten ergeben, umfassen eine

Zusammenstellung ausreichender Informationen über die für die Bewertung relevanten leittechnischen Funktionen.

Funktionsspezifische Informationen - (A-c006-e000)

Im Anschluss an die Spezifizierung aller für die Bewertung relevanten leittechnischen Funktionen zusammen mit eindeutigen Informationen über jede der Funktionen müssen spezifische Informationen über die einzelnen leittechnischen Funktionen gesammelt werden. Diese Informationen enthalten Einzelheiten über die Rolle der zu bewertenden leittechnischen Einrichtungen/Komponenten im Signalweg und damit für die Ausführung der leittechnischen Funktion.

Für jede der im Arbeitsblatt "I&C functions within scope of assessment" aufgeführten leittechnischen Funktionen wird eine Kopie eines weiteren, speziell erstellten CAMIC-Arbeitsblatts mit der Bezeichnung "Function-specific information on I&C architecture" zur Verfügung gestellt. Erwartete Zwischenergebnisse, wie sie durch aufwendige Analyseschritte erzielt werden, umfassen eine Zusammenstellung ausreichender Informationen über die Rolle, die jede für die Bewertung relevante leittechnische Einrichtung/Komponente für die Ausführung einer leittechnischen Funktion spielt. Die Informationen werden für jede Leittechnikfunktion separat erfasst, so dass kompakte, funktionsspezifische Informationen über die von der Modifikation/Nachrüstung/Installation betroffenen leittechnischen Einrichtungen/Komponenten innerhalb des Signalpfades zur Verfügung stehen.

Normen und Anforderungen - (A-c007-e000)

Die Detaillierung der technischen Situation und der Pläne sowie die strukturierte Zusammenstellung der Informationen innerhalb von CAMIC stellt eine Säule für die Beurteilung dar. Die andere Säule setzt sich aus allen relevanten Anforderungen zusammen. Daher ist die Zusammenstellung relevanter normativer Dokumente und anderer Dokumente, die Anforderungen an die zu bewertende leittechnische Einrichtung und leittechnische Architektur enthalten (z. B. regulatorische Anforderungsdokumente, Normen, Sicherheitsspezifikationen, Sicherheitsanalysen, Qualifizierungsdokumente sowie ggf. darüber hinaus gehende Anforderungen durch Auftraggeber oder Zielvorgaben), von entscheidender Bedeutung.

Dieser Analyseschritt erleichtert den Import solcher Dokumente in die CAMIC-Datenbank oder - falls ein Dokument selbst eingeschränkt oder vertraulich ist - die Eingabe der entsprechenden Dokumentdaten. Erwartete Zwischenergebnisse, wie sie sich

aus den aufwendigen Analyseschritten ergeben, umfassen eine Zusammenstellung von ausreichender Dokumentation zu den für die Bewertung relevanten Anforderungen in der CAMIC-Datenbank.

Themensuche - (A-c008-e000)

Dies ist ein optionaler Schritt des CAMIC-Workflows, der zur Zusammenstellung themenspezifischer Informationen führt, die für die Bewertung relevant sind. Solche themenspezifischen Informationen können Anforderungen, Zitate, Zahlen und Definitionen umfassen. Die Verwendung dieses optionalen Schritts hilft bei der strukturierten Informationsbeschaffung für ein oder mehrere ausgewählte Themen.

- **Vorgehensweise bei der Themensuche**: Die Bearbeitung einer Themensuche ist unabhängig von einem Projekt. Die Auswahl, welche Abschnitte eines Dokuments für eine *Topic reference* relevant sind, ergibt sich aus der Liste an Suchbegriffen und der inhaltlichen Beschreibung der *Topic reference*. Ob ein Abschnitt darüber hinaus für das aktuelle Projekt relevant ist, hat mit der Themensuche zunächst nichts zu tun und wird an anderer Stelle festgelegt.
- Die Bearbeitung einer Themensuche umfasst pro Dokument folgende Schritte:

    1. Feststellen, ob das Dokument bereits in der Datenbank erfasst ist. Dies ist über die Benutzeroberfläche *Selection of document data* oder die Benutzeroberfläche *Document information* möglich.

    2. Falls das Dokument noch nicht angelegt ist, weiter bei Schritt 4.

    3. Feststellen, ob die Themensuche für die gewählte *Topic reference* bereits abgeschlossen ist. Dies ist über die Benutzeroberfläche *Selection of sections* oder die Benutzeroberfläche *Topic input* möglich. Falls ja, ist die Bearbeitung beendet. Falls nein, weiter bei Schritt 5

    4. Anlegen des Dokuments über die Benutzeroberfläche *Input of document data*.

    5. Für jede *Topic reference* gibt es eine abzuarbeitende Liste an Suchbegriffen (*Einzelfehlerkriterium*, *Redundanz*, *CCF*, *Diversität*, *Programmierbare und rechnerbasierte Geräte*, *Instandhaltung*). Durchsuchen des Dokuments nach allen Suchbegriffen der Liste.

    6. Reduktion der Suchergebnisse auf korrekte, inhaltlich relevante Treffer, d. h. Treffer, die die Suchbegriffe im gewünschten Zusammenhang enthalten. Der

gewünschte Zusammenhang ist für jede *Topic reference* detailliert beschrieben. Wichtig: Fällt bei der Arbeit mit dem Dokument auf, dass inhaltlich für die gewählte *Topic reference* relevante Abschnitte über die angegebenen Suchschritte nicht gefunden werden, muss die Liste der Suchbegriffe erweitert werden. Da dies aber Auswirkungen auf alle früher eingepflegten Dokumente haben kann, ist hierzu eine Absprache mit einem Entwickler der CAMIC-Anwendung erforderlich.

7. Einpflegen aller Abschnitte, die relevante Suchergebnisse enthalten, in die Datenbank. Dies geschieht über die Benutzeroberfläche *Section input*. Vor der Zuordnung der *Topic reference*, müssen alle Abschnitte, die im Rahmen der Themensuche gefunden wurden, in der Datenbank erfasst werden. Die Zuordnung der *Topic reference* erfolgt erst danach für alle relevanten Abschnitte gemeinsam.

    a. Zunächst Erfassen der nicht bereits früher erfassten Abschnitte im Bereich *Section input*. Hierbei können für jeden Abschnitt auch Zitate erfasst werden. Ist bereits ein Zitat für den Abschnitt in der Datenbank hinterlegt, kann dieses nicht verändert werden, sondern es muss ein weiteres Zitat hinterlegt werden (ggf. auch mit textlichen Überschneidungen zu bereits hinterlegten Zitaten). Zusätzlich können auch Bilddateien in der Datenbank hinterlegt werden. Das Einpflegen von Zitaten und Bildern ist optional.

    b. Sobald alle unter Schritt 1 gefundenen Abschnitte mit zutreffendem Zitat in der Datenbank erfasst sind, kann im Bereich *Topic input* die *Topic reference* über das Setzen von Häkchen diesen Abschnitten zu geordnet werden.

    c. Nach Abschluss der Zuordnung der *Topic reference* zu allen gefundenen Abschnitten, setzen des Häkchens *Topic input completed*. Wichtig: Die Bearbeitung für die Themensuche darf bei einem Dokument nur als *abgeschlossen* angezeigt werden, nachdem alle Bearbeitungsschritte wie angegeben durchgeführt wurden.

Erwartete Zwischenergebnisse, die sich aus den aufwendigen Analyseschritten ergeben, umfassen eine Zusammenstellung themenspezifischer Informationen für alle ausgewählten Dokumente und Themen.

3.1.3 CAMIC-Prozessschritt: DO

Der Prozessschritt DO ist der umfangreichste Prozessschritt, welcher in CAMIC realisiert wurde, da er alle Analyseschritte enthält, die sich auf die technischen Aspekte der geplanten Änderungen an der leittechnischen Architektur beziehen. Um viele Zustände des Systems adäquat zu erfassen, wurde der Prozessschritt DO in unterschiedliche Teilschritte unterteilt. Je nach LTE und Anforderung, kann dieser Prozessschritt unterschiedlich durchlaufen werden. In dem ersten Teilschritt, DO-Einstieg, wird die geeignete Vorgehensweise für die vorliegende LTE, anhand verschiedener Entscheidungskriterien ermittelt. Die Zusammenstellung der einzelne Analyseschritte ist in den verschiedenen möglichen Vorgehensweisen des CAMIC-Prozessschritts DO unterschiedlich. Allerdings werden einige Analyseschritte in mehreren Vorgehensweisen verwendet, was letztlich Verknüpfungen zwischen den einzelnen Vorgehensweisen herstellt. So ist beispielsweise in Vorgehensweise C der auch in Vorgehensweise A eingebundene FMEA-Analyseschritt vorgesehen. Der Ablauf der Analyseschritte sieht daher einen Wechsel von Vorgehensweise C in Vorgehensweise A zur Durchführung der FMEA vor. Nach dem Ausführen des Analyseschritts in Vorgehensweise A wird wieder in die Ausgangsvorgehensweise, hier Vorgehensweise C, zurückgekehrt. Im Folgenden werden die Teilschritte des Prozessschritts DO übersichtlich zusammengefasst und anschließend als Flowchart dargestellt.

3.1.3.1 DO–Einstieg

Vor der eigentlichen technischen Bewertung der LTE werden bei dem Teilschritt DO-Einstieg gezielt Informationen über die LTE abgefragt. Im vorausgehenden Prozessschrittes PLAN wurde bereits sichergestellt, dass die benötigten Informationen in CAMIC zur Verfügung stehen. Durch die Beantwortung einer Reihe von Entscheidungskriterien durch den Anwender werden diese Informationen nun zur Vorbereitung der eigentlichen Bewertung eingesetzt. Basierend auf den getroffenen Entscheidungen wird dem Anwender eine passende Vorgehensweise vorgeschlagen (Abb. 3.10 und Abb. 3.11).

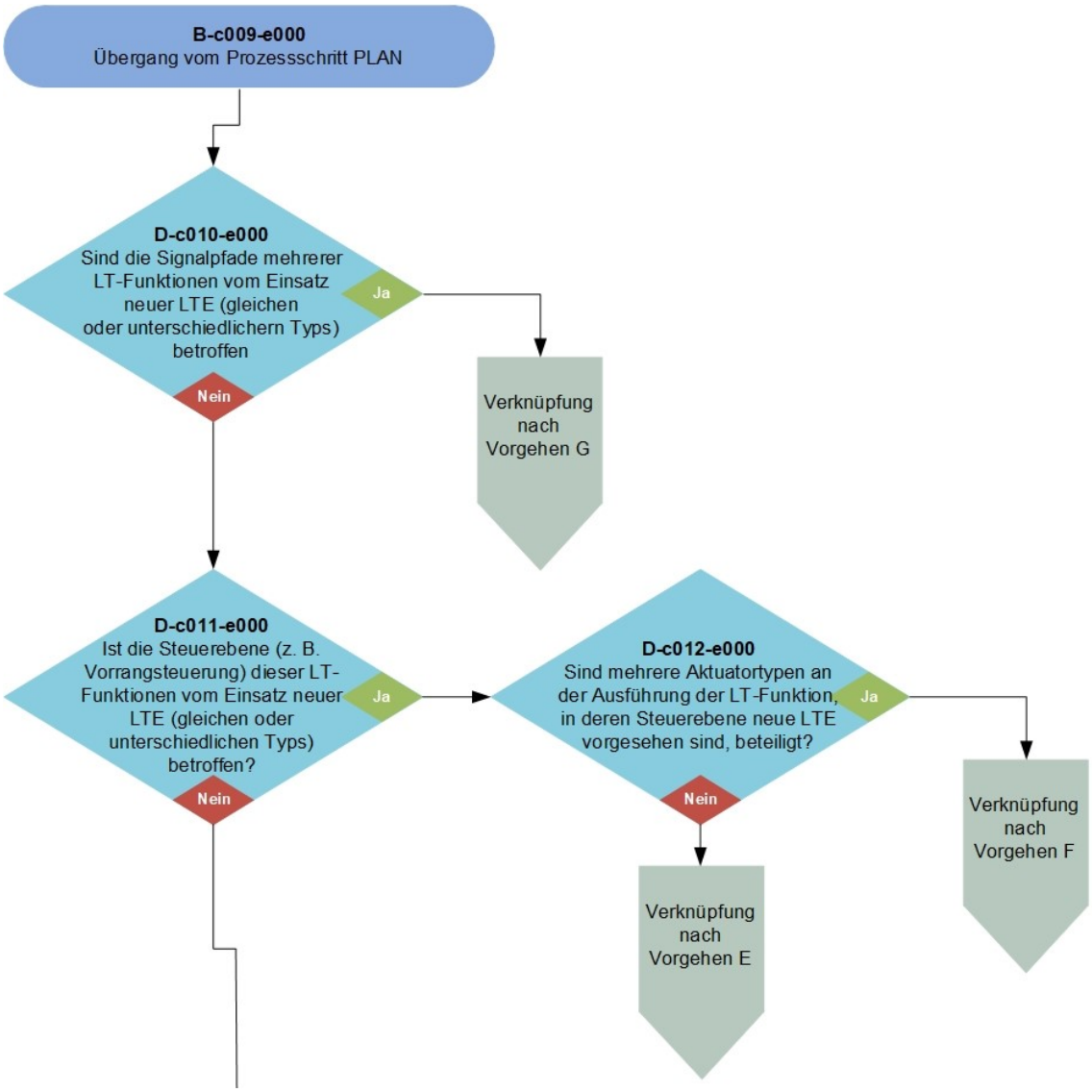


Abb. 3.10 Prozessschritt DO–Einstieg, Bild 1

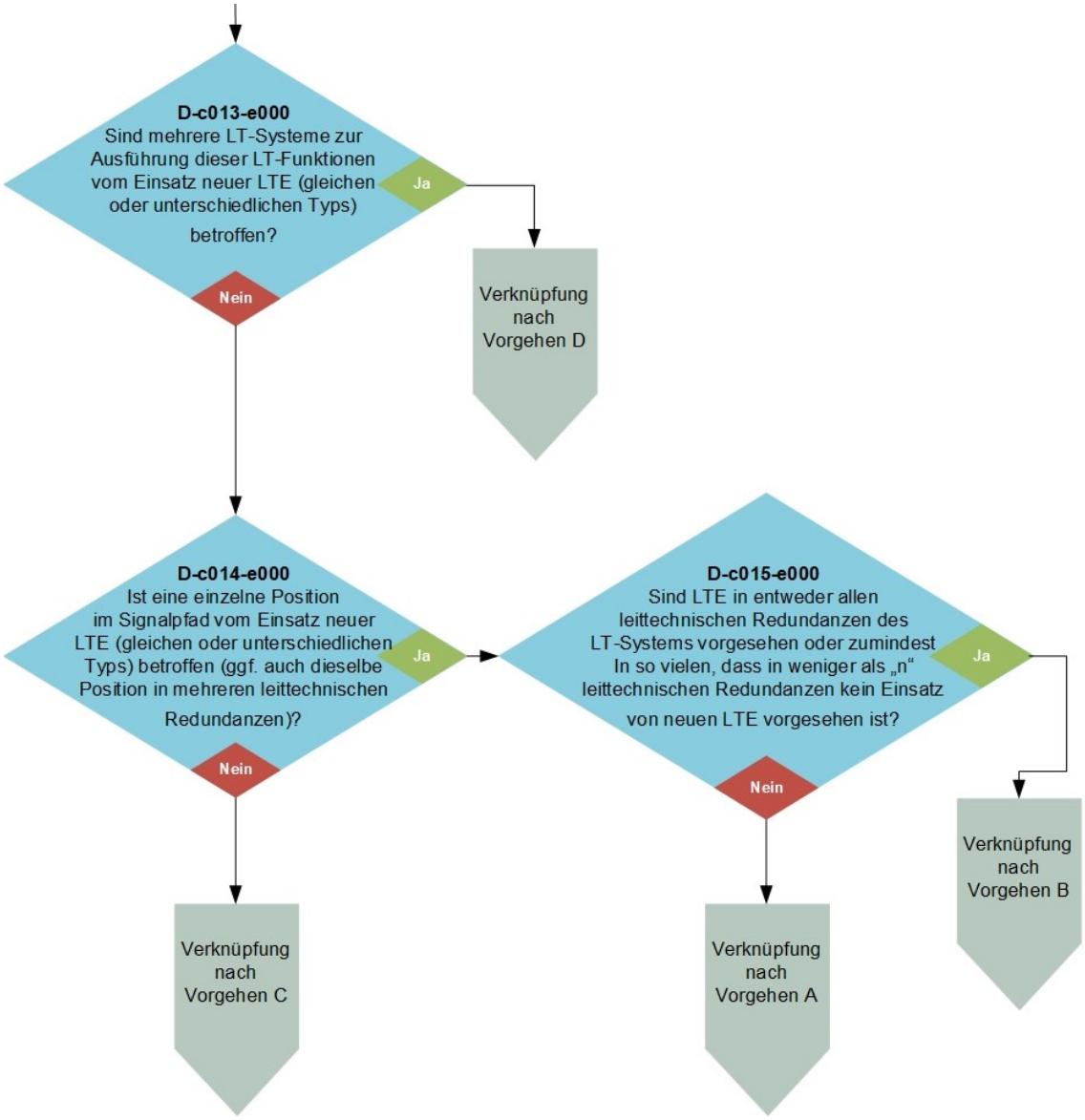


Abb. 3.11 Prozessschritt DO–Einstieg, Bild 2

3.1.3.2 DO – Vorgehensweise A

Diese Vorgehensweise umfasst eine FMEA der LTE (Abb. 3.12). Gegeben sein müssen folgende Randbedingungen:

- Die vorgesehene LTE betrifft eine LT-Funktion, weitere LT-Funktionen sind zunächst nicht betroffen.
- Die LTE ist in einem, aber nicht in mehreren LT-Systemen vorgesehen.
- Die LTE sind in einer oder mehreren Redundanzen des LT-Systems vorgesehen, wobei nur eine Position im Signalpfad betroffen ist, d. h. bei mehreren betroffenen Redundanzen soll der Einsatz von LTE in jeder Redundanz an der gleichen Position

des Signalpfades erfolgen. Voraussetzung hierbei ist, dass mindestens n Redundanzen nicht vom hier geplanten Einsatz von LTE betroffen sind, wobei n die für die Bildung eines korrekten Signals notwendige Zahl an leittechnischen Redundanzen ist.

- Die Steuerebene ist durch den Einsatz der LTE nicht betroffen

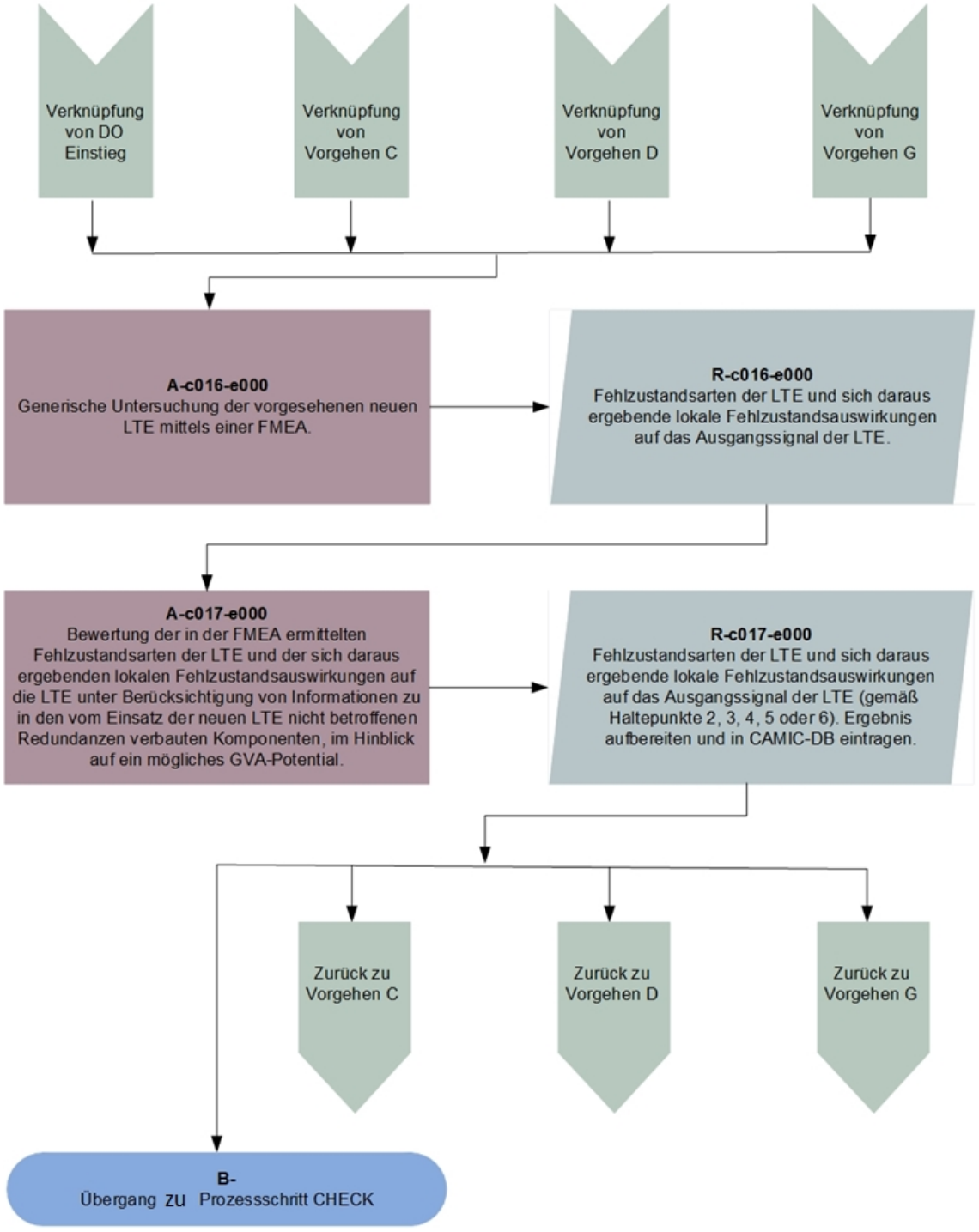


Abb. 3.12 Prozessschritt DO – Vorgehensweise A

3.1.3.3 DO – Vorgehensweise B

Durchführen einer FMEA der LTE und des LT-Systems sowie Untersuchung der Diversität der Komponenten (Abb. 3.13 bis Abb. 3.16). Vorgehensweise B wird für Fälle mit den folgenden Randbedingungen angewendet:

- Der vorgesehene Einsatz von LTE betrifft nur eine LT-Funktion, weitere LT-Funktionen sind zunächst nicht betroffen.
- Der Einsatz von LTE ist nur einem LT-System vorgesehen.
- LTE sind in allen Redundanzen des LT-Systems vorgesehen, wobei nur eine Position im Signalpfad betroffen ist, d. h. bei mehreren betroffenen Redundanzen soll der Einsatz von LTE in jeder Redundanz an der gleichen Position des Signalpfades erfolgen.
- Es ist in allen Redundanzen des LT-Systems derselbe Typ LTE vorgesehen, oder es sind unterschiedliche Typen vorgesehen.
- Sofern sich die Vorgehensweise B nicht direkt, sondern im Rahmen von Vorgehensweise C ergibt, können auch Kombinationen und „Additionen“ von Positionen im Signalpfad betrachtet werden. Diese werden dann innerhalb der Vorgehensweise B so behandelt, als wenn es sich um eine einzige Position handeln würde.
- Die Steuerebene ist nicht betroffen.

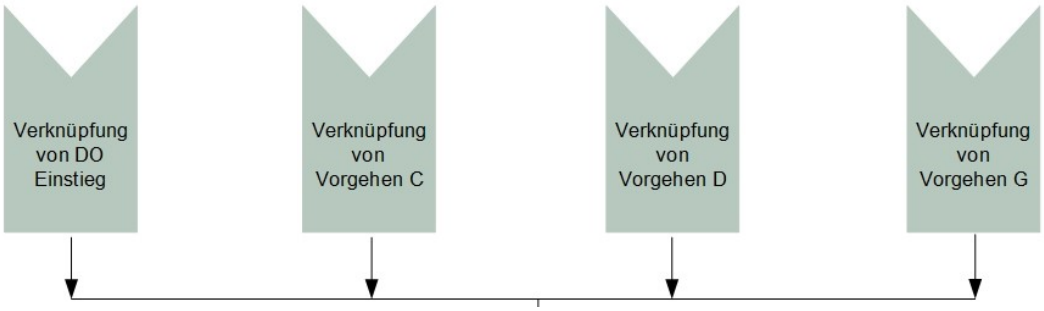


Abb. 3.13 Prozessschritt DO – Vorgehensweise B, Bild 1

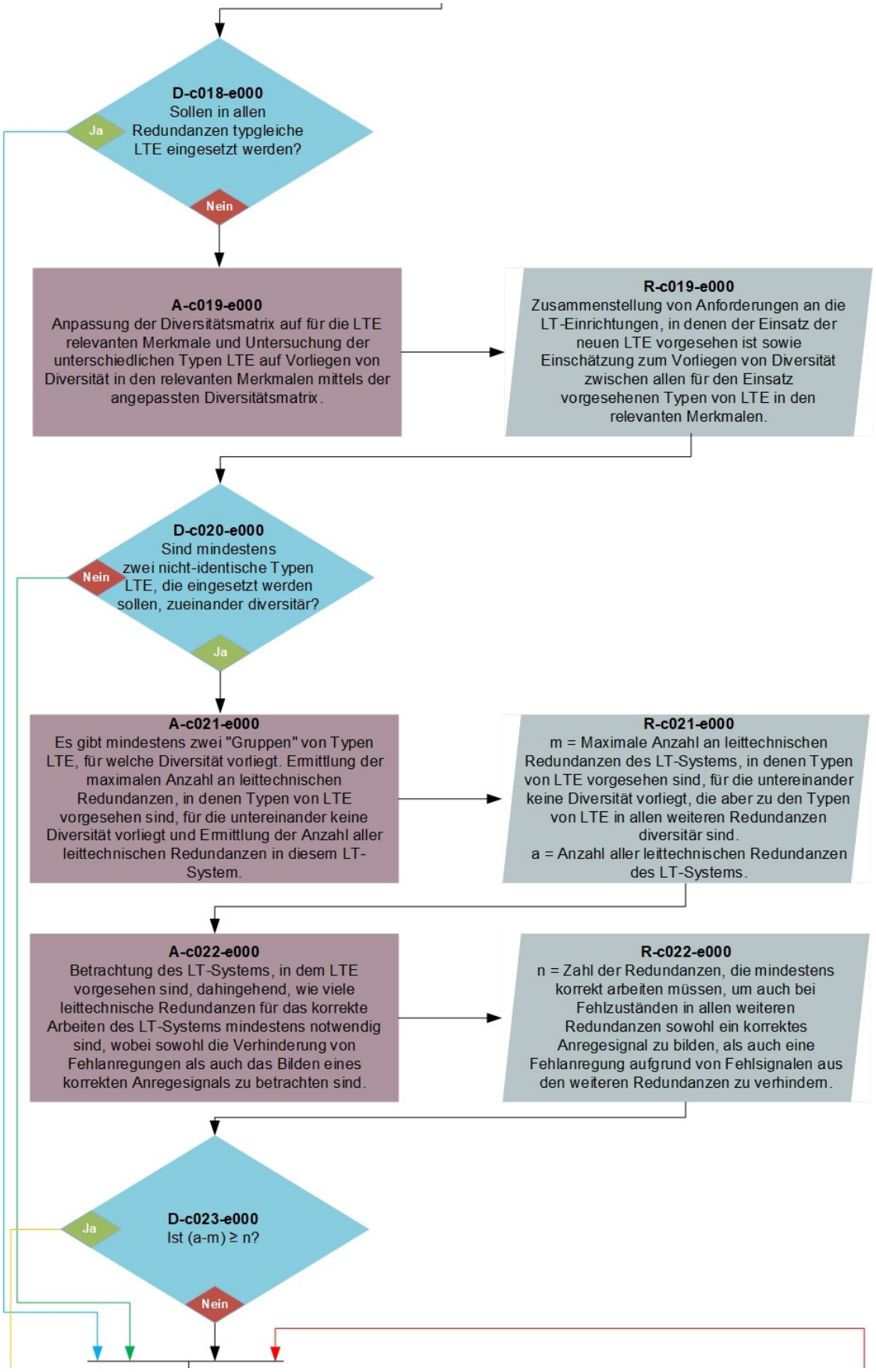


Abb. 3.14 Prozessschritt DO – Vorgehensweise B, Bild 2

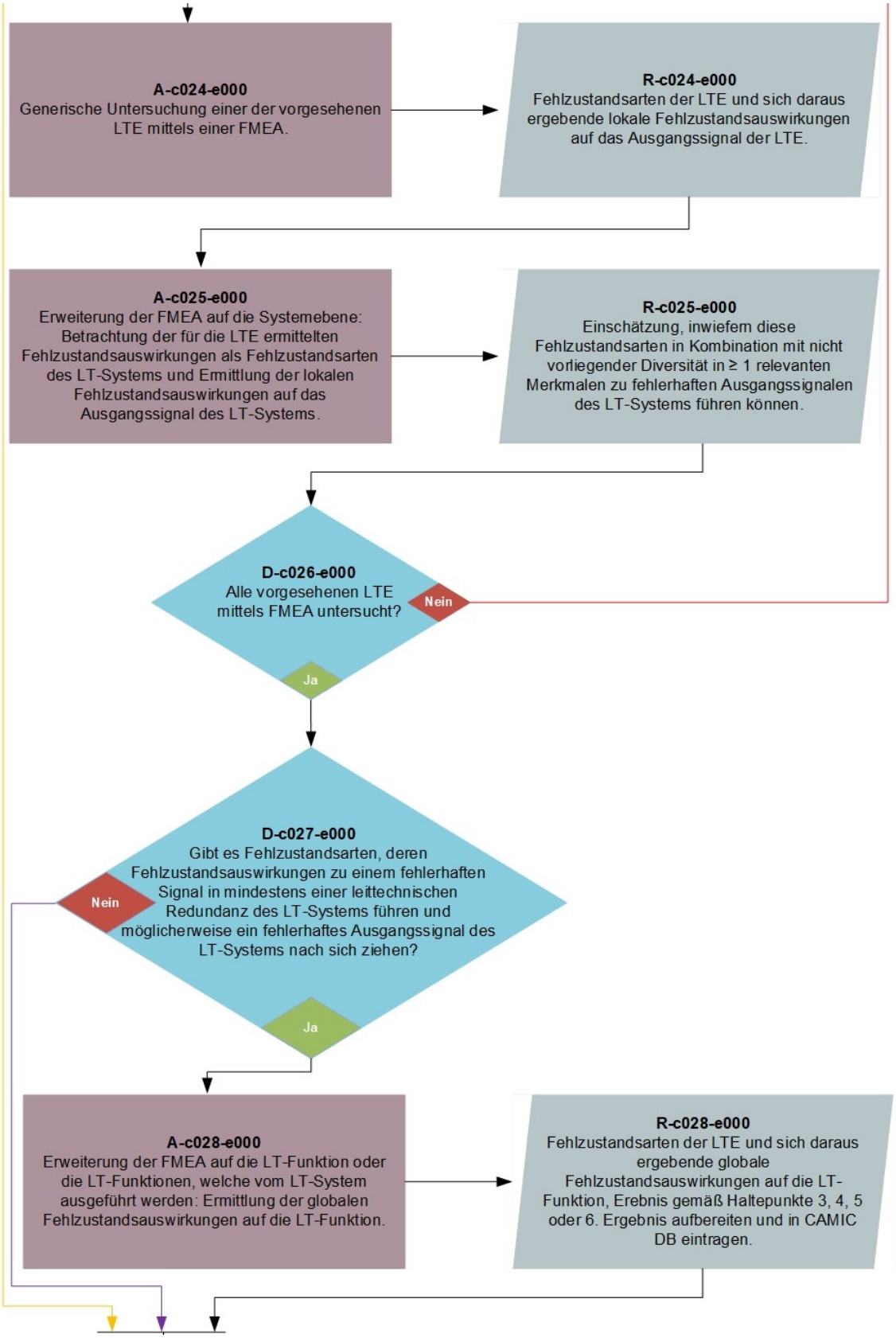


Abb. 3.15 Prozessschritt DO – Vorgehensweise B, Bild 3

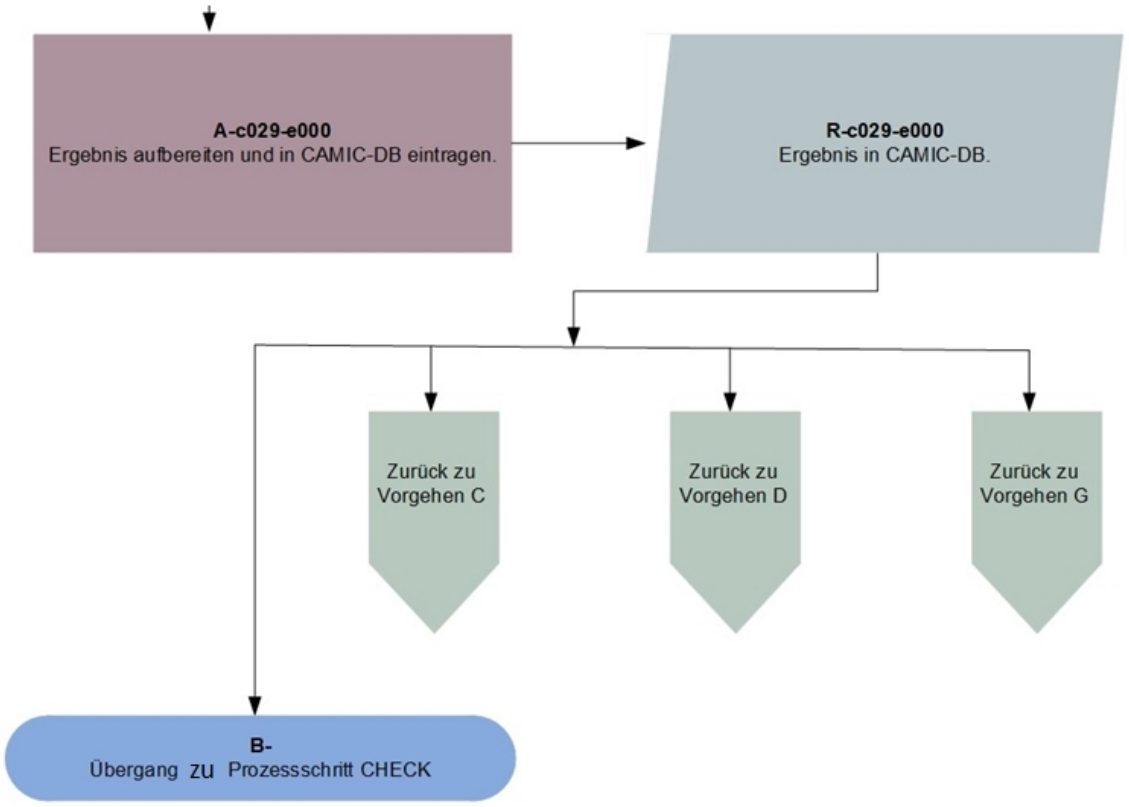


Abb. 3.16 Prozessschritt DO – Vorgehensweise B, Bild 4

3.1.3.4 DO – Vorgehensweise C

Im Rahmen dieser Vorgehensweise zur Bewertung der möglichen Fehlzustandsauswirkungen, die sich aufgrund von Fehlzuständen der LTE bei einem Einsatz entsprechend der im Prozessschritt PLAN zugrunde gelegten Planungen ergeben können, werden zunächst zu vermeidende Ausfallarten des LT-Systems ermittelt. Diese werden als Hauptereignisse in jeweils einer eigenen Fehlzustandsbaumanalyse untersucht. Die Ergebnisse der Analyse der Minimal-Schnitte der ermittelten Fehlzustandsbäume werden in einer Übersichtstabelle dokumentiert. Ebenfalls in der Übersichtstabelle erfasst sind Kombinationen aus Positionen oder „Additionen“ von Positionen, welche ebenfalls zum Eintritt eines Hauptereignisses führen können, was im Wesentlichen den Eintritt eines Fehlzustands des LT-Systems bedeutet. Aufbauend auf die Fehlzustandsbaumanalyse sieht Vorgehensweise C die Durchführung einer FMEA vor. Vorgehensweise C ist in Abb. 3.17 bis Abb. 3.21 dargestellt. Folgende Randbedingungen müssen für die Anwendung von Vorgehensweise C erfüllt sein:

- Der vorgesehene Einsatz von LTE betrifft eine LT-Funktion, weitere LT-Funktionen sind zunächst nicht betroffen.

- Der Einsatz von LTE ist in genau einem LT-Systemen vorgesehen.
- LTE sind mehreren Stellen des Signalpfades innerhalb von Anregeebene oder Logikebene des LT-Systems vorgesehen, wobei es zunächst keine Rolle spielt, ob hierbei jeweils alle Redundanzen des LT-Systems betroffen sind.
- Es ist entweder an allen Stellen des Signalpfades derselbe Typ LTE vorgesehen, oder es sind unterschiedliche Typen vorgesehen.
- Die Steuerebene ist nicht betroffen.

