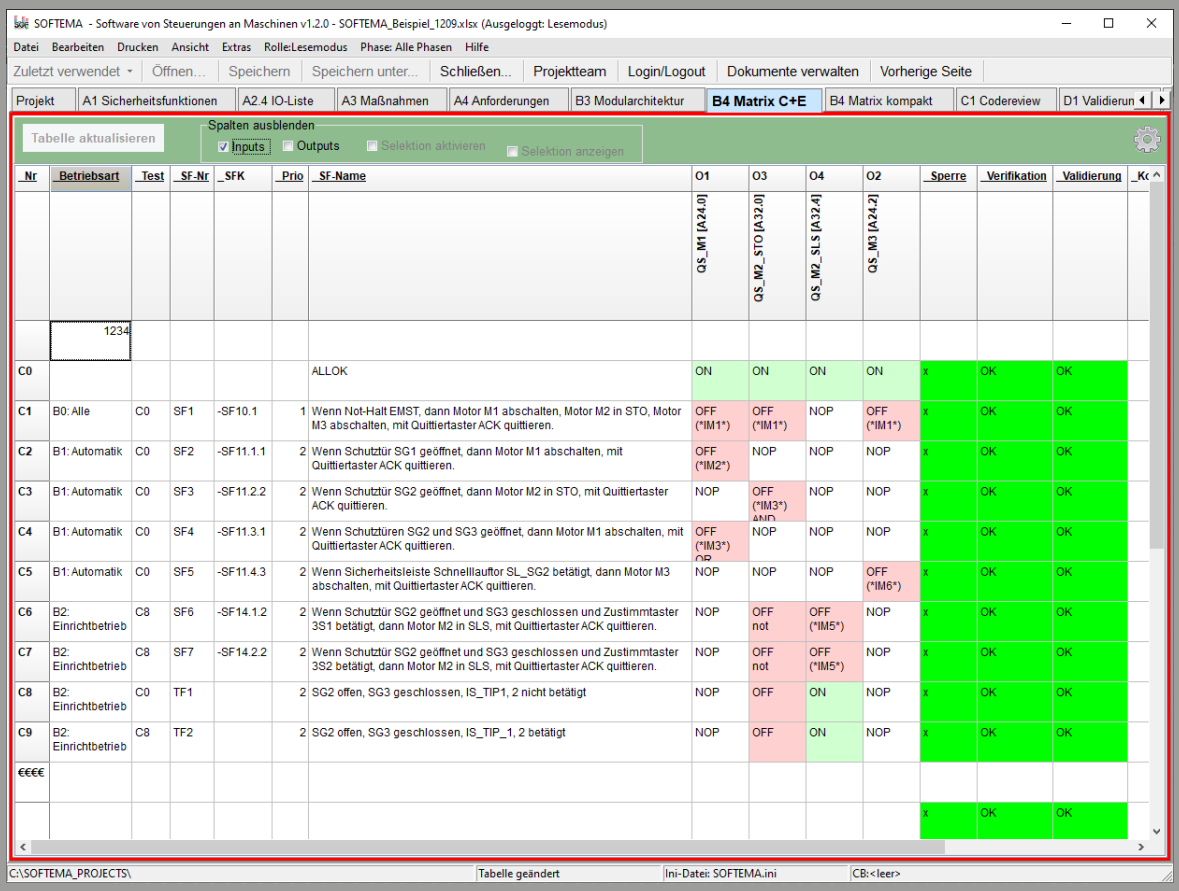
IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Das SOFTEMA-Kochbuch 2

Projektierungsleitfaden zu SOFTEMA



Verfasser: Albert Bohlscheid, Andy Lungfiel, Michael Huelke
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstr. 111
53757 Sankt Augustin
Telefon: +49 30 13001-0
Telefax: +49 30 13001-38001
Internet: www.dguv.de/ifa

Herausgeber: Deutsche Gesetzliche Unfallversicherung (DGUV)
Glinkastraße 40
10117 Berlin

– Januar 2025 –

Inhaltsverzeichnis

1 Einleitung 6

2 Über diesen Leitfaden 7

3 SOFTEMA im Überblick 9

3.1 Was kann SOFTEMA? 9

3.2 Wie wird SOFTEMA verwendet? – Ein kurzer Rundgang durch das Programm 9

3.3 Wo ist SOFTEMA erhältlich? 11

3.4 Installation und Versionierung 11

3.5 Schnittstellen zu SOFTEMA 11

3.6 Das Rollenkonzept 12

3.7 Die Benutzerverwaltung 12

4 Vorbereitung der Projektierung mit SOFTEMA 13

4.1 Spezifikation der Sicherheitsanforderungen 13

4.2 Liste der Signale und Funktionsbausteine 13

4.3 Fehlervermeidende/fehlerbeherrschende Maßnahmen 13

5 Einrichten einer Projektdatei 14

5.1 Projektorganisation festlegen 14

5.2 Projektverzeichnis auswählen und einrichten 14

5.3 Optionen für SOFTEMA einstellen 14

5.4 Passende Projektvorlage auswählen 14

5.5 Projektvorlage anpassen 15

6 Eintragen der Projektinformationen und -daten 19

6.1 Projektinformationen eintragen 19

6.2 Sicherheitsfunktionen definieren 20

6.3 Ein- und Ausgangssignale eintragen 20

6.4 Tabellen für Maßnahmen und Anforderungen konfigurieren 21

6.5 Modularchitektur eintragen 21

6.6 Tabelle „Personen“ über die Benutzerverwaltung ergänzen 21

6.7 Tabelle „Dokumente“ ergänzen 21

7 Softwareentwurf 23

7.1 Tabelle „B4 Matrix C+E“ aktualisieren und ergänzen 23

7.2 Tabelle „B4 Matrix kompakt“ aktualisieren....26
7.3 Verifikations- und Validierungspläne....27
8 Codierung des Anwendungsprogramms....28
8.1 Maßnahmen im Rahmen der Toolqualifizierung....28
9 Verifikation des codierten Programms....29
9.1 Maßnahmen im Rahmen der Toolqualifizierung....29
9.2 Verifikation in der Tabelle „A2.4 IO-Liste“....29
9.3 Verifikation in der Tabelle „A3 Maßnahmen“....29
9.4 Verifikation in der Tabelle „B3 Modularchitektur“....30
9.5 Verifikation in der Tabelle „B4 Matrix C+E“....30
9.6 Verifikation in der Tabelle „B4 Matrix kompakt“....30
9.7 Verifikation in der Tabelle „Codereview“....30
10 Validierung des Anwendungsprogramms....31
10.1 Maßnahmen im Rahmen der Toolqualifizierung....31
10.2 Validierung in der Tabelle „A2.4 IO-Liste“....31
10.3 Validierung in der Tabelle „B4 Matrix C+E“....31
10.4 Validierung in der Tabelle „B4 Matrix kompakt“....31
10.5 Validierung in der Tabelle „A1 Sicherheitsfunktionen“....31
10.6 Validierung in der Tabelle „A4 Anforderungen“....32
10.7 Validierung in der Tabelle „Validierung“....32
11 Prüfung der Projektdatei....33
11.1 Sichtprüfung in den Tabellen....33
11.2 Kommentierung in den Tabellen....33
11.3 Protokollfelder....33
12 Druckfunktionen....34
12.1 Druckeinrichtung....34
12.2 Tabellen drucken....34
12.3 Zusammenfassung erstellen....35
13 Dokumentation zum Anwendungsprogramm....39
14 Modifikation des Anwendungsprogramms....40
14.1 Modifikation von Projektdaten....40

14.2 Aktualisierung der Spezifikationstabellen 40
14.3 Verifikation, Validierung und Prüfung der Modifikationen 41
14.4 Dokumentation der Modifikationen 41
Anhang A: Literatur 42
Anhang B: Abkürzungsverzeichnis 43

1 Einleitung

Maschinenhersteller realisieren Sicherheitsfunktionen immer mehr durch die Programmierung sicherheitsgerichteter programmierbarer Steuerungen. Die Normen DIN EN ISO 13849-1 [1] und DIN EN 62061 [2] definieren unter anderem Anforderungen an die Softwareentwicklung von Sicherheitsfunktionen. Dadurch sollen gefährliche systematische Fehler in der Anwendungssoftware für eine Maschine vermieden werden.

Im DGUV-Projekt FF-FP0319 „Normgerechte Entwicklung und Dokumentation von sicherheitsbezogener Anwendersoftware im Maschinenbau“ [3] (2011 bis 2013) wurde von der Hochschule Bonn-Rhein-Sieg eine konkrete Vorgehensweise für die Umsetzung der in den neuen Normen enthaltenen Anforderungen an die Softwareentwicklung von Sicherheitsfunktionen für Maschinen erarbeitet und anhand von industriellen Beispielen evaluiert und dokumentiert. Die Projektergebnisse hat das IFA anschließend als Teil des IFA Reports 2/2016 „Sicherheitsbezogene Anwendungssoftware von Maschinen – Die Matrixmethode des IFA“ [4] veröffentlicht. Zur Umsetzung und einfacheren Anwendung dieser Matrixmethode entwickelt das IFA die Software SOFTEMA [5], das wie das IFA-Tool SISTEMA [6] zum freien Download verfügbar ist.

Als Programmdokumentation und Referenzhandbuch steht das SOFTEMA-Kochbuch 1 in SOFTEMA über den Menübefehl HILFE → SOFTEMA-KOCHBUCH 1 zur Verfügung. Dieses Kochbuch 2 beschreibt dagegen die Schritte zur Anwendung von SOFTEMA entlang des Entwicklungsprozesses (Menübefehl HILFE → SOFTEMA-KOCHBUCH 2).

Hinweis: Es wird dringend empfohlen, vor der Anwendung von SOFTEMA den IFA Report 2/2016 sowie das zur Version passende SOFTEMA-Kochbuch 1 zu lesen.

Wichtige Voraussetzung für die Arbeit mit SOFTEMA und den Projektdateien ist, dass die Anwendung der IFA-Matrixmethode sowie allgemein der Normenreihe EN ISO 13849 verstanden wurde. Das IFA unterstützt dabei mit kostenlosen Publikationen:

- Die Informationen zur Normenreihe EN ISO 13849 stellt das IFA unter http://www.dguv.de/webcode/d18471 zur Verfügung
- und Informationen zu SOFTEMA auf der Seite http://www.dguv.de/webcode/d1082520.
- Weitere Informationen, Anleitungen und Beispiele zur Anwendungsprogrammierung nach der IFA-Matrixmethode finden Sie im IFA Report 2/2016 [4] und in den SOFTEMA-Beispielen zum Download: http://www.dguv.de/webcode/d1023063
- Die Definition von Sicherheitsfunktionen ist im SISTEMA-Kochbuch 6 [7] beschrieben, siehe http://www.dguv.de/webcode/d109240.

2 Über diesen Leitfaden

Sicherheitsbezogene Anwendungssoftware für Maschinen kann nach der Matrixmethode des IFA normgerecht spezifiziert, validiert und dokumentiert werden. Mit der IFA-Software SOFTEMA lassen sich Excel-Projektdateien zur Umsetzung dieser IFA-Matrixmethode bearbeiten.

Hinweis: SOFTEMA muss – wie jedes Software-Tool für die Entwicklung und Verifikation sicherheitsgerichteter Steuerungen – für die Anwendung qualifiziert werden. SOFTEMA fällt dabei in die Kategorie „Offline Support Tools“. Daher sind bei der Anwendung von SOFTEMA die Auswirkungen potenzieller Toolfehler sowie die erforderliche Risikoreduzierung der entwickelten Sicherheitsfunktionen zu bewerten, um entsprechende fehlervermeidende Maßnahmen festzulegen (z. B. Review der SOFTEMA-Ergebnisse; Test der mit den SOFTEMA-Ergebnissen entwickelten Softwarebausteine; u. a.).
Beachten Sie daher unbedingt im SOFTEMA-Kochbuch 1 die Vorgaben zur Toolqualifizierung und zu den erforderlichen fehlervermeidenden Maßnahmen durch die Anwenderinnen und Anwender von SOFTEMA. In den folgenden Kapiteln sind diese Maßnahmen in den Projektphasen jeweils konkret benannt.