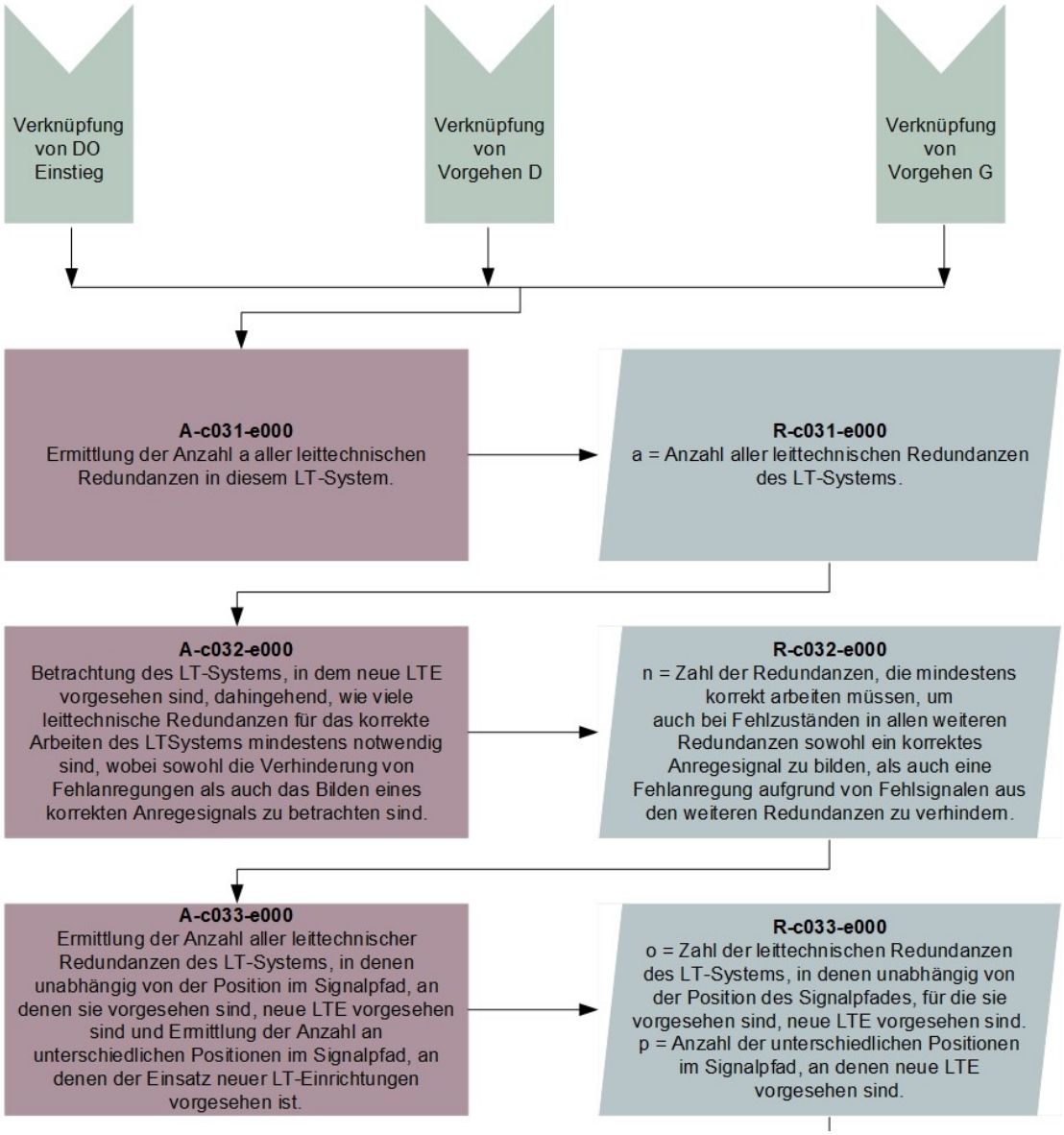


Abb. 3.17 Prozessschritt DO – Vorgehensweise C, Bild 1

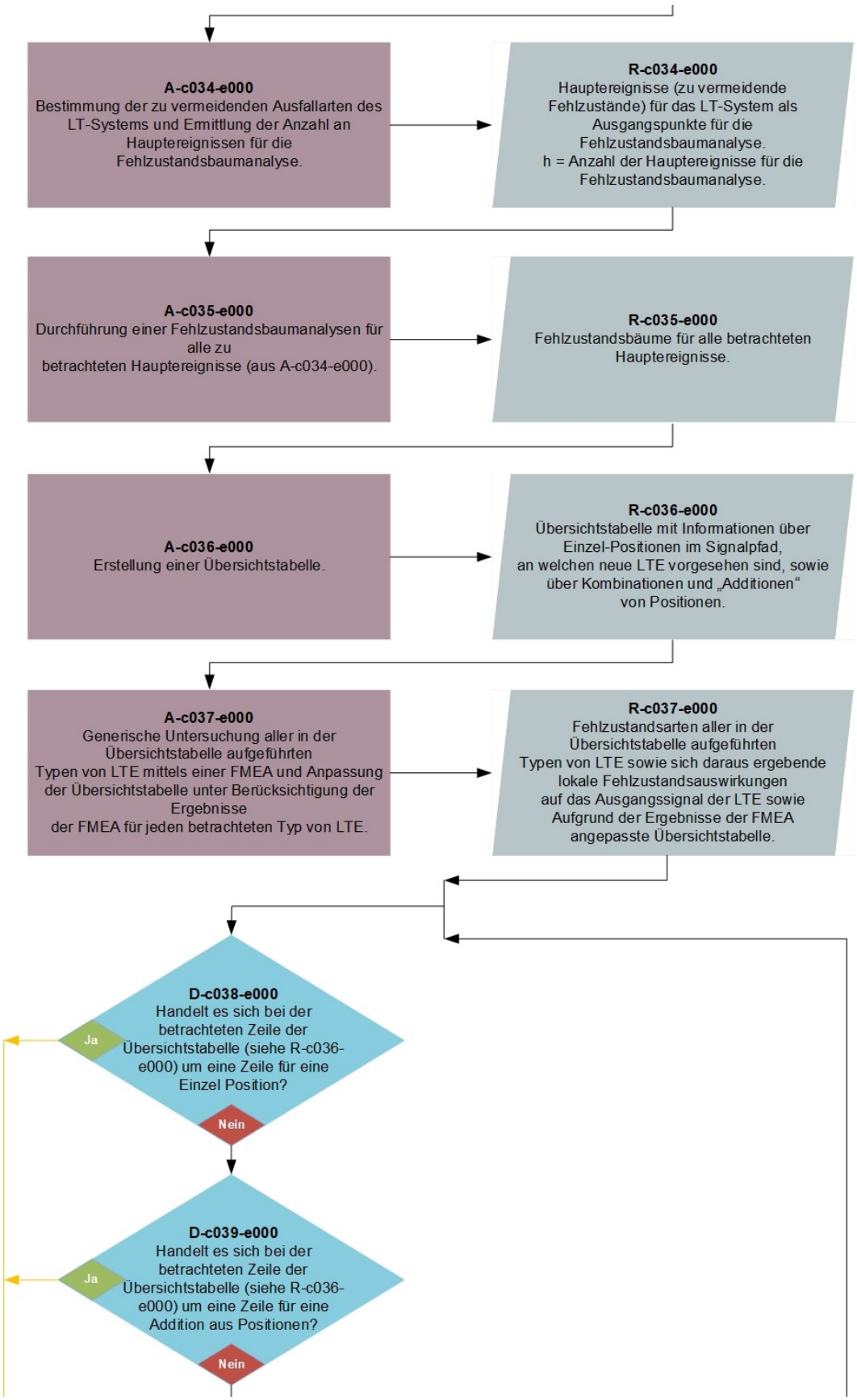


Abb. 3.18 Prozessschritt DO – Vorgehensweise C, Bild 2

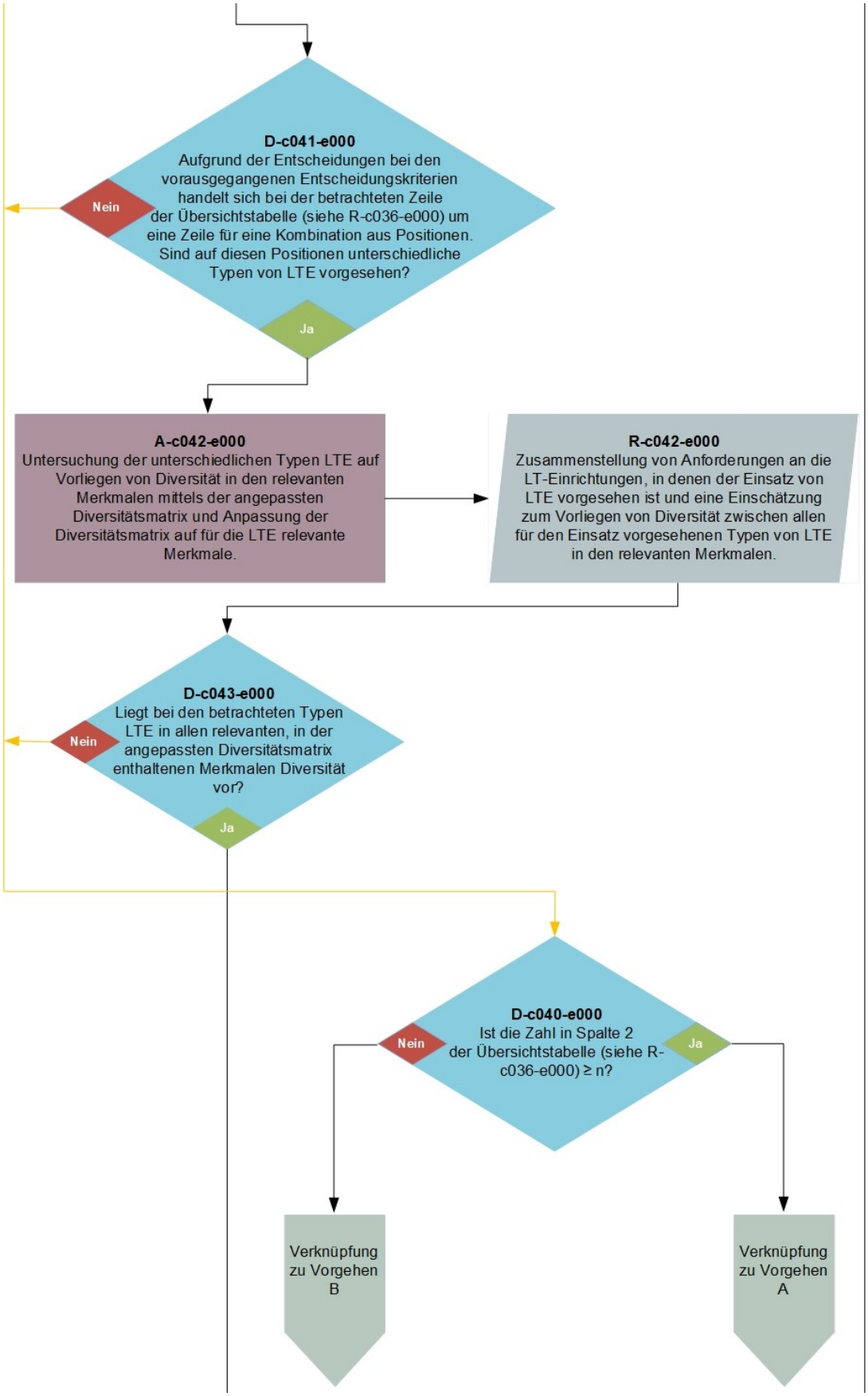


Abb. 3.19 Prozessschritt DO – Vorgehensweise C, Bild 3

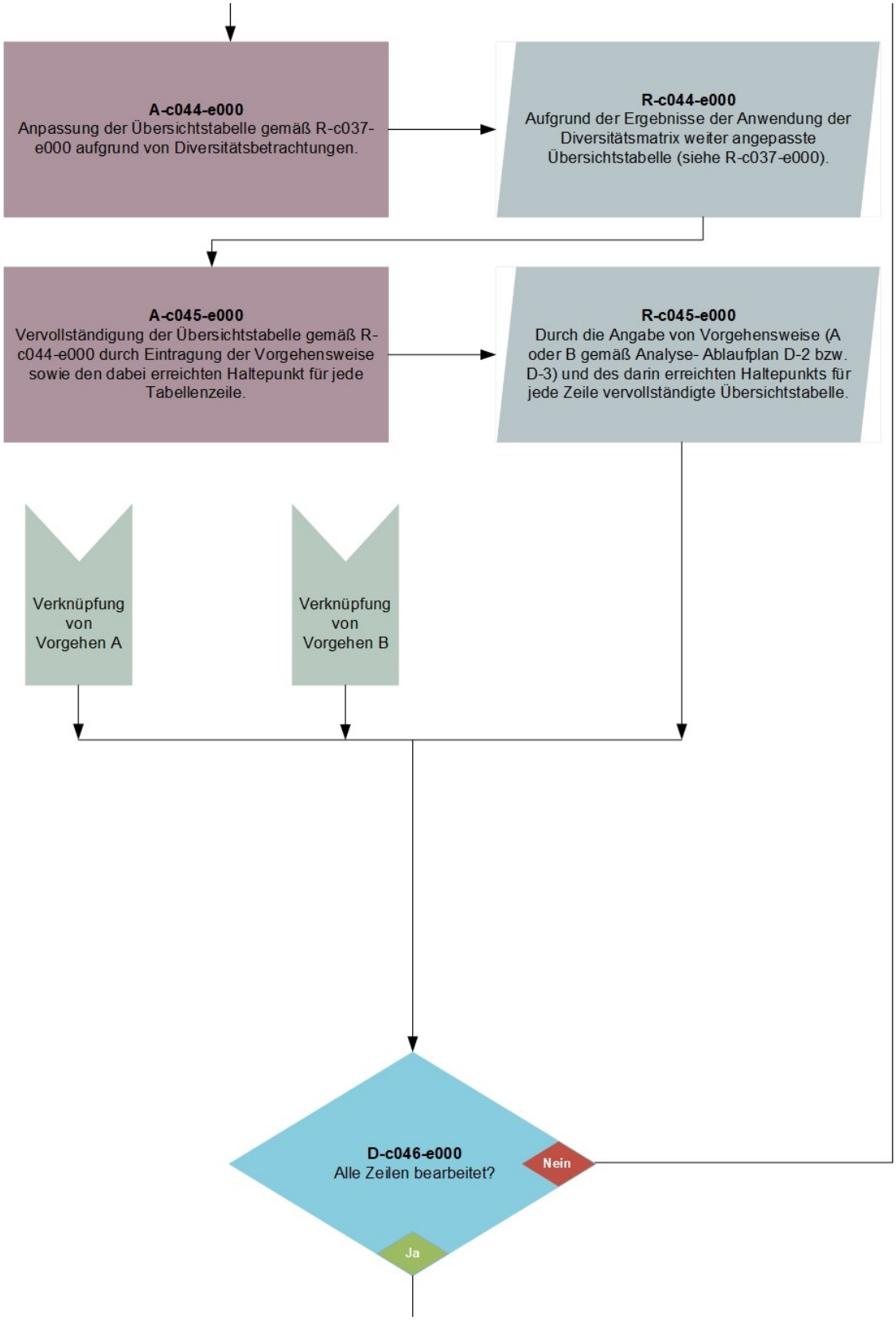


Abb. 3.20 Prozessschritt DO – Vorgehensweise C, Bild 4

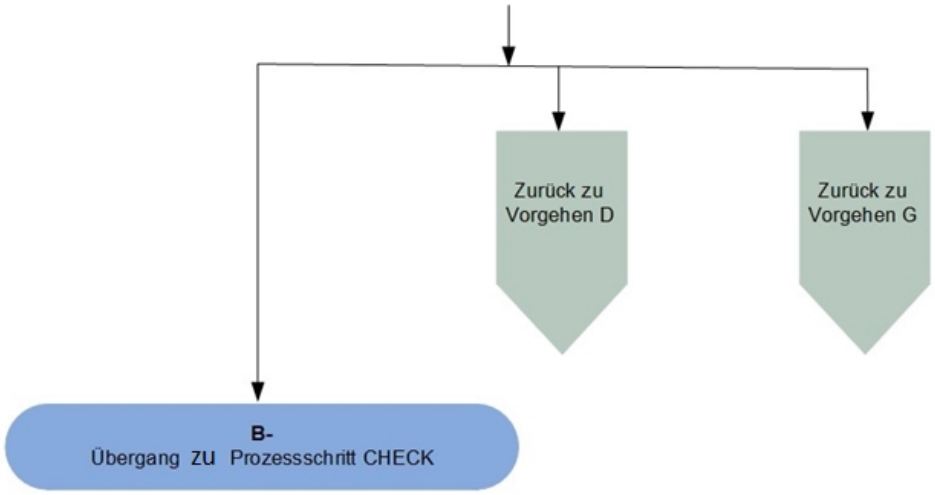


Abb. 3.21 Prozessschritt DO – Vorgehensweise C, Bild 5

3.1.3.5 DO – Vorgehensweise D

Vorgehensweise D befasst sich mit Fällen, in denen in mehreren LT-Systemen zur Ausführung derselben LT-Funktion der Einsatz einer oder mehrerer zu untersuchender LTE vorgesehen sind oder mehrere leittechnische Systeme in der Bewertung berücksichtigt werden müssen. Jedes dieser LT-Systeme muss in der Analyse einzeln untersucht werden, wobei zu beachten ist, dass es möglich ist, einzelne Analyseschritte wie beispielsweise die Anpassung der Diversitätsmatrix und die Untersuchung der LT-Systeme oder auch der darin eingesetzten LTE, welche formal in den Vorgehensweisen für mehrere oder alle beteiligten LT-Systeme enthalten sein können, bei identischen Randbedingungen nur bei der Analyse des ersten LT-Systems durchzuführen und die Ergebnisse dann bei der Analyse der weiteren LT-Systeme zu übernehmen (Abb. 3.22 bis Abb. 3.24). Folgende Randbedingungen müssen für die Anwendung von Vorgehensweise D erfüllt sein:

- Der vorgesehene Einsatz von LTE betrifft eine LT-Funktion, weitere LT-Funktionen sind zunächst nicht betroffen.
- Der Einsatz von LTE ist in mehreren LT-Systemen zur Ausführung dieser LT-Funktion vorgesehen.
- LTE sind in diesen LT-Systemen entweder an einer Stelle des Signalpfades oder an mehreren Stellen des Signalpfades vorgesehen, wobei es zunächst keine Rolle spielt, ob hierbei jeweils alle Redundanzen des LT-Systems betroffen sind.
- Es ist entweder an allen Stellen des Signalpfades derselbe oder es sind unterschiedliche Typen LTE vorgesehen. Hierbei wird, wie schon bei den Vorgehensweisen B

und C davon ausgegangen, dass das LT-System über maximal vier Redundanzen verfügt, woraus sich ergibt, dass in diesem LT-System pro Position im leittechnischen Signalpfad mindestens ein bis maximal vier unterschiedliche Typen LTE vorgesehen sein können.

- Die Steuerebene ist nicht betroffen.

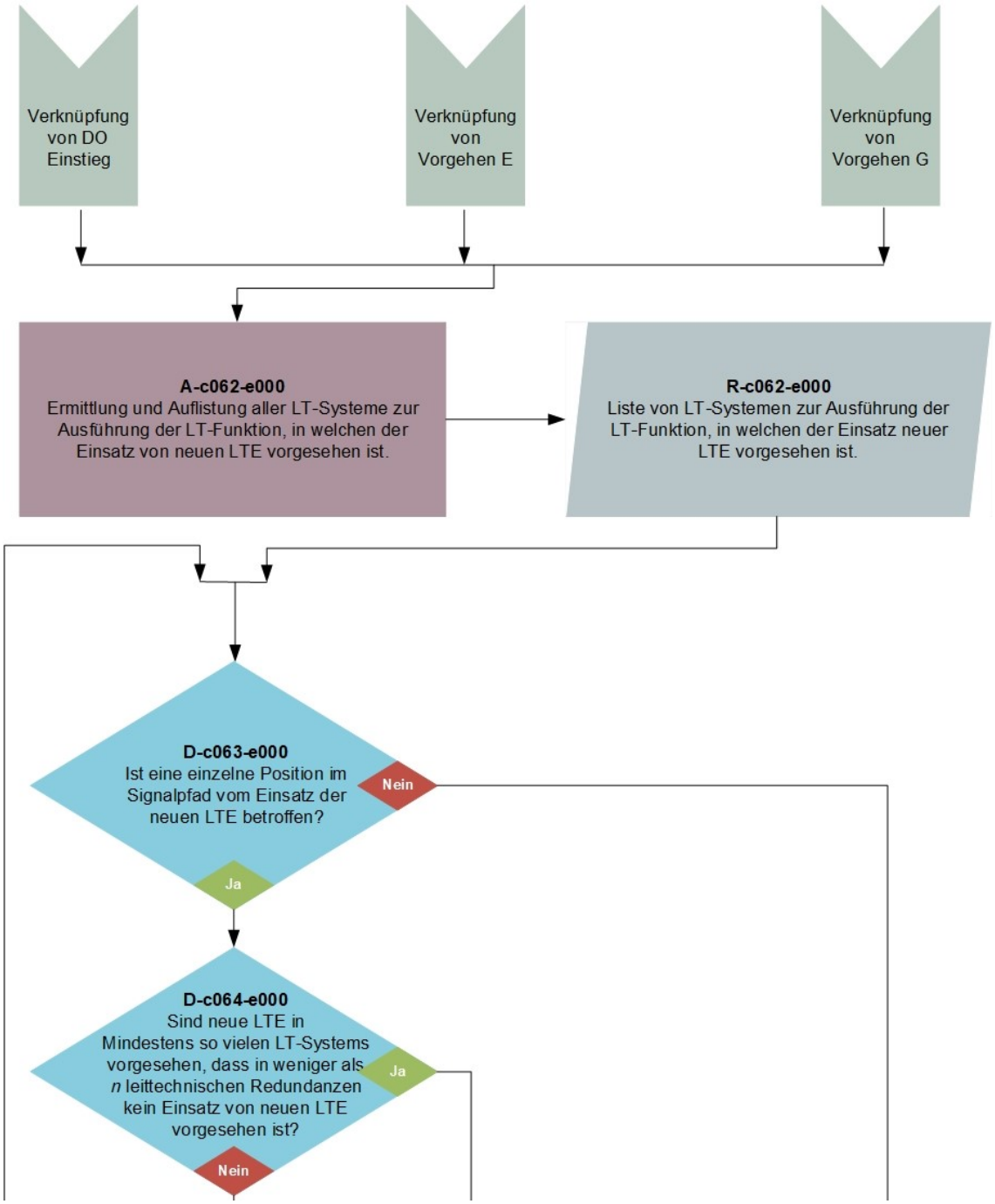


Abb. 3.22 Prozessschritt DO – Vorgehensweise D, Bild 1

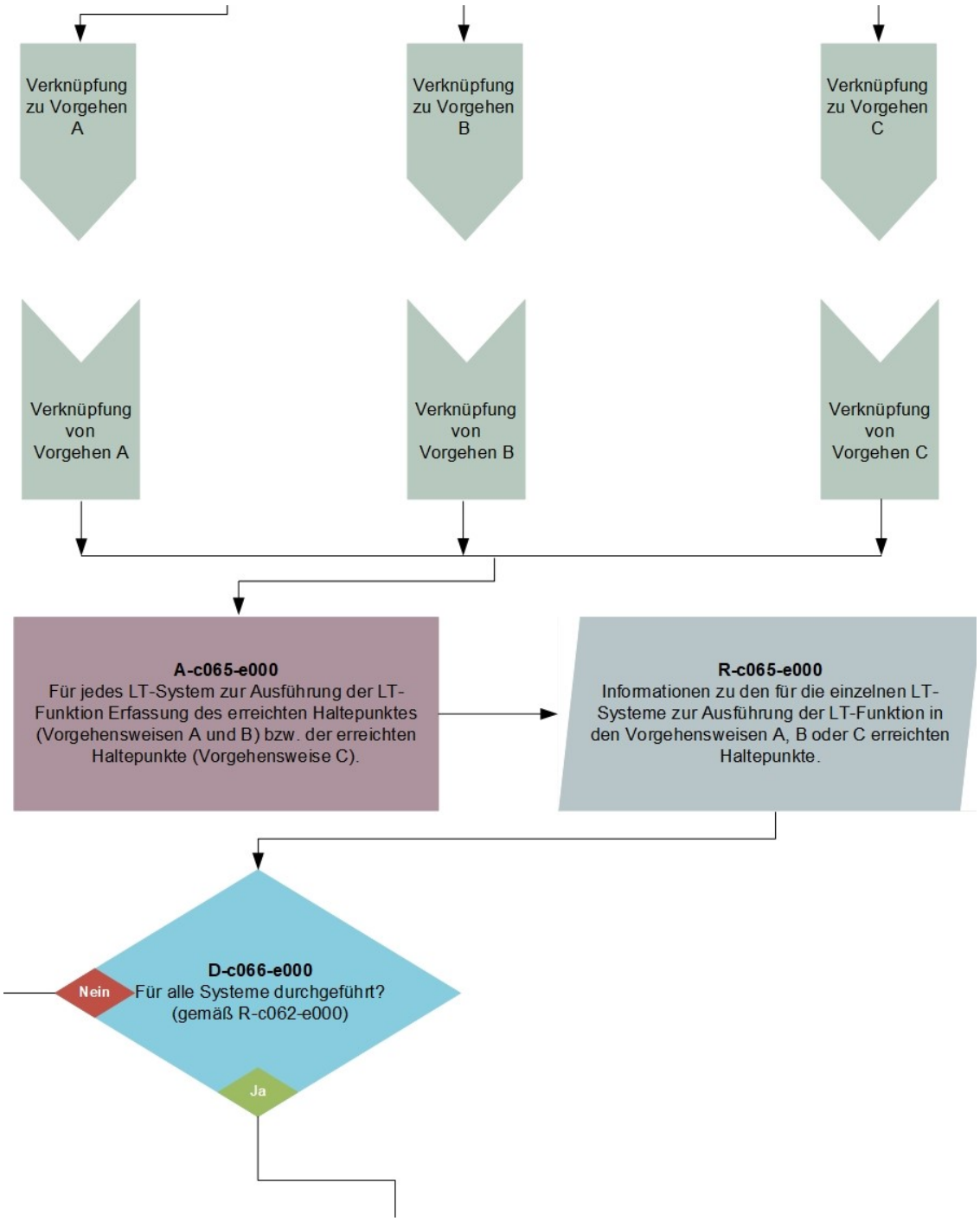


Abb. 3.23 Prozessschritt DO – Vorgehensweise D, Bild 2

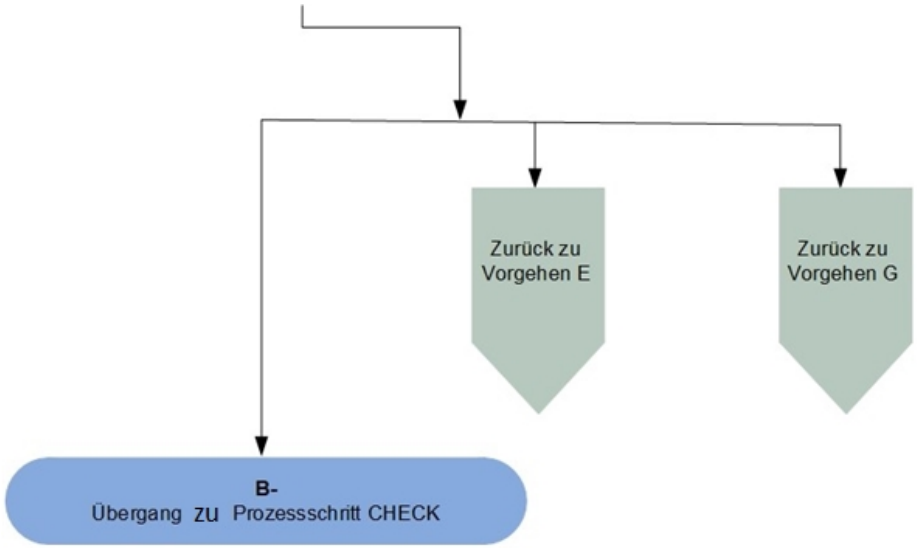


Abb. 3.24 Prozessschritt DO – Vorgehensweise D, Bild 3

3.1.3.6 DO – Vorgehensweise E

Diese Vorgehensweise befasst sich mit der Bewertung von LTE in der Steuerebene einer einzelnen LT-Funktion. Hierbei wird unterschieden, ob auf der Steuerebene ein Typ oder mehrere Typen LTE vorgesehen sind (Abb. 3.25 bis Abb. 3.30). Folgende Randbedingungen müssen für die Anwendung von Vorgehensweise E erfüllt sein:

- Der vorgesehene Einsatz von LTE betrifft eine LT-Funktion, weitere LT-Funktionen sind zunächst nicht betroffen,
- Es sind LTE in der Steuerebene vorgesehen,
- Der Einsatz von LTE auf der Steuerebene betrifft einen Aktuatortyp,
- Der Einsatz von LTE in einem oder mehreren LT-Systemen zur Ausführung dieser LT-Funktion ist möglicherweise ebenfalls vorgesehen.

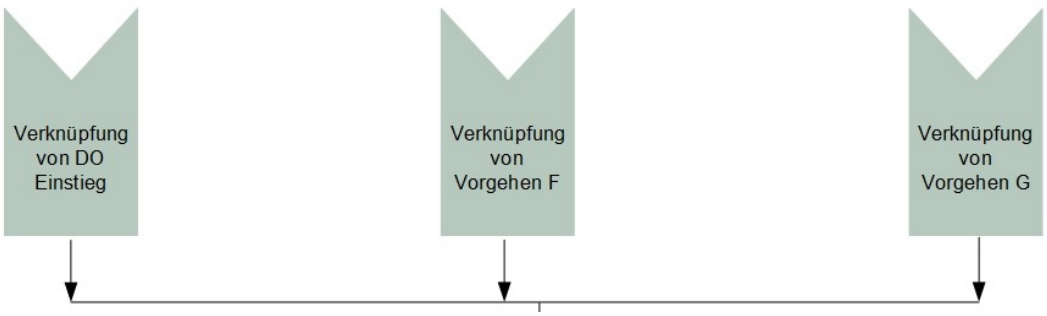


Abb. 3.25 Prozessschritt DO – Vorgehensweise E, Bild 1

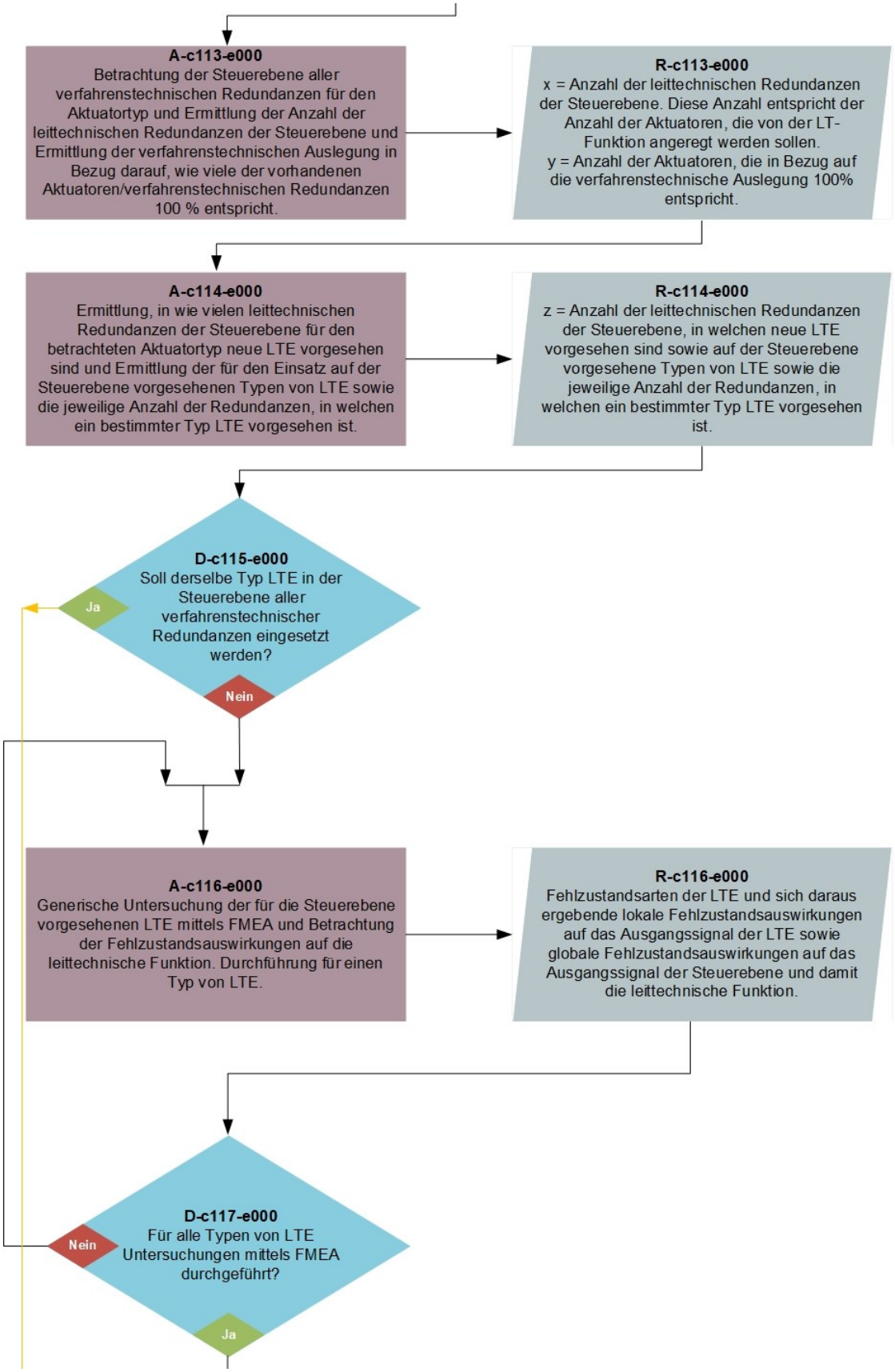


Abb. 3.26 Prozessschritt DO – Vorgehensweise E, Bild 2

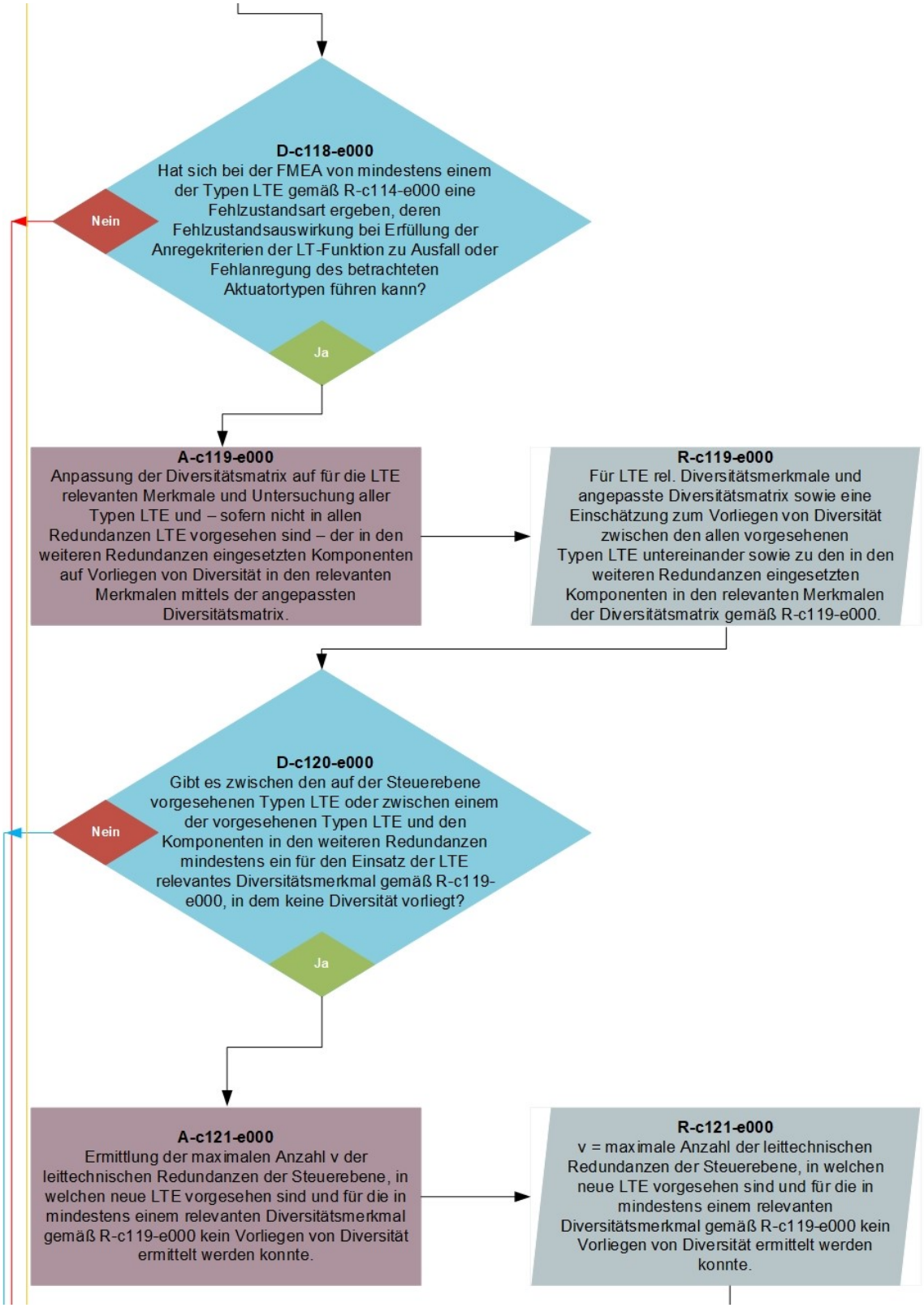


Abb. 3.27 Prozessschritt DO – Vorgehensweise E, Bild 3

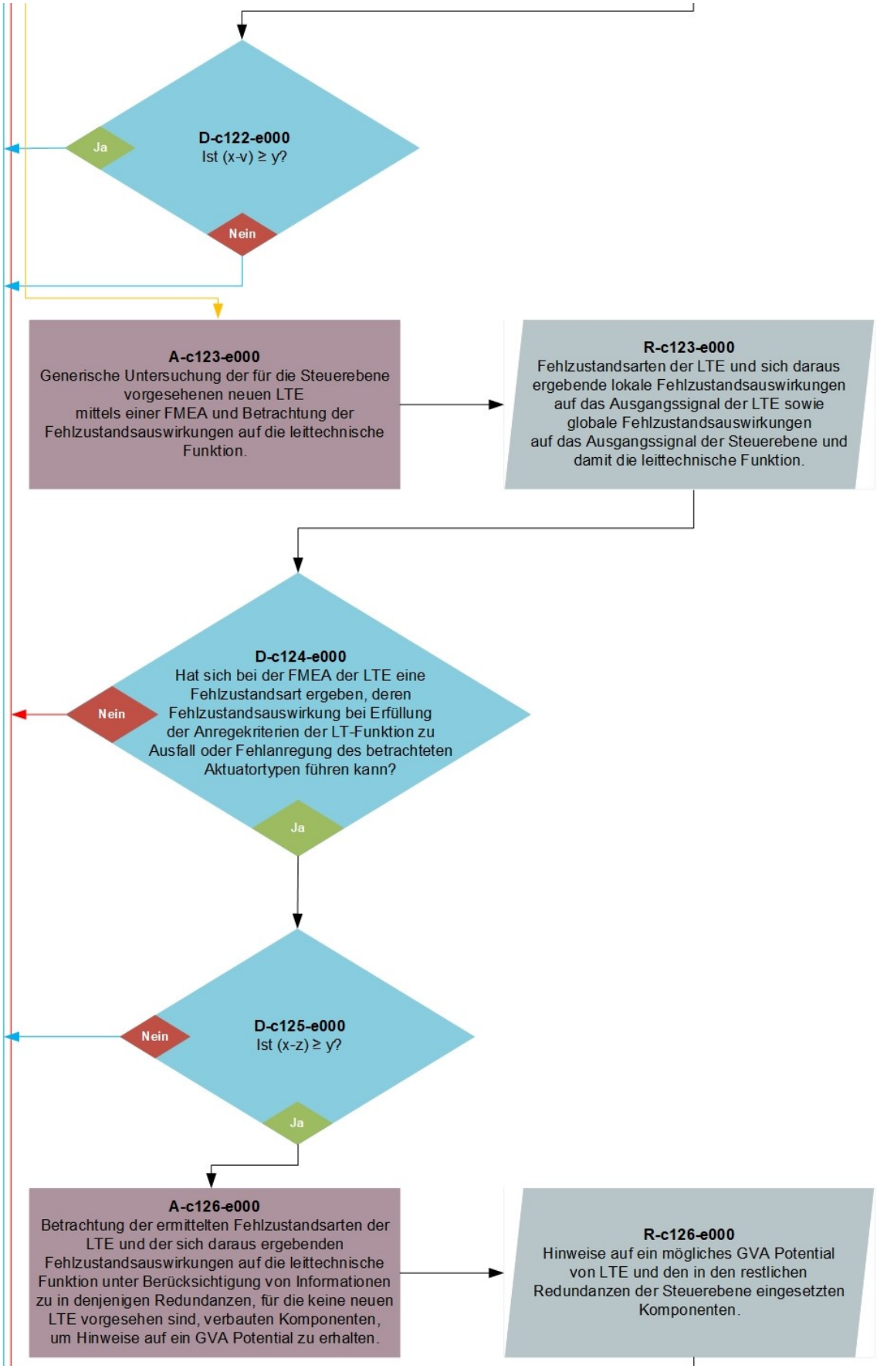


Abb. 3.28 Prozessschritt DO – Vorgehensweise E, Bild 4

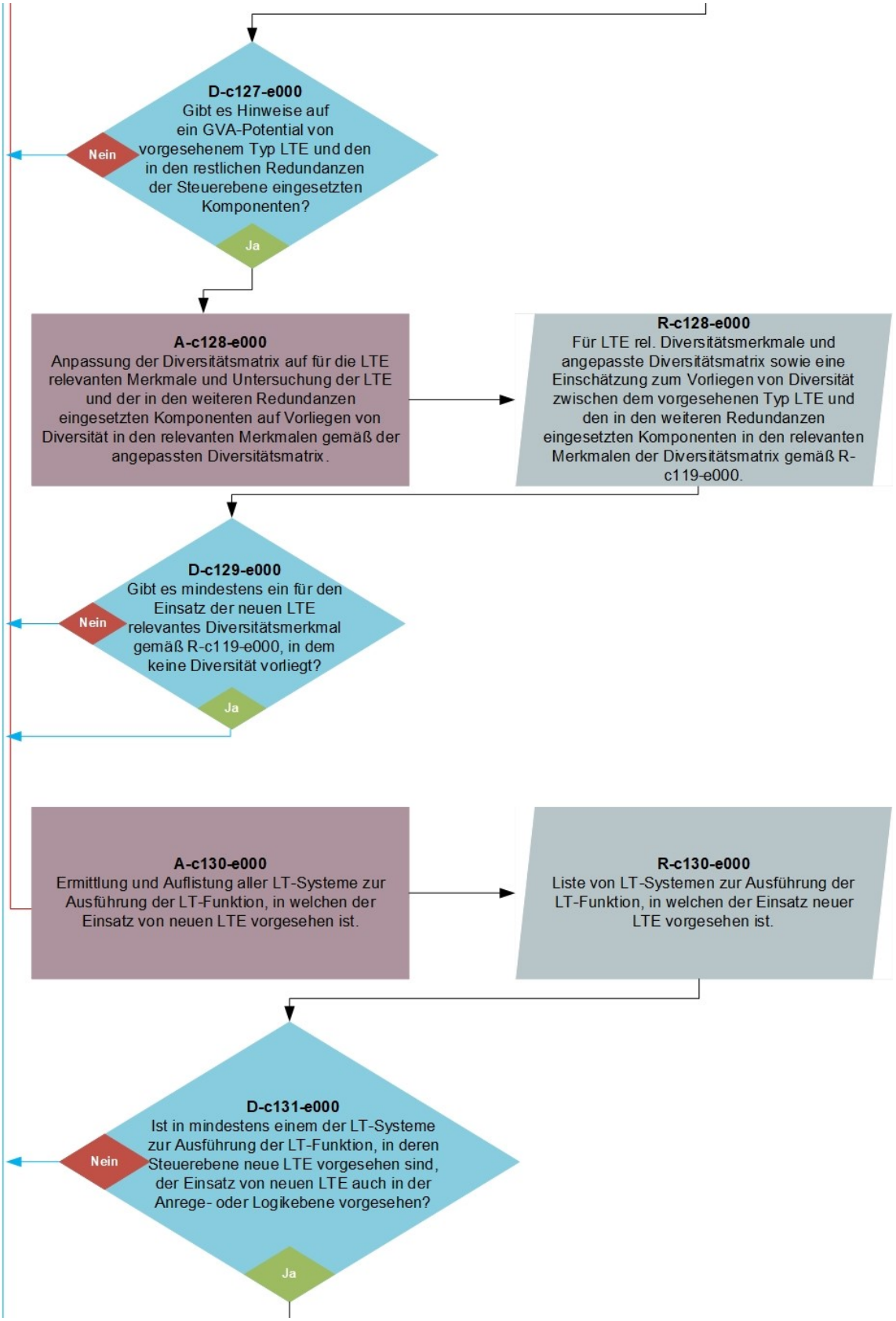


Abb. 3.29 Prozessschritt DO – Vorgehensweise E, Bild 5

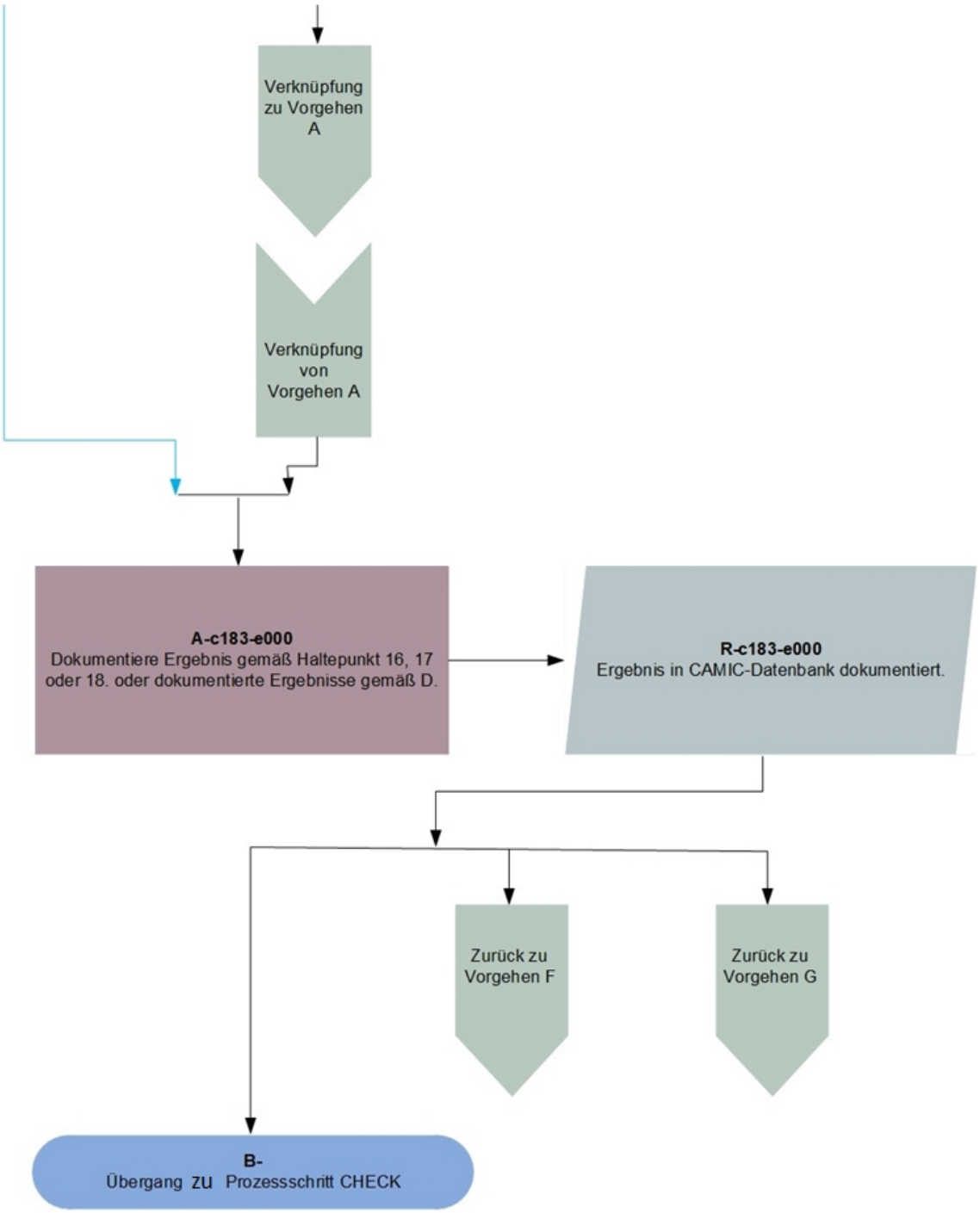


Abb. 3.30 Prozessschritt DO – Vorgehensweise E, Bild 6

3.1.3.7 DO – Vorgehensweise F

Diese Vorgehensweise befasst sich mit Fällen, bei denen mehrere Aktuatortypen an der Ausführung der betrachteten LT-Funktion, in deren Steuerebene die LTE vorgesehen sind, beteiligt sind. Betrachtet werden hier alle Aktuatortypen, die von der LT-Funktion angeregt werden sollen und deren Anregung unter Beteiligung einer LTE innerhalb der

Steuerebene (z. B. Vorrangmodul) erfolgen soll. Jeder der an der Ausführung der betrachteten LT-Funktion beteiligten Aktuatortypen muss in der Analyse berücksichtigt werden (Abb. 3.31 und Abb. 3.32). Folgende Randbedingungen müssen für die Anwendung von Vorgehensweise F erfüllt sein:

- Der vorgesehene Einsatz von LTE betrifft eine leittechnische Funktion, weitere leittechnische Funktionen sind zunächst nicht betroffen,
- Es sind LTE in der Steuerebene vorgesehen,
- Der Einsatz von LTE auf der Steuerebene betrifft mehrere Aktuatortypen,
- Der Einsatz von LTE in einem oder mehreren LT-Systemen zur Ausführung dieser LT-Funktion ist möglicherweise ebenfalls vorgesehen.

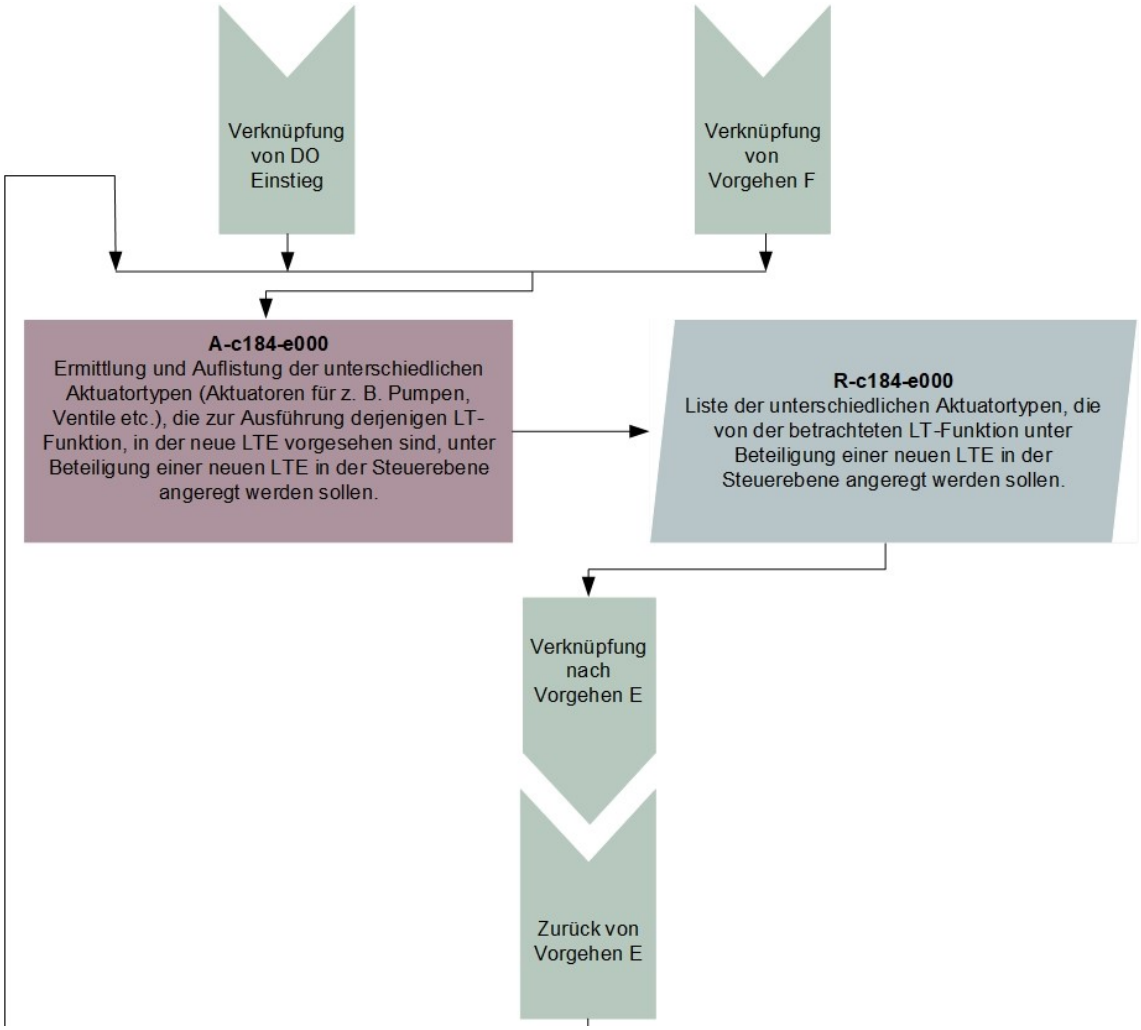


Abb. 3.31 Prozessschritt DO – Vorgehensweise F, Bild 1

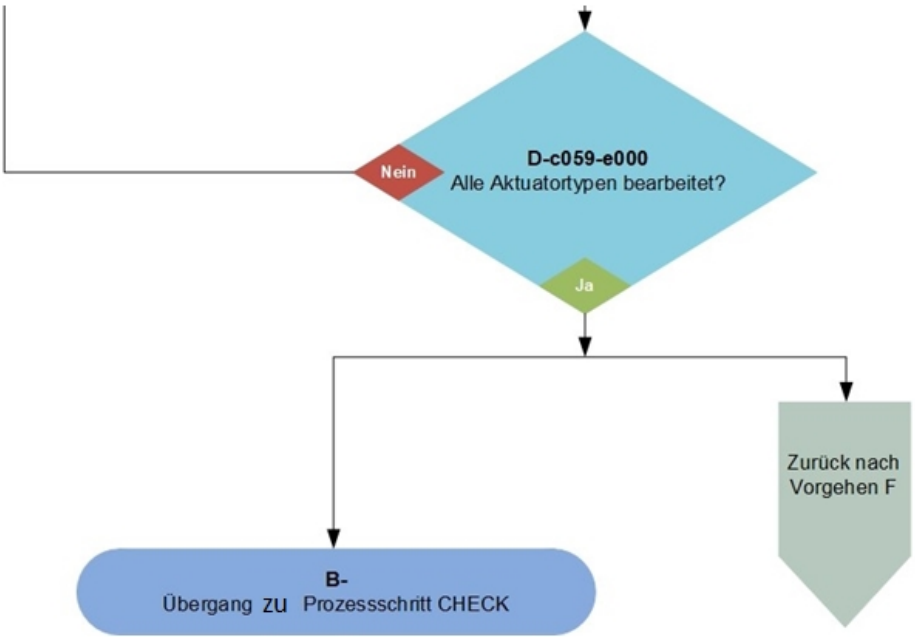


Abb. 3.32 Prozessschritt DO – Vorgehensweise F, Bild 2

3.1.3.8 DO – Vorgehensweise G

Diese Vorgehensweise befasst sich mit Fällen, in denen mehrere leittechnische Funktionen vom geplanten Einsatz von LTE betroffen sind. Jede dieser LT-Funktionen muss im Prozessschritt DO untersucht werden (Abb. 3.33 bis Abb. 3.36). Folgende Randbedingungen müssen für die Anwendung von Vorgehensweise G erfüllt sein:

- Der vorgesehene Einsatz von LTE betrifft mehrere leittechnische Funktionen,
- Der Einsatz von LTE auf der Steuerebene einer oder mehrerer leittechnischer Funktionen ist möglicherweise ebenfalls vorgesehen,
- Der Einsatz von LTE in einem oder mehreren LT-Systemen, die der Ausführung einer dieser LT-Funktionen dienen, ist möglicherweise ebenfalls vorgesehen.

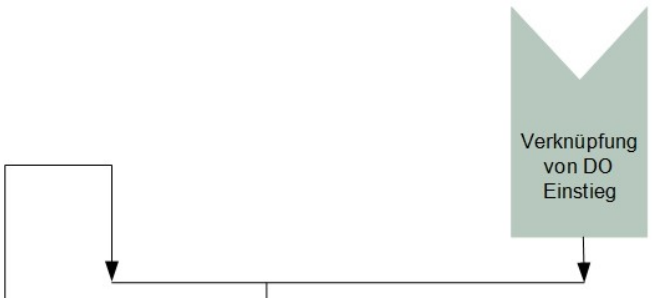


Abb. 3.33 Prozessschritt DO – Vorgehensweise G, Bild 1

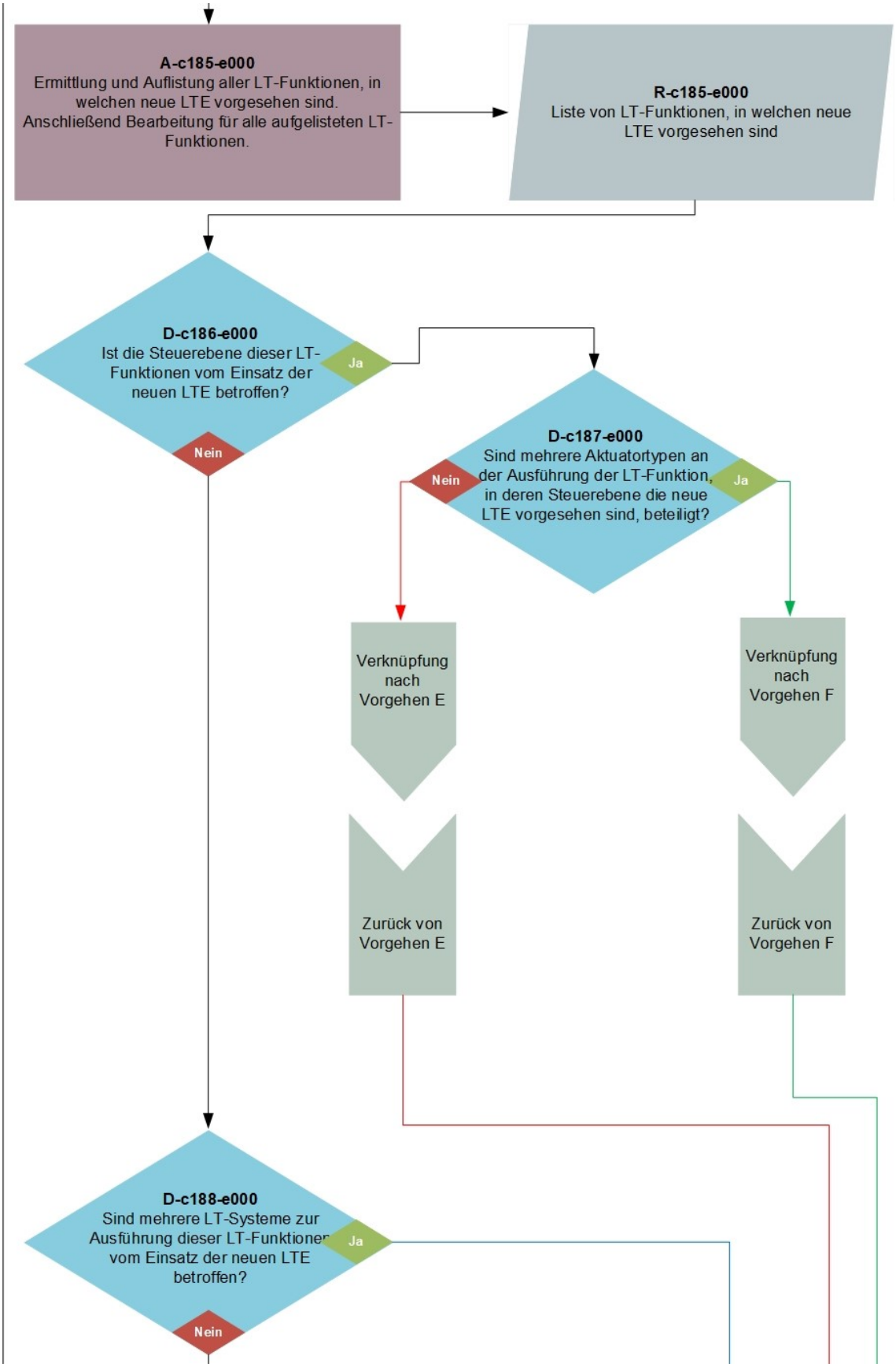


Abb. 3.34 Prozessschritt DO – Vorgehensweise G, Bild 2

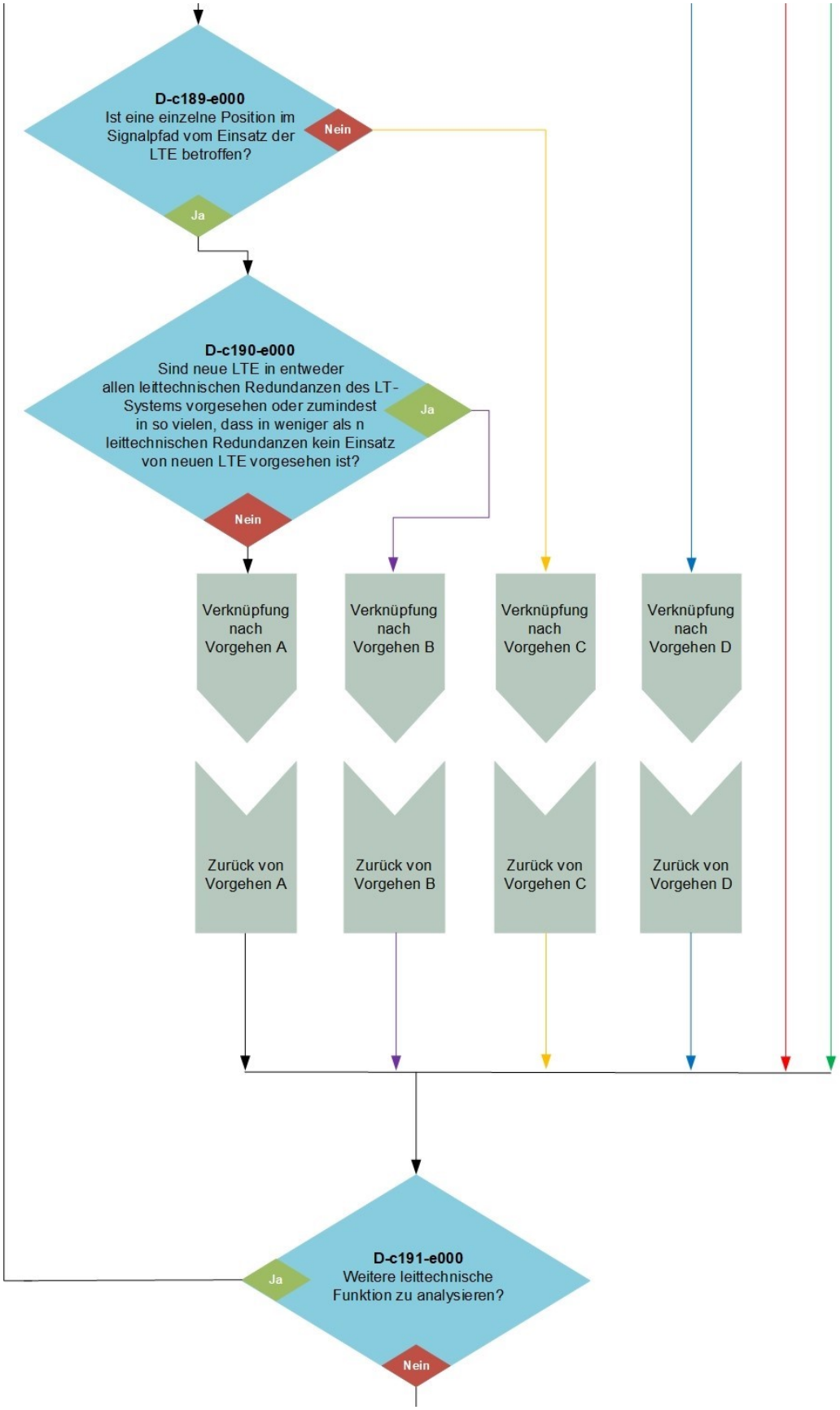


Abb. 3.35 Prozessschritt DO – Vorgehensweise G, Bild 3

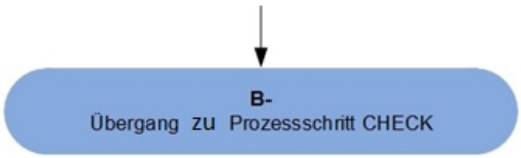


Abb. 3.36 Prozessschritt DO – Vorgehensweise G, Bild 4

3.1.4 CAMIC-Prozessschritt: CHECK

In diesem Prozessschritt (Abb. 3.37 und Abb. 3.38) erfolgt ein Abgleich der Analyseergebnisse aus dem Prozessschritt DO mit den im Prozessschritt PLAN zusammengestellten Anforderungen an die LT-Einrichtungen, in denen der Einsatz von LTE vorgesehen ist. Daran schließt sich die Beantwortung der Frage an, ob alle diese Anforderungen auch bei den ermittelten Fehlzuständen der LTE und den dadurch möglichen Fehlzustandsauswirkungen auf die LTE, das LT-System oder die LT-Funktion erfüllt sind.

Erfüllt der Einsatz der geplanten LTE eine oder mehrere Anforderungen nicht, wird dies detailliert für den nächsten Prozessschritt dokumentiert, um das weitere Vorgehen vorzubereiten. Bei Erfüllung der Anforderungen, wird direkt zum nachfolgendem Prozessschritt gewechselt.

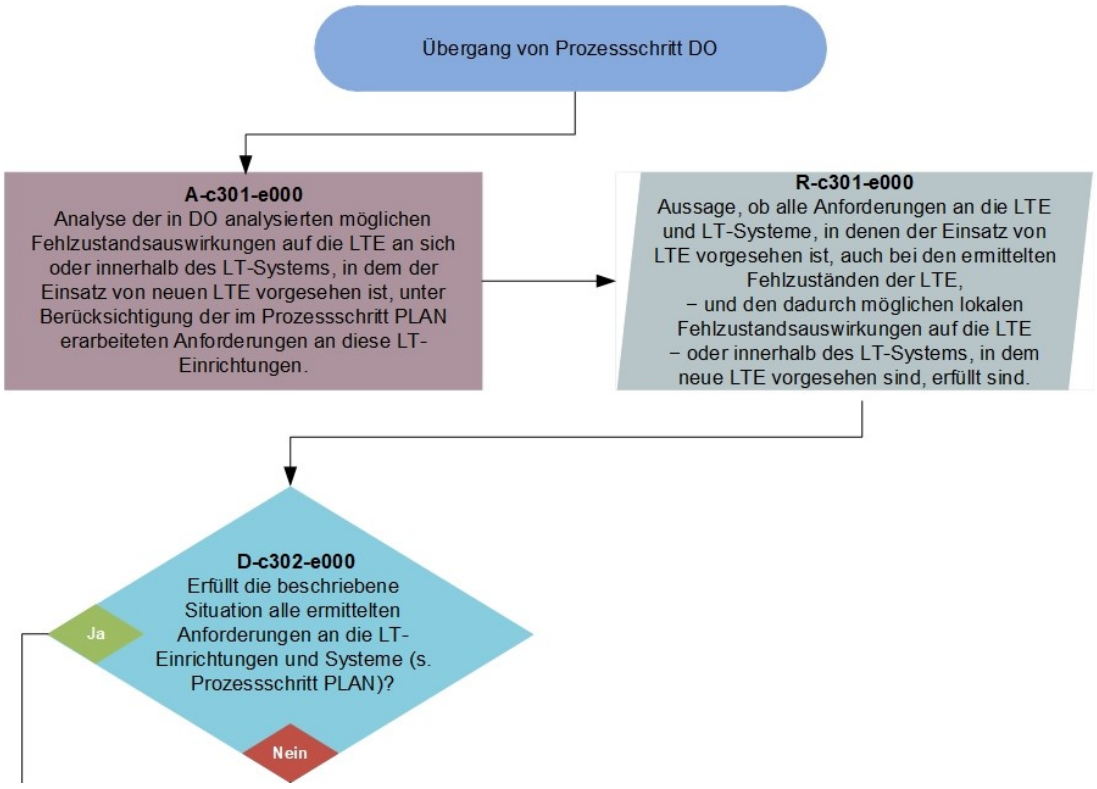


Abb. 3.37 Prozessschritt CHECK, Bild 1

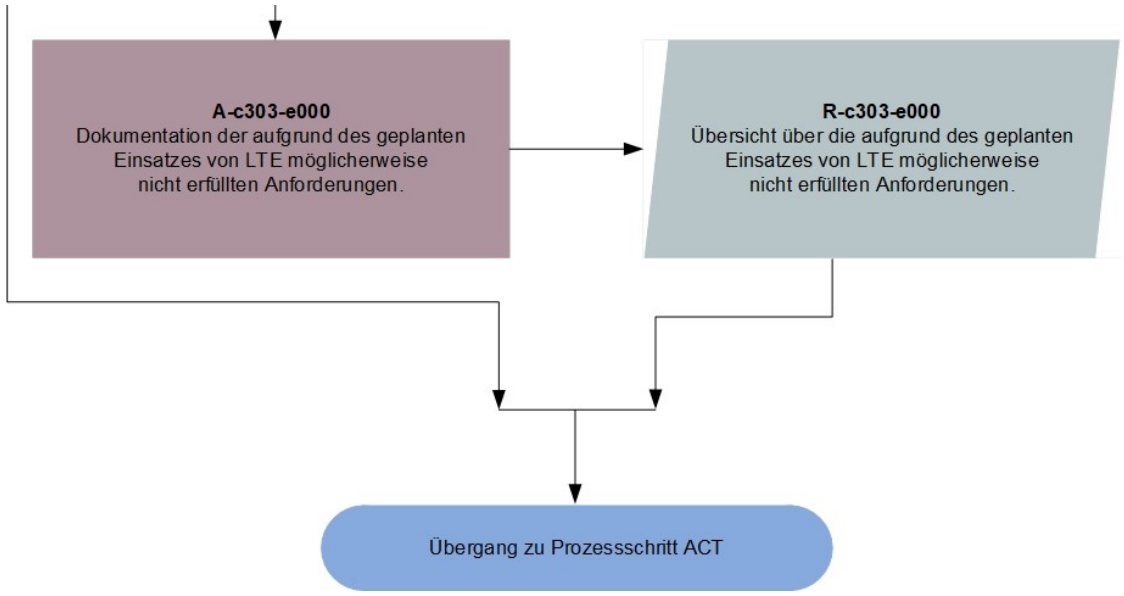


Abb. 3.38 Prozessschritt CHECK, Bild 2

3.1.5 CAMIC-Prozessschritt: ACT

Der letzte Prozessschritt der CAMIC Methode bezieht sich auf den Bewertungsprozess. Entscheidungen zum Einsatz von LTE oder Änderungen an der geplanten Auslegung liegen außerhalb dieses Prozesses. Im PDCA-Zyklus für die Bewertung ist hierzu die Informationsweitergabe an den Prozess für die Planung der LTE und Rückmeldungen aus diesem Prozess vorgesehen.

Die Ziele des Prozessschrittes ACT sind vielfältig und hängen sowohl von den Ergebnissen des Prozessschrittes CHECK als auch – im Unterschied zu allen anderen Prozessschritten – von Entscheidungen ab, die auch außerhalb des Prozesses getroffen werden.

Abhängig von den Ergebnissen des Prozessschrittes CHECK muss eine Entscheidung getroffen werden, ob der Einsatz der LTE wie vorgesehen erfolgen kann und, falls dies der Fall ist, auch wie vorgesehen erfolgen soll. Dazu folgt zunächst im Teilprozessschritt ACT ein Einstieg woraus sich zwei weitere Vorgehensweisen abzweigen. Die Frage danach, ob der Einsatz auch wie geplant erfolgen soll, muss insbesondere unter Berücksichtigung aller im Prozessschritt DO identifizierten Fehlzustandsauswirkungen auf leittechnische Funktionen, gesondert beantwortet werden. Soll der Einsatz der LTE wie vorgesehen erfolgen, wird die Bewertung der LTE abgeschlossen und der PDCA-Zyklus von CAMIC verlassen.

Ist dies nicht der Fall (beispielsweise falls eine oder mehrere Fehlzustandsauswirkungen auf leittechnische Funktionen als inakzeptabel eingestuft werden) oder kann der Einsatz der LTE aufgrund der Ergebnisse des Prozessschrittes CHECK nicht wie geplant erfolgen (was typischerweise die Nicht-Erfüllung von Anforderungen beinhaltet), stehen in CAMIC weitere, optionale Analyseschritte zur Verfügung (Vorgehensweise H und I). Diese optionalen Schritte umfassen auch eine Analyse der LT-Architektur mit dem Fokus auf der Identifikation von für die Ausbreitung von Fehlzustandsauswirkungen relevanten Stellen im Signalpfad. In ihrem Ergebnis liefern diese optionalen Analyseschritte Hinweise auf Möglichkeiten zur Kompensation von Fehlzustandsauswirkungen. Die Bewertung kann hierbei entweder auf die LT-Funktion oder das LT-System ausgerichtet sein, in dem der Einsatz der LTE vorgesehen ist. Diese Erkenntnisse werden wiederum Prozessen außerhalb des Bewertungsprozesses wie beispielsweise dem Prozess, der für die Änderungen an der leittechnischen Architektur verantwortlich ist, zur Verfügung gestellt und können so zunächst in die Planungen für den Einsatz der LTE innerhalb der LT-Architektur einfließen und daran anschließend auch in einen möglichen weiteren Durchlauf des CAMIC PCDA-Zyklus.

Wird die Durchführung der Analyseschritte abgelehnt oder führt die Weitergabe der ermittelten Ergebnisse an den Prozess, der die Planung der LTE umfasst, nicht zu einer wesentlichen Änderung an den Planungen, ist ein negativer Ausstieg aus dem Bewertungsprozess (Projektabschluss) vorgesehen, d. h. die Planungen zum vorgesehenen Einsatz der LTE werden verworfen und der CAMIC PDCA-Zyklus daher abgebrochen.

Die CAMIC-Methode kann, mit den verschiedenen Iterationsschritten, bei den Planungen für Änderungen an der leittechnischen Architektur den Nutzer kontinuierlich begleiten, ohne den PDCA-Zyklus verlassen zu müssen, so lange bis mit der Umsetzung der Planungen begonnen wird.

3.1.5.1 ACT – Einstieg

Der Prozessschritt ACT wird im Folgendem anhand des Flussdiagramms erläutert.

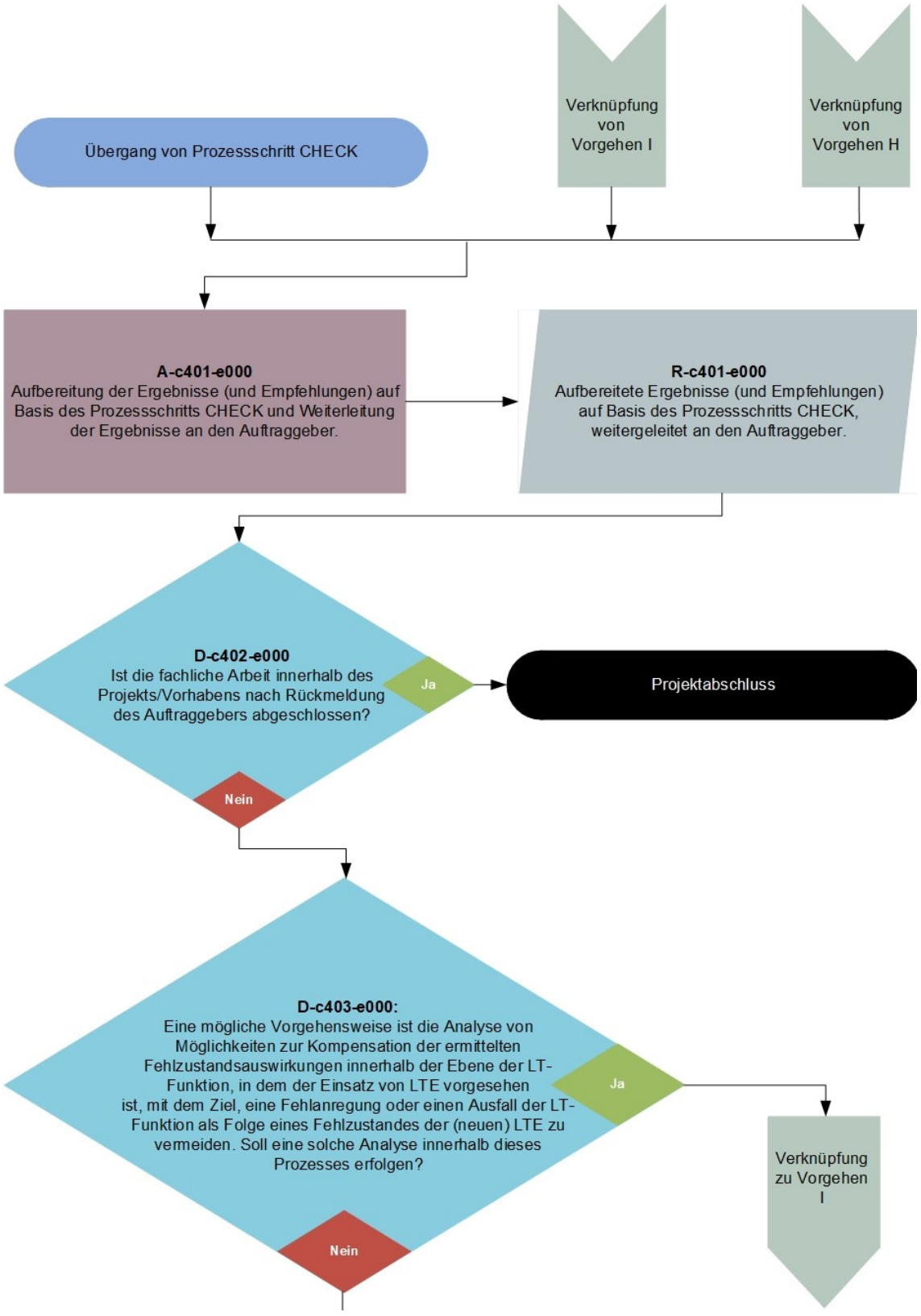


Abb. 3.39 Prozessschritt ACT, Bild 1

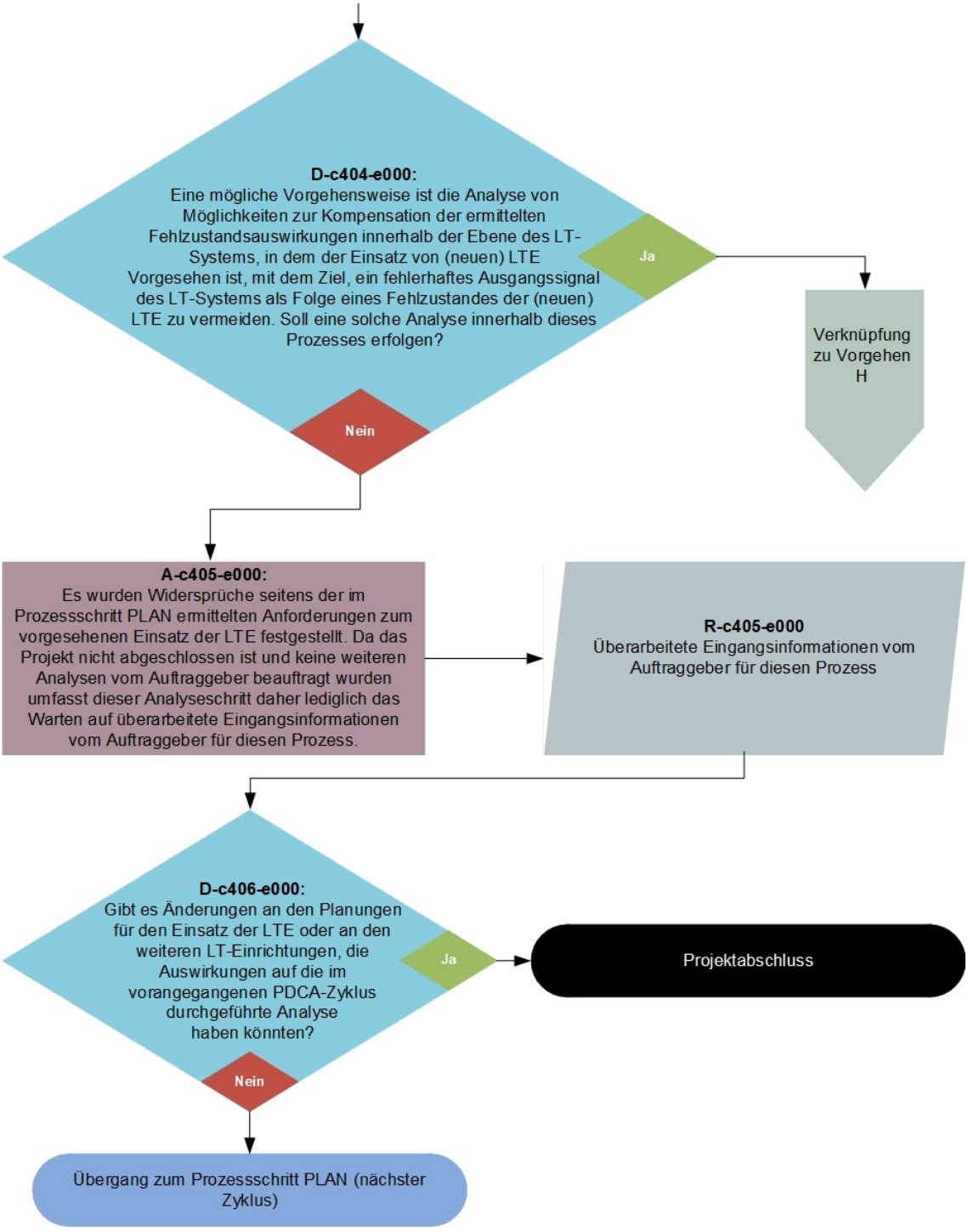


Abb. 3.40 Prozessschritt ACT, Bild 2

3.1.5.2 ACT – Vorgehensweise H

Vorgehensweise H untersucht Möglichkeiten zur Kompensation der ermittelten Fehlzustandsauswirkungen innerhalb der Ebene des LT-Systems, in dem der Einsatz von LTE vorgesehen ist, mit dem Ziel, ein fehlerhaftes Ausgangssignal des LT-Systems als Folge eines Fehlzustandes der LTE zu vermeiden.

Es werden Hinweise auf Verbesserungsmöglichkeiten für den geplanten Einsatz der LTE ermittelt. Dabei werden sowohl der ursprünglich gewählte Typ LTE an sich als auch das LT-System mit einbezogen. Die ermittelten Hinweise werden an den Prozess für die Planung der LTE übergeben und anschließend ist die Berücksichtigung von Rückmeldungen aus diesem Prozess vorgesehen. Anhand dieser Rückmeldungen wird entschieden, ob ein weiterer Durchlauf des PDCA Zyklus sinnvoll ist, oder ob ein negativer Ausstieg aus dem Bewertungsprozess erfolgt.