Dieser Leitfaden beschreibt die Anwendung von SOFTEMA entlang des Entwicklungsprozesses (vereinfachtes V-Modell: Abbildung 1) in folgenden Kapiteln:

- kurze Beschreibung von SOFTEMA in Kapitel 3
- vorbereitende Projektarbeiten in den Kapiteln 4, 5 und 6
- konstruktive Tätigkeiten mit Softwareentwurf und Codierung in den Kapiteln 7 und 8
- überprüfende Tätigkeiten mit Verifikation, Validierung und Prüfung in den Kapiteln 9, 10 und 11
- abschließende Arbeiten in den Kapiteln 12 und 13
- Modifikation von Anwendungsprogrammen in Kapitel 14

Die Anhänge A und B liefern Literaturhinweise und nützliche Informationen.

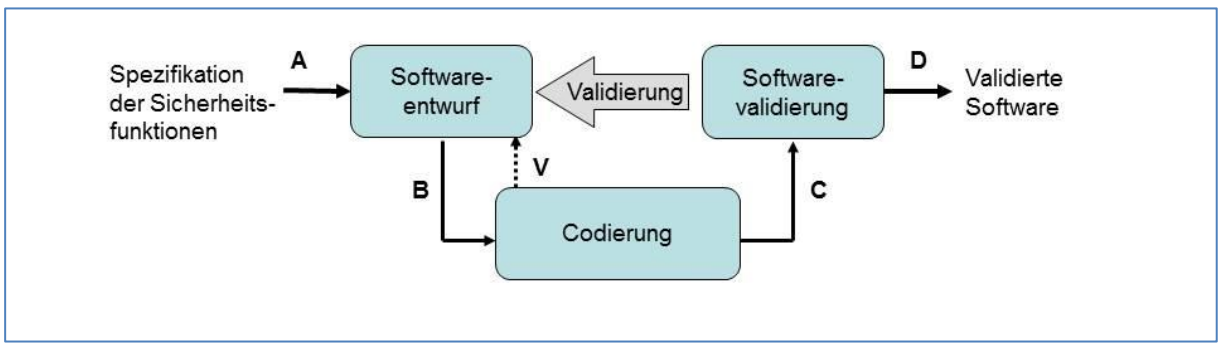


Abbildung 1: V-Modell zur Softwareentwicklung von Sicherheitsfunktionen

Änderungshistorie

Die Version dieses Kochbuchs entspricht der zugehörigen SOFTEMA-Version. Änderungen gegenüber der vorherigen Kochbuchversion sind im Text gelb markiert.

1.0.0: Kochbuch 2 zu SOFTEMA Version 1.0.0

1.1.0: Kochbuch 2 zu SOFTEMA Version 1.1.0

- Keine Änderungen

Layoutkonventionen

In diesem Kochbuch werden folgende Formate verwendet:

Kursivschrift
: wird für Dateinamen und -endungen, neue Begriffe und Hervorhebungen verwendet.

KAPITÄLCHEN
: kennzeichnen Elemente der Benutzeroberfläche wie Menünamen und Schaltflächen.

Tabellenschrift
: wird für in Tabellen verwendete Spalten- und Zeilenbezeichner verwendet (während die Tabellen*namen* in Anführungszeichen gesetzt sind).

Kästen
: heben Hinweise und Warnungen hervor.

3 SOFTEMA im Überblick

Dieses Kapitel gibt einen Überblick über die grundlegenden Merkmale und Funktionen dieses Tools. Weitergehende Informationen und Benutzerhilfen (z. B. weitere SOFTEMA-Kochbücher) finden Sie auf der Downloadseite von SOFTEMA (http://www.dguv.de/webcode/d1082520).

3.1 Was kann SOFTEMA?

SOFTEMA kann jeweils nur eine Projektdatei für die Spezifikation und Dokumentation eines Anwendungsprogrammes öffnen und bearbeiten. Die Software kann aber mehrfach ausgeführt werden, um verschiedene Projekte und Programme parallel betrachten und bearbeiten zu können. Somit können Projektdaten zwischen mehreren SOFTEMA-Instanzen (oder Excel-Instanzen) über die Zwischenablage kopiert und eingefügt werden.

SOFTEMA-Projektdateien verwenden den Dateityp einer Microsoft-Excel-Arbeitsmappe (**.xlsx*). Die Projektdateien können wahlweise mit SOFTEMA, aber auch mit Microsoft Excel direkt bearbeitet werden. Mit Excel sind alle Tabellen der Arbeitsblätter frei editierbar, unter SOFTEMA sind die Inhalte durch die Benutzerverwaltung geschützt. Nur unter SOFTEMA sind naturgemäß die spezialisierten Funktionen verfügbar, wie sie unten beschrieben sind. Die Projektdateien enthalten keine Makros und SOFTEMA kann auch keine Microsoft-Excel-Arbeitsmappen mit Makros öffnen. Alle SOFTEMA-Funktionen sind in die Software eingebunden und geschützt. Unter Excel können aber zusätzliche Arbeitsblätter eingefügt und für die Entwicklung und Dokumentation genutzt werden, z. B. für die Dokumentation der Steuerungshardware. SOFTEMA kann diese zusätzlichen Arbeitsblätter laden und anzeigen, aber nicht editieren.

3.2 Wie wird SOFTEMA verwendet? – Ein kurzer Rundgang durch das Programm

SOFTEMA verwaltet die für die Matrixmethode des IFA [4] notwendigen Tabellen und darüber hinaus auch die für das Projektmanagement notwendigen Informationen wie Projektbeschreibung, Benutzerverwaltung, Änderungsprotokolle, Dokumentenmanagement usw. Abbildung 2 zeigt z. B. die Cause&Effect-(C&E)-Matrix für die Softwarespezifikation eines Projektes in SOFTEMA.