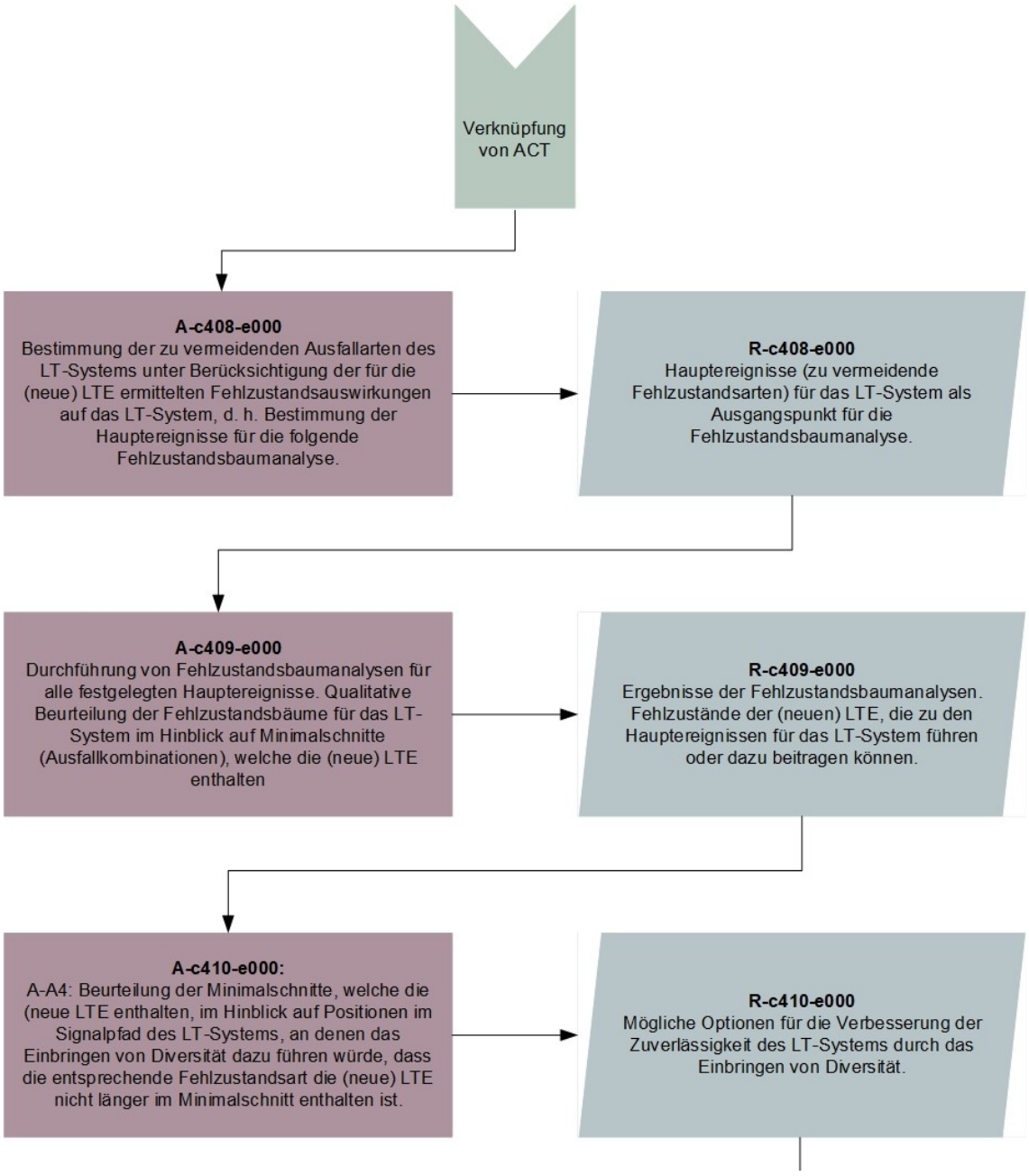


Abb. 3.41 Prozessschritt ACT – Vorgehensweise H, Bild 1

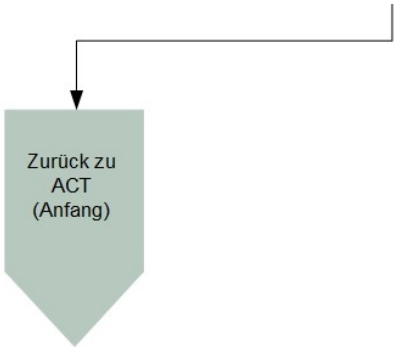


Abb. 3.42 Prozessschritt ACT – Vorgehensweise H, Bild 2

3.1.5.3 ACT – Vorgehensweise I

Bei Vorgehensweise I werden Möglichkeiten zur Kompensation der ermittelten Fehlzustandsauswirkungen innerhalb der Ebene der LT-Funktion, in dem der Einsatz von LTE vorgesehen ist, untersucht. Dies hat das Ziel, eine Fehlanregung oder einen Ausfall der LT-Funktion als Folge eines Fehlzustandes der LTE zu vermeiden.

Es werden Hinweise auf Verbesserungsmöglichkeiten für die geplante LTE ermittelt. Dabei werden sowohl der ursprünglich gewählte Typ LTE an sich als auch das LT-System sowie die leittechnischen Funktionen, die vom Einsatz der PLD-LTE betroffen sind, mit einbezogen. Die ermittelten Hinweise werden an den Prozess für die Planung der LTE übergeben und anschließend ist die Berücksichtigung von Rückmeldungen aus diesem Prozess vorgesehen. Anhand dieser Rückmeldungen wird entschieden, ob ein weiterer Durchlauf des PDCA-Zyklus sinnvoll ist, oder ob ein negativer Ausstieg aus dem Bewertungsprozess erfolgt.

Abb. 3.43 Prozessschritt – Vorgehensweise I, Bild 1

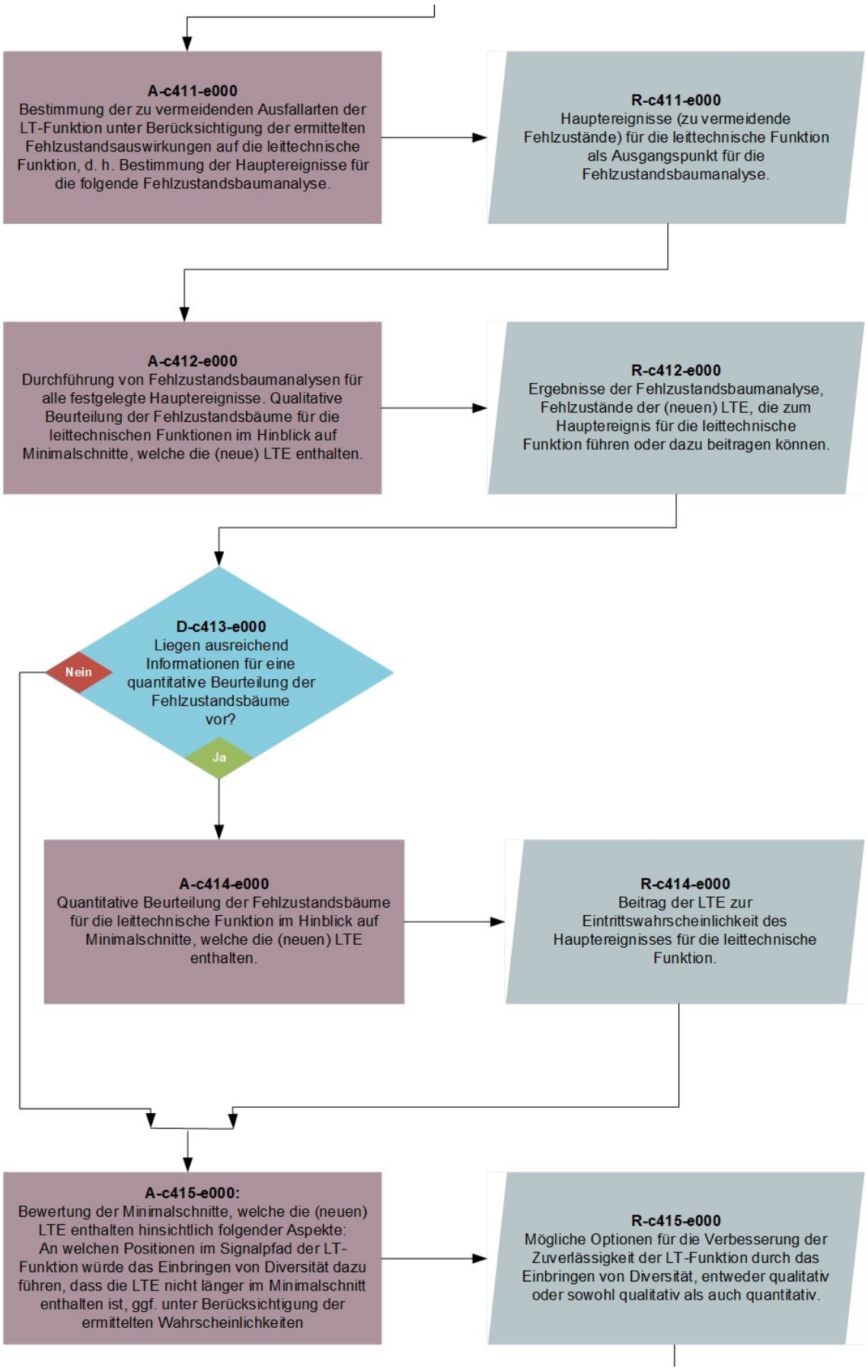


Abb. 3.44 Prozessschritt – Vorgehensweise I, Bild 2

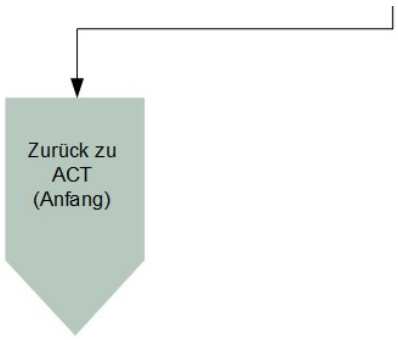


Abb. 3.45 Prozessschritt – Vorgehensweise I, Bild 3

3.2 Erweiterung von CAMIC hinsichtlich der Ausgabe relevanter Anforderungen

Zunächst wurde eine Recherche von nationalen Regelwerken und Normen sowie internationalen Standards unter Berücksichtigung der festgelegten Themen „Einzelfehlerkriterium“, „Redundanz“, „GVA“, „Diversität“, „Programmierbare und rechnerbasierte Geräte“ sowie „Instandhaltung“ durchgeführt und repräsentative Normen wurden ausgewählt. Die Themensuche erfolgte dabei sowohl auf Deutsch als auch auf Englisch. Um eine höhere Vergleichbarkeit der Ergebnisse zu erreichen, wurden sowohl deutschsprachige als auch englischsprachige Regelwerke zugrunde gelegt:

- Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Sicherheitsanforderungen an Kernkraftwerke, November 2012 (deutsche Fassung); Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Safety Requirements for Nuclear Power Plants, November, 22nd 2012 (englische Fassung)
- Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke, November 2013 (deutsche Fassung); Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, Interpretations of the Safety Requirements for NPPs of 22/11/2012, November, 29th 2013 (englische Fassung)
- IEC 61513, Nuclear power plants Instrumentation and control important to safety General requirements for systems, August 2011 (englische Fassung)
- Sicherheitstechnische Regel des KTA, KTA 3501, Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems, Fassung 2015-11 (deutsche Fassung); Safety Standards of the Nuclear Safety Standards Commission (KTA),

KTA 3501, Reactor Protection System and Monitoring Equipment of the Safety System, November 2015 (englische Fassung)

Im darauffolgenden Schritt wurden Kriterien für die Themensuchen zu diesen festgelegten Themen erarbeitet, was eine eindeutige Kodierung der recherchierten Anforderungen mit Bezug zu einem oder mehreren Themen ermöglichte. Für alle Themen wurden die Kriterien in deutscher und englischer Sprache erarbeitet. Für jede Themensuche, sowohl in Deutsch als auch in Englisch, wurde ein schrittweises Vorgehen erstellt, das sicherstellt, dass die Themensuche immer dieselben Ergebnisse liefert, unabhängig von der Person, welche die Themensuche durchführt. Jede Themensuche muss dadurch für einen Standard oder Regelwerkstext nur ein einziges Mal in CAMIC durchgeführt werden. Bei nachfolgenden Bewertungen stehen die Kodierungen bzw. die Ergebnisse der Themensuchen dann schon zur Verfügung und es kann direkt auf diese zurückgegriffen werden. Zusätzlich bietet sich auch immer die Möglichkeit, weitere Regelwerkstexte, in denen die gewünschten Themensuchen bereits durchgeführt worden sind, zu informativen Zwecken oder für alternative Aussagen heranzuziehen, allein über die entsprechende Auswahl in der CAMIC Anwendung. Diese Funktionalität soll sowohl für nationale Regelwerke und Normen als auch für internationale Standards nutzbar sein. Dieses Vorgehen ist auch für Bewertungen innerhalb Deutschlands deshalb wichtig, weil internationales Regelwerk typischerweise zuerst in der englischen Fassung überarbeitet oder erstellt worden ist und die deutschsprachige Fassung erst mit teilweise erheblichem zeitlichem Verzug erscheint. Um für eine Bewertung auch in Deutschland das aktuelle Regelwerk zugrunde zu legen, muss man deshalb immer davon ausgehen, dass einige Standards nicht oder noch nicht in deutscher Version vorliegen.

Die Benutzeroberflächen und Funktionalitäten zur Umsetzung der Themensuchen mit Erfassung, Kodierung und Anzeige relevanter Anforderungen wurde in der CAMIC-Anwendung implementiert. Die Umsetzung ist derart erfolgt, dass sich der Funktionsumfang der CAMIC-Anwendung an dieser Stelle nicht auf Anforderungen beschränkt, sondern auch Definitionen, weitere Zitate und Abbildungen aus Dokumenten wie Regelwerken und Standards erfasst, kodiert und angezeigt werden können. Dies ermöglicht zum einen ein hohes Maß an Flexibilität bezüglich der für eine sicherheitstechnische Bewertung wesentlichen Informationen und zum anderen die Erstellung einer umfassenden Bewertungsgrundlage innerhalb der CAMIC-Anwendung und zu einer damit ständig wachsenden Wissensbasis in CAMIC, auf die man während einer Bewertung oder auch unabhängig davon zurückgreifen kann. Auch die Selektion und automatisierte Ausgabe von relevanten Anforderungen für die aktuell durchzuführende Bewertung wurde

ermöglicht. Dies wurde im Rahmen der Konzeptionierung und Umsetzung des Prozessschrittes PLAN der rechnergestützten CAMIC-Anwendung mit den zugehörigen Benutzeroberflächen und Werkzeugen durchgeführt, da die Auswahl und Erfassung von relevanten Dokumenten (wie Regelwerke und Normen) sowie die Realisierung der Themensuchen in diesem Prozessschritt erfolgt. Die CAMIC-Anwendung wurde so konzipiert, dass die Erweiterung auf weitere Themen und die Integration der entsprechenden Themensuchen in die CAMIC-Anwendung einfach umgesetzt werden kann.

4 Werkzeugentwicklung für die rechnergestützte Anwendung der CAMIC-Methode

Die Durchführung einer Bewertung mittels der CAMIC-Methode stützte sich im Vorgängervorhaben RS1525 auf die manuelle Auswertung von Abfragen, Analyseschritten und Entscheidungskriterien. In diesem Vorhaben ist eine rechnergestützte CAMIC-Anwendung entwickelt worden, welche den Anwender in den verschiedenen Prozessschritten unterstützt. Auf diese Weise wurde der Bewertungsprozess der CAMIC-Methode zum einen erleichtert und zum anderen konsistent und jederzeit nachvollziehbar gestaltet.

Der Fokus bei der Umsetzung der Rechnerunterstützung für die CAMIC-Methode ist auf die Realisierung aller PDCA-Schritte in der rechnergestützten CAMIC-Anwendung gelegt worden. Darüber hinaus erfolgte die Detaillierung folgender Aspekte:

- Erfassung aller Bausteine der CAMIC-Vorgehensweise,
- Einbindung der Diversitätsmatrix,
- Dokumentation des Bewertungsprozesses und Ausgabe von Informationen,
- Durchführung von Themensuchen und Ausgabe von Anforderungen.

Diese Aspekte werden in den folgenden Abschnitten näher beschrieben.

4.1 Entwicklung der CAMIC-Anwendung

Das Aufgabenziel dieser Teilaufgabe war die eigentliche Entwicklung der CAMIC-Anwendung. Dafür erfolgte zunächst eine grobe Konzeptionierung der gesamten Anwendung als Grundlage. Hierzu zählten, beginnend mit der Auswahl der geeigneten Software, vor allem die Spezifikation der Funktionalitäten und die Struktur von Benutzeroberflächen, Datenbanken und Software. Anschließend lag der Schwerpunkt darin die Prozessschritte der CAMIC-Methode in der Anwendung zu implementieren.

Zunächst wurde ermittelt, welche Funktionen der CAMIC-Methode in der CAMIC-Anwendung umgesetzt werden sollen. Dazu wurden anhand des Flowchart der CAMIC-Methode die zu implementierenden Funktionen ermittelt und ein Konzept zur Umsetzung entwickelt. Darüber hinaus wurden zusätzliche übergeordnete Funktionalitäten zur Planung, Durchführung und Dokumentation von Bewertungen in der CAMIC-Anwendung

festgelegt. Im Anschluss erfolgte die Erstellung des Layouts der CAMIC-Anwendung. Komplette Oberflächen und einzelne Elemente der CAMIC-Anwendung wurden als Vektorgrafik designt. Auf Grundlage des entwickelten Konzepts musste als nächstes eine geeignete Softwareumgebung gefunden werden. Um eine möglichst große Flexibilität der Anwendung zu erreichen und die Umsetzung aller genannten Aspekte zu erlauben, wurde entschieden, für die CAMIC-Anwendung die Programmiersprache *Python* zu verwenden. Für das Speichern von Dokumenten, das Anlegen von Benutzerprofielen in der CAMIC-Anwendung sowie der Schaffung einer Möglichkeit mit mehreren Personen an einem Projekt zu arbeiten war es notwendig eine Datenbank anzulegen. Als geeignete Datenbankstruktur wurde entschieden *MySQL* zu verwenden. MySQL erlaubt eine einfache Datenbankstruktur aufzubauen, die aber für die CAMIC-Anwendung alle relevanten Anforderungen erfüllt.

Die Datenbank sollte zwei Anforderungen erfüllen. Zum einen soll die Möglichkeit bestehen Informationen zu den dazugehörigen Projekten zentral abzuspeichern. Zum anderen sollten alle projektzugehörige Person Zugriff auf die gespeicherten Projektinformationen haben. Mit MySQL wurden beide Anforderungen erfüllt. Dafür wurde ein GRS-interner Server am Standort Garching eingerichtet. Innerhalb des GRS Netzwerks (an den Standorten der GRS oder per VPN) ist es möglich, Zugriff auf die Datenbank zu bekommen.

Eine Benutzerverwaltung wurde implementiert, damit nur berechtigte Personen Zugriff auf die gespeicherten Projektdaten haben. Als berechtigte Personen zählen entweder Administratoren oder projektzugehörige Personen. Administratoren sollen nur bei Störungen in der Datenbank und mit Genehmigung des Projektleiters projektbezogene Daten ändern. Projektzugehörige Personen können entweder nur Leserechte oder Schreibrechte erhalten. Um Personen einem Projekt zuzuweisen, müssen Benutzerkonten erstellt werden. Benutzerkonten für den Zugriff auf die CAMIC-Datenbank erstellen die Administratoren. Ein Aktivierungspasswort wird dabei dem Benutzer mitgeteilt. Das Aktivierungspasswort sollte aber bei erstmaliger Verwendung der CAMIC-Anwendung durch den Nutzer geändert werden. Damit bleibt ein Missbrauch durch Fremde ausgeschlossen.

Für die Softwareoberfläche (engl. GUI – Graphical User Interface) der CAMIC-Anwendung wurde das Pythonpaket *Tkinter* verwendet. Mit Tkinter konnte die GUI entsprechend der Anforderung an das Grafikdesign, mit geringem Aufwand, realisiert werden. Im Folgendem wird die Benutzeroberfläche der CAMIC-Anwendung im Detail erläutert.

4.1.1 Anmeldefenster

Beim Starten der CAMIC-Anwendung wird zunächst der Benutzername und das Benutzerpasswort abgefragt (Abb. 4.1).

Für die Verwendung von CAMIC muss ein Benutzerkonto vorliegen. Die Anmeldedaten werden bei der Erstellung des Kontos in der CAMIC-Datenbank abgelegt. Bei einem Anmeldeversuch wird der hier eingegebene Benutzername und das Passwort mit den Daten in der Datenbank abgeglichen. Der Nutzer hat 3 Anmeldeversuche, bevor die Anmeldung blockiert wird.

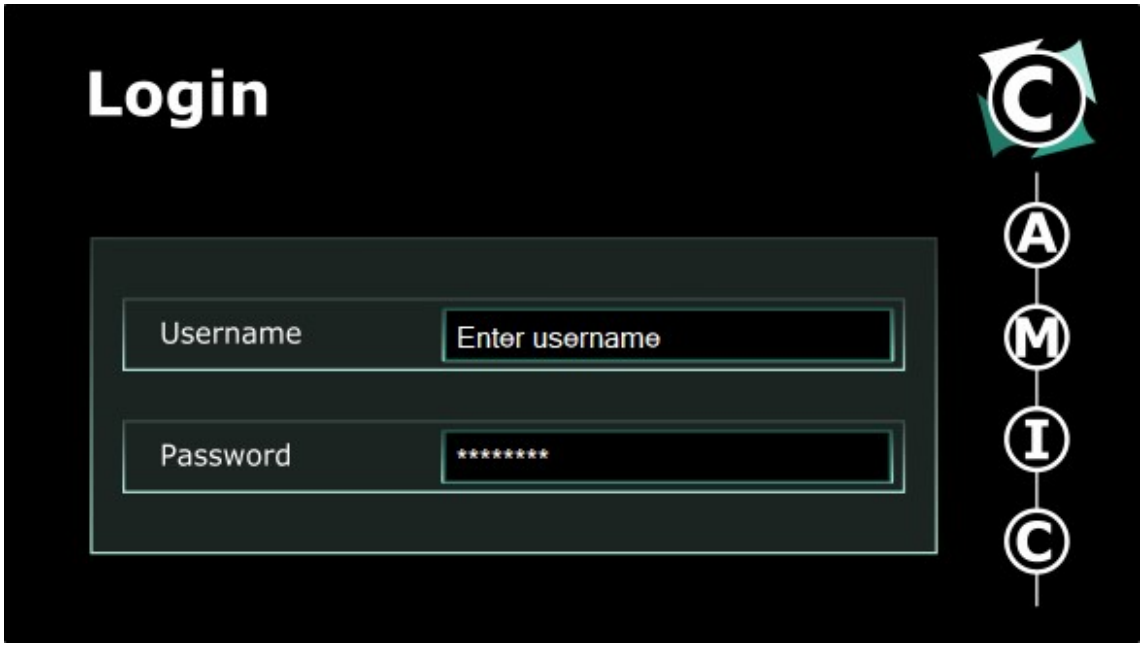


Abb. 4.1 CAMIC Anmeldefenster

4.1.2 Struktur der einzelnen Fenster der Benutzeroberfläche

Jedes weitere Fenster der CAMIC-Anwendung ist in drei Bereiche aufgeteilt (Abb. 4.2).

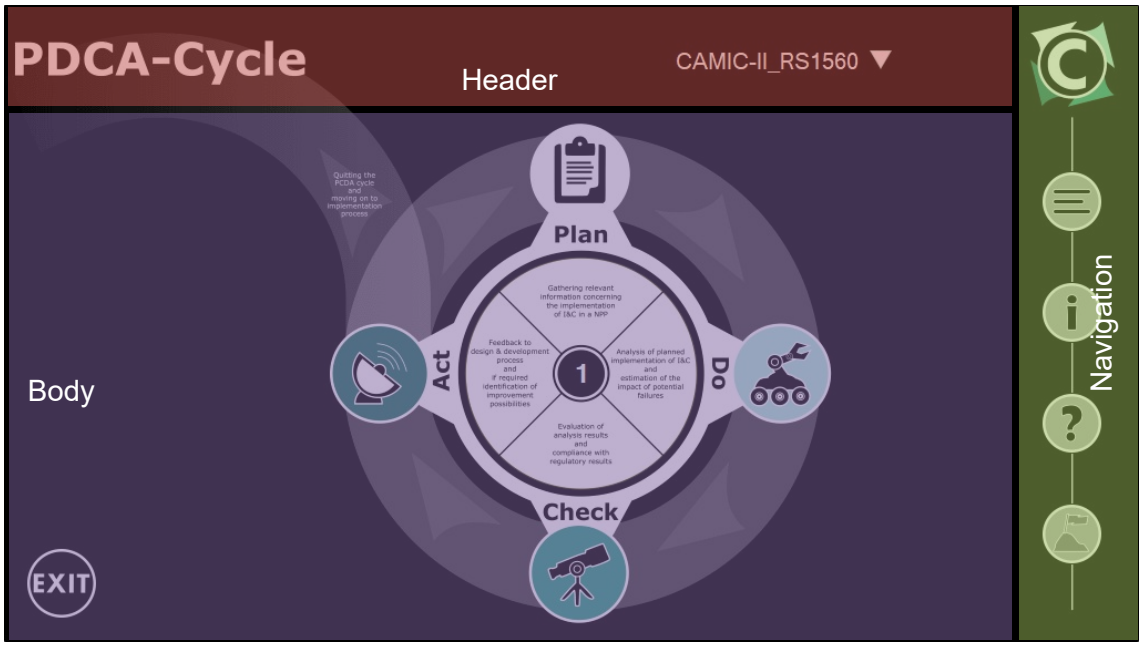


Abb. 4.2 Aufteilung der CAMIC Benutzeroberfläche

Der obere Bereich ist der sogenannte *Header*. Hier stehen alle hilfreichen Informationen für den Nutzer. Hier wird der Name des aktuell ausgewählten Projekts, der Name des geöffneten Fensters oder der aktuelle Prozessschritt der CAMIC-Methode angezeigt. An der rechten Seite befindet sich die *Navigationsleiste*. Je nach aktuell geöffnetem Bereich der CAMIC-Anwendung werden hier unterschiedliche Funktionen zur Verfügung gestellt. Zum Beispiel kann von der Navigationsleiste zum zuvor geöffneten Fenster zurückgekehrt, der Fortschritt gespeichert oder eine Hilfe aufgerufen werden. Der Hauptbereich jedes CAMIC-Fensters wird *Body* genannt. Hier sind alle Funktionen und Informationen zu dem aktuellen Bereich der CAMIC-Anwendung implementiert.

4.1.3 Hauptfenster

Nach erfolgreicher Anmeldung öffnet sich das Hauptfenster der CAMIC-Anwendung (Abb. 4.3).

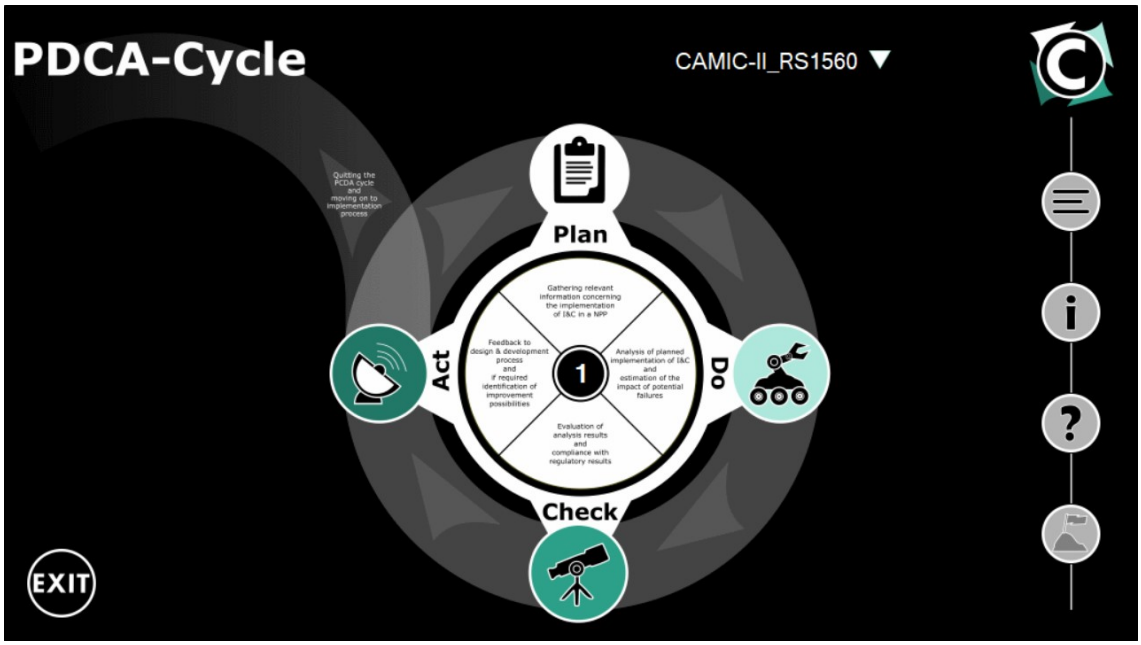


Abb. 4.3 Hauptfenster der CAMIC-Anwendung

Dieses Fenster ist der zentrale Ausgangspunkt der CAMIC-Anwendung. Im Header wurde ein *Dropdownmenü* implementiert. Mittels dieses Dropdownmenüs kann ein zugewiesenes Projekt geöffnet werden (Abb. 4.4).

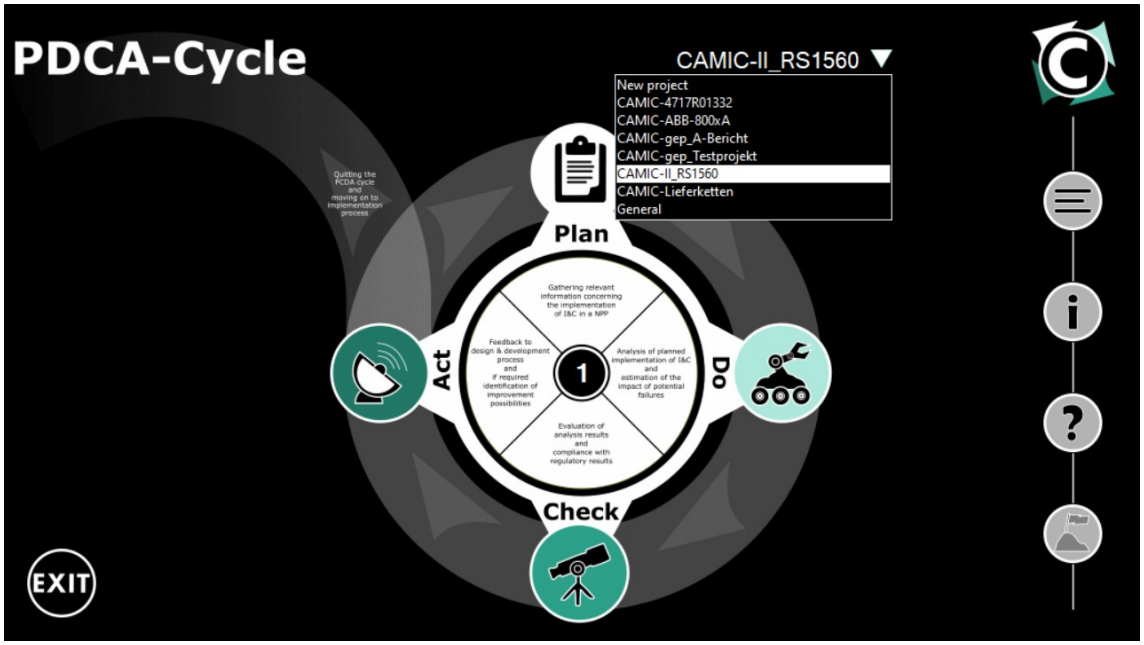


Abb. 4.4 Hauptfenster mit geöffnetem Dropdownmenü für die Auswahl eines zugewiesenen Projekts

Angezeigt werden hier nur dem Nutzer zugewiesene Projekte. Die Zuweisung der Projekte übernimmt der Projektleiter. Dies kann entweder bei der Erstellung des Projekts oder später erfolgen. Durch die Auswahl von *New project* ist es außerdem möglich, ein neues Projekt anzulegen. Dazu wird der Nutzer auf die Seite *Project information* weitergeleitet (Abschnitt 4.1.5).

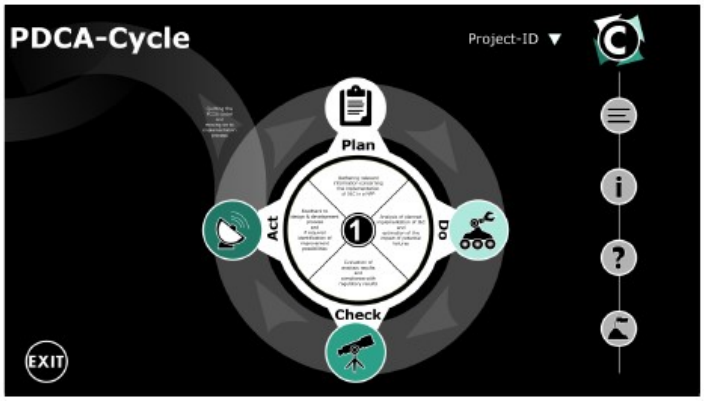
Mit dem obersten Button der Navigationsleiste auf dem Hauptfenster kann zu *CAMIC output* (siehe Abschnitt 4.1.7) gewechselt werden. Hier können alle wichtigen projektbezogenen Informationen als PDF-Datei ausgegeben werden. Der Button mit dem *i* führt ebenfalls in den Bereich der *Project information* (Abschnitt 4.1.5), wo alle notwendigen Informationen zum ausgewählten Projekt geändert werden können. Als letzte Funktion wurde in die Navigationsleiste das Öffnen einer CAMIC-Hilfe implementiert (*Fragezeichen-Button*). Diese öffnet ein PDF-Dokument mit einer Hilfeseite zum aktuell geöffneten CAMIC-Bereich.

Das Hauptfenster der CAMIC-Anwendung bietet als einziges die Möglichkeit die CAMIC-Anwendung zu schließen. Dafür wurde im Body der *Exit-Button* implementiert. Ebenfalls im Body ist die Möglichkeit gegeben in den aktuellen PDCA-Zyklus zu wechseln. Die Zahl in der Mitte des Kreises gibt den aktuellen Zyklus wieder, hier 1. Die vier Buttons (*Plan, Do, Check, Act)* bieten die Möglichkeit, den aktuellen Prozessschritt des PDCA-Zyklus zu öffnen.

4.1.4 Hilfe

Zur Unterstützung des Anwenders wurde eine Hilfefunktion in der CAMIC-Anwendung implementiert. Die Hilfefunktion wird durch den *Fragezeichen-Button,* welcher in der Navigationsleiste zu finden ist, aufgerufen. Als Hilfe öffnet sich eine PDF-Datei mit Erläuterungen zu dem aktuell geöffneten Bereich der CAMIC-Anwendung (Abb. 4.5).

CAMIC-Hilfeseite: Benutzeroberfläche „PDCA-Cycle“



Diese Benutzeroberfläche dient der Navigation innerhalb der Anwendung, es können hier keine Informationen in der Datenbank abgelegt werden. Bis auf eine Ausnahme – das Pull-down-Menü „Project-ID“ – handelt es sich bei allen Schaltflächen um Buttons zur Navigation bzw. zum Öffnen von Dokumenten oder um Symbole zur Anzeige von Informationen aus der Datenbank.

Anlegen eines neuen Projekts

- Auswahl von „New project“ im Pull-down Menü „Project-ID“ (rechts oben)
- Anschließend erfolgt ein automatischer Wechsel zur Benutzeroberfläche „Project information“, dort erfolgt die Eingabe der Projektinformationen

Öffnen eines bereits angelegten Projekts

- Auswahl der entsprechenden Projekt-ID im Pull-down-Menü „Project-ID“ (rechts oben)
    - Anm.: Dem aktuellen Benutzer werden nur die Projekte angezeigt, an denen er selbst beteiligt ist oder die als nicht vertraulich eingestuft wurden

1

Abb. 4.5 Beispiel einer Hilfedatei der CAMIC-Anwendung

4.1.5 Eingabe/Ändern von Projektinformationen

Wie in Abschnitt 4.1.3 erwähnt, können Projektinformationen über den *i-Button* in der Navigationsleiste der Hauptseite geändert oder neue Projekte angelegt werden. Dieser Button führt auf eine übersichtliche Eingabemaske aller relevanten projektbezogenen Informationen (Abb. 4.6). Die gleiche Eingabemaske wird auch über *New project* des Dropdownmenüs im Header der Hauptseite erreicht.

Abb. 4.6 Übersichtliche Darstellung aller relevanten projektbezogenen Informationen

Über diese Maske können neue Projekte angelegt oder existierende Projekte bearbeitet werden. Das Schema, nach dem ein Projekt in der CAMIC-Datenbank angelegt werden sollte, wird in dem passenden Hilfedokument genauer erläutert, daher wird an dieser Stelle darauf verzichtet.

Unten rechts im Body wird der Status der Prozessschritte des PDCA-Zyklus angezeigt. Wie auch in den Ausgangsfenstern der Prozessschritte bedeutet ein graues Zahnrad, dass sich der Prozessschritt aktuell in Bearbeitung befindet. Ein schwarzes Zahnrad bedeutet, der Prozessschritt ist abgeschlossen. Bei einem kaputten Zahnrad wurde die Bearbeitung dieses Prozessschritts abgebrochen. Ist das Feld leer, wurde mit der Bearbeitung dieses Prozessschritts noch nicht begonnen.

Weiter kann in dieser Eingabemaske ein neuer Benutzer dem Projekt zugewiesen werden. Nur zugewiesene Benutzer können das angelegte Projekt sehen, das schließt die

projektspezifischen Dokumente mit ein, und diese Teilschritte bearbeiten. Die Möglichkeit, eine Person dem Projekt zuzuweisen haben nur die Projektleiter und die Administratoren.

4.1.6 Implementierung des PDCA-Zyklus in der CAMIC-Anwendung

Wie im vorherigen Abschnitt erläutert, werden die einzelnen Prozessschritte des PDCA-Zyklus vom Hauptfenster der CAMIC-Anwendung aus erreicht. Im folgendem wird die Umsetzung des PDCA-Zyklus in der CAMIC-Anwendung im Detail erläutert.

4.1.6.1 PLAN

In Abb. 4.7 ist das Ausgangsfenster des CAMIC-Prozessschritts PLAN abgebildet.

Abb. 4.7 Ausgangsfenster des CAMIC-Prozessschritts PLAN

Die Buttons der Navigationsleiste bieten die Möglichkeit eine Hilfeseite für die PLAN Benutzeroberfläche zu öffnen, zum Hauptfenster der CAMIC-Anwendung zurückzukehren (Pfeil-Button) oder den Fortschritt des Bewertungsprozesses zu speichern (unterster Button). Der oberste Button in der Navigationsleiste zeigt den aktuellen Status des Prozessschritts PLAN. Ist das Zahnrad grau befindet sich der Prozessschritt aktuell in Bearbeitung, ist das Zahnrad schwarz wurde der Prozessschritt abgeschlossen, bei kaputtem Zahnrad wurde die Bearbeitung dieses Prozessschritts abgebrochen.

Im Body des PLAN Ausgangsfensters wurden sechs Buttons integriert, diese werden im Folgendem erläutert.

4.1.6.1.1 Continue analysis

Der Button *Continue analysis* führt den Anwender zum aktuellen Bearbeitungsstand des Bewertungsprozesses. Hier werden entweder *Analyseschritte*, *Entscheidungskriterien* oder *Übergangsschritte* zum nachfolgendem Prozessschritt dargestellt. Es ist nicht relevant ob Continue analysis vom Ausgangsfenster der Prozessschritte PLAN, DO, CHECK oder ACT aufgerufen wird, der Anwender wird immer zum letzten Bearbeitungsstand der Bewertung weitergeleitet.

Zunächst erfolgte die Umsetzung der im BMWi-Vorhaben RS1525 entwickelten CAMIC-Methode in der CAMIC-Anwendung. Dies beinhaltete die Erfassung des CAMIC-Flussdiagramms und relevanter Teildiagramme für die Prozessschritte PLAN, DO, CHECK und ACT, der zugrundeliegenden Entscheidungskriterien, Tabellen und Analyseschritte sowie der Analysewerkzeuge. Jede Weiterentwicklung der CAMIC-Methode, wie in diesem Vorhaben vorgesehen und unter Abschnitt 3 beschrieben, zog eine Erweiterung des CAMIC-Flussdiagramms sowie der Gesamtheit der Entscheidungskriterien, Tabellen und Analyseschritte nach sich. Daher wurden bei der Konzeptionierung der Anwendung bereits Erweiterungsmöglichkeiten der CAMIC-Vorgehensweise und ihre direkte Erfassung in der Anwendung vorgesehen. Dies bildet die Grundlage für die Erfassung der erweiterten CAMIC-Methode innerhalb der Anwendung.