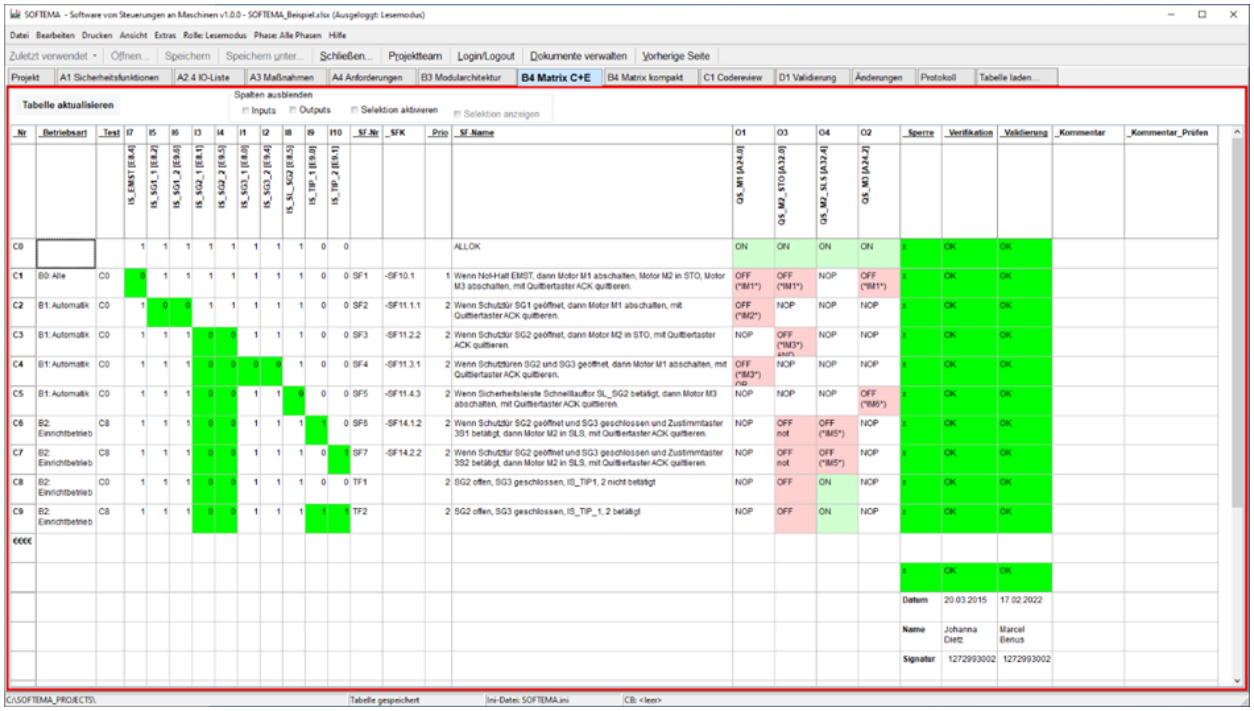


Abbildung 2: C&E-Matrix in SOFTEMA

Für ein neues Projekt eröffnet der Benutzer eine leere, aber schon vorformatierte Projektvorlage. Nach Ausfüllen der Projektbeschreibung (Tabelle „Projekt“) werden in Tabelle „A1 Sicherheitsfunktionen“ die Sicherheitsfunktionen mit ihren Eigenschaften wie PL_r, Betriebsart, Priorität usw. eingetragen (siehe SISTEMA Kochbuch 6 [7]). In Tabelle „A2.4 IO-Liste“ werden die Ein- und Ausgangssignale eingetragen, jeweils mit Variablennamen und Hardware/Netzwerk-Adressen. In alle Tabellen können auch externe Inhalte über die Zwischenablage kopiert und eingefügt werden.

Der Katalog fehlervermeidender Maßnahmen und die Programmierregeln können in Tabelle „A3 Maßnahmen“ ausgewählt und angepasst werden. Die Tabellen „A3 Maßnahmen“ und „A4 Anforderungen“ sollten schon vorab in der Projektvorlage vorbelegt sein. Anhand der Sicherheitsfunktionen, der Peripheriehardware und der I/O-Liste ergibt sich die Liste der erforderlichen Funktionsbausteine für Vorverarbeitungs- und Ansteuerungsebene. Diese sollten in Tabelle „B3 Modularchitektur“ verwaltet werden.

Mit diesen Vorbereitungen kann die Tabelle „B4 Matrix C+E“ ausgefüllt werden. Dies erfolgt mit den Schaltflächen zur automatischen Aktualisierung für I/O-Signale, Module und Sicherheitsfunktionen. Die eigentliche Softwarespezifikation erfolgt dann durch

- Zuordnen von Eingangssignalen zu den einzelnen Sicherheitsfunktionen und
- Eintragen der logischen Verknüpfung der Eingangssignale mit den Schaltvorgängen der Ausgangssignale.

Der zweite Punkt wird für die Codierung der Ansteuerlogik benötigt. Ein spezialisierter Editor hilft bei dieser Verknüpfung. Bei umfangreichen Projekten hilft die kompakte Darstellung in

Tabelle „B4 Matrix kompakt“. Man erstellt diese Tabelle allein durch die Aktualisierungsfunktion, die die Tabelle „B4 Matrix C+E“ automatisch umwandelt. Spätestens zu diesem Zeitpunkt sollten alle verfügbaren Funktionen zur formalen Verifikation der genannten Tabellen genutzt worden sein, um Auslassungen, Dubletten und Widersprüche aufdecken und korrigieren zu können.

Nach der Verifikation aller Eingangsdokumente und der oben beschriebenen Spezifikation kann die Codierung des Programms in der für die Steuerung gewählten Sprache erfolgen. Der Code wird ebenfalls verifiziert. Dieser Vorgang wird in verschiedenen Tabellen im Detail und zusammenfassend auch in „C1 Codereview“ dokumentiert. Danach wird das Programm validiert, was ebenfalls in verschiedenen Tabellen einzeln dokumentiert und in Tabelle „D1 Validierung“ zusammengefasst wird. In den Tabellen C1 und D1 können die Fragen nach Bedarf angepasst und auch ergänzt werden. Personen, die anschließend das Projekt prüfen, können ihre Tätigkeit ebenfalls dokumentieren und kommentieren.

Bei Modifikationen der Sicherheitsfunktionen, der I/O-Signale oder der Funktionsbausteine werden die Änderungen aus den Tabellen A1, A2.4 und B3 wiederum in den Spezifikationstabellen automatisch aktualisiert und manuell überarbeitet. Alle Modifikationen werden zunächst farblich (gelb) markiert. Die Markierungen werden nach Abschluss der erneuten Codierung, Verifikation und Validierung dieser Modifikationen manuell gelöscht.