Die Flussdiagramme der CAMIC-Methode wurden Element für Element in die CAMIC-Anwendung integriert. Diese Elemente sind *Analyseschritte, Entscheidungskriterien* und *Übergangsschritt.* Sie sind als Teilschritte der Bewertung zu verstehen. Erreicht werden diese Teilschritte über den Button *Continue analysis* welcher auf dem jeweiligen Ausgangsfenster jedes der vier Prozessschritte implementiert wurde. Dadurch öffnet sich die Benutzeroberfläche Current flow chart element, die immer denjenigen Teilschritt des Bewertungsprozesses anzeigt, an dem gerade gearbeitet wird. Dies ist immer der erste Prozesschritt im Flussdiagramm, dessen Bearbeitung noch nicht abgeschlossen wurde. Diese Benutzeroberfläche unterscheidet sich je nachdem, ob es sich bei dem aktuell zu bearbeitendem Element des Flussdiagramms um einen Analyseschritt, ein Entscheidungskriterium oder einen Übergangsschritt handelt. Auf den auf die drei unterschiedlichen Elementtypen zugeschnittenen Benutzeroberflächen stehen dem Benutzer mehrere Handlungsmöglichkeiten zur Verfügung, die aber mindestens die Möglichkeit

beinhalten, sich eine detaillierte Beschreibung des aktuellen Teilschrittes anzeigen zu lassen, sowie die Möglichkeit, die Bearbeitung des aktuellen Teilschrittes abzuschließen und in den nächsten Teilschritt zu wechseln. Ein Zurückkehren in den vorherigen Teilschritt ist nicht vorgesehen. Im Folgenden werden Beispiele für jeden Elementtypen des Flussdiagramms vorgestellt.

4.1.6.1.1.1 Analyseschritte

Im oberen Bereich des Fensters (Abb. 4.8) ist eine Kurzbeschreibung des aktuellen Analyseschritts gegeben. Unmittelbar darunter befinden sich Informationen zu möglichen Abhängigkeiten sowie die Bezeichnung des vorherigen Analyseschritts. Diese Informationen fließen in die Analyse mit ein.

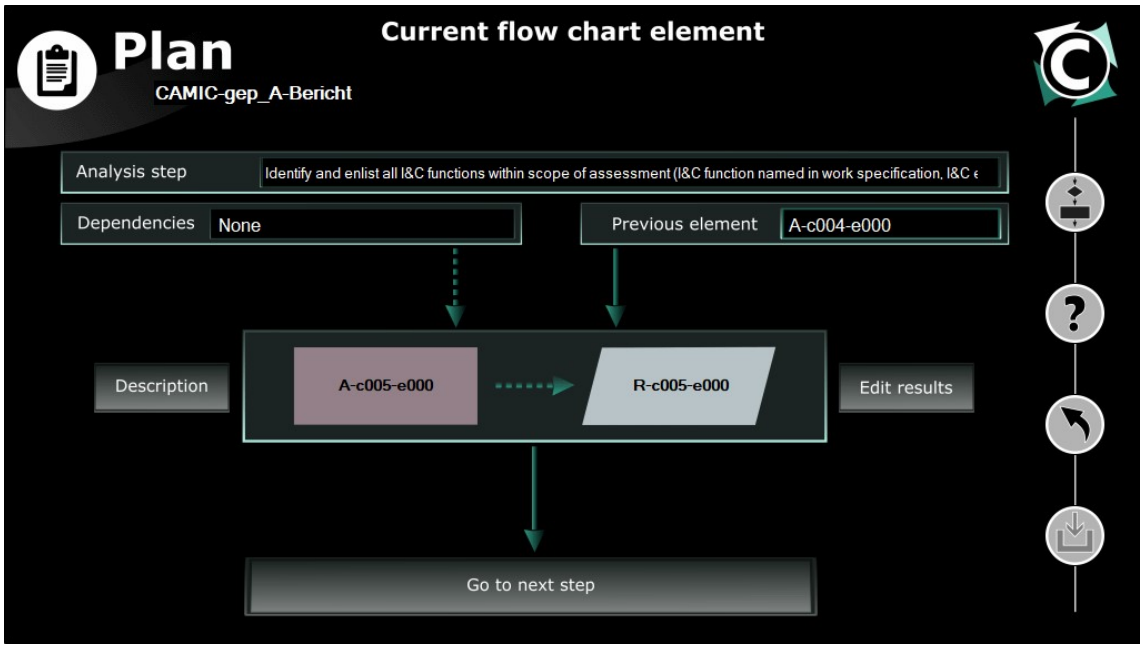


Abb. 4.8 Ausgangsfenster des Teilschritts *Analyseschritt* der implementierten CAMIC-Methode

Eine genaue Beschreibung der durchzuführenden Analyse kann unter Descriptions aufgerufen werden (Abb. 4.9).

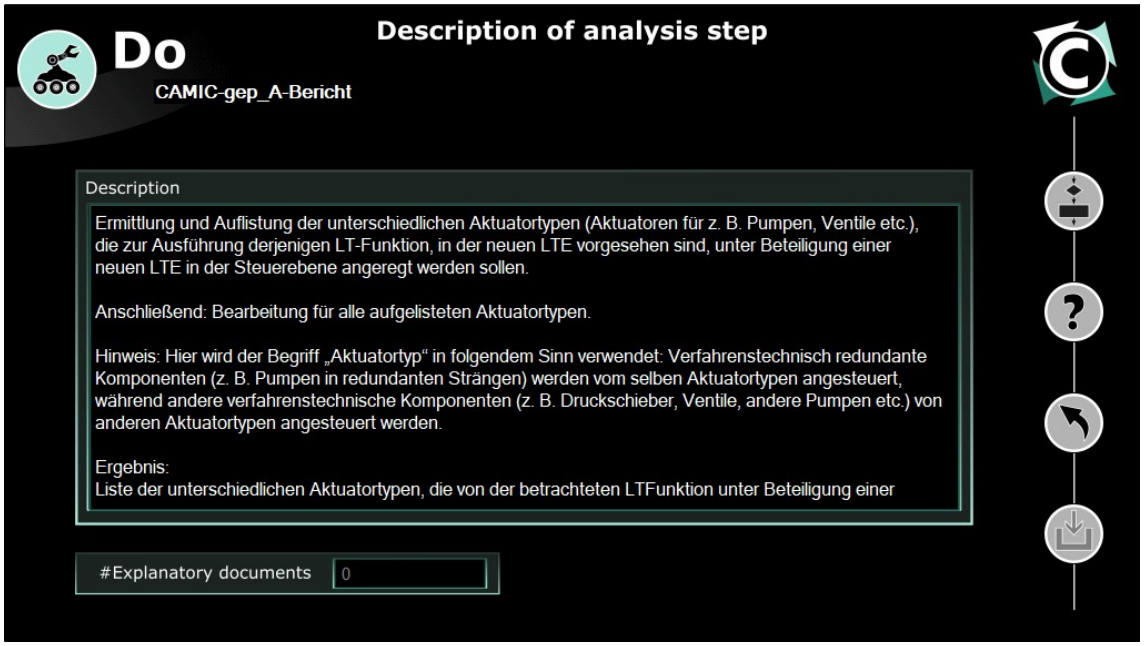


Abb. 4.9 Beschreibung der durchzuführenden Analyse

Nach der Durchführung des Analyseschritts, können die Ergebnisse unter *Edit results* (Abb. 4.10) importiert (z. B. Word-, Excel-, PDF-, TXT-Dateien) werden.

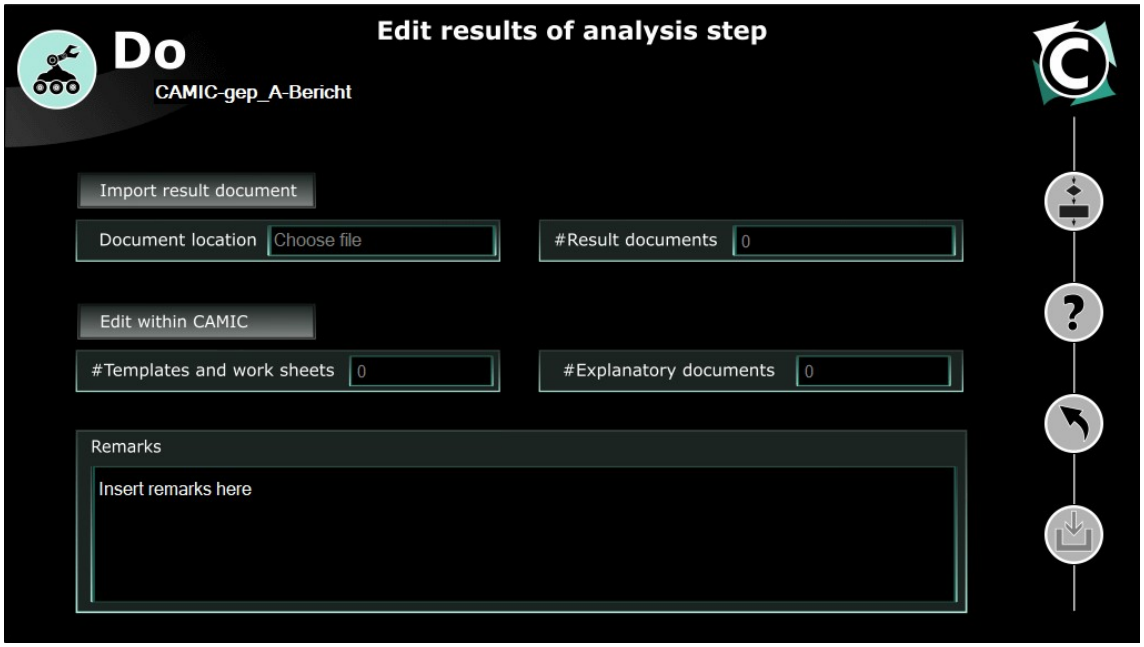


Abb. 4.10 Eintragen der Zwischenergebnisse aus der Analyse

Diese Ergebnisse werden dann als Zwischenergebnisse in der Datenbank abgelegt. Die Funktion *Edit within CAMIC* wurde an dieser Stelle noch nicht umgesetzt. In zukünftigen Versionen der CAMIC-Anwendung soll hier die Möglichkeit bestehen, direkt zu

implementierten Analysemethoden, wie Beispielsweise der Diversitätsmatrix, weitergeleitet zu werden.

Der obere Button in der Navigationsleiste (siehe Abb. 4.8, Abb 4.9 und Abb. 4.10) öffnet eine Übersicht aller durchgeführten Teilschritte des kompletten Projekts (Abb. 4.11).

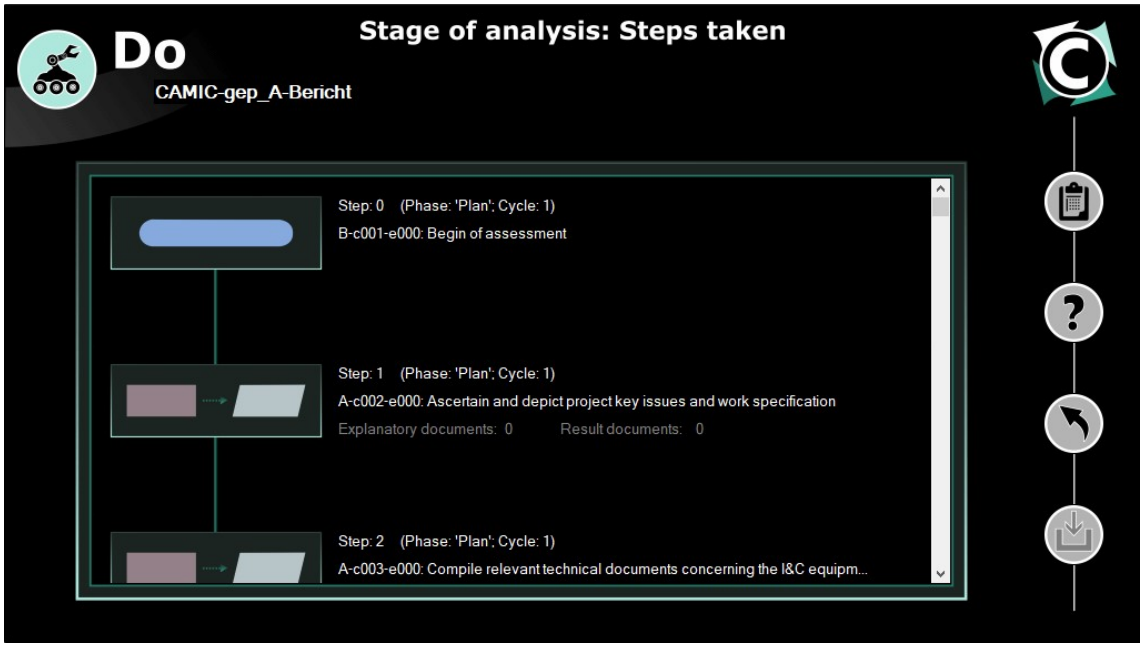


Abb. 4.11 Übersicht aller durchgeführter Teilschritte inklusive verknüpfter Dokumente

In der Übersicht werden außerdem alle verknüpften Dokumente angezeigt.

Über das Ausgangsfenster des Teilschritts (Abb. 4.8) kann durch die Schaltfläche *Go to next step* der Teilschritt abgeschlossen werden. Anschließend wird dieser Schritt als abgeschlossen angezeigt und der nächste Teilschritt wird geöffnet. Ein Zurückkehren zu diesem Teilschritt ist dann aber nicht mehr möglich, damit die Konsistenz der CAMIC-Methode sichergestellt wird. Veränderungen an einem abgeschlossenen Teilschritt erfordern einen erneuten Durchlauf des PDCA-Zyklus.

4.1.6.1.1.2 Entscheidungskriterien

Der Teilschritt *Entscheidungskriterium* wird in Abb. 4.12 gezeigt. Der Aufbau dieses Fensters ähnelt dem der Analyseschritte. Jedoch entfällt die Funktionalität zum Abspeichern der Zwischenergebnisse, da bei einem Entscheidungskriterium keine Zwischenergebnisse erzielt werden. Zunächst befindet sich die Beschreibung des Entscheidungskriteriums wieder unter *Descriptions.* Jedes Entscheidungskriterium repräsentiert eine Frage an den Benutzer, der die Bewertung durchführt. Die Antwort auf diese Frage kann

nur mit Ja oder Nein beantwortet werden. Zum Beantworten dieser Frage stehen auf der Benutzeroberfläche zwei Schaltflächen für Ja und Nein zur Verfügung. Durch den Benutzer muss nun das jeweilige Feld aktiviert werden. Erst nach Beantwortung der Frage des Entscheidungskriteriums ist der unmittelbar auf das Entscheidungskriterium folgende Analyseschritt festgelegt. Daher ist es erst dann möglich, zum nächsten Teilschritt des Bewertungsprozesses zu gelangen. Dazu wurde erneut der Button *Go to next step* implementiert.

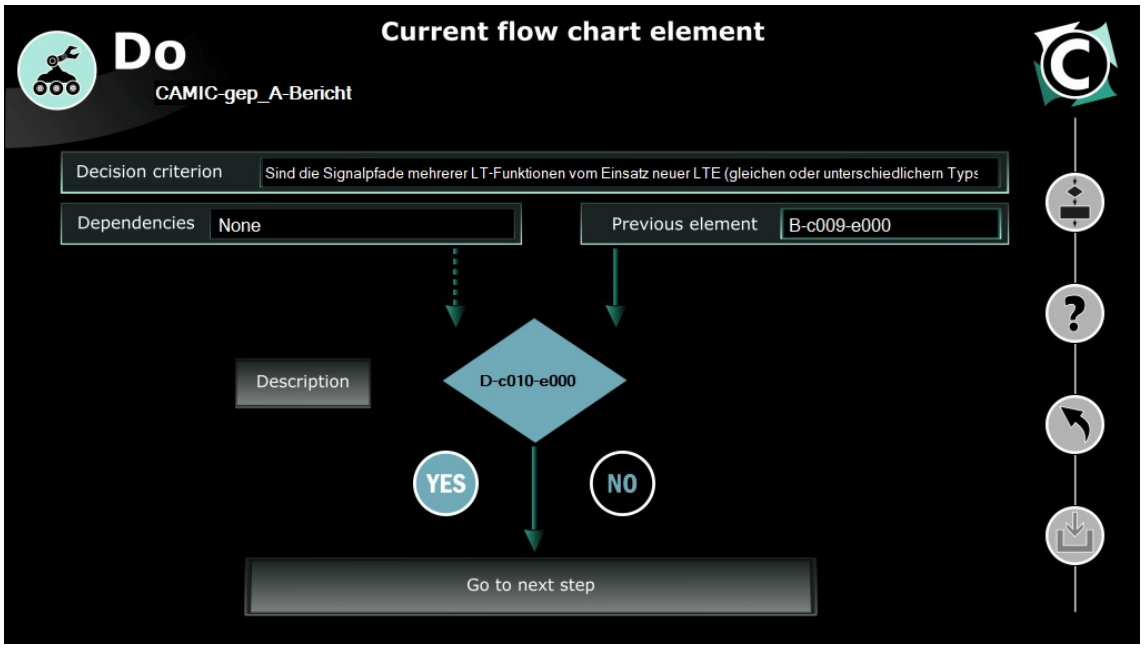


Abb. 4.12 Ausgangsfenster des Teilschritts *Entscheidungskriterium* der implementierten CAMIC-Methode

4.1.6.1.1.3 Übergangsschritt

Der letzte Teilschritt der implementierten CAMIC-Methode ist der *Übergangsschritt* (Abb. 4.13).

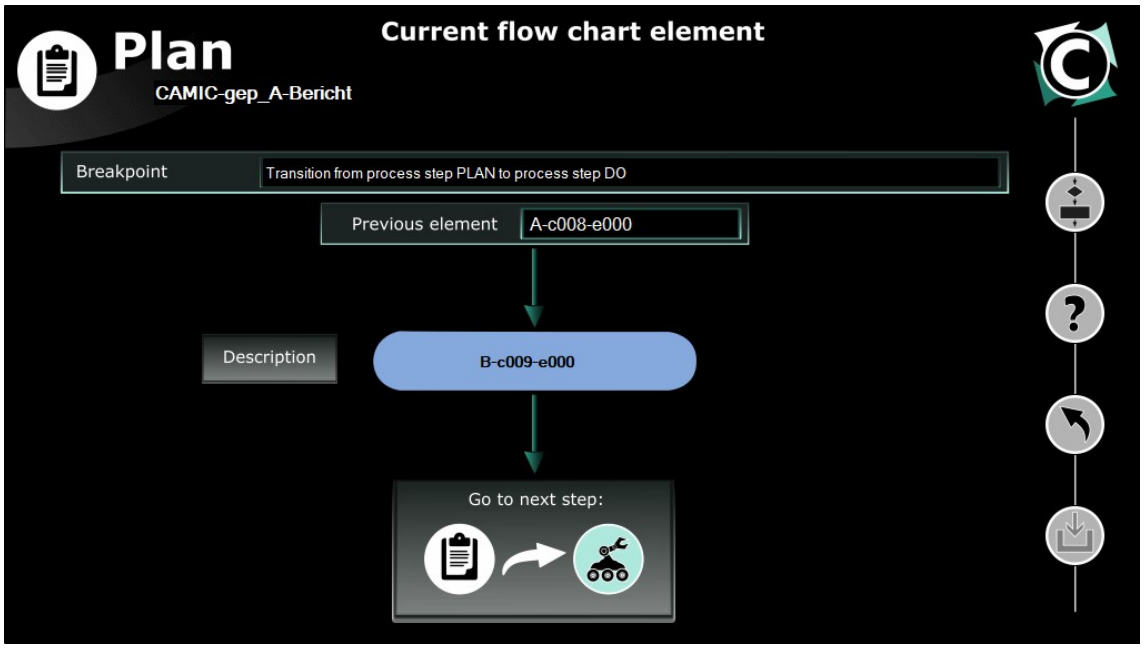


Abb. 4.13 Ausgangsfenster des Teilschritts *Übergangsschritt* der implementierten CAMIC-Methode

Dieses Fenster führt den Anwender zum nachfolgendem Prozessschritt des PDCA-Zyklus und schließt den aktuellen Prozessschritt ab.

4.1.6.1.2 Flow chart overview

Wie der Name schon sagt, wird der Anwender hier auf eine Übersicht des PLAN-Flussdiagramms geführt. Die Darstellung der Flussdiagramme erfolgt grafisch mit der Möglichkeit, dass sich der Nutzer Informationen zu den Schritten des aktuellen Flussdiagramms ausgeben lassen kann. Eine Übersicht über die Flussdiagramme wird vom jeweiligen Ausgangsfenster der CAMIC-Prozessschritte aufgerufen. Die Abb. 4.14, Abb. 4.15, Abb. 4.16 und Abb. 4.17 zeigen die Darstellung aller Flussdiagramme der CAMIC-Prozessschritte.

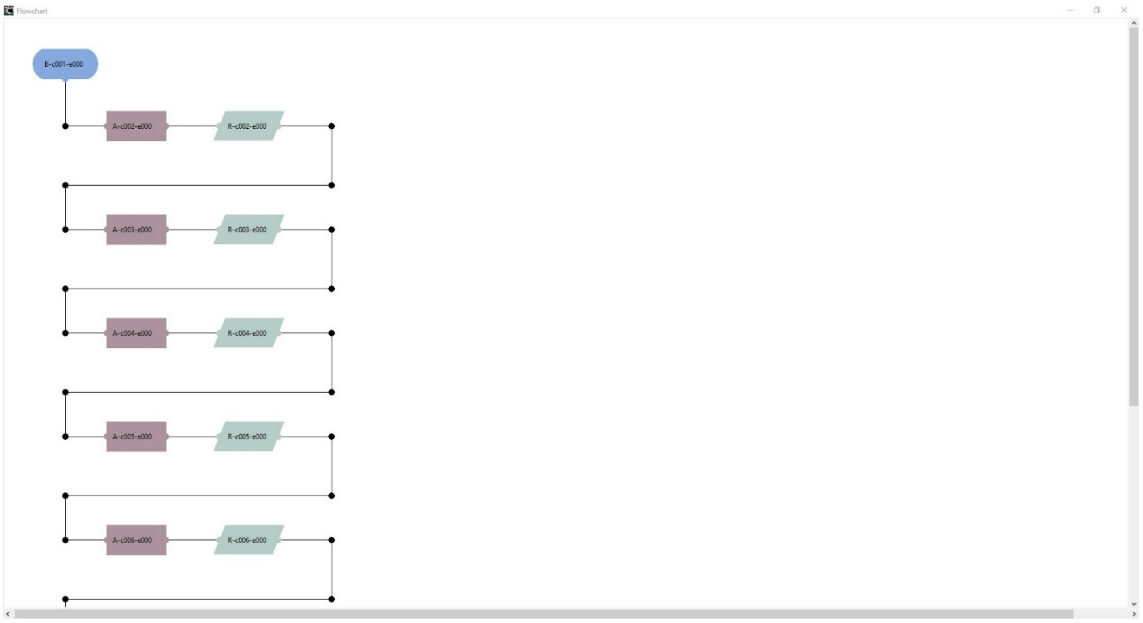


Abb. 4.14 Darstellung eines Ausschnitts des Flussdiagramms des CAMIC-Prozessschritts PLAN

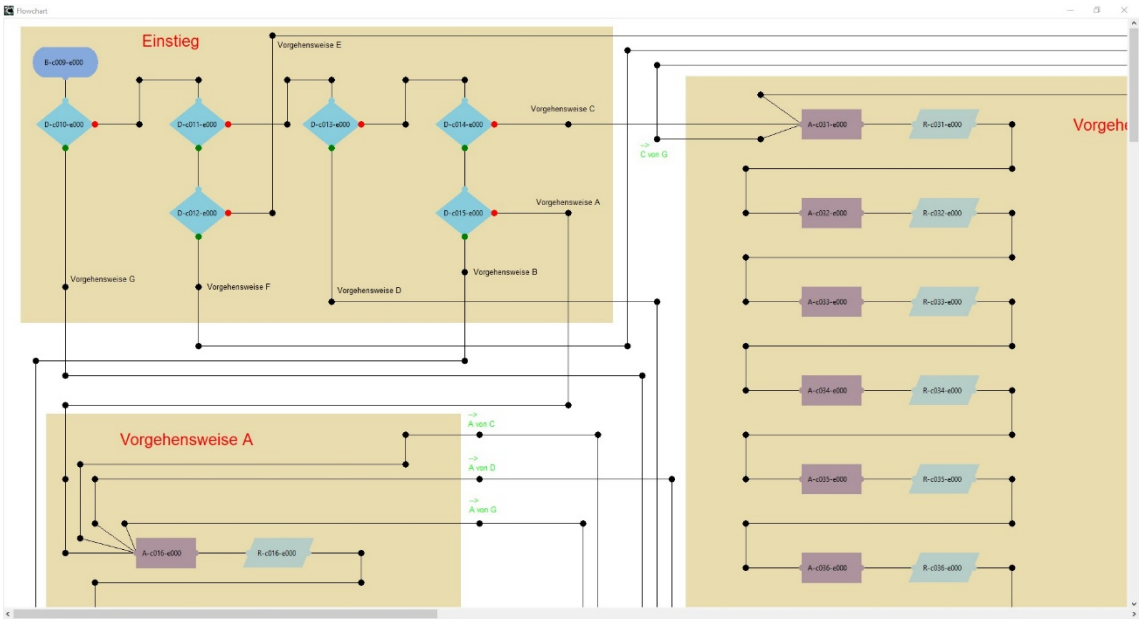


Abb. 4.15 Darstellung eines Ausschnitts des Flussdiagramms des CAMIC-Prozessschritts DO

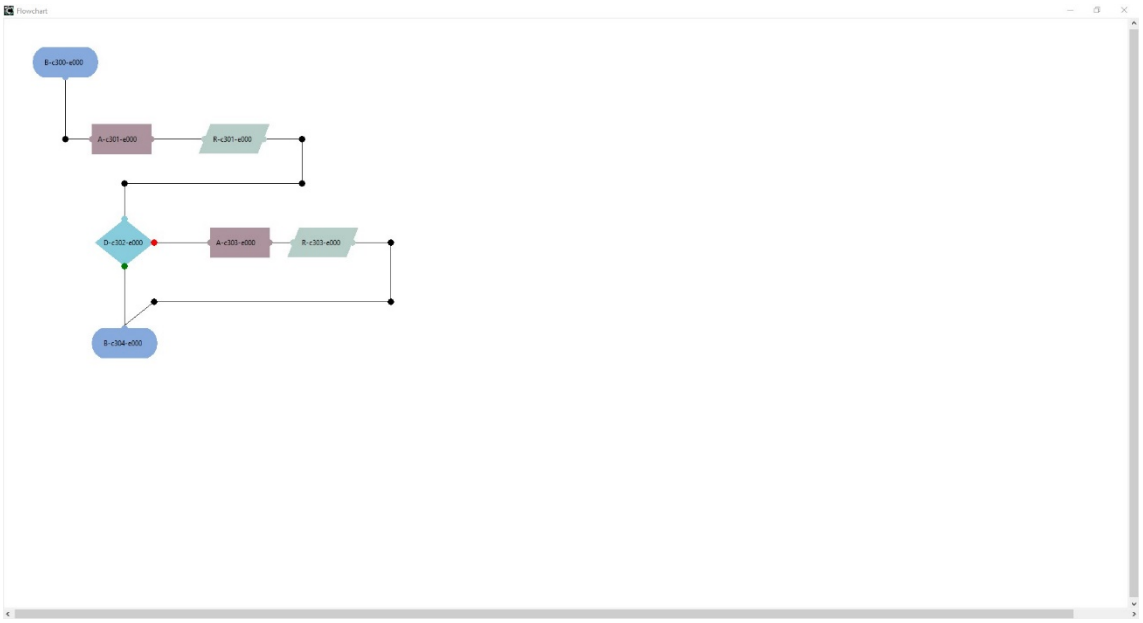


Abb. 4.16 Darstellung des Flussdiagramms des CAMIC-Prozessschritts CHECK

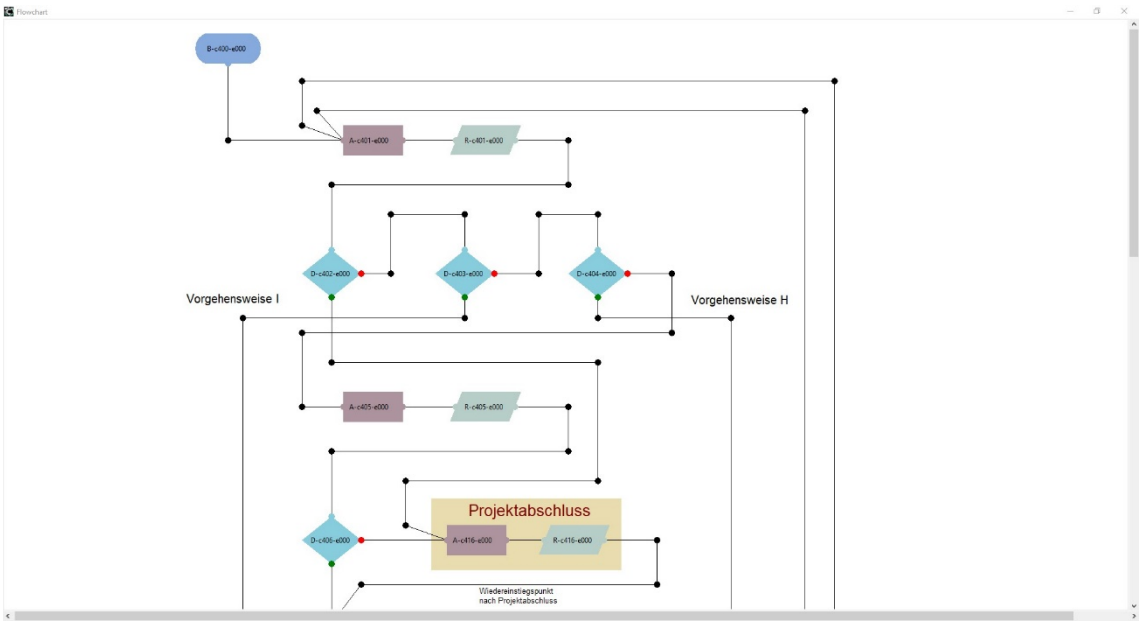


Abb. 4.17 Darstellung eines Ausschnitts des Flussdiagramms des CAMIC-Prozessschritts ACT

Die Elemente in dieser Darstellung wurden intuitiv gestaltet. Der Nutzer hat die Möglichkeit durch einen Doppelklick auf eines der Elemente, eine Beschreibung des Teilschritts zu öffnen. In Abb. 4.18 wird diese Funktion beispielhaft für das Flussdiagramm des CAMIC-Prozessschritts PLAN dargestellt.

Abb. 4.18 Darstellung eines Ausschnitts des Flussdiagramms des CAMIC-Prozessschritts PLAN mit geöffneter Beschreibung

4.1.6.1.3 Interim results

In diesem Fenster der CAMIC-Anwendung werden die Zwischenergebnisse der CAMIC-Methode aufgelistet (Abb. 4.19).

Alle Informationen zu den Zwischenergebnissen werden hier übersichtlich und kompakt dargestellt. Aufgelistet wird die Bezeichnung des Analyseschritts, eine Beschreibung des Analyseschritts, eingetragene Kommentare und das Zwischenergebnis. Auch hier ist nicht relevant, ob die Interim results vom Ausgangsfenster der Prozessschritte PLAN, DO, CHECK oder ACT aufgerufen werden, hier werden die Zwischenergebnisse aller Prozessschritte aufgelistet.

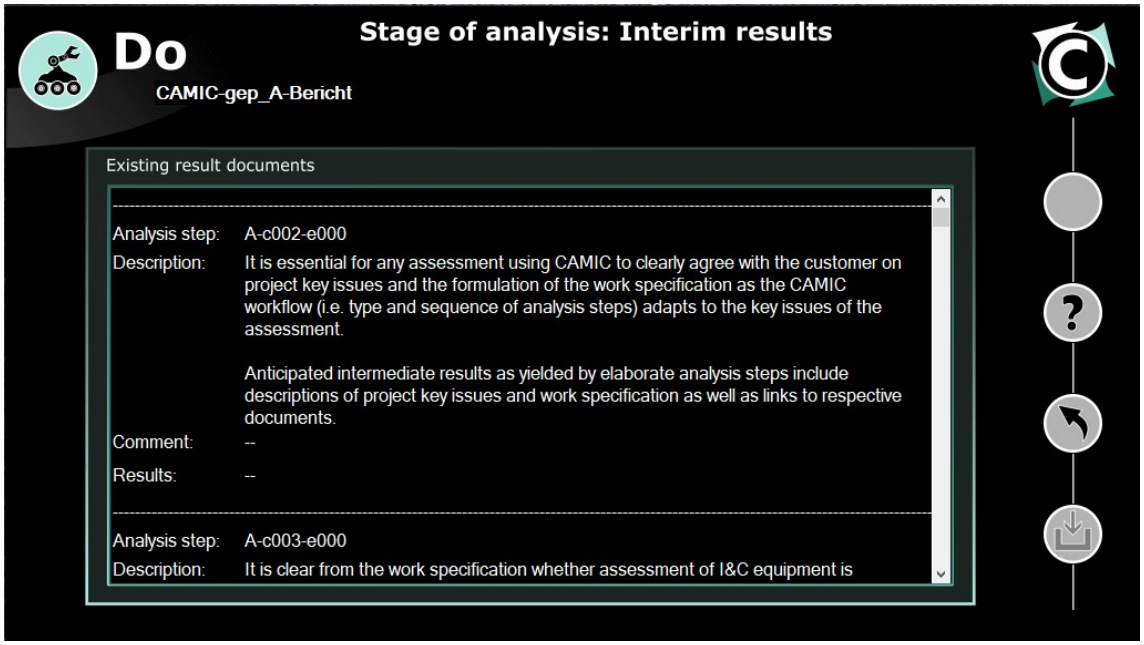


Abb. 4.19 Auflistung der Zwischenergebnisse

4.1.6.1.4 Document data

Aufbauend auf der Realisierung der Themensuchen innerhalb der CAMIC-Anwendung ist hier die Durchführung der Themensuchen für die ausgewählten Normen nach den zuvor festgelegten Kriterien erfolgt. Die dabei ermittelten Anforderungen zu den einzelnen Themen müssen in der CAMIC-Anwendung erfasst und entsprechend kodiert werden. Neben der Erfassung, Kodierung und Anzeige von Anforderungen und weiteren Textstellen mit Bezug zu einem der festgelegten Themen ist auch die Selektion und automatisierte Ausgabe von relevanten Anforderungen implementiert worden.

Für die zuvor ausgewählten Normen wurden die Themensuchen zu allen festgelegten Themen *Einzelfehlerkriterium*, *Redundanz*, *CCF*, *Diversität*, *Programmierbare und rechnerbasierte Geräte* sowie *Instandhaltung* durchgeführt. Entsprechend der im Vorhaben erarbeiteten Kriterien für jede Themensuche wurden Anforderungen, Definitionen, weitere Zitate und Abbildungen in der CAMIC-Anwendung erfasst und kodiert. Dabei können diejenigen ausgewählten Normen und Regelwerke, die sowohl in deutscher als auch in englischer Sprache vorliegen, in beiden Sprachen erfasst werden. Hierbei wurden die Kriterien für die Themensuchen in deutschen bzw. englischen Dokumenten so lange überarbeitet und verfeinert, bis für jedes Thema beide Sprachvarianten der Kriterien zur Identifikation übereinstimmender Anforderungen, Definitionen, Zitate und Abbildungen mit Bezug zum gewählten Thema führten. Sind Dokumente mit bestimmten Themen verknüpft, können diese bei der Suche nach einem bestimmten Thema gefiltert werden.

Die Benutzeroberfläche *Selection of document data* (Abb. 4.20) dient der Anzeige aller in der Datenbank erfassten Dokumente aller Projekte, bei denen aktuelle Nutzer zumindest Leserechte hat, und der Auswahl von projektrelevanten Dokumenten. Sie wird von der Benutzeroberfläche „PLAN“ über die Schaltfläche *document data* erreicht.

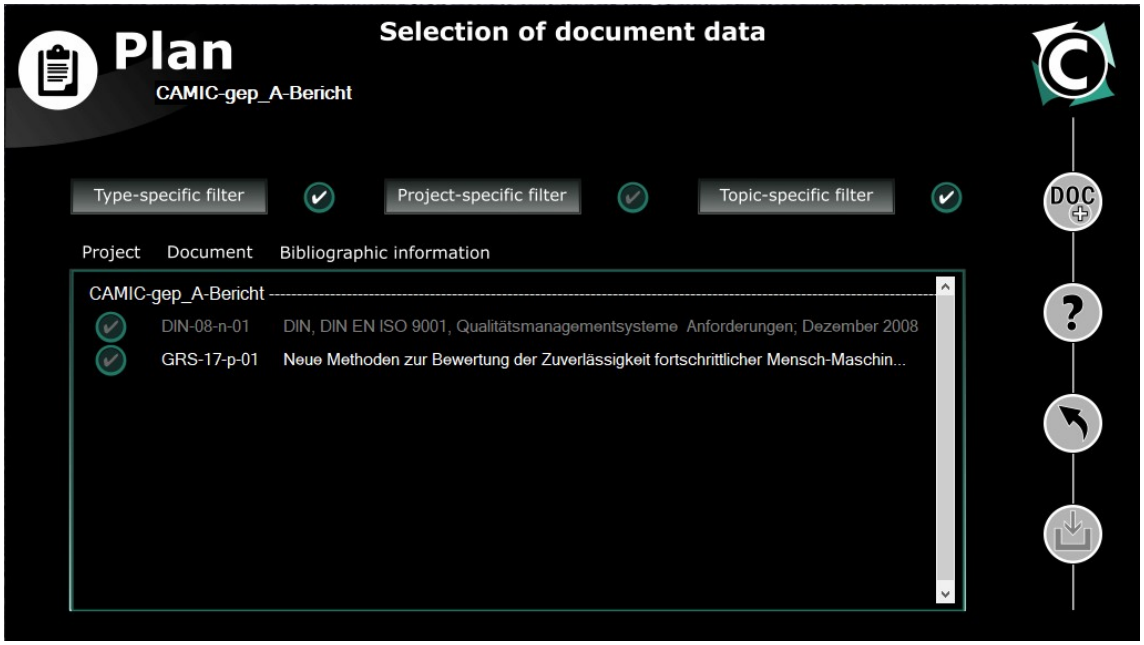


Abb. 4.20 Auflistung der in der Datenbank erfassten Dokumente aller dem Nutzer zugewiesener Projekte

Für eine bessere Übersichtlichkeit wurden Filter implementiert. Gefiltert werden kann nach Dokumententyp, Projekt oder Thema. Es ist möglich, alle Dokumente nach bestimmten Themen zu durchsuchen. Über die Schaltfläche *DOC+* in der Navigationsleiste können neue Dokumente der CAMIC-Datenbank hinzugefügt werden. Dazu öffnet sich eine dafür vorgesehene Eingabemaske (Abb. 4.21), in welcher alle relevanten Informationen eingegeben werden können.