3.3 Wo ist SOFTEMA erhältlich?

Das Tool SOFTEMA wird auf den Internetseiten des IFA als Freeware zur kostenlosen Benutzung angeboten. Aktuelle Informationen über den Entwicklungsstand, Betaversionen sowie der Link zum Download sind unter der Internetadresse http://www.dguv.de/webcode/d1082520 erhältlich.

3.4 Installation und Versionierung

SOFTEMA wird mit dem mitgelieferten Installationsprogramm installiert. SOFTEMA-Projektdateien sind mit einer vierstelligen Versionsnummer x.y.z.B versehen. Sie entstammt dem SOFTEMA-Programm, mit dem sie erstellt bzw. geändert wurden. Weitere Informationen zu diesen Themen finden sich im SOFTEMA-Kochbuch 1, der Information „SOFTEMA – Erste Schritte“ sowie in der SOFTEMA FAQ.

3.5 Schnittstellen zu SOFTEMA

In SOFTEMA selbst sind in der aktuellen Version keine Schnittstellen implementiert. Es bietet sich eher an, Schnittstellen direkt zur Excel-Datei zu realisieren, um Daten importieren und exportieren zu können.

3.6 Das Rollenkonzept

In SOFTEMA sind verschiedene Rollen für die projektbeteiligten Personen definiert. Jede beteiligte Person sollte sich die für die Aufgabe passende Rolle auswählen. Jede Rolle hat in den Tabellen festgelegte Berechtigungen. Dadurch werden unberechtigte und unbeabsichtigte Änderungen vermieden. So kann z. B. eine Person in der Rolle Prüfen1 keine Tabelleninhalte ändern, sondern nur lesen. Einzig die Spalte _Kommentar_Prüfen und ihre Protokollfelder (Prüfen1, Datum) können in dieser Rolle beschrieben werden. Die aktuelle Definition der Rollen ist im SOFTEMA-Kochbuch 1, Abschnitt 4.10 beschrieben.

3.7 Die Benutzerverwaltung

Die aktuelle Beschreibung der Benutzerverwaltung ist im SOFTEMA-Kochbuch 1, Abschnitt 4.11 zu finden.

4 Vorbereitung der Projektierung mit SOFTEMA

Dieses Kapitel beschreibt, welche Unterlagen und Informationen vorliegen müssen, damit eine Projektierung mit SOFTEMA beginnen kann.

4.1 Spezifikation der Sicherheitsanforderungen

Eine ganz grundlegende Voraussetzung für die Programmierung von Sicherheitsfunktionen ist das Vorliegen der Sicherheitsanforderungen für eine projektierte Maschine. Ein allgemeines Gliederungsschema für eine Spezifikation der Sicherheitsanforderungen wird im IFA-Report 2/2017 [8], Kasten 6.1 vorgeschlagen. Zu diesen Sicherheitsanforderungen gehört auch die Liste der Sicherheitsfunktionen, die im Kapitel 5 desselben Reports eingeführt werden. Die Definition von Sicherheitsfunktionen ist im SISTEMA-Kochbuch 6 [7] im Detail beschrieben. Alle Sicherheitsfunktionen einschließlich ihrer Eigenschaften müssen vorliegen, damit sie in die Tabelle „A1 Sicherheitsfunktionen“ der Projektdatei eingetragen werden können.

Über die Windows-Zwischenablage können einzelne Texte oder eine Auswahl mehrerer Zellen in die Tabelle eingefügt werden; der Import einer kompletten Liste über eine Datenschnittstelle ist in SOFTEMA aktuell nicht implementiert.

4.2 Liste der Signale und Funktionsbausteine

Auf Basis der funktionalen und der Sicherheitsanforderungen wird die Steuerungshardware spezifiziert und projektiert. Daraus ergeben sich ebenfalls wichtige Informationen für die Projektierung mit SOFTEMA.

Für die Spezifikation der Sicherheitsfunktionen müssen auch die sicherheitsbezogenen Ein- und Ausgangssignale vorliegen. Diese sind in die Tabelle „A2.4 IO-Liste“ einzutragen.

Zusätzlich können die für die Vorverarbeitungs- und Ansteuerungsebene verwendeten, vom Hersteller oder selbst entwickelten Funktionsbausteine in die Tabelle „B3 Modularchitektur“ eingetragen werden.

Über die Windows-Zwischenablage können einzelne Texte oder eine Auswahl mehrerer Zellen in die Tabelle eingefügt werden; der Import dieser Listen über eine Datenschnittstelle ist in SOFTEMA aktuell nicht implementiert.

4.3 Fehlervermeidende/fehlerbeherrschende Maßnahmen

Vor der Projektierung muss festgelegt werden, welche fehlervermeidenden/fehlerbeherrschenden Maßnahmen angewendet werden sollen. Nähere Informationen zu wichtigen Maßnahmen finden sich im IFA-Report 2/2016, Kapitel 5. Diese Maßnahmen, weitere Projektierungsregeln und technische Merkmale sind in der Projektvorlagedatei in die Tabelle „A3 Maßnahmen“ einzutragen (Abschnitt 5.5.5).

5 Einrichten einer Projektdatei

In diesem Kapitel wird dargestellt, wie SOFTEMA und die verwendete Projektvorlagedatei konfiguriert werden.

5.1 Projektorganisation festlegen

Vor dem Einrichten einer Projektdatei ist Folgendes zu klären: Welche Personen arbeiten an welchen Projekten bzw. Applikationen in welcher Rolle? Projektleitende Personen übernehmen in der Vorbereitung eines SOFTEMA-Projektes eine wichtige Rolle, denn sie sind in der Regel für die Projektqualität und die Umsetzung von Maßnahmen gegen Softwarefehler verantwortlich. Dazu gehören die Festlegung von Anforderungen und fehlervermeidenden Maßnahmen (Abschnitt 5.5.5) sowie die Gestaltung geeigneter Prüfprotokolle (Abschnitte 5.5.10 und 5.5.11).