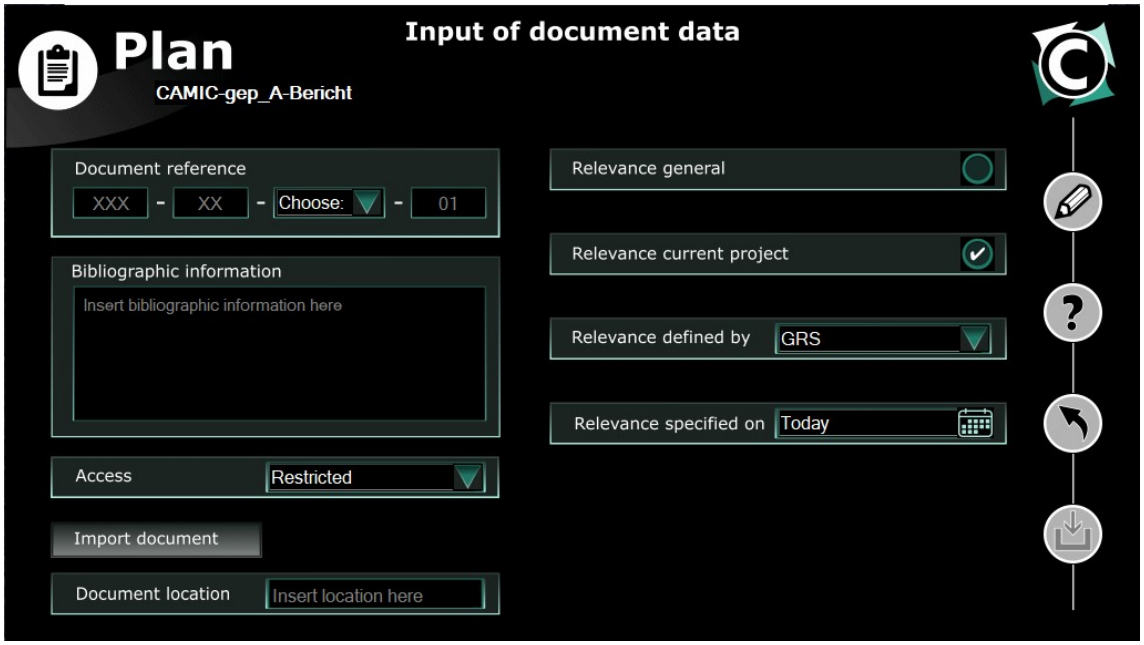


Abb. 4.21 Eingabemaske für das Verknüpfen von projektbezogenen Dokumenten

Allen in der Datenbank erfassten Dokumenten ist ein Dokumententyp zugeordnet (möglich sind bislang 14 unterschiedliche Typen von Dokumenten). Diese sind in Tab. 4.1 aufgelistet.

Tab. 4.1 Auflistung der verschiedenen Dokumententypen

Dokumententyp	Beschreibung
(b)ook	Bücher
(c)ontracts	Verträge und andere vertragliche Dokumente
(d)ata	Datenblätter und allgemeine Herstellerinformationen
(f)urther	Weitere Dokumente, die unter keine der anderen Kategorien zu finden ist.
(i)ncident	Vorkommnismeldungen und WLNs
(j)ournal	Artikel
(l)etter	Korrespondenz (auch elektronisch)
(m)emo	Memos und Meetingprotokolle
(n)ormative	Normative Dokumente
(o)ffer	Angebote
(p)roject	Projektberichte, Kurzberichte, Checklisten, Exceltabellen
(r)eport	Stellungnahmen und Gutachten
(t)echnical	Technische Berichte
(w)eb	Internet

Außerdem wurde die Möglichkeit vorgesehen, ein Dokument als vertraulich oder nicht vertraulich zu deklarieren. Ist ein Dokument vertraulich – entweder aus Gründen des Geheimschutzes (z. B. VS-NfD, VS-V) oder aus anderen Gründen (z. B. Betriebsgeheimnisse) – ist es nicht möglich, das Dokument direkt in der Datenbank abzulegen, es kann aber ein physischer Ablageort angegeben werden. Als zusätzliche nützliche Funktion kann dem Dokument eine Relevanz zugeordnet werden. Damit ist das Dokument entweder nur für das aktuelle Projekt relevant und damit nicht sichtbar in anderen Projekten oder das Dokument ist für alle Projekte relevant und überall sichtbar. Generell müssen Dokumente nur ein einziges Mal in die Anwendung eingegeben werden, bereits zugefügte Dokumente können direkt mit dem aktuellen Projekt verknüpft werden. Dies führt aufgrund des laufend wachsenden Bestands an Dokumenten in der Datenbank zu einer immer ausgeprägteren Zeitersparnis bei der Erfassung projektrelevanter Dokumente in der Datenbank. Auch wird jedem Dokument eine eindeutige CAMIC-ID zugeordnet, über die das Dokument dann in allen Projekten und den darin erstellten Berichten einheitlich identifiziert werden kann.

4.1.6.1.5 Document sections and topics

Eine weitere Benutzeroberfläche, welche über das Ausgangsfenster des Prozessschritts PLAN zu erreichen ist, ist *Document information* (Abb. 4.22). In diesem Fenster kann ein bestehendes Dokument für eine weitere Verarbeitung ausgewählt werden.

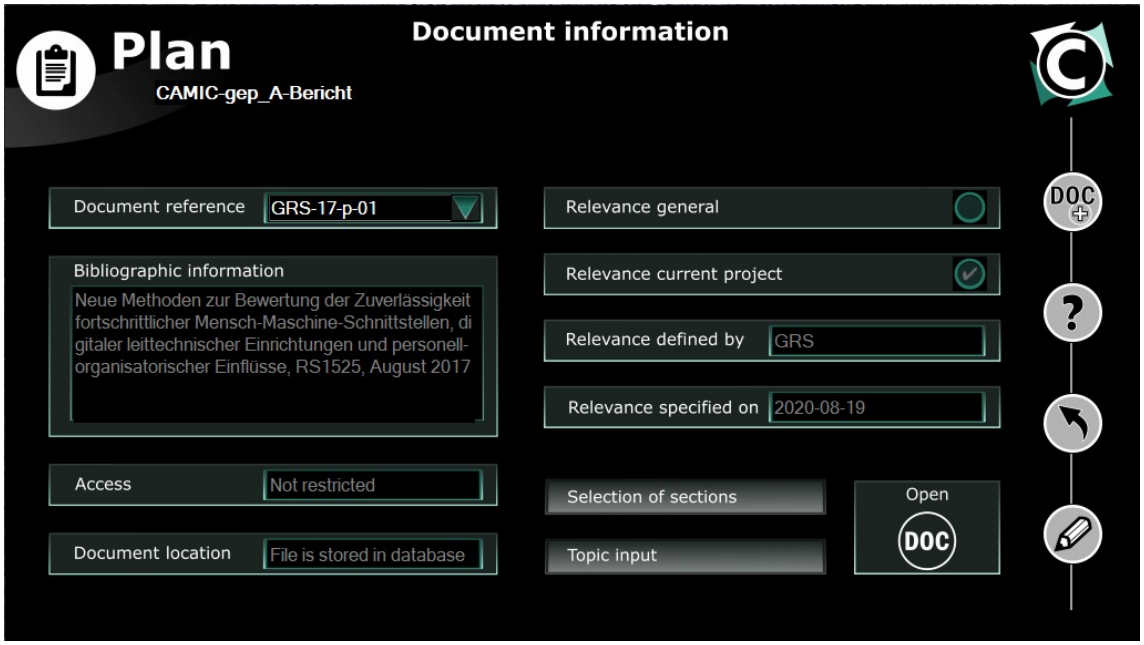


Abb. 4.22 Benutzeroberfläche zum Bearbeiten projektbezogener Dokumente

Ist zum gewählten Dokument eine Datei in der Datenbank hinterlegt, kann diese unter *Open DOC* mit der Standardanwendung geöffnet werden. Andernfalls wird der aktuelle physische Ablageort in einem Dialog ausgegeben. In der Benutzeroberfläche *Selection of sections* werden erfasste Abschnitte für das gewählte Dokument angezeigt (Abb. 4.23).

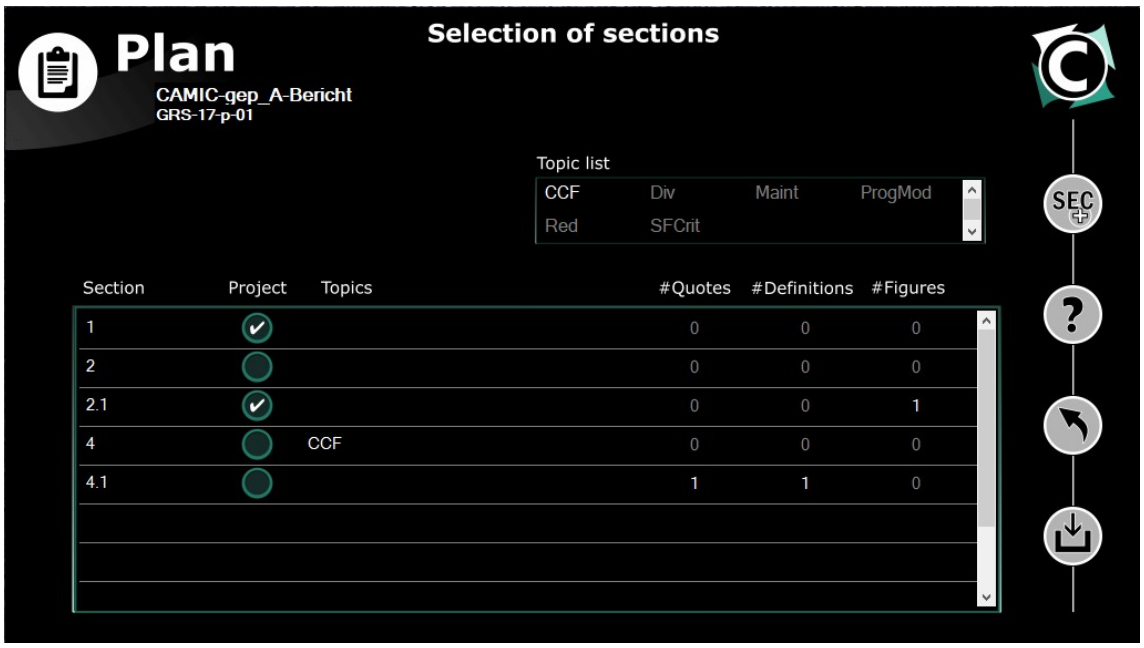


Abb. 4.23 Hier können einzelne Abschnitte eines zuvor ausgewählten Dokuments hinzugefügt werden

Hier besteht die Möglichkeit, einzelne Abschnitte des Dokuments für die Themensuche zuzuordnen. Die Erfassung weiterer Abschnitte erfolgt über die Benutzeroberfläche *Section input* welche über die Schaltfläche *SEC+* erreichbar ist (Abb. 4.24).

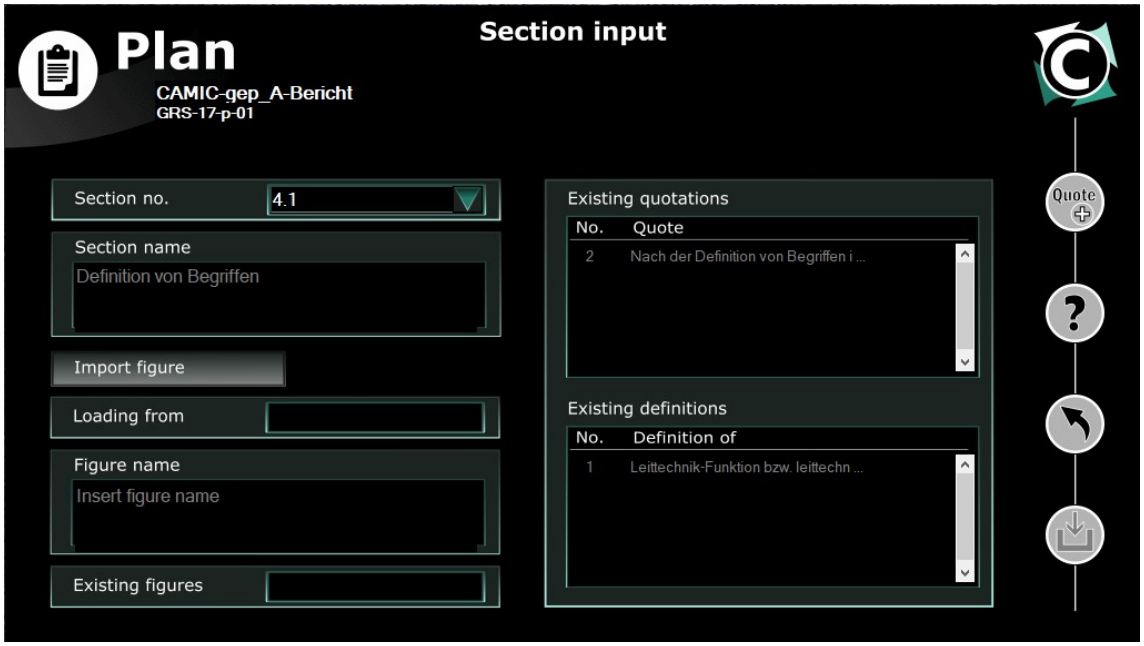


Abb. 4.24 Oberfläche zum Verknüpfen von Abbildungen, Zitaten und Definitionen

In Section input können zum ausgewählten Abschnitt Abbildungen (*Import figure)*, Zitate oder Definitionen (*Quote+*) eingetragen und zur Datenbank hinzugefügt werden.

4.1.6.1.6 Document overview

Der letzte Button *Document overview* öffnet eine übersichtliche, kompakte Liste aller projektrelevanten und für den Nutzer sichtbaren Dokumente (Abb. 4.25).

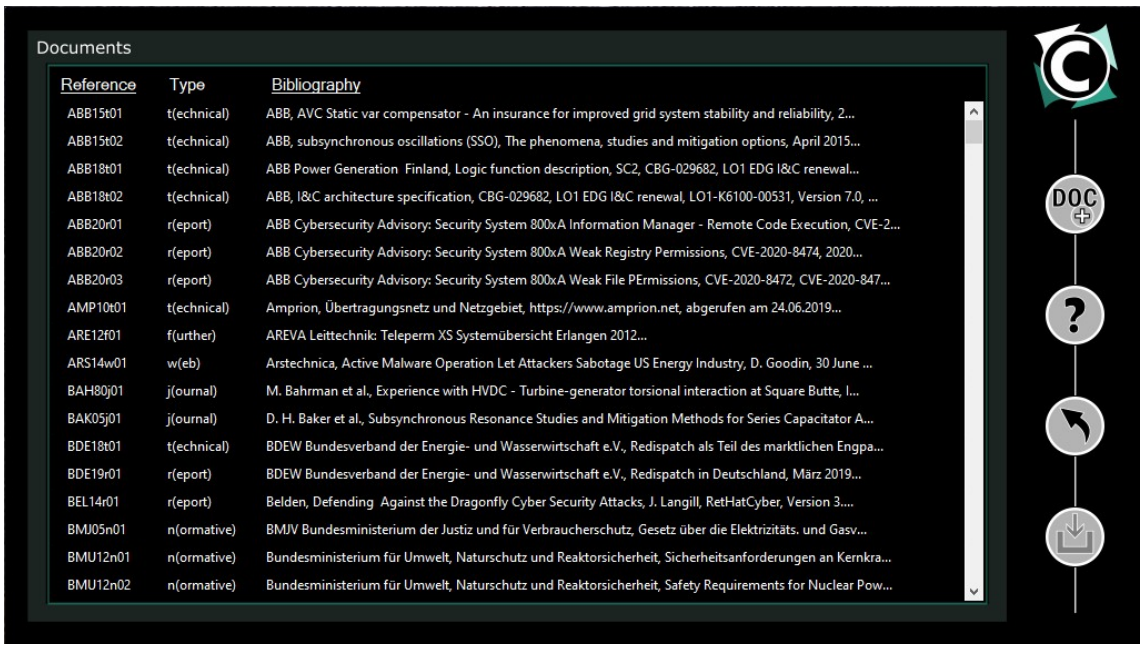


Abb. 4.25 Auflistung aller Dokumente

4.1.6.2 DO

Die Umsetzung des CAMIC-Prozessschritts DO ist in Abb. 4.26 dargestellt.

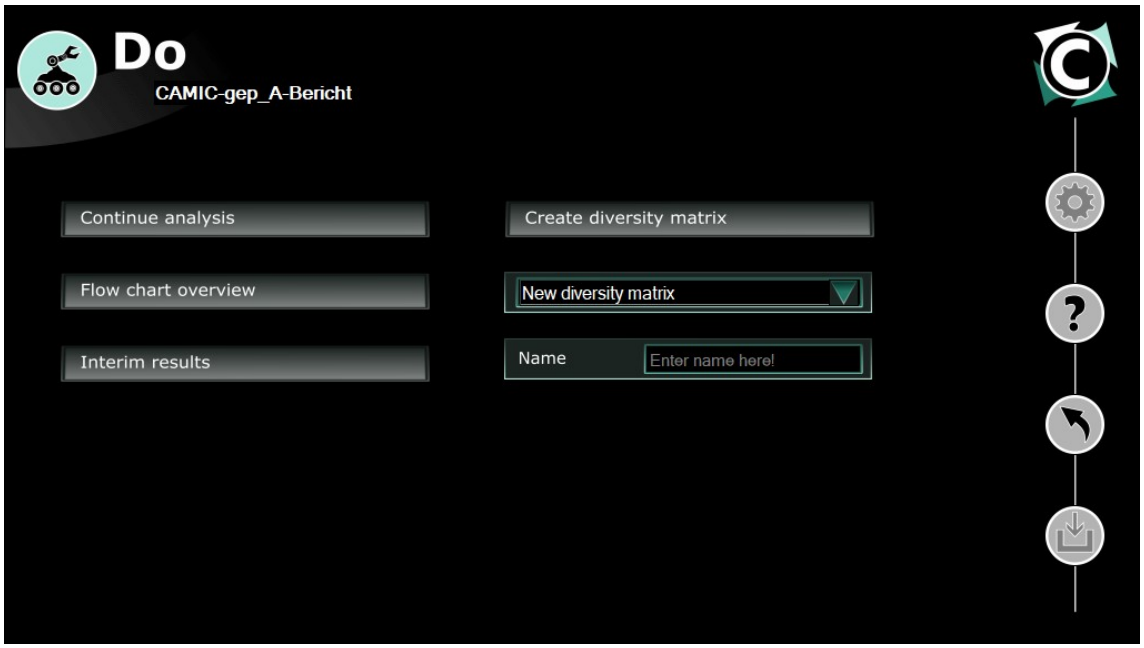


Abb. 4.26 Ausgangsfenster des CAMIC Prozessschritts DO

Die Buttons *Continue analysis, Flow chart overview und Interim results* wurden bereits erläutert. Auf dieser Benutzeroberfläche besteht darüber hinaus die Möglichkeit eine bestehende Diversitätsmatrix auszuwählen. Nachdem eine bestehende Diversitätsmatrix aus dem Dropdown Menü ausgewählt wurde, ändert sich der *Create diversity matrix Button* zu *Work on diversity matrix* (Abb. 4.27).

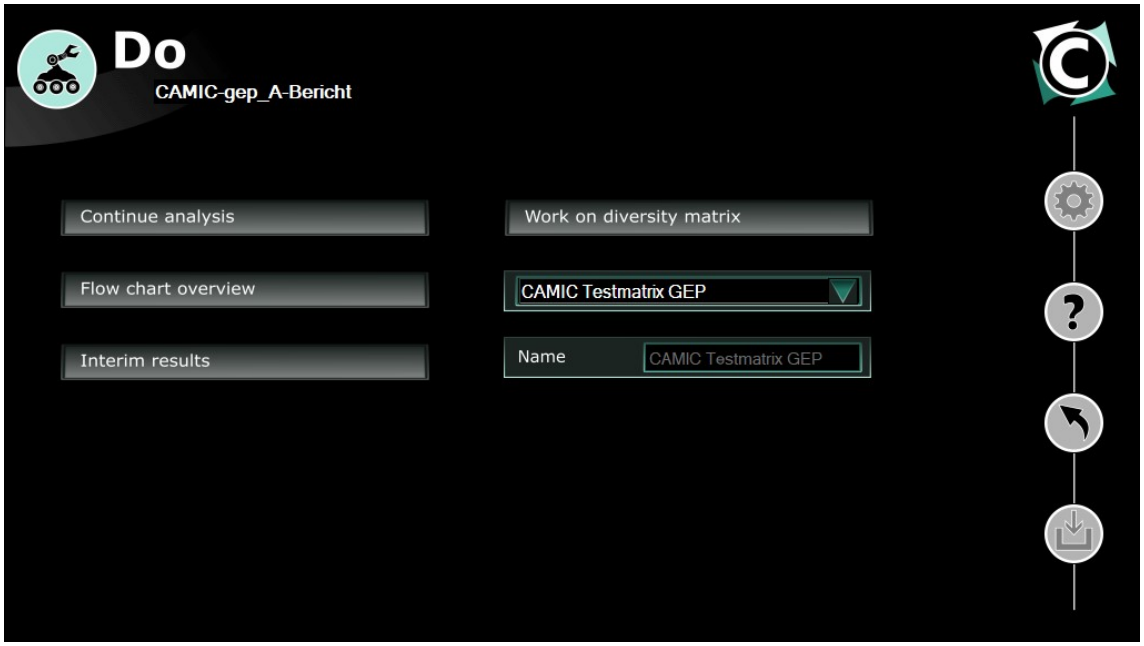


Abb. 4.27 Ausgangsfenster des CAMIC Prozessschritts DO mit ausgewählter Matrix

Mit diesen beiden genannten Schaltflächen wird der Nutzer auf die Benutzeroberfläche der Diversitätsmatrix weitergeleitet.

4.1.6.2.1 Diversitätsmatrix

Ein weiterer wesentlicher Aspekt bei der Bewertung rechnerbasierter oder programmierbarer Leittechnik ist die Betrachtung der Diversität. Je nach Fragestellung sind unterschiedliche Diversitätsmerkmale relevant. Die gesamte, von der GRS entwickelte Diversitätsmatrix für programmierbare und rechnerbasierte, leittechnische Einrichtungen findet als Teil der CAMIC-Toolbox Eingang in die Anwendung. Die Diversitätsmatrix ist im ersten Schritt als Datenbank hinterlegt. Innerhalb der Anwendung werden Abfragen realisiert, die zum einen die Selektion relevanter Diversitätsmerkmale und zum anderen die Charakterisierung der zu betrachtenden Leittechnik erlauben. Darauf aufbauend erfolgt die automatisierte Erstellung der bewertungsspezifischen Diversitätsmatrix. Ebenfalls ist eine Funktionalität, welche die Erstellung eines Dokuments mit einer Übersicht sowie Beschreibungen der für die aktuelle Bewertung relevanten Diversitätsmerkmale enthalten.

In der Oberfläche der Diversitätsmatrix können Merkmale der ausgewählten Diversitätsmatrix und Bestandteile des Leittechniksystems angegeben werden (Abb. 4.28).

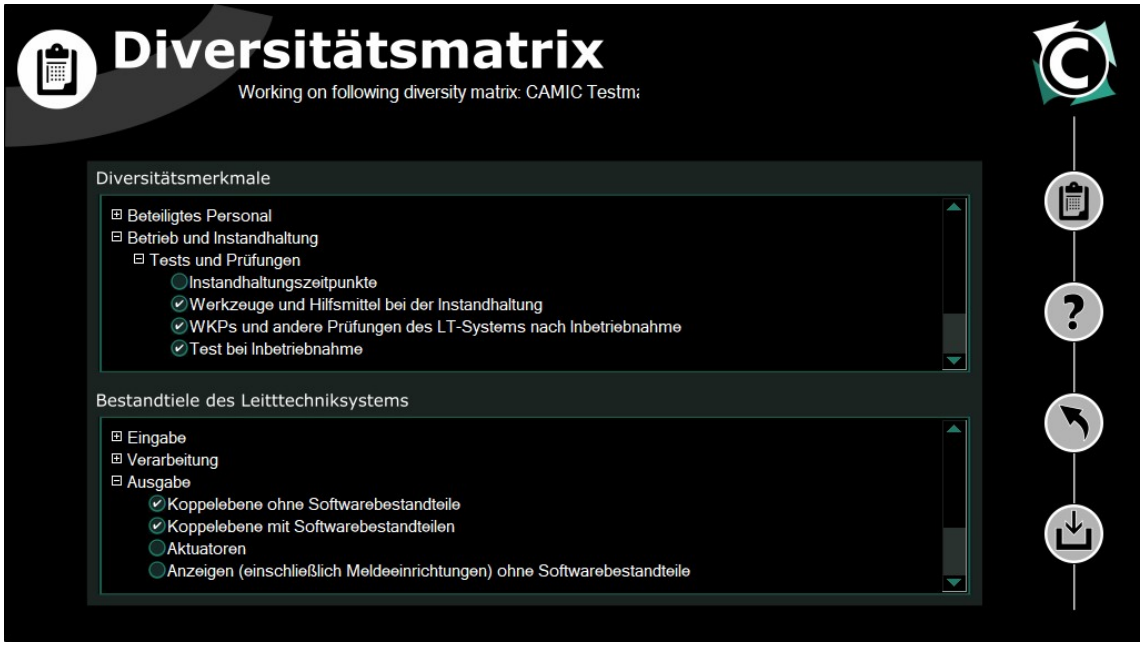


Abb. 4.28 Benutzeroberfläche zum Bearbeiten der Spalten und Zeilen der Diversitätsmatrix

Von diesem Fenster aus ist eine Darstellung der Matrix über den obersten Button der Navigationsleiste erreichbar (Abb. 4.29).

Abb. 4.29 Darstellung der Diversitätsmatrix

Innerhalb der dargestellten Diversitätsmatrix ist eine Bearbeitung der Einträge direkt in den Spalten und Zeilen der Matrix realisiert. Ebenfalls realisiert wurde das Öffnen der Diversitätsmatrix in dem Standard Tabellenkalkulationsprogramm des Nutzers. Diese

Funktion wurde in dem obersten Button der Navigationsleiste implementiert. Nähere Informationen zur Diversitätsmatrix werden in Abschnitt 4.1.6.2.1 erläutert.

4.1.6.3 CHECK und ACT

Die Ausgangsbenutzeroberflächen der CAMIC-Prozessschritte CHECK und ACT sind an Abb. 4.30 bzw. Abb. 4.31 dargestellt.

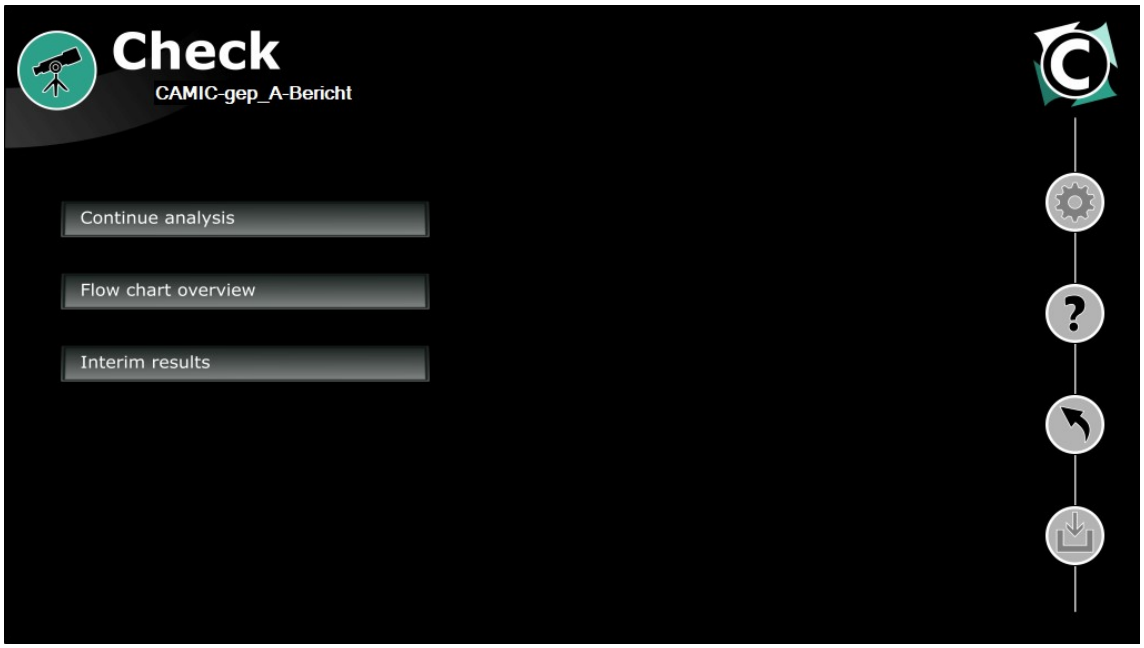


Abb. 4.30 Ausgangsfenster des CAMIC-Prozessschritts CHECK

Abb. 4.31 Ausgangsfenster des CAMIC-Prozessschritts ACT

Die hier angebotenen Funktionen wurden bereits in Abschnitt 4.1.6.1 erläutert. Daher wird an dieser Stelle nicht erneut darauf eingegangen.

4.1.7 Ausgabe der durchgeführten Bewertung

Die konsistente und nachvollziehbare Gestaltung des Bewertungsprozesses mit der CAMIC-Anwendung ist ein weiterer, wichtiger Aspekt. Hierzu ist in der CAMIC-Anwendung eine Funktionalität für die strukturierte Dokumentation des Bewertungsprozesses innerhalb der Anwendung sowie die Ausgabe von relevanten Informationen zum Bewertungsprozess implementiert worden. Es wurden eine detaillierte Konzeptionierung der Benutzerschnittstellen und Funktionalitäten für die strukturierte Dokumentation des Bewertungsprozesses innerhalb der Anwendung sowie die Ausgabe von relevanten Informationen zum Bewertungsprozess umgesetzt.

CAMIC ist so konzipiert, dass die Durchführung der Bewertung und die einzelnen Zwischenergebnisse klar strukturiert dokumentiert werden. Diese Dokumentation steht nach der Bewertung dem Nutzer flexibel zur Verfügung. Dafür wurde in der CAMIC-Anwendung die Möglichkeit geschaffen, eine automatisierte Berichterstellung durchzuführen. Der generierte Bericht enthält alle wichtigen Informationen, die für die Bewertung der LTE wichtig sind. Die Ausgabemaske (Abb. 4.32) ist über den obersten Button in der Navigationsleiste auf der Hauptseite der CAMIC-Anwendung erreichbar.

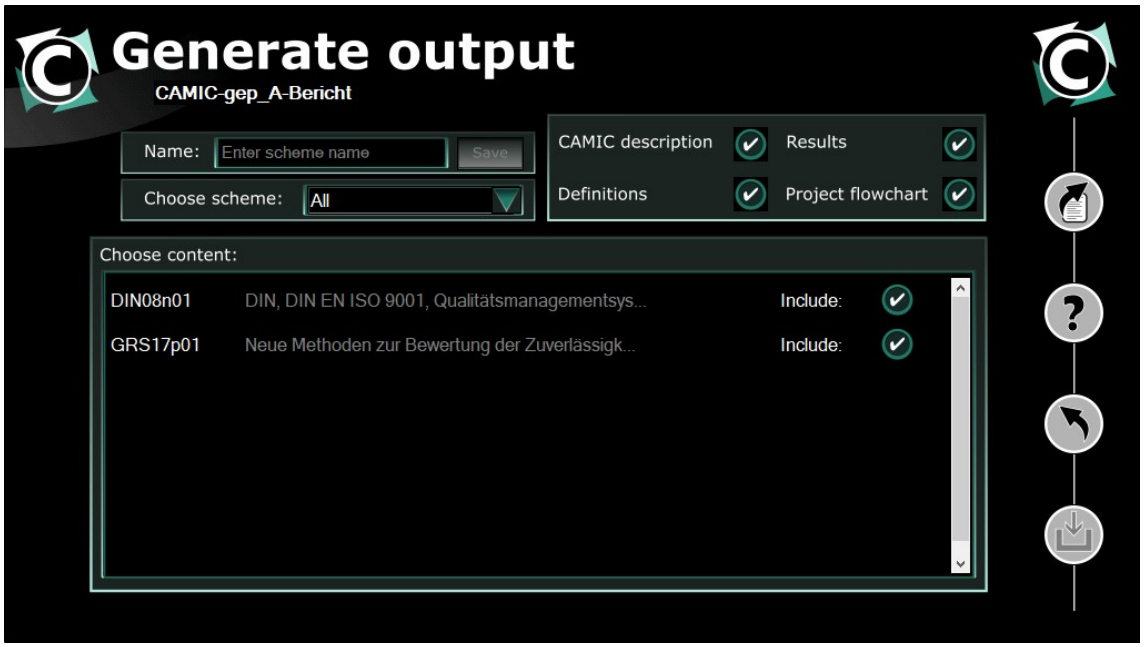


Abb. 4.32 Ausgabemaske der CAMIC-Anwendung

Das Anlegen und die Verwendung von Ausgabeformaten in der Benutzeroberfläche der CAMIC-Ausgabe beschleunigt die Erstellung eines Dokumentes. Eine Selektion der auszugebenden Kategorien wurde zusätzlich implementiert. Die anwählbaren Kategorien sind:

- CAMIC descriptions – Beschreibung der CAMIC-Methode
- Results – Ergebnisse der Bewertung
- Definitions – Relevante Definitionen
- Projekt flowcharts – Übersicht über das ausgeführte Flowchart

Durch das Klicken auf ein Dokument in der Liste öffnet sich zudem ein Untermenü (Abb. 4.33), um einzelne Abschnitte des angewählten Dokuments selektieren zu können.

Die Ausgabe der Bewertung erfolgt als PDF, welches durch den obersten Button in der Navigationsleiste der Ausgabenmaske (Abb. 4.32 und Abb. 4.33) erzeugt wird.

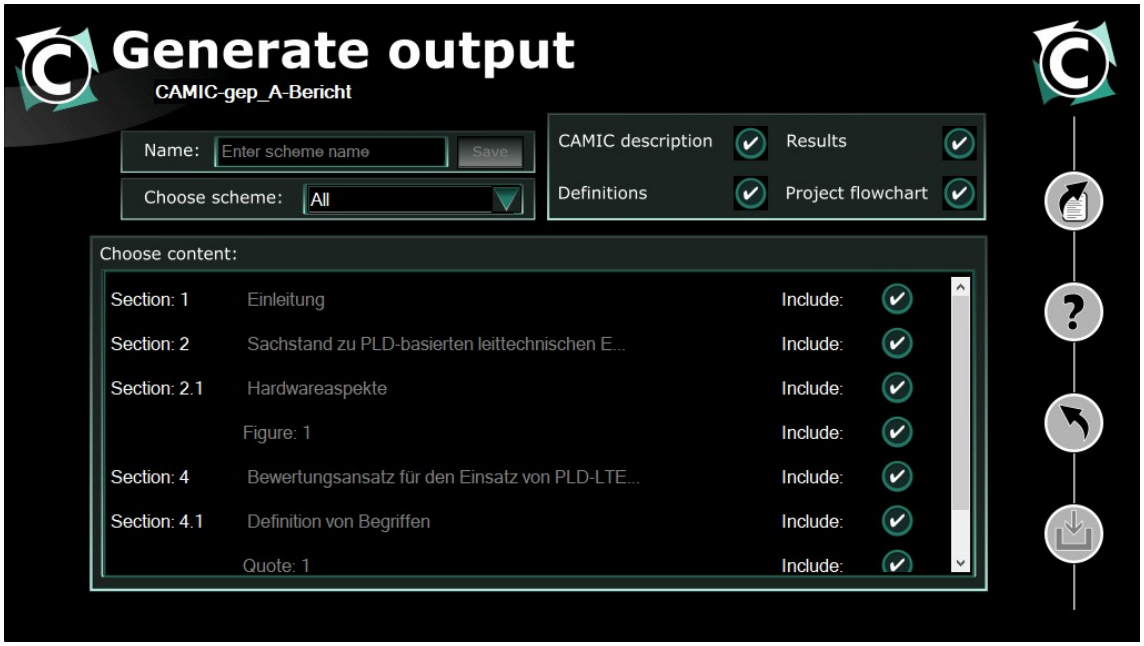


Abb. 4.33 Ausgabemaske der CAMIC-Anwendung mit geöffnetem Untermenü

4.1.8 Anbindung der CAMIC-Anwendung an die Datenbank

Für die Speicherung projektbezogener Daten und aller für die Anwendung der CAMIC-Methode notwendigen Informationen, wurde eine Datenbank aufgebaut. Als Datenbankverwaltungssystem wurde MySQL ausgewählt, da dieses als Open-Source-Software frei verfügbar und das weltweit am stärksten verbreitete relationale Datenbankverwaltungssystem ist /WIK 21/. Dementsprechend stehen unter der für die CAMIC-Anwendung verwendeten Programmiersprache Python ebenfalls frei verfügbare Module für die Verwaltung und den Zugriff auf die Daten in MySQL-Datenbanken zur Verfügung, wodurch die Umsetzung der CAMIC-Datenbank vergleichsweise wenig Aufwand erforderte.

Die relationale CAMIC-Datenbank besteht insgesamt aus 36 Tabellen. Neben der Verwaltung der rein projektbezogenen Daten, wie beispielsweise Projektinformationen, Dokumenteninformationen, etc., werden die für die CAMIC-Methode notwendigen Flussdiagramme und auch die auf die jeweiligen Projekte bezogenen Abarbeitungsstände und Ergebnisse in dieser Datenbank verwaltet. Zusätzlich werden auch Updates der CAMIC-Anwendung über diese Datenbank verteilt und installiert.

5 Modellbasierte Erprobung der Methode

Die modellbasierte Erprobung der CAMIC-Methode mit Hilfe der in diesem Vorhaben entwickelten CAMIC-Anwendung erfolgte u. a. auf Basis generischer Leittechnikmodelle und Projektszenarien. Ziel dieser Szenarien war die Prüfung, ob die Anwendung der CAMIC-Methode zu nachvollziehbaren und konsistenten Ergebnissen führt.

Um möglichst viele Aspekte der CAMIC-Methode und deren Umsetzung in der CAMIC-Anwendung zu prüfen, wurden die Projektszenarien auf Basis bzw. in Anlehnung an in der Vergangenheit durchgeführten realen Projekte entwickelt und anschließend mit der CAMIC-Anwendung zu Testzwecken bearbeitet. Als generische Leittechnikmodelle wurden hierfür insbesondere Modellsysteme aus /GRS 18/ und /GRS 21/ herangezogen.

In den nachfolgenden Abschnitten 5.1 und 5.2 werden zunächst repräsentativ zwei Projektszenarien und deren Bearbeitung zum Test der CAMIC-Methode und -Anwendung beispielhaft beschrieben. Dabei wird zusätzlich auch ein Eindruck davon vermittelt, wie die Projektabwicklung durch die CAMIC-Anwendung geführt und unterstützt wird.

Die zusammenfassende Bewertung der durchgeführten Tests befindet sich in Abschnitt 5.3 dieses Kapitels.

5.1 Beispiel: CAMIC-Test TeSys 1

5.1.1 Szenario und erwarteter Ablauf

Im Szenario CAMIC-Test TeSys 1 wurde davon ausgegangen, dass ein Auftraggeber („GRS“) eine Änderung an seiner Anlage TeSys („**Te**st**Sys**tem“) plant. Bei TeSys handelt es sich um ein nicht-sicherheitsrelevantes und vergleichsweise einfaches System aus zwei miteinander verbundenen Tanks. Aus dem höher gelegenen Tank kann über ein Ventil Wasser in den tieferliegenden Tank abgelassen werden. Umgekehrt kann aus dem tiefer gelegenen Tank Wasser über eine Pumpe in den höher gelegenen Tank gepumpt werden. Die Füllstände der beiden Tanks werden durch Füllstandssensoren (jeweils nur eine Redundanz) gemessen und durch ein Leittechniksystem überwacht, um insbesondere ein Trockenlaufen der Pumpe zu verhindern (vgl. /GRS 21/).

Der hypothetische Auftraggeber plante laut Szenario, die bisherigen Füllstandssonden durch einen anderen Typ zu ersetzen. Der Auftragnehmer sollte untersuchen, ob sich

hierdurch negative Auswirkungen auf die Zuverlässigkeit des Leittechniksystems ergeben könnten. Konkret sollte analysiert werden, ob sich durch den Austausch der Sensoren neue und daher im Leittechniksystem noch nicht berücksichtigte Ausfallarten ergeben könnten.

Vom Auftraggeber wurden die folgenden Dokumente zur Verfügung gestellt:

- Datenblatt des ursprünglichen Sensortyps,
- Datenblatt des neuen Sensortyps,
- Eine Beschreibung des Systems (Verfahrenstechnik und Leittechnik).

Aus der Beschreibung des Systems geht hervor, dass nur eine einzige Leittechnikfunktion von der geplanten Änderung betroffen war. Als Projektbeginn wurde der 01.05.2021 vereinbart, die Arbeiten sollen noch vollständig im selben Kalenderjahr erfolgen.

Die Beschreibung des Projektszenarios ist so erstellt worden, dass für die Bearbeitung nur einfache FMEA-Analysen durchgeführt werden sollten. Als Ergebnis wurde erwartet, dass sich keine neuen Ausfallarten durch die geplanten Änderungen ergeben.

5.1.2 Testdurchführung

Zunächst wurde das entsprechende Projekt in der CAMIC-Anwendung angelegt und, da die Bearbeitung unmittelbar beginnen sollte, dieses als *in execution stage* gekennzeichnet (Abb. 5.1).