5.2 Projektverzeichnis auswählen und einrichten

Zunächst muss das Projektverzeichnis festgelegt werden. Es kann sich auf einem lokalen oder auf einem vernetzten Datenträger befinden. Volle Schreib- und Leserechte müssen vorhanden sein. In diesem Verzeichnis werden eine oder mehrere Projektdateien für ein oder mehrere Steuerungsprogramm/e (z. B. für eine Maschine) bearbeitet. Alle diese Projektdateien werden durch die INI-Dateien im Projektverzeichnis gleichartig konfiguriert (siehe Abschnitt 5.3). Dokumente sollten ebenfalls in einem Unterverzeichnis des Projektverzeichnisses gespeichert werden. Auf diese Weise kann das Projektverzeichnis mit allen zusammengehörigen Dateien mit einem Archivierungstool archiviert werden.

5.3 Optionen für SOFTEMA einstellen

Mögliche Bearbeitungsoptionen sind im SOFTEMA-Kochbuch 1, Kapitel 9 „Optionen“ beschrieben. SOFTEMA kann „projektbezogene“ Optionen über verschiedene Initialisierungsdateien (kurz INI-Dateien) einlesen. Diese INI-Dateien wirken auf alle Projektdateien im selben Verzeichnis.

Außerdem gibt es „SOFTEMA-bezogene“ Optionen: Sie wirken auf das generelle Verhalten von SOFTEMA für alle Projektdateien (unabhängig von ihrem Speicherort und werden über die Menüleiste mit dem Befehl EXTRAS → OPTIONEN eingestellt. Diese globalen Einstellungen werden von SOFTEMA in der Windows-Registrierungsdatenbank (des Anwenders) abgelegt – d. h., zu diesen Optionen gibt es keine Initialisierungsdateien!

5.4 Passende Projektvorlage auswählen

SOFTEMA kann keine neuen Projektdateien generieren. Es wird stattdessen eine vorbereitete Projektdatei als Vorlage (Template) verwendet und in SOFTEMA geöffnet. Zum

Testen von SOFTEMA kann man direkt mit der installierten Standardvorlagedatei *__SOFTEMA_Template__.xlsx* beginnen. Darauf aufbauend wird es erforderlich und sinnvoll sein, diese Standardvorlagedatei zu erweitern, um eine unternehmens- bzw. projekt-spezifische Projektvorlage zu erhalten. Die regelmäßige Pflege und Verwendung solch einer individuell angepassten Projektvorlage erhöht sicherlich die Akzeptanz und Effizienz der Matrixmethode mit SOFTEMA. Im folgenden Abschnitt 5.5 sind die Schritte der Vorlage-anpassung beschrieben. Ist bereits eine angepasste Projektvorlage vorhanden, dann kann dieser Abschnitt übersprungen werden.

5.5 Projektvorlage anpassen

Ausgehend von der Standardvorlagedatei *__SOFTEMA_Template__.xlsx* können einige Tabellen direkt in der Benutzeroberfläche von SOFTEMA bearbeitet werden, wobei diese Tabellen eventuell einfacher mit Microsoft Excel anzupassen sind. Beide Wege sind möglich.

Andere Tabellen der Projektvorlage können dagegen nur mit Microsoft Excel bearbeitet werden. Dies trifft insbesondere auf die Tabellen mit Maßnahmen und Anforderungen sowie die Protokolltabellen zu.

Hinweis: In allen Tabellen können zudem individuelle Spalten und Zeilen ergänzt werden (siehe SOFTEMA-Kochbuch 1, Kapitel „Beschreibung des Datenformats für SOFTEMA“). Dies ist meistens nur mit Microsoft Excel möglich. Darüber hinaus können in den Tabellenbereichen über dem Start-Steuerzeichen bzw. unterhalb des Ende-Steuerzeichens Hinweise, Logos etc. eingetragen werden. Nach der Bearbeitung mit Excel passt allerdings die Prüfsumme der Projektdatei nicht mehr und beim Öffnen mit SOFTEMA erscheint eine Fehlermeldung. Man kann trotzdem weiterarbeiten und beim nächsten Speichern wird die Prüfsumme korrekt gesetzt.

5.5.1 Tabelle „Personen“ anpassen bzw. Benutzerverwaltung anlegen

Zuallererst sollte die zuständige Person, die das SOFTEMA-Template anpasst, eine Benutzerverwaltung anlegen, da andernfalls die Bearbeitung verschiedener Tabellen in SOFTEMA nicht möglich ist. Dieser Schritt muss in SOFTEMA erfolgen, da für die Tabelle ein „Blattschutz“ aktiv ist, um sie vor Manipulation zu schützen.

Hinweis: Das Tabellenblatt „Personen“ wird von SOFTEMA für die Benutzerverwaltung verwendet und darf nicht mit Excel bearbeitet werden!

Das SOFTEMA-Template verfügt zu Beginn nur über einen Benutzer, den „Admin“. Sein Standard-Passwort zu Beginn ist „admin“ und muss zwingend nach dem ersten Login geändert werden!

Eine genaue Beschreibung der Benutzerverwaltung findet sich in SOFTEMA-Kochbuch 1, Kapitel 4.11 „Benutzerverwaltung“.

Zum Anpassen des SOFTEMA-Templates empfiehlt es sich, einen Benutzer mit Superuser-Rechten anzulegen. Dieser kann alle Tabellen bearbeiten und ggf. am Ende der Bearbeitung gelöscht werden.

5.5.2 Tabelle „Projekt“ anpassen

In Microsoft Excel können zusätzliche Zeilen P17 bis P20 und P24 bis Pxy mit eigenen Bezeichnungen ergänzt werden (siehe SOFTEMA-Kochbuch 1, Abschnitt „Registerkarte Projekt“). Auch zusätzliche Kommentarzeilen (ohne Zeilenbezeichner der Spalte _Nr) sind möglich.

5.5.3 Tabelle „A1 Sicherheitsfunktionen“ anpassen

Mit Microsoft Excel können in der Projektvorlage bereits Kommentarzeilen (ohne Zeilenbezeichner der Spalte _Nr) ergänzt werden z. B. „Automatikbetrieb“, „Einrichtbetrieb“ o.Ä. Dies kann aber auch später über das Kontextmenü in SOFTEMA erfolgen.

5.5.4 Tabelle „A2.4 IO-Liste“ anpassen

Mit Microsoft Excel können in der Projektvorlage bereits Kommentarzeilen (ohne Zeilenbezeichner der Spalte _Nr) ergänzt werden z. B. „Eingangssignale“, „Ausgangssignale“ o.Ä. Dies kann aber auch später über das Kontextmenü in SOFTEMA erfolgen.

5.5.5 Tabelle „A3 Maßnahmen“ anpassen

Diese Tabelle dokumentiert alle getroffenen Maßnahmen (Programmierregeln, Tools, Konventionen, Fehlererkennung und -beherrschung etc.) für dieses Programmierprojekt. Mit Microsoft Excel können Zeilen mit den einzelnen Maßnahmen ergänzt, editiert oder gelöscht werden. Jede Maßnahme muss dann durch einen Zeilenbezeichner der Form Rx in der Spalte _Nr eindeutig benannt werden. Zusätzliche Kommentarzeilen (ohne Zeilenbezeichner der Spalte _Nr) helfen, die Maßnahmen zu strukturieren und mit Überschriften zu versehen. Die Tabelle der Standardvorlagedatei dient dabei nur als Beispiel und darf keinesfalls unverändert weiterverwendet werden.

Während der späteren Projektierung mit SOFTEMA kann die Rolle „Projektleiten“ einzelne Maßnahmen deaktivieren (Spalte _Aktiv) und ändern.

5.5.6 Tabelle „A4 Anforderungen“ anpassen

Diese Tabelle dokumentiert, welche normativen Anforderungen für das Projekt relevant sind. Mit Microsoft Excel können Zeilen mit den einzelnen Anforderungen ergänzt, editiert oder gelöscht werden. Jede Anforderung muss dann durch einen Zeilenbezeichner der Form Ax in der Spalte _Nr eindeutig benannt werden. Zusätzliche Kommentarzeilen (ohne Zeilenbezeichner der Spalte _Nr) helfen, die Anforderungen zu strukturieren und mit Überschriften

zu versehen. Die Tabelle der Standardvorlagedatei kann dabei als Beispiel dienen, enthält sie doch typische Anforderungen der DIN EN ISO 13849-1:2016 [1], Abschnitt 4.6, an Anwendungssoftware.

Während der späteren Projektierung mit SOFTEMA können einzelne Anforderungen deaktiviert (Spalte _Aktiv), aber nicht mehr geändert werden.

5.5.7 Tabelle „B3 Modularchitektur“ anpassen

Mit Microsoft Excel können in der Projektvorlage bereits Kommentarzeilen (ohne Zeilenbezeichner der Spalte _Nr) ergänzt werden z. B. „Eingangsmodule“, „Ausgangsmodule“ o. Ä.. Dies kann aber auch später über das Kontextmenü in SOFTEMA erfolgen. Weiterhin könnten typische, immer wieder verwendete Funktionsbausteine schon vorab in die Projektvorlage eingetragen oder über die Initialisierungsdatei *SOFTEMA_FB.INI* eingelesen werden (siehe SOFTEMA-Kochbuch 1, Kapitel „Optionen“).

5.5.8 Tabelle „Personen“ anpassen bzw. neue Teammitglieder anlegen

Über die Benutzerverwaltung von SOFTEMA können schon bei der Vorlagedatei alle typischerweise beteiligten internen und externen Personen mit ihren Kontaktdaten eingetragen werden. Im Laufe des Projekts können über die Benutzerverwaltung jederzeit Benutzer editiert/hinzugefügt/gelöscht werden. Welche dieser Personen in welcher Rolle letztlich an einem bestimmten Projekt beteiligt sind wird auch über die Benutzerverwaltung von SOFTEMA administriert.

5.5.9 Tabelle „Dokumente“ anpassen

In dieser Tabelle können schon bei der Vorlagedatei solche Dokumente eingetragen werden, die bei jedem konkreten Projekt von Bedeutung sein können (Richtlinien, Normen, Anweisungen, Programmierregeln, usw.). Jedes Dokument muss dann durch einen Zeilenbezeichner der Form Dx in der Spalte _Nr eindeutig benannt werden. Während des Projektes kann die Tabelle noch über das Kontextmenü in SOFTEMA bearbeitet und um projektspezifische Dokumente erweitert werden.

5.5.10 Protokolltabelle „C1 Codereview“ anpassen

Diese Tabelle enthält Fragen zum Codereview. Die Inhalte der Standardvorlagedatei können als Beispiel verwendet werden, aber auch in der Spalte _Beschreibung geändert und darüber hinaus um eigene spezifische Fragen oder Aspekte ergänzt werden. Weitere Details finden Sie im SOFTEMA-Kochbuch 1, Abschnitt „Registerkarte: C1 Codereview“. Jede Protokollzeile muss dann durch einen Zeilenbezeichner der Form Rx in der Spalte _Nr eindeutig benannt werden. Während der späteren Projektierung mit SOFTEMA können einzelne Protokollfragen nicht mehr über das Kontextmenü geändert werden, sondern nur in Excel.

5.5.11 Protokolltabelle „D1 Validierung“ anpassen

Diese Tabelle enthält Fragen zur abschließenden Validierung, wobei diese in zwei Tabellenbereichen (oben zu Validierungsschritten und unten zur Projektdokumentation) dargestellt werden. Die Inhalte der Standardvorlagedatei können als Beispiel verwendet werden, aber auch in der Spalte _Beschreibung geändert und darüber hinaus um eigene spezifische Fragen oder Aspekte ergänzt werden. Für weitere Details lesen Sie bitte SOFTEMA-Kochbuch 1, Abschnitt „Registerkarte: D1 Validierung“. Jede Protokollzeile muss dann durch einen Zeilenbezeichner der Form Vx (für Fragen/Aspekte der Validierung) bzw. Dx (für Fragen/Aspekte der Dokumentation) in der Spalte _Nr eindeutig benannt werden. Während der späteren Projektierung mit SOFTEMA können einzelne Protokollfragen nicht mehr über das Kontextmenü geändert werden, sondern nur in Excel.