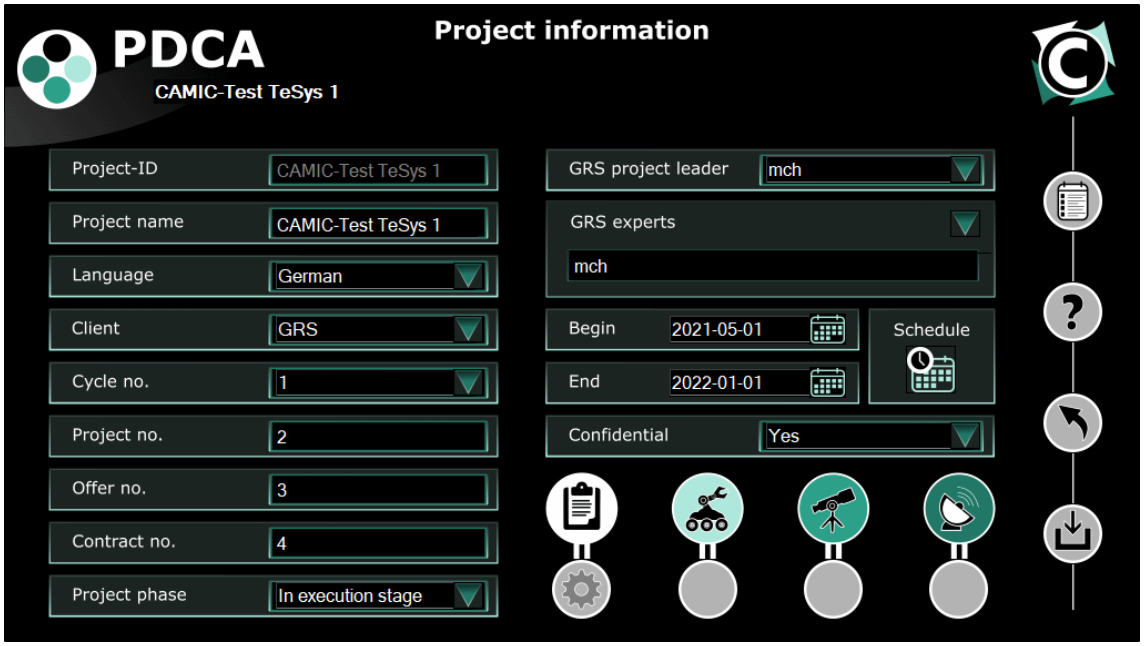


Abb. 5.1 Anlegen des Projekts „CAMIC-Test TeSys 1“ in der CAMIC-Anwendung

Anmerkung: Da es sich um ein reines Testprojekt handelt, wurden die Projekt-, Angebots- und die Vertragsnummern willkürlich vergeben. Ferner wurde das Projekt als vertraulich (*Confidential: Yes*) eingestuft, damit dieses reine Testprojekt später für andere Bearbeiter nicht mehr sichtbar ist.

Anschließend wurde unmittelbar mit der Bearbeitung des Projekts mit Hilfe der CAMIC-Anwendung begonnen. Hierzu wurde unter *PLAN Continue analysis* ausgewählt (siehe Abb. 5.2).

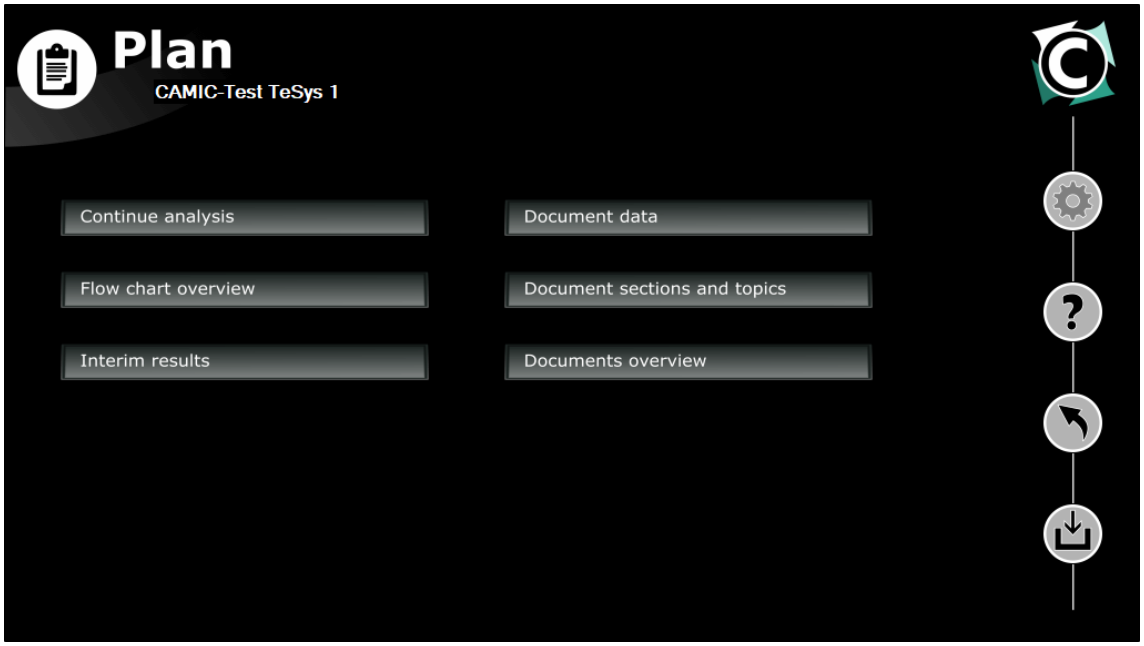


Abb. 5.2 Die Bearbeitung des Projekts wird über Continue analysis begonnen

Die nacheinander bearbeiteten Schritte gemäß der CAMIC-Methode für das erste Testszenario sind in Tab. 5.1 in der Übersicht dargestellt. Diese Informationen sind entweder in der CAMIC-Anwendung selbst ablesbar (Abb. 5.3) oder können als Teil eines automatisch generierten Reports jederzeit tabellarisch in einem Word-Dokument ausgegeben werden (siehe auch Abschnitt 4.1.7).

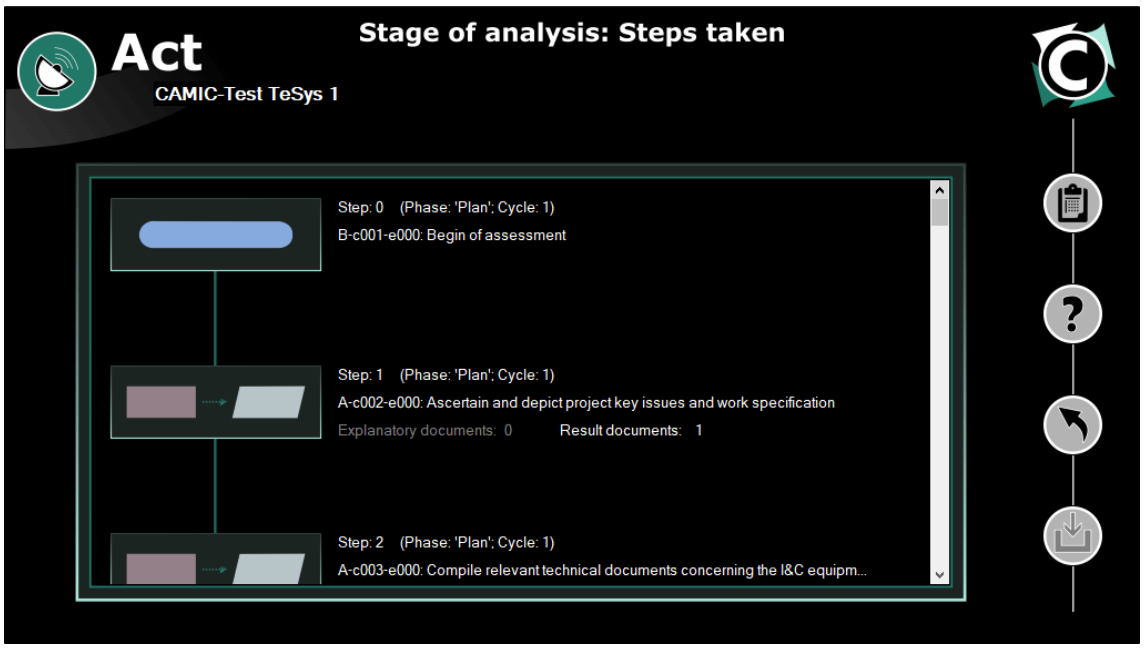


Abb. 5.3 Übersicht über die bisher durchgeführten Schritte in der CAMIC-Anwendung

Tab. 5.1 Übersicht über die durchgeführten Schritte im Rahmen des ersten Tests

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
0	1	plan	B-c001-e000	Beginn des Prozessschritts *PLAN*.
1	1	plan	A-c002-e000	Ermittlung und Darstellung der Projektschwerpunkte und Leistungsbeschreibung.
2	1	plan	A-c003-e000	Zusammenstellung relevanter technischer Dokumente zu den zu begutachtenden leittechnischen Einrichtungen.

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
3	1	plan	A-c004-e000	Zusammenstellung der Informationen über die künftig vorgesehene und die bereits vorhandene Leittechnik-Architektur sowie zu den geplanten Änderungen (Signalwege, Schnittstellen, vorgesehener Funktionsumfang, Stromversorgung usw.).
4	1	plan	A-c005-e000	Sammeln funktionsspezifischer Informationen (mit Hilfe des CAMIC-Worksheets *I&C functions within scope of assessment*).
5	1	plan	A-c006-e000	Sammeln funktionsspezifischer Informationen (mit Hilfe des CAMIC-Worksheets *Function-specific information on I&C architecture*).
6	1	plan	A-c007-e000	Zusammenstellung relevanter normativer Dokumente und weiterer Dokumente, die Anforderungen an die zu bewertende/n Leittechnikeinrichtungen und -Architektur enthalten.
7	1	plan	A-c008-e000	Durchführung von Themensuchen für alle projektbezogenen Dokumente.
8	1	plan	B-c009-e000	Haltepunkt, Übergang von *PLAN* nach *DO*.
9	1	do	B-c009-e000	Beginn des Prozessschritts *DO.*
10	1	do	D-c010-e000	Sind die Signalpfade mehrerer Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?
11	1	do	D-c011-e000	Ist die Steuerebene (z. B. Vorrangsteuerung) dieser Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
12	1	do	D-c013-e000	Sind mehrere LT-Systeme zur Ausführung dieser LT-Funktionen vom Einsatz neuer LTE (gleichen oder unterschiedlichen Typs) betroffen?
13	1	do	D-c014-e000	Ist eine einzelne Position im Signalpfad vom Einsatz neuer LTE (gleichen oder unterschiedlichen Typs) betroffen (ggf. auch dieselbe Position in mehreren leittechnischen Redundanzen)?
14	1	do	D-c015-e000	Sind LTE in entweder allen leittechnischen Redundanzen des LT-Systems vorgesehen oder zumindest in so vielen, dass in weniger als n leittechnischen Redundanzen kein Einsatz von neuen LTE vorgesehen ist?
15	1	do	D-c018-e000	Sollen in allen Redundanzen typgleiche LTE eingesetzt werden?
16	1	do	A-c024-e000	Generische Untersuchung einer der vorgesehenen LTE mittels einer FMEA.
17	1	do	A-c025-e000	Erweiterung der FMEA auf die Systemebene: Betrachtung der für die LTE ermittelten Fehlzustandsauswirkungen als Fehlzustandsarten des LT-Systems und Ermittlung der lokalen Fehlzustandsauswirkungen auf das Ausgangssignal des LT-Systems.
18	1	do	D-c026-e000	Alle vorgesehenen LTE mittels FMEA untersucht?
19	1	do	D-c027-e000	Gibt es Fehlzustandsarten, deren Fehlzustandsauswirkungen zu einem fehlerhaften Signal in mindestens einer leittechnischen Redundanz des LT-Systems führen und möglicherweise ein fehlerhaftes Ausgangssignal des LT-Systems nach sich ziehen?
20	1	do	A-c029-e000	Ergebnis aufbereiten und in CAMIC-DB eintragen.

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
21	1	do	D-c050-e000	Vorgehensweise C?
22	1	do	D-c051-e000	Vorgehensweise D oder E oder F?
23	1	do	D-c052-e000	Vorgehensweise G?
24	1	do	B-c196-e000	Haltepunkt, Übergang von *DO* nach *CHECK*.
25	1	check	B-c300-e000	Beginn des Prozessschritts *CHECK*.
26	1	check	A-c301-e000	Analyse, der in *DO* analysierten, möglichen Fehlzustandsauswirkungen auf die LTE an sich oder innerhalb des LT-Systems, in dem der Einsatz von neuen LTE vorgesehen ist, unter Berücksichtigung der im Prozessschritt *PLAN* erarbeiteten Anforderungen an diese LT-Einrichtungen.
27	1	check	D-c302-e000	Erfüllt die beschriebene Situation alle ermittelten Anforderungen an die LT-Einrichtungen und Systeme (siehe Prozessschritt *PLAN*)?
28	1	check	B-c304-e000	Haltepunkt, Übergang von *CHECK* nach *ACT*.
29	1	act	B-c400-e000	Beginn des Prozessschritts *ACT*.
30	1	act	A-c401-e000	Aufbereitung und Weiterleitung der Ergebnisse an den Auftraggeber.
31	1	act	D-c402-e000	Ist die fachliche Arbeit innerhalb des Projekts/Vorhabens nach Rückmeldung des Auftraggebers abgeschlossen?

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
32	1	act	A-c416-e000	Erstellung der evtl. noch notwendigen Enddokumentation.
33	1	act	B-c407-e000	Haltepunkt, Ende des Projekts oder Übergang von *ACT* nach *PLAN*.

Nachfolgend werden für das erste Projektszenario die einzelnen in der Tabelle oben aufgelisteten Schritte bzw. deren Bearbeitung im Rahmen der Testdurchführung näher beschrieben.

Schritt 0: B-c001-e000:

Beginn des Prozessschritts PLAN.

Die einzelnen Prozessschritte der CAMIC-Methode (*PLAN*, *DO*, *CHECK*, *ACT*) haben in der CAMIC-Anwendung jeweils einen definierten Startpunkt. Für den Prozessschritt *PLAN* ist dies der Startpunkt B-c001-e000, der programmiertechnisch wie ein Haltepunkt (daher „B-…“) behandelt wird. Dieser wird allerdings von der CAMIC-Anwendung automatisch bestätigt, so dass vom Anwender hier keine Eingaben erforderlich sind.

Schritt 1: A-c002-e000:

Ermittlung und Darstellung der Projektschwerpunkte und Leistungsbeschreibung.

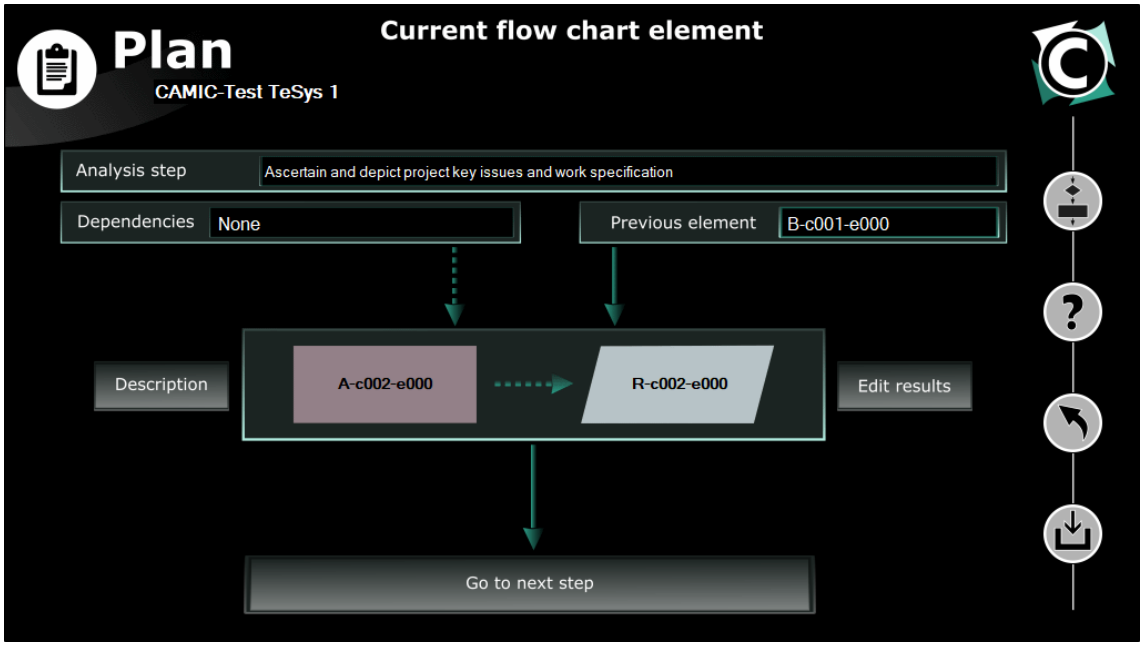


Abb. 5.4 Analyseschritt (hier: A-c002-e000) in der CAMIC-Anwendung

Für Bewertungen mit CAMIC ist es von entscheidender Bedeutung, sich mit dem Auftraggeber über die Projektschwerpunkte und die Formulierung der Leistungsbeschreibung zu verständigen, da sich hieraus wesentlich der weitere Verlauf (Typen und Reihenfolge der Analyseschritte) der Anwendung der CAMIC-Methode ergibt.

Für den hier beschriebenen Testfall wurde der Auftrag in einem externen Dokument beschrieben und (in einem unter *Edit results* erreichbaren Anwendungsfenster, siehe Abb. 5.4) hochgeladen.

Schritt 2: A-c003-e000

Zusammenstellung relevanter technischer Dokumente zu den zu begutachtenden leittechnischen Einrichtungen.

In diesem Schritt erfolgt die Zusammenstellung der technischen Informationen, wie z. B. Systembeschreibungen, technische Handbücher, Datenblätter. Die entsprechenden Dokumente werden entweder in die Datenbank der CAMIC-Anwendung hochgeladen oder, falls dies nicht möglich oder erlaubt ist, beispielsweise der physische Standort der Dokumente in der Datenbank hinterlegt.

Anmerkung: Dokumente, die nicht direkt in die Datenbank hochgeladen werden dürfen, sind beispielsweise DIN-Normen, die grundsätzlich nicht kopiert werden dürfen, oder aus anderen Gründen vertraulich zu behandelnden Unterlagen.

Das Einpflegen der Dokumente erfolgt in einem eigens hierfür vorgesehenen Bereich der CAMIC-Anwendung (Abb. 5.5, siehe auch Abschnitt 3.1.2).

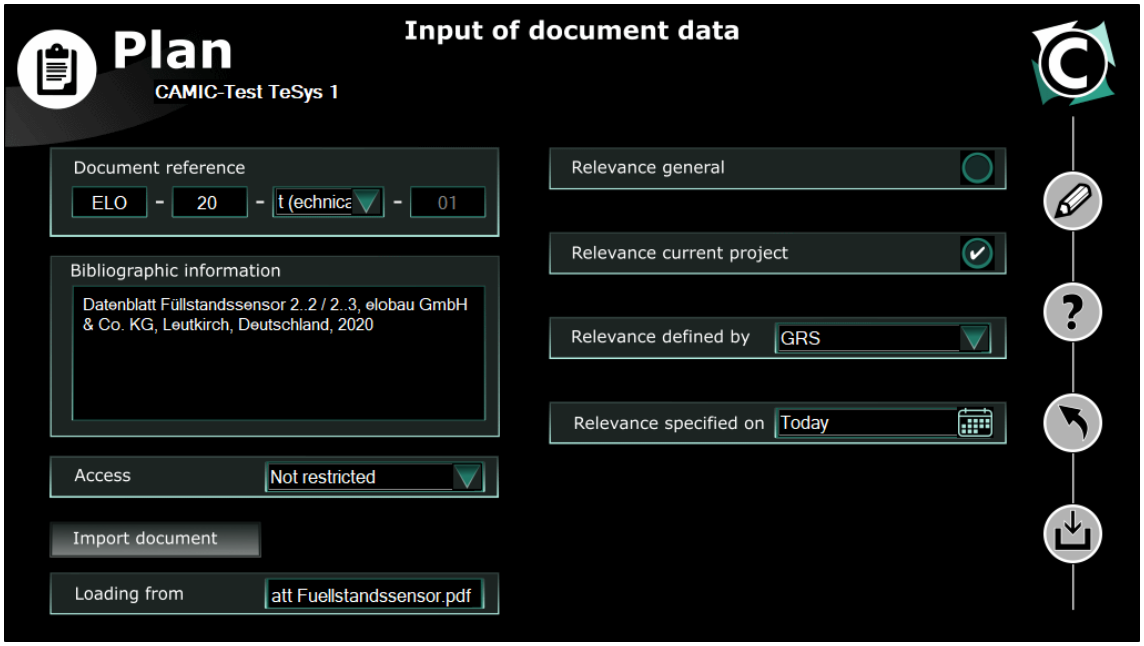


Abb. 5.5 Hochladen eines Dokuments in die Datenbank der CAMIC-Anwendung

Im Rahmen der Testdurchführung wurden die vom Auftraggeber zur Verfügung gestellten technischen Unterlagen in die Datenbank hochgeladen (z. B. das Datenblatt des ursprünglich verbauten Füllstandssensors in Abb. 5.5). Diese sind anschließend in der Datenbank dem entsprechenden Projekt zugordnet und können auch direkt aus der CAMIC-Anwendung heraus jederzeit abgerufen und ggf. auch geöffnet werden (Abb. 5.6).

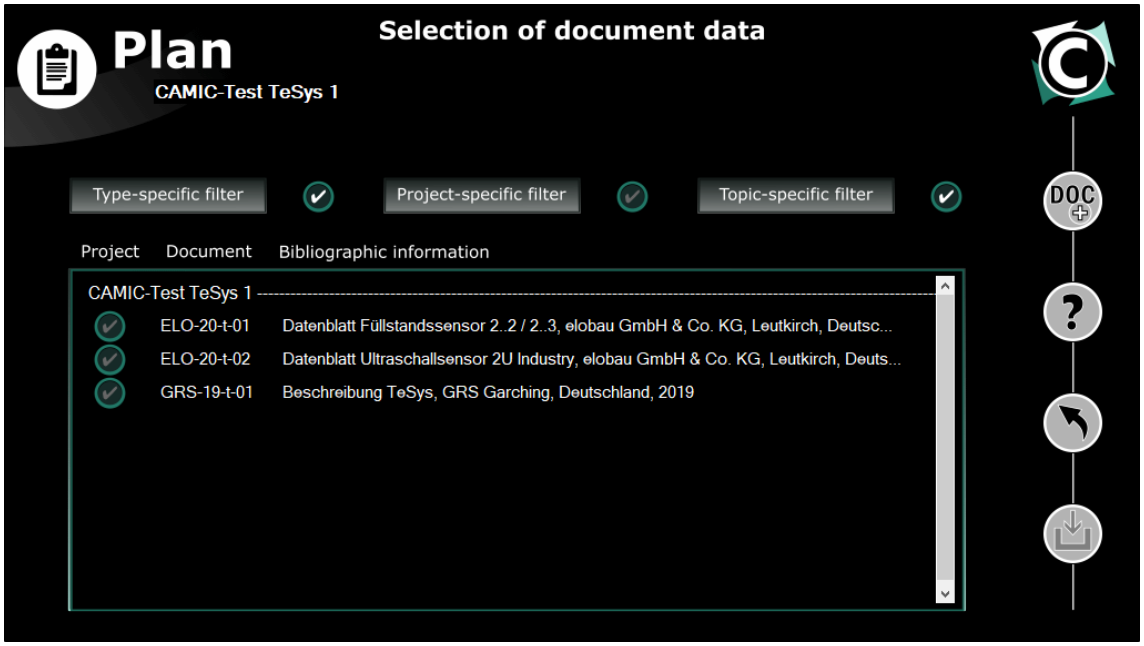


Abb. 5.6 Die im Schritt A-c003-e000 hochgeladenen Dokumente in der Übersicht

Schritt 3: A-c004-e000:

Zusammenstellung der Informationen über die künftig vorgesehene und die bereits vorhandene Leittechnik-Architektur sowie zu den geplanten Änderungen (Signalwege, Schnittstellen, vorgesehener Funktionsumfang, Stromversorgung usw.).

In diesem Schritt werden detaillierte Informationen sowohl über die bestehende als auch über die nach der geplanten Änderung vorhandene Leittechnik-Architektur zusammengestellt und ggf. auch in die Datenbank der Anwendung hochgeladen.

Im Rahmen des betrachteten Testszenarios waren keine Änderungen an der Leittechnik-Architektur vorgesehen, es sollten lediglich innerhalb der gleichbleibenden Architektur an den beiden Messstellen (oberer und unterer Tank von TeSys) die Messsensoren ausgetauscht werden. Daher wurde eine kurze Übersicht der betroffenen Leittechnikfunktionen mit einer entsprechenden Anmerkung in die Datenbank hochgeladen.

Schritt 4: A-c005-e000:

Sammeln funktionsspezifischer Informationen (mit Hilfe des CAMIC-Worksheets „I&C functions within scope of assessment“).

In diesem Schritt werden die Spezifikationen aller für die Bewertung relevanten Leittechnikfunktionen (hierfür wird in CAMIC ein Worksheet mit dem Titel *I&C functions within scope of assessment* zur Verfügung gestellt) gesammelt und in der CAMIC-Datenbank als Zwischenergebnis hinterlegt.

Im bearbeiteten Beispielszenario war hier nur eine einzelne Eingabe notwendig, da laut Beschreibung des Szenarios nur eine Leittechnikfunktion von den geplanten Änderungen betroffen ist. Die entsprechenden Informationen wurden als Zwischenergebnis in die Datenbank hochgeladen.

Schritt 5: A-c006-e000:

Sammeln funktionsspezifischer Informationen (mit Hilfe des CAMIC-Worksheets „Function-specific information on I&C architecture“).

Nach der Spezifikation aller für die Bewertung relevanten Leittechnikfunktionen im unmittelbar vorausgegangenen Schritt, wird für jede dieser Leittechnikfunktionen jeweils zusätzlich ein eigenes weiteres Worksheet mit dem Titel *Function-specific information*

on I&C architecture bearbeitet (dieses ist ebenfalls Bestandteil von CAMIC und enthält auch Anweisungen zu dessen Bearbeitung).

Im bearbeiteten Beispielszenario waren hierfür nur sehr wenige Eingaben notwendig, da lediglich zwei Komponenten gleichen Typs ausgetauscht werden sollten, die gemeinsam für eine einzige Leittechnikfunktion benötigt werden. Die entsprechenden Informationen wurden als Zwischenergebnis in die Datenbank hochgeladen.

Schritt 6: A-c007-e000:

Zusammenstellung relevanter normativer Dokumente und weiterer Dokumente, die Anforderungen an die zu bewertenden Leittechnikeinrichtungen und -Architektur enthalten.

Relevante Dokumente im Sinne dieses Schritts können z. B. regulatorische Anforderungen, Standards, Sicherheitsspezifikationen, Sicherheitsanalysen oder Qualifizierungsdokumente sein, die in diesem Schritt erfasst und, falls erlaubt, auch in die Datenbank hochgeladen werden. Alternativ können auch bereits in der CAMIC-Datenbank vorhandene Dokumente mit dem aktuellen Projekt verknüpft werden (so dass beispielsweise normative Dokumente nur ein einziges Mal in die Datenbank eingepflegt werden müssen).

Im Rahmen des Testszenarios wurden keine entsprechenden Dokumente hochgeladen oder mit dem Testprojekt verknüpft, da dies für die Durchführung des Projektauftrags und allgemein für diesen Test nicht notwendig war.

Schritt 7: A-c008-e000:

Durchführung von Themensuchen für alle projektbezogenen Dokumente.

Hierbei handelt es sich um einen optionalen Schritt, in dem die Themensuchen für die projektbezogenen Dokumente durchgeführt werden können (siehe hierzu Abschnitt 3.1.2).

Bei der Testdurchführung sind hier keine Arbeiten durchgeführt worden.

Schritt 8: B-c009-e000:

Haltepunkt, Übergang von „PLAN“ nach „DO“.

Diesen Haltepunkt (B – „Breakpoint“) erreicht man nach Beendigung aller Schritte des CAMIC-Prozessschritts *PLAN*. An dieser Stelle sind keine Arbeiten oder Analysen vorgesehen, er erlaubt ausschließlich den bewussten Wechsel in den nachfolgenden CAMIC-Prozessschritt *DO*, in dem dann die eigentlichen Analysen erfolgen.

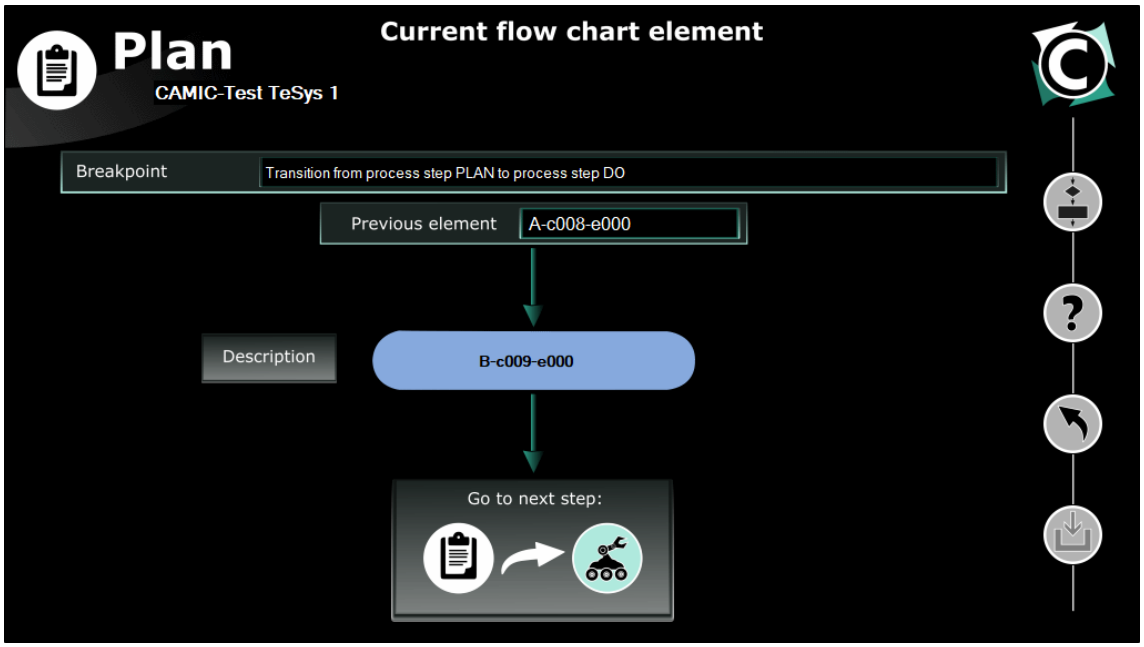


Abb. 5.7 Übergang von *PLAN* nach *DO* im Haltepunkt A-c008-e000

Durch Betätigung des Buttons *Go to next step* wurde bei der Testdurchführung der Abschluss des Prozessschritts *PLAN* bestätigt.

Schritt 9: B-c009-e000:

Beginn des Prozessschritts DO.

Die einzelnen Prozessschritte der CAMIC-Methode (*PLAN*, *DO*, *CHECK*, *ACT*) haben programmiertechnisch in der CAMIC-Anwendung jeweils einen definierten Startpunkt. Für den Prozessschritt *DO* ist dies der Startpunkt B-c009-e000, der programmiertechnisch wie ein Haltepunkt (daher „B-…“) behandelt wird. Dieser wird allerdings von der CAMIC-Anwendung automatisch bestätigt, so dass vom Anwender hier keine Eingaben erforderlich sind.

Anmerkung: Die Schritte 8 und 9 können demnach formal als ein einziger gemeinsamer Schritt aufgefasst werden (daher auch nur eine Bezeichnung: B-c009-e000). Aus

programmiertechnischen Gründen ist dieser einmal als Haltepunkt für den Prozessschritt *PLAN* und ein weiteres Mal als Startpunkt für den Prozessschritt *DO* in den Flowcharts hinterlegt.

Schritt 10: D-c010-e000:

Sind die Signalpfade mehrerer Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?

In diesem und den nachfolgenden Schritten erfolgen Abfragen, die der Nutzer auf Basis der in dem CAMIC-Prozessschritt *PLAN* durchgeführten Analysen jeweils mit *Ja* (*YES*) oder *Nein* (*NO*) beantworten muss. Aufgrund der gegebenen Antworten werden dann automatisch unterschiedliche Vorgehensweisen (gemäß der CAMIC-Methode) für die Analyse ausgewählt.

Konkret wird in D-c010-e000 abgefragt, ob die Signalpfade mehrerer Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen betroffen sind (Abb. 5.8).

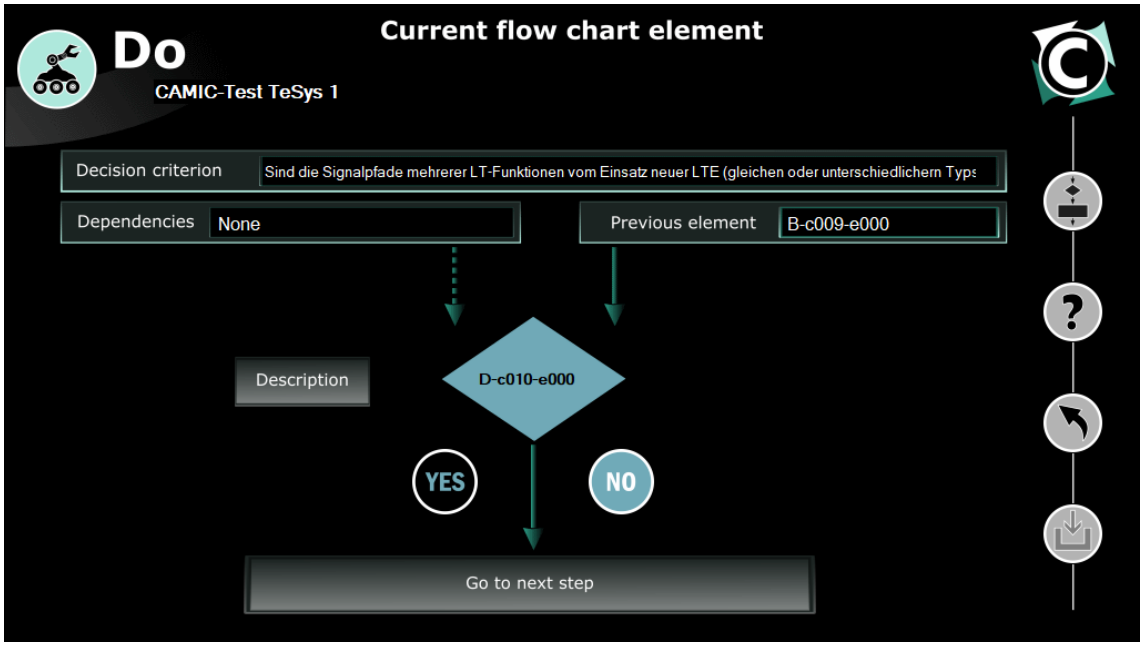


Abb. 5.8 Erste Abfrage einer Entscheidung (D – „Decision“) im Schritt D-c010-e000 der CAMIC-Anwendung

Da im betrachteten Testfall nur Signalpfade einer einzigen Leittechnikfunktion durch den angenommenen Austausch der Füllstandssensoren betroffen sind, wurde diese Frage mit *Nein* (*NO*) beantwortet.

Schritt 11: D-c011-e000:

Ist die Steuerebene (z. B. Vorrangsteuerung) dieser Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?

Änderungen finden laut Testszenario ausschließlich auf der Erfassungsebene statt. Da laut Szenario auch keine sicherheitsrelevante leittechnische Einrichtung betrachtet werden sollte, ist hier auch keine indirekte Auswirkung auf die Steuerebene zu betrachten. Dementsprechend wurde die Abfrage bei der Testdurchführung mit *Nein* (*NO*) beantwortet.

Anmerkung: Die Formulierung „betroffen“ ist evtl. für einen unerfahrenen Nutzer nicht eindeutig genug. Versteht man dies nämlich dahingehend, dass hier abgefragt wird, ob Änderungen auf der Steuerebene stattfinden, wird diese Abfrage unter Umständen falsch beantwortet. Der Erläuterungstext sollte daher bei einer zukünftigen Weiterentwicklung der Methode und Anwendung erweitert werden.

Schritt 12: D-c013-e000:

Sind mehrere LT-Systeme zur Ausführung dieser LT-Funktionen vom Einsatz neuer LTE (gleichen oder unterschiedlichen Typs) betroffen?

Im Testszenario wird nur ein einzelnes Leittechniksystem (mit nur einer einzigen Redundanz) betrachtet. Dementsprechend wurde diese Abfrage mit *Nein* (*NO*) beantwortet.

Schritt 13: D-c014-e000:

Ist eine einzelne Position im Signalpfad vom Einsatz neuer LTE (gleichen oder unterschiedlichen Typs) betroffen (ggf. auch dieselbe Position in mehreren leittechnischen Redundanzen)?

Dies ist in betrachteten Testszenario der Fall, dementsprechend wurde diese Abfrage bei der Testdurchführung mit *Ja* (*YES*) beantwortet.

Schritt 14: D-c015-e000:

Sind LTE in entweder allen leittechnischen Redundanzen des LT-Systems vorgesehen oder zumindest in so vielen, dass in weniger als n leittechnischen Redundanzen kein Einsatz von neuen LTE vorgesehen ist?

Die zu diesem Element hinterlegte Beschreibung (durch Auswahl von „Description“ auf der entsprechenden Seite zu erreichen) führt hierzu weiter aus:

> n ist hierbei die für die Bildung eines korrekten Signals notwendige Zahl an leittechnischen Redundanzen (z. B. n-von-m-Auswahlschaltung). Dies ist sowohl in Bezug auf die Bildung eines korrekten Anregesignals als auch auf das Ausbleiben einer Fehlanregung zu verstehen. Gibt es beispielsweise drei leittechnische Redundanzen mit einer 2-von-3-Auswahlschaltung, dann sind n = 2 Redundanzen für die Bildung eines korrekten Anregesignals notwendig. Ebenso sind korrekte Signale aus n=2 Redundanzen notwendig, um eine Fehlanregung zu verhindern. Das Entscheidungskriterium wäre in diesem Fall also erfüllt, sobald in mindestens zwei Redundanzen keine neue LTE vorgesehen ist, da beim postulierten Ausfall die erforderliche Funktion ausgeführt wird.

Die Bearbeitung im Rahmen der Testdurchführung berücksichtigte die Tatsache, dass in diesem konkreten Fall das betrachtete System per Definition (siehe Beschreibung des Szenarios) als nicht sicherheitsrelevant (im Sinne der CAMIC-Methode) eingestuft wurde. Dieser Tatsache wurde berücksichtigt, in dem die Antwort *Ja* (*YES*) ausgewählt wurde, da hier grundsätzlich keine (n=0) Redundanz „notwendig“ ist.

Anmerkung: Hier sollte evtl. die Beschreibung des Elements D-c015-e000 dahingehend erweitert werden, dass hier auch grundsätzlich mit „Ja“ geantwortet werden sollte, falls die betrachtete Leittechnikfunktion nicht sicherheitsrelevant ist. Allerdings ist in realen Projekten nicht zu erwarten, dass nicht sicherheitsrelevanten Leittechnikfunktionen untersucht werden sollen.

Schritt 15: D-c018-e000:

Sollen in allen Redundanzen typgleiche LTE eingesetzt werden?

Da im Testszenario nur eine einzelne Redundanz betrachtet wurde, lautete die Antwort auf diese Abfrage bei der Testdurchführung *Ja* (*YES*). Durch Abgleich mit der Flowchart-Übersicht, welche auch aus der CAMIC-Anwendung selbst erreichbar ist, wurde an dieser Stelle ebenfalls festgehalten, dass gemäß CAMIC-Methode die Vorgehensweise B durch die Beantwortung dieser und der vorausgegangenen Fragen ausgewählt wurde.

Anmerkung: Welche Vorgehensweise ausgewählt wurde, ist für den Nutzer zunächst einmal scheinbar irrelevant. Diese muss derzeit aber noch festgehalten werden (z. B. durch die Kommentierungsfunktion für die CAMIC-Schritte), da derzeit im weiteren Verlauf der Bearbeitung noch Fragen nach der Vorgehensweise an den Nutzer gestellt werden (siehe z. B. Schritt 21 unten). Diese Abfragen vom Nutzer sollen in einer zukünftigen Version der CAMIC-Anwendung durch stärkere Automatisierung überflüssig werden.

Schritt 16: A-c024-e000:

Generische Untersuchung einer der vorgesehenen LTE mittels einer FMEA.

An dieser Stelle wurde bei der Testdurchführung eine einfache FMEA durchgeführt und das Zwischenergebnis in die CAMIC-Datenbank hochgeladen. Das Zwischenergebnis beschrieb die Fehlzustandsarten der leittechnischen Einrichtung und sich daraus ergebende lokale Fehlzustandsauswirkungen auf das Ausgangssignal der leittechnischen Einrichtung.

Schritt 17: A-c025-e000:

Erweiterung der FMEA auf die Systemebene: Betrachtung der für die LTE ermittelten Fehlzustandsauswirkungen als Fehlzustandsarten des LT-Systems und Ermittlung der lokalen Fehlzustandsauswirkungen auf das Ausgangssignal des LT-Systems.

In diesem Schritt soll eingeschätzt werden, inwiefern Fehlzustandsarten der einzelnen vorgesehenen leittechnischen Einrichtungen (vgl. auch vorangegangener Schritt) in Kombination mit nicht vorliegender Diversität insgesamt zu fehlerhaften Ausgangssignalen des Leittechniksystems führen können. Im Testszenario wird von nur einer einzigen geänderten leittechnischen Einrichtung ausgegangen und die Frage nach der Diversität durch die Beschreibung des Szenarios ohnehin ausgeschlossen, so dass bei der Testdurchführung hier keine weiteren Arbeiten erforderlich waren.

Schritt 18: D-c026-e000:

Abfrage: Alle vorgesehenen LTE mittels FMEA untersucht?

Diese Abfrage in der CAMIC-Methode und -Anwendung realisiert eine Schleife, durch die die Analysen der Elemente A-c024-e000 und A-c025-e000 solange wiederholt werden, bis FMEAs für alle vorgesehenen leittechnischen Einrichtungen durchgeführt wurden. Im Rahmen des Testszenarios mussten diese Analysen nur ein einziges Mal durchgeführt werden, so dass hier unmittelbar die Auswahl *Ja* (*YES*) getroffen wurde.

Schritt 19: D-c027-e000:

Abfrage: Gibt es Fehlzustandsarten, deren Fehlzustandsauswirkungen zu einem fehlerhaften Signal in mindestens einer leittechnischen Redundanz des LT-Systems führen und möglicherweise ein fehlerhaftes Ausgangssignal des LT-Systems nach sich ziehen?

Prinzipiell könnte man diese Frage bei der Testdurchführung mit *Ja* beantworten, da im konkreten Fall des Testszenarios dies aufgrund einer einzigen vorhandenen Redundanz immer der Fall ist. Dies war jedoch auch schon vor der geplanten hypothetischen Änderung der Fall, so dass sich hier keine geänderte Situation ergibt. Es gibt also keine NEUEN Fehlzustandsarten (aufgrund der geplanten Änderung), die zu einem fehlerhaften Ausgangssignal führen können.

Anmerkung: Wie bei der Beschreibung des Elements D-c015-e000, wird hier ein solches Szenario in der Beschreibung nicht explizit in Betracht gezogen. Auch hier könnte man die Beschreibung in Zukunft noch für Untersuchungen für nicht sicherheitsrelevante Leittechnikfunktionen erweitern. Allerdings ist auch hier in realen Projekten nicht zu erwarten, dass nicht sicherheitsrelevanten Leittechnikfunktionen untersucht werden sollen.

Im Rahmen der Testdurchführung wurde hier die Auswahl *Nein* (*NO*) getroffen.

Schritt 20: A-c029-e000:

Ergebnis aufbereiten und in CAMIC-DB eintragen.

Im Rahmen der Testdurchführung wurden die Ergebnisse der FMEAs in einem Dokument zusammengefasst und als Zwischenergebnisse in die CAMIC-Datenbank hochgeladen.

Schritt 21: D-c050-e000:

Abfrage: Vorgehensweise C?

Dieser sowie die nächsten beiden Schritte sollen in zukünftigen Versionen der CAMIC-Anwendung nicht mehr durch den Benutzer zu beantworten sein, da die Beantwortung dieser Fragen einfach zu automatisieren ist. Wie im Schritt 15 ausgeführt, hat die CAMIC-Anwendung die Vorgehensweise B ausgewählt, weswegen die Antwort auf diese Abfrage bei der Testdurchführung *Nein* (*NO*) lautete.

Schritt 22: D-c051-e000:

Abfrage: Vorgehensweise D oder E oder F?

Wie im Schritt 15 ausgeführt, hat die CAMIC-Anwendung die Vorgehensweise B ausgewählt, weswegen die Antwort auf diese Abfrage bei der Testdurchführung *Nein* (*NO*) lautete.

Schritt 23: D-c052-e000:

Abfrage: Vorgehensweise G?

Wie im Schritt 15 ausgeführt, hat die CAMIC-Anwendung die Vorgehensweise B ausgewählt, weswegen die Antwort auf diese Abfrage bei der Testdurchführung *Nein* (*NO*) lautete.

Schritt 24: B-c196-e000:

Haltepunkt, Übergang von „DO“ nach „CHECK“.

Diesen Haltepunkt (B – Breakpoint) erreicht man nach Beendigung aller Schritte des CAMIC-Prozessschritts *DO*. An dieser Stelle sind keine Arbeiten oder Analysen vorgesehen, er erlaubt ausschließlich der bewussten Wechsel in den nachfolgenden CAMIC-Prozessschritt *CHECK*.

Schritt 25: B-c300-e000:

Beginn des Prozessschritts „CHECK“.

Die einzelnen Prozessschritte der CAMIC-Methode (*PLAN*, *DO*, *CHECK, ACT*) haben programmiertechnisch in der CAMIC-Anwendung jeweils einen definierten Startpunkt. Für den Prozessschritt *CHECK* ist dies der Startpunkt B-c300-e000, der programmiertechnisch wie ein Haltepunkt (daher „B-…“) behandelt wird. Dieser wird allerdings von der CAMIC-Anwendung automatisch bestätigt, so dass vom Anwender hier keine Eingaben erforderlich sind.

Anmerkung: Die Schritte 24 und 25 können demnach formal als ein einziger gemeinsamer Schritt aufgefasst werden. Die Schritte 24 und 25 haben allerdings im Unterschied zum Übergang von *PLAN* nach *DO* (siehe Schritte 8 und 9) verschiedene Bezeichnungen, da der Prozessschritt *CHECK* von verschiedenen Haltepunkten des Prozessschritts *DO* erreicht werden kann.

Schritt 26: A-c301-e000:

Analyse, der in DO analysierten, möglichen Fehlzustandsauswirkungen auf die LTE an sich oder innerhalb des LT-Systems, in dem der Einsatz von neuen LTE vorgesehen ist, unter Berücksichtigung des im Prozessschritts PLAN erarbeiteten Anforderungen an diese LT-Einrichtungen.

In diesem Schritt werden die in *DO* analysierten möglichen Fehlzustandsauswirkungen auf die leittechnische Einrichtung an sich oder innerhalb des Leittechniksystems gesamt, unter Berücksichtigung der in *PLAN* erarbeiteten Anforderungen, analysiert. Als

Zwischenergebnis erhält man eine Aussage, ob alle Anforderungen an die leittechnischen Einrichtungen und Systeme, auch unter den neu ermittelten Fehlzuständen erfüllt sind.

Bei der Testdurchführung sind aufgrund des Szenarios keine Anforderungen zu erfüllen. Dementsprechend wurden hier keine weiteren Arbeiten durchgeführt.

Schritt 27: D-c302-e000:

Erfüllt die beschriebene Situation alle ermittelten Anforderungen an die LT-Einrichtungen und Systeme (siehe Prozessschritt PLAN)?

Da laut Beschreibung des Projektszenarios keine Anforderungen zu erfüllen sind, wurde dies Abfrage bei der Testdurchführung mit *Ja* (*YES*) beantwortet.

Schritt 28: B-c304-e000:

Haltepunkt, Übergang von „CHECK“ nach „ACT“.

Diesen Haltepunkt (B – Breakpoint) erreicht man nach Beendigung aller Schritte des CAMIC-Prozessschritts *DO*. An dieser Stelle sind keine Arbeiten oder Analysen vorgesehen, er erlaubt ausschließlich der bewussten Wechsel in den nachfolgenden CAMIC-Prozessschritt *CHECK*.

Schritt 29: B-c400-e000:

Beginn des Prozessschritts „ACT“.

Die einzelnen Prozessschritte der CAMIC-Methode (*PLAN, DO, CHECK, ACT*) haben programmiertechnisch in der CAMIC-Anwendung jeweils einen definierten Startpunkt. Für den Prozessschritt *ACT* ist dies der Startpunkt B-c400-e000, der programmiertechnisch wie ein Haltepunkt (daher „B-…“) behandelt wird. Dieser wird allerdings von der CAMIC-Anwendung automatisch bestätigt, so dass vom Anwender hier keine Eingaben erforderlich sind.

Anmerkung: Die Schritte 28 und 29 können demnach formal als ein einziger gemeinsamer Schritt aufgefasst werden. Die Schritte 28 und 29 haben allerdings im Unterschied zum Übergang von *PLAN* nach *DO* (siehe Schritte 8 und 9) verschiedene Bezeichnungen, da der Prozessschritt *CHECK* von verschiedenen Haltepunkten des Prozessschritts *DO* erreicht werden kann.

Schritt 30: A-c401-e000:

Aufbereitung und Weiterleitung der Ergebnisse an den Auftraggeber.

In diesem Schritt finden die Aufbereitung und Weiterleitung der Ergebnisse des Prozessschritts *CHECK* an den Auftraggeber statt. Die Weiterleitung der Ergebnisse kann auf unterschiedliche Weise erfolgen (in Abhängigkeit dessen, was mit dem Auftraggeber vereinbart wurde (z. B. E-Mail, Telefonanruf, ...)). In Abhängigkeit von der Rückmeldung des Auftraggebers ergibt sich das nachfolgende weitere Vorgehen.

Für die Testdurchführung wurden hier keine Arbeiten durchgeführt.

Schritt 31: D-c402-e000:

Ist die fachliche Arbeit innerhalb des Projekts/Vorhabens nach Rückmeldung des Auftraggebers abgeschlossen?

Die im Projektszenario spezifizierte Aufgabe wurde komplett abgearbeitet, weswegen bei der Durchführung des Tests die Auswahl *Ja* (*YES*) getroffen wurde.

Schritt 32: A-c416-e000:

Erstellung der evtl. noch notwendigen Enddokumentation.

Im Rahmen der Testdurchführung wurde das Ergebnis des Tests dokumentiert und in die Datenbank hochgeladen. Damit war die Enddokumentation abgeschlossen.

Schritt 3: B-c407-e000:

Haltepunkt, Ende des Projekts oder Übergang von ACT nach PLAN.

Dieser Schritt stellte für den Test den formalen Endpunkt der Projektabwicklung dar.

5.1.3 Bewertung des Tests

Der Ablauf der Projektbearbeitung gemäß der CAMIC-Methode mit Hilfe der CAMIC-Anwendung verlief für das erste Projektszenario erfolgreich. Insbesondere die automatisch ausgewählten Analysemethoden entsprechen vollständig den vorab formulierten Erwartungen (Durchführung von FMEAs). An einzelnen Stellen wurde ein geringer zukünftiger Nachbesserungsbedarf entdeckt (siehe z. B. Beschreibung der Schritte 11, 14), dieser steht aber einer Anwendung der CAMIC-Methode und -Anwendung im aktuellen Zustand nicht entgegen.

5.2 Beispiel: CAMIC-Test TeSys 2

5.2.1 Szenario und erwarteter Ablauf

Im Projektszenario CAMIC-Test TeSys 2 wurde davon ausgegangen, dass ein Auftraggeber („GRS“) eine neue Anlage TeSys („**T**est**Sys**tem“) plant. Im Gegensatz zum ersten Szenario (siehe Abschnitt 5.1.1), handelte es sich bei TeSys in diesem Szenario allerdings um ein sicherheitsrelevantes System. Ansonsten war TeSys wie im ersten Szenario aufgebaut. Es handelt sich bei TeSys um ein vergleichsweise einfaches System aus zwei miteinander verbundenen Tanks. Aus dem höher gelegenen Tank kann über ein Ventil Wasser in den tieferliegenden Tank abgelassen werden. Umgekehrt kann aus dem tiefer gelegenen Tank Wasser über eine Pumpe in den höher gelegenen Tank gepumpt werden. Die Füllstände der beiden Tanks werden durch Füllstandssensoren (jeweils nur eine Redundanz) gemessen und durch ein Leittechniksystem überwacht, um beispielsweise ein Trockenlaufen der Pumpe zu verhindern (vgl. /GRS 21/).

Der Auftragnehmer sollte untersuchen, ob TeSys das Einzelfehlerkriterium erfüllt, wie es in der KTA-Regel 3501 formuliert ist.

Vom Auftraggeber wurde das folgende Dokument zur Verfügung gestellt:

- Eine Beschreibung des Systems (Verfahrenstechnik und Leittechnik).

Als Projektbeginn wurde der 01.05.2021 vereinbart, die Arbeiten sollten noch vollständig im selben Kalenderjahr erfolgen.

Die Beschreibung des Projektszenarios wurde so erstellt, dass für die Bearbeitung eine FMEA-Analyse notwendig ist. Außerdem wurde erwartet, dass die zu erwartende fehlende Diversität (in diesem Szenario hat das System sogar nur eine einzige Redundanz) mit Hilfe einer Diversitätsmatrix untersucht und dokumentiert wird.

5.2.2 Testdurchführung

Wie im ersten Szenario, wurde zunächst ein Testprojekt („CAMIC-Test TeSys 2“) in der CAMIC-Anwendung angelegt und anschließend mit der Analyse gemäß der CAMIC-Methode begonnen. Tab. 5.2 zeigt die Übersicht aller beim zweiten Test durchgeführten Schritte der CAMIC-Methode.

Tab. 5.2 Übersicht über die durchgeführten Schritte im Rahmen des zweiten Tests

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
0	1	plan	B-c001-e000	Beginn des Prozessschritts *PLAN*.
1	1	plan	A-c002-e000	Ermittlung und Darstellung der Projektschwerpunkte und Leistungsbeschreibung.
2	1	plan	A-c003-e000	Zusammenstellung relevanter technischer Dokumente zu den zu begutachtenden leittechnischen Einrichtungen.
3	1	plan	A-c004-e000	Zusammenstellung der Informationen über die künftig vorgesehene und die bereits vorhandene Leittechnik-Architektur sowie zu den geplanten Änderungen (Signalwege, Schnittstellen, vorgesehener Funktionsumfang, Stromversorgung usw.).
4	1	plan	A-c005-e000	Sammeln funktionsspezifischer Informationen (mit Hilfe des CAMIC-Worksheets *I&C functions within scope of assessment*).
5	1	plan	A-c006-e000	Sammeln funktionsspezifischer Informationen (mit Hilfe des CAMIC-Worksheets *Function-specific information on I&C architecture*).
6	1	plan	A-c007-e000	Zusammenstellung relevanter normativer Dokumente und weiterer Dokumente, die Anforderungen an die zu bewertenden Leittechnikeinrichtungen und -Architektur enthalten.
7	1	plan	A-c008-e000	Durchführung von Themensuchen für alle projektbezogenen Dokumente.
8	1	plan	B-c009-e000	Haltepunkt, Übergang von *PLAN* nach *DO*.
9	1	do	B-c009-e000	Beginn des Prozessschritts *DO*.

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
10	1	do	D-c010-e000	Sind die Signalpfade mehrerer Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?
11	1	do	D-c011-e000	Ist die Steuerebene (z. B. Vorrangsteuerung) dieser Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?
12	1	do	D-c012-e000	Sind mehrere Aktuatortypen an der Ausführung der LT-Funktion, in deren Steuerebene neue LTE vorgesehen sind, beteiligt?
13	1	do	A-c113-e000	Betrachtung der Steuerebene aller verfahrenstechnischen Redundanzen für den Aktuatortyp und Ermittlung der Anzahl der leittechnischen Redundanzen der Steuerebene bzw. der Vorrangmodule für den hier betrachteten Aktuatortypen.
14	1	do	A-c114-e000	Ermittlung, in wie vielen leittechnischen Redundanzen der Steuerebene für den betrachteten Aktuatortyp neue LTE vorgesehen sind.
15	1	do	D-c115-e000	Soll derselbe Typ LTE in der Steuerebene aller verfahrenstechnischer Redundanzen eingesetzt werden?
16	1	do	A-c123-e000	Generische Untersuchung der für die Steuerebene vorgesehenen neuen LTE mittels einer FMEA und Betrachtung der Fehlzustandsauswirkungen auf die leittechnische Funktion.
17	1	do	D-c124-e000	Hat sich bei der FMEA der LTE eine Fehlzustandsart ergeben, deren Fehlzustandsauswirkung bei Erfüllung der Anregekriterien der LT-Funktion zu Ausfall oder Fehlanregung des betrachteten Aktuatortypen führen kann?

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
18	1	do	D-c125-e000	Ist (x-z) >= y?
19	1	do	A-c126-e000	Betrachtung der ermittelten Fehlzustandsarten der LTE und der sich daraus ergebenden Fehlzustandsauswirkungen auf die leittechnische Funktion.
20	1	do	D-c127-e000	Gibt es Hinweise auf ein GVA-Potential des vorgesehenen Typ LTE und den in den restlichen Redundanzen der Steuerebene eingesetzten Komponenten?
21	1	do	A-c128-e000	Anpassung der Diversitätsmatrix auf für die LTE relevanten Merkmale.
22	1	do	D-c129-e000	Gibt es mindestens ein für den Einsatz der neuen LTE relevantes Diversitätsmerkmal, in dem keine Diversität vorliegt?
23	1	do	A-c183-e000	Dokumentiere Ergebnis gemäß Haltepunkt 16, 17 oder 18. Oder dokumentiere Ergebnisse gemäß D.
24	1	do	D-c057-e000	Vorgehensweise F?
25	1	do	D-c058-e000	Vorgehensweise G?
26	1	do	B-c199-e000	Haltepunkt, Übergang von *DO* nach *CHECK*.
27	1	check	B-c300-e000	Beginn des Prozessschritts *CHECK*.

Schritt	Zyklus	Prozessschritt	Element	Kurze Beschreibung
28	1	check	A-c301-e000	Analyse, der in *DO* analysierten, möglichen Fehlzustandsauswirkungen auf die LTE an sich oder innerhalb des LT-Systems, in dem der Einsatz von neuen LTE vorgesehen ist, unter Berücksichtigung der im Prozessschritt *PLAN* erarbeiteten Anforderungen an diese LT-Einrichtungen.
29	1	check	D-c302-e000	Erfüllt die beschriebene Situation alle ermittelten Anforderungen an die LT-Einrichtungen und Systeme (siehe Prozessschritt *PLAN*)?
30	1	check	A-c303-e000	Dokumentation der aufgrund des geplanten Einsatzes von LTE möglicherweise nicht erfüllten Anforderungen.
31	1	check	B-c304-e000	Haltepunkt, Übergang von *CHECK* nach *ACT*.
32	1	act	B-c400-e000	Beginn des Prozessschritts *ACT*.
33	1	act	A-c401-e000	Aufbereitung und Weiterleitung der Ergebnisse an den Auftraggeber.
34	1	act	D-c402-e000	Ist die fachliche Arbeit innerhalb des Projekts/Vorhabens nach Rückmeldung des Auftraggebers abgeschlossen?
35	1	act	A-c416-e000	Erstellung der evtl. noch notwendigen Enddokumentation.
36	1	act	B-c407-e000	Haltepunkt, Ende des Projekts oder Übergang von *ACT* nach *PLAN*.

Im Unterschied zur Darstellung für das erste Szenario (Abschnitt 5.1.2), werden nachfolgend nicht mehr durchweg alle Schritte nacheinander detailliert beschrieben. Stattdessen wird an dieser Stelle nur noch auf einige wichtige Punkte eingegangen, die für das Nachvollziehen des Testverlaufs von besonderer Bedeutung sind.

Die Bearbeitung des Prozessschritts *PLAN* lief weitgehend identisch wie beim ersten Szenario ab. Allerdings wurden im zweiten Szenario weniger Dokumente in die CAMIC-Datenbank hochgeladen und insbesondere bei der Dokumentation der Anforderungen („KTA 3501“) konnte auf das bereits in der Datenbank vorhandene Dokument zurückgegriffen werden.

Danach wurden in dem Prozessschritt *DO* die folgenden Antworten auf die einleitenden Fragen zur Bestimmung der Vorgehensweise gegeben:

Schritt 10: D-c010-e000:

Sind die Signalpfade mehrerer Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?

Da nur eine Leittechnikfunktion im Szenario betrachtet wurde, wurde diese Frage mit *Nein* (*NO*) beantwortet.

Schritt 11: D-c011-e000:

Ist die Steuerebene (z. B. Vorrangsteuerung) dieser Leittechnikfunktionen vom Einsatz neuer leittechnischer Einrichtungen (gleichen oder unterschiedlichen Typs) betroffen?

Da es sich laut Szenario um ein geplantes System inklusive Steuerebene handelt, wurde diese Abfrage mit *Ja* (*YES*) beantwortet.

Schritt 12: D-c012-e000:

Sind mehrere Aktuatortypen an der Ausführung der LT-Funktion, in deren Steuerebene neue LTE vorgesehen sind, beteiligt?

Das im Testszenario betrachtete System enthält nur eine Leittechnikfunktion zum Schutz eines einzelnen Aktuators. Dementsprechend wurde diese Abfrage mit *Nein* (*NO*) beantwortet.

Durch die Antworten in den Schritten 10, 11 und 12 wurde somit insgesamt die Vorgehensweise E der CAMIC-Methode ausgewählt. Einige wichtige Schritte (Abfragen und Analyseschritte) dieser Vorgehensweise werden nachfolgend näher betrachtet.

Schritt 15: D-c115-e000:

Soll derselbe Typ LTE in der Steuerebene aller verfahrenstechnischer Redundanzen eingesetzt werden?

Da nur eine einzige Redundanz im betrachteten System vorhanden ist, wurde diese Frage mit *Ja* (*YES*) beantwortet.

Schritt 16: A-c123-e000:

Generische Untersuchung der für die Steuerebene vorgesehenen neuen LTE mittels einer FMEA und Betrachtung der Fehlzustandsauswirkungen auf die leittechnische Funktion.

In diesem Schritt wurde eine FMEA durchgeführt. Dabei wurde festgestellt, dass es eine Fehlzustandsart gibt, die zu einem Ausfall des einzigen betrachteten Aktuators kommen kann.

Schritt 17: D-c124-e000:

Hat sich bei der FMEA der LTE eine Fehlzustandsart ergeben, deren Fehlzustandsauswirkung bei Erfüllung der Anregekriterien der LT-Funktion zu Ausfall oder Fehlanregung des betrachteten Aktuatortypen führen kann?

Aufgrund des Ergebnisses der vorangegangenen Analyse (siehe Schritt 16), wurde diese Frage bei der Testdurchführung mit *Ja* (*YES*) beantwortet. Nach der Bearbeitung der sich anschließenden Schritte 18 und 19 (D-c125-e000 und A-c126-e000) ließ sich unmittelbar folgern, dass hier keine ausreichende Diversität (genaugenommen noch nicht einmal Redundanz) vorliegt.

Schritt 20: D-c127-e000:

Gibt es Hinweise auf ein GVA-Potential von vorgesehenem Typ LTE und in den restlichen Redundanzen der Steuerebene eingesetzten Komponenten?

Auf Basis der vorausgegangenen Analysen und insbesondere der Tatsache, dass hier nur eine einzige Redundanz vorgesehen ist, wurde dies Abfrage mit *Ja* (*YES*) beantwortet.

Schritt 21: D-c128-e000:

Anpassung der Diversitätsmatrix auf für die LTE relevanten Merkmale?

In diesem Schritt wurde die innerhalb der CAMIC-Anwendung verfügbare Methode der Diversitätsmatrix zur Dokumentation der fehlenden Diversität verwendet. Da die fehlende Diversität in diesem Testszenario offensichtlich ist, wurden bei der Testdurchführung lediglich einige repräsentative Diversitätsmerkmale und Bestandteile des Leittechniksystems betrachtet und somit die fehlende Diversität dokumentiert (Abb. 5.9).

Mehr Details zur Diversitätsmatrix können im Abschnitt 4.1.6.2.1 nachgelesen werden.

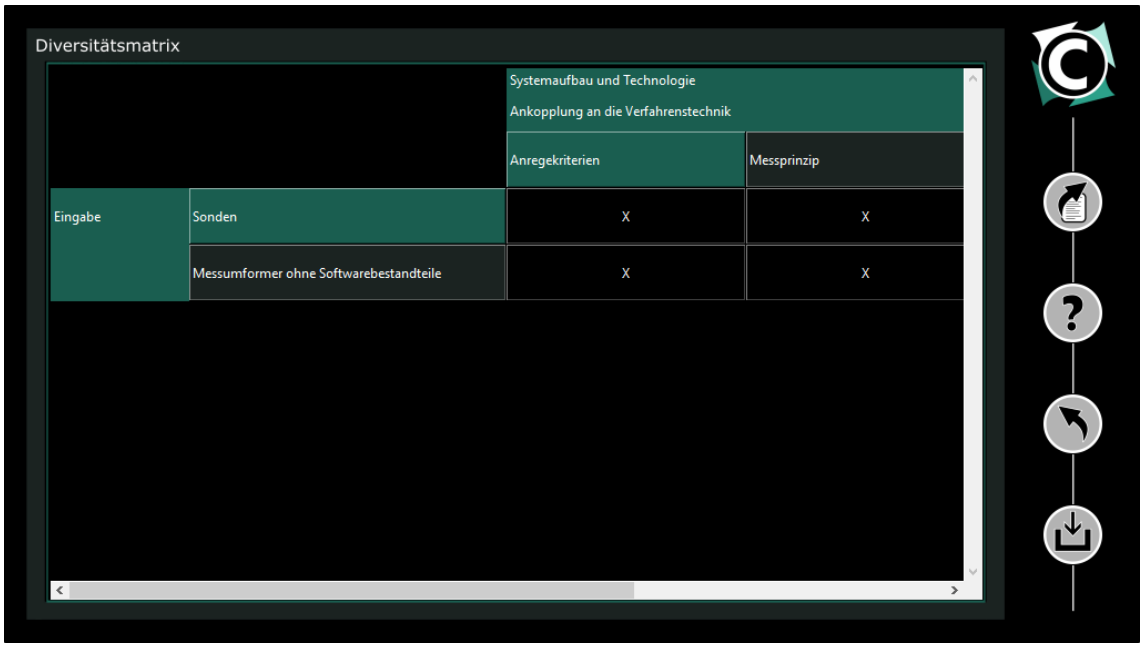


Abb. 5.9 Diversitätsmatrix im zweiten Testszenario

Nach einigen weiteren Abfragen und der Dokumentation der Zwischenergebnisse in den Schritten 22 bis 26 wurde der Prozessschritt *DO* beendet. Die Bearbeitung der nachfolgenden Prozessschritte *CHECK* und *ACT* erfolgte weitgehend analog zur Bearbeitung im ersten Testszenario. Im Gegensatz zum ersten Szenario wurde allerdings in diesem Szenario festgestellt, dass die Anforderungen an das Leittechniksystem nicht erfüllt sind (siehe Schritt 29, D-c302-e000) und eine entsprechende Rückmeldung an den Auftraggeber erstellt.

5.2.3 Bewertung des Tests

Der Ablauf der Projektbearbeitung gemäß der CAMIC-Methode mit Hilfe der CAMIC-Anwendung verlief für das Projektszenario CAMIC-Test TeSys 2 erfolgreich. Insbesondere die automatisch ausgewählten Analysemethoden entsprechen vollständig den vorab formulierten Erwartungen (Durchführung einer FMEA sowie eine Analyse mit Hilfe der Diversitätsmatrix). An einzelnen Stellen wurde auch bei diesem Test ein geringer zukünftiger Nachbesserungsbedarf entdeckt, dieser steht aber eine Anwendung der Methode und Software im aktuellen Zustand nicht entgegen.

5.3 Zusammenfassung und Gesamtbewertung der durchgeführten Tests

Die CAMIC-Methode und deren Umsetzung mit der CAMIC-Anwendung wurde modellbasiert erprobt, wie es in den beiden vorausgegangenen Abschnitten 5.1 und 5.2 anhand zweier Beispiele dargestellt ist. Die durchgeführten Tests dieser Art waren durchgängig erfolgreich, evtl. bestehende Verbesserungspotentiale für zukünftige Weiterentwicklungen wurden dabei dokumentiert.

Darüber hinaus wurden weitere Tests, sowohl einzelner Funktionen der Anwendung als auch Teilsequenzen der CAMIC-Methode, durchgeführt. Aufgrund der großen Vielzahl möglicher Entscheidung und Verläufe, ist der vollständige Test aller denkbaren Abläufe innerhalb unterschiedlicher, denkbarer Projekte nicht praktikabel und zielführend. Um zumindest die korrekte Abarbeitung aller Prozessschritte durch die Anwendung sicherzustellen, wurden auch alle Pfade der Flowcharts innerhalb der Anwendung durchfahren und damit auf grundsätzlich korrekte Funktionalität überprüft.

Mit Abschluss des aktuellen Vorhabens ist somit die CAMIC-Anwendung und damit die CAMIC-Methode vollständig einsatzbereit. Im Sinne einer agilen Entwicklung ist es auch möglich, zusätzliche Features jederzeit innerhalb kurzer Zeit zu implementieren.

6 Fazit und Ausblick

6.1 Fazit

Die im Vorhaben RS1525 entwickelten Analysemethoden und Werkzeuge wurden im aktuellen Vorhaben weiter verbessert und auf die gesamte rechnerbasierte und programmierbare Leittechnik erweitert. Darüber hinaus wurde auch eine rechnergestützte CAMIC-Anwendung entwickelt, die den Nutzer durch die Bewertung mittels der CAMIC-Methode führt.

Für die Erweiterung der CAMIC-Methode auf die Bewertung der gesamten rechnerbasierten und programmierbaren Leittechnik wurden die Flussdiagramme modifiziert. Die erweiterte CAMIC-Methode wurde anschließend als rechnergestützte CAMIC-Anwendung umgesetzt. Die gesamte CAMIC-Methode inklusive der weiterentwickelten Flussdiagramme wurden in die CAMIC-Anwendung implementiert. Darüber hinaus ist es in der CAMIC-Anwendung möglich eine Themensuche durchzuführen, neue Dokumente in der CAMIC-Anwendung hinzuzufügen, einen Bewertungsbogen im Word Format zu erstellen und den Fortschritt der Bewertung unter dem eigenen Benutzerprofil zu speichern.

Als letzter Schritt, wurden sowohl die CAMIC-Methode als auch die CAMIC-Anwendung einer modellbasierten Erprobung unterzogen.

Die angestrebte Erweiterung der CAMIC-Methode auf die Bewertung komplexer rechnerbasierter und programmierbarer Leittechnik wurde erfolgreich umgesetzt. Das Flussdiagramm der CAMIC-Methode wurde detailliert angepasst und es wurde gezeigt wie sinnvoll eine enge Benutzerführung ist. Des Weiteren ist die CAMIC-Methode als Anwendung entwickelt worden. Dadurch wurde die angestrebte Konsistenz der Bewertung erreicht. Das Vorhaben RS1560 wurde vollständig und erfolgreich abgeschlossen.

6.2 Ausblick

Für eine erweiterte Bewertung von rechnerbasierter und programmierbarer LTE bietet die CAMIC-Methode bislang noch keine ausreichende Analyse im Hinblick auf gemeinsam verursachte Ausfälle. Eines der wissenschaftlichen Arbeitsziele eines möglichen nächsten Vorhabens wäre daher die Entwicklung einer Methode für die Analyse im Hinblick auf gemeinsam verursachte Ausfälle in der Leittechnik und die Integration der

entwickelten Methode in die CAMIC-Methode und anschließende Implementierung in die CAMIC-Anwendung.

Die CAMIC-Methode basiert auf dem PDCA-Zyklus (PLAN-DO-CHECK-ACT-Zyklus). Der Vorteil der Anwendung dieses Verfahrens ist das systematische Vorgehen. Beim Einhalten der Vorgaben innerhalb der CAMIC-Methode ist ein eindeutiges Ergebnis zu erwarten. Jedoch kann es vorkommen, dass zusätzliche Informationen oder Änderungen über die zu untersuchenden, rechnerbasierten oder programmierbaren LTE während eines laufenden Bewertungsprozesses berücksichtigt werden müssen. Ein weiteres technisches Arbeitsziel wäre eine modulare Erweiterung der CAMIC-Methode dahingehend, dass eine Bewertung mit einer flexibleren Auswahl der Analyseschritte möglich ist, ohne dabei den PDCA-Zyklus zu unterbrechen. Anschließend würde diese Erweiterung in die CAMIC-Anwendung integriert werden

Die CAMIC-Anwendung unterstützt den Nutzer bei der Durchführung einer Bewertung mit Hilfe der CAMIC-Methode. Darüber hinaus eröffnet die CAMIC-Anwendung die Möglichkeit, mit mehreren Personen an der Bewertung einer rechnerbasierten oder programmierbaren LTE, in Form eines Projekts, zu arbeiten. Die eigentliche Bewertung der einzusetzenden, rechnerbasierten oder programmierbaren LTE erfolgt aktuell jedoch für viele Analyseschritte mit Werkzeugen außerhalb der CAMIC-Anwendung (per Hand, Excel etc.). Für diese Analyseschritte werden die Ergebnisse in CAMIC abgelegt. Eine automatisierte Weiterverwendung dieser Ergebnisse in weiteren Analyseschritten oder eine Plausibilitätsprüfung der erfassten Ergebnisse erfolgt bislang nicht. Letzteres ist allerdings eine wichtige Voraussetzung dafür, zuverlässig vergleichbare und personenunabhängige Bewertungsergebnisse zu erzielen. Ein weiteres technisches Arbeitsziel für ein mögliches Folgeprojekt wäre daher, eine Implementierung einzelner Analysemethoden, wie der FMEA, innerhalb der CAMIC-Anwendung umzusetzen, um eine noch schnellere und konsistentere Bewertung der rechnerbasierten und programmierbaren Leittechnik zu gewährleisten.

Darüber hinaus würde es durch die oben angesprochene, modulare Erweiterung zusätzlich möglich sein, nicht nur einen umfassenden Bewertungsprozess mittels CAMIC anzuwenden, sondern auch gezielt auf einzelne Analysemethoden zuzugreifen und für sehr spezifische Fragestellungen sogenannte „standalone“-Analysen mit CAMIC durchzuführen. Dies würde die Bewertung mit CAMIC noch flexibler gestalten.

Bei der Bewertung komplexer, rechnerbasierter und programmierbarer LTE, zum Beispiel bei der Durchführung einer FMEA, können nicht reproduzierbare Fehler auftreten. Ein möglicher Grund dafür sind menschliche Fehler bei der Bearbeitung komplexer FMEA-Tabellen. Deshalb könnte in einem Folgevorhaben vorgesehen werden, innerhalb der CAMIC-Anwendung die Durchführung der FMEA oder FTA weitestgehend auf Basis der abgefragten Informationen und erzielten Zwischenergebnisse zu automatisieren.

Literaturverzeichnis

/BFS 05/ Bundesamt für Strahlenschutz, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-37/05, ISBN 3-86509-414-7, Salzgitter, 2005.

/BMU 10/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU): Sicherheitsanforderungen an die Endlagerung wärmeentwickelnder radioaktiver Abfälle, 21 S., Bonn, 30. September 2010.

/DIN 06/ Deutsches Institut für Normung (DIN) e. V.: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA), DIN EN 60812, Beuth-Verlag, Berlin, 2006.

/DIN 07/ Deutsches Institut für Normung (DIN) e. V.: Fehlzustandsbaumanalyse, DIN EN 61025, Beuth-Verlag, Berlin, 2007.

/DIN 08/ Deutsches Institut für Normung (DIN) e. V.: Qualitätsmanagementsysteme – Anforderungen, DIN EN ISO 9001, Beuth-Verlag, Berlin, 2008.

/DIN 13/ Deutsches Institut für Normung (DIN) e. V.: Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen, DIN EN 61513, Beuth-Verlag, Berlin, 2013.

/DIN 81/ Deutsches Institut für Normung (DIN) e. V.: Fehlerbaumanalyse – Teil 1: Methoden und Bildzeichen, DIN 25424, Beuth-Verlag, Berlin, 1981.

/DIN 84/ Deutsches Institut für Normung (DIN) e. V.: Informationsverarbeitung: Sinnbilder und ihre Anwendung, DIN 66001, Beuth-Verlag, Berlin, 1984.

/GRS 15a/ GRS, Aufstellung von Kriterien zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken, GRS-395, ISBN 978-3-944161-76-1, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2015.

/GRS 15b/ GRS, Entwicklung und Einsatz von Analysemethoden zur Beurteilung softwarebasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken, GRS-355, ISBN 978-3-944161-36-5, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, März 2015.

/GRS 16/ Zuverlässigkeitsbewertung unter neuen Anforderungen an Sicherheitsleittechnik in Kernkraftwerken: Analysen der Anwendungspraxis, GRS-441, ISBN 978-3-946607-23-6, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Oktober 2016.

/GRS 17/ GRS, Neue Methoden zur Bewertung der Zuverlässigkeit fortschrittlicher Mensch-Maschine-Schnittstellen, digitaler leittechnischer Einrichtungen und personell-organisatorischer Einflüsse, GRS-A-3890, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2017.

/GRS 18/ GRS, Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik, GRS-494, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2018.

/GRS 20a/ GRS, Erforschung von Ausbreitungswegen von Softwarefehlern in softwarebasierter Leittechnik in Kernkraftwerken, GRS-599, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2020.

/GRS 20b/ GRS, Diversitätsbewertung von komplexen elektronischen Komponenten für den Einsatz in sicherheitstechnisch wichtigen Einrichtungen in Kernkraftwerken, GRS-579, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2020.

/GRS 21/ GRS, AnTeS – Entwicklung und Anwendung des Analyse- und Testsystems der GRS, GRS-648, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2021.

/GRS 21a/ GRS, Forschungsarbeiten zur Entwicklung einer Bewertungsgrundlage für rechnerbasierte und programmierbare Leittechniksysteme in kerntechnischen Anlagen und Erforschung des Weiterentwicklungsbedarfs der dazugehörigen Anforderungen in der Leittechnik, GRS-649, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, 2021.

/KTA 15/ Kerntechnischer Ausschuss (KTA): Sicherheitstechnische Regel des KTA: KTA 3501, Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems, Fassung: November 2015.

/KTA 15a/ Kerntechnischer Ausschuss (KTA): Sicherheitstechnische Regel des KTA: KTA 3503, Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik, Fassung: November 2015.

/KTA 15b/ Kerntechnischer Ausschuss (KTA): Sicherheitstechnische Regel des KTA: KTA 3505, Typprüfung von Messwertgebern und Messumformern der Sicherheitsleittechnik, Fassung: November 2015.

/NUM 21/ NumPy, Oliphant, T., et al.: https://numpy.org/, 2021.

/MAT 21/ Matplotlib, Hunter, J., et al.: https://matplotlib.org/, 2021.

/MYS 21/ MySQL, Oracle Corporation: https://www.mysql.com/de/, 2021

/PAN 21/ pandas, McKinney, W., et al.: https://pandas.pydata.org/, 2021.

/PSF 21/ Python Software Foundation, von Rossum, G., et al.: https://www.python.org/, 2021.

/TKI 21/ Tkinter, Ousterhout, J., et al.: https://docs.python.org/3/library/tkinter.html, 2021

/WER 11/ Werdich, Martin: FMEA – Einführung und Moderation, ISBN 978-3-8348-9951-4, Vieweg + Teubner, Wiesbaden, 2011

/WIK 21/ MySQL, https://de.wikipedia.org/wiki/MySQL, Stand: 20. September 2021 um 13:28 Uhr

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BMU	Bundesministerium für Umwelt
BMWi	Bundesministerium für Wirtschaft und Energie
CAMIC	cyclic analytic method for instrumentation and control
CCF	common cause failure (engl. für GVA)
FMEA	failure mode and effects analysis
FTA	fault tree analysis
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
GUI	graphical user interface
GVA	Gemeinsam Verursachte Ausfälle
I&C	instrumation and control
LT	Leittechnik
LT-Architektur	Leittechnische Architektur
LTE	Leittechnische Einrichtung
LT-Funktion	Leittechnische Funktionen
LT-System	Leittechnisches System
PDCA	Plan-Do-Check-Act
PDF	portable document format
PLD	programmable logic device
VPN	virtual private network

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

Forschungszentrum
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 978-3-949088-46-9