5.5.12 Weitere Tabellen anpassen

Es gibt weitere Tabellen, die keine Anpassung in der Vorlagedatei erfahren. Gleichwohl müssen in allen Tabellen die Steuerzeichen („$$$$“) und die Spaltenbezeichner eingetragen sein, sonst kann die Datei nicht geöffnet werden. Im Einzelnen sind es:

- Die Tabelle „B4 Matrix C+E“ wird von SOFTEMA anhand der Projektvorgaben automatisch generiert und von den SOFTEMA-Anwenderinnen und -Anwendern vervollständigt. Inhaltszeilen mit dem Zeilenbezeichner Cx können also vorab nicht eingetragen werden, die Tabelle ist in der Projektvorlage leer.
- Die Tabelle „Änderungen“ ist in der Projektvorlage leer und wird von den SOFTEMA-Anwenderinnen und Anwendern während des Projektes gefüllt.
- Die Tabellen „B4 Matrix kompakt“ und „Protokoll“ werden vollständig von SOFTEMA generiert und aktualisiert. Daher können und dürfen diese Tabellen vorher nicht angepasst werden und enthalten in der Vorlagedatei keine Inhaltszeilen mit dem jeweiligen Zeilenbezeichner.

5.5.13 Optionale Projekttabellen

Bei der Vorbereitung einer projektspezifischen Vorlagedatei können weitere optionale Tabellen als Excel-Arbeitsblätter ergänzt werden. Diese Tabellen mit Texten und Grafiken können von SOFTEMA in einer eigenen Registerkarte geladen und angezeigt (siehe SOFTEMA-Kochbuch 1, Abschnitt „Registerkarte: Tabelle laden“), aber nicht dort bearbeitet werden.

6 Eintragen der Projektinformationen und -daten

Vor Beginn einer SOFTEMA-Projektierung liegen typischerweise schon eine Reihe von Informationen und Daten aus der Risikobeurteilung, der Projekt- und der Hardwareplanung vor. In diesem Kapitel wird beschrieben, wie diese Informationen und Daten in die verwendete Projektvorlagedatei (Abschnitt 5) eingetragen werden sollen bzw. müssen. Dies sollte in der Regel über die Benutzeroberfläche von SOFTEMA erfolgen. Bei größeren Datenmengen kann aber die Projektdatei auch noch mit Microsoft Excel bearbeitet werden, wobei sehr auf die korrekte Formatierung der Tabellen zu achten ist.

6.1 Projektinformationen eintragen

Im SOFTEMA-Kochbuch 1 ist im Kapitel „Aufbau und Funktionen der Registerkarten und Tabellen“ die Registerkarte PROJEKT mit den Spalten- und Zeilenbezeichnern beschrieben. Einige Zeilen werden von SOFTEMA gefüllt. Folgende Zeilen (Tabelle 1) sollten manuell zu Projektbeginn eingetragen werden:

Tabelle 1: Projektinformationen

_Bezeichnung	Beschreibung
Projektname Projektstatus Projektversion Projektnummer Auftraggeber Auftragnehmer	Der Projektname und die Projektnummer werden im Projektverlauf typischerweise konstant bleiben, während der Projektstatus je nach Fortschritt angepasst werden sollte. Die Auswahl für den Projektstatus ist konfigurierbar. Die Projektversion ist ggf. gemäß Projektfortschritt und nach Modifikationen anzupassen.
Projektleiten Projektieren Inbetriebnehmen Validieren Prüfen1 Prüfen2	Die Namen der Personen mit diesen Rollen können manuell editiert oder aus der Dropdown-Liste gewählt werden. Die Liste wertet dabei die Tabelle „Personen“ aus, die zuvor ausgefüllt worden sein sollte. Damit können die beteiligten Personen und auch deren Unabhängigkeitsgrade [4] dokumentiert werden.
Anlage/Maschine Dokumentation Dokument	Mit diesen Zeilen kann die projektierte Anlage/Maschine beschrieben werden, z. B. durch ein verlinktes Dokument wie etwa eine Projektspezifikation.

_Bezeichnung	Beschreibung
Projektspezifische Zeilen	In der Tabelle „Projekt“ können zusätzliche projektspezifische Zeilen ergänzt werden (siehe SOFTEMA-Kochbuch 1). Die Beschreibungen sind auch entsprechend auszufüllen.

6.2 Sicherheitsfunktionen definieren

Im SOFTEMA-Kochbuch 1 ist die „Registerkarte A1 Sicherheitsfunktionen“ beschrieben. Im Rahmen der Risikobeurteilung werden üblicherweise die Sicherheitsfunktionen definiert [7]. Diese sind dann möglichst vollständig in dieser Registerkarte einzutragen – als Vorgabe für die mit SOFTEMA durchzuführende Softwarespezifikation. Dabei gibt es zwei Wege, die im SOFTEMA-Kochbuch 1 detailliert beschrieben sind:

- Die Funktionsbezeichnung kann in der Spalte _Beschreibung direkt eingetragen und um die Spalten _PLr bis _Betriebsart ergänzt werden oder
- sie wird nach vorherigem Konfigurieren der Funktionen in den Spalten _Schutz bis Bx generiert und ebenfalls um die Spalten _PLr bis _Betriebsart ergänzt.

Um eine eindeutige Nachverfolgbarkeit im Rahmen der gesamten Maschinen/Anlagen-Projektierung zu ermöglichen, sollte jeder Sicherheitsfunktion eine Kennung der Sicherheitsfunktion _SFK zugeordnet und in anderen Projektdokumenten referenziert werden.

Mit den Befehlen des Kontextmenüs lassen sich neue Tabellenzeilen (Sicherheitsfunktionen) erstellen bzw. vorhandene Zeilen kopieren und anpassen. Die Zeilenbezeichner gelöschter Zeilen werden nicht wiederverwendet.

6.3 Ein- und Ausgangssignale eintragen

Im SOFTEMA-Kochbuch 1 ist die „Registerkarte A2.4 IO-Liste“ beschrieben. Im Rahmen der Hardware-Projektierung werden üblicherweise die Ein- und Ausgangssignale der programmierten Steuerung mit ihren Adressen, Variablensymbolen und Bezeichnungen festgelegt. Sie sind dann möglichst vollständig in dieser Registerkarte einzutragen – als Vorgabe für die mit SOFTEMA durchzuführende Softwarespezifikation.

Dabei gibt es in der aktuellen SOFTEMA-Version zwei Wege:

- Direktes Eintragen der Signale in den Spalten _Beschreibung bis _Modul oder
- Kopieren dieser Spalteninhalte aus einer bereits vorhandenen externen Signalliste in die Windows-Zwischenablage und Einfügen in vorher erstellte, leere Signalzeilen dieser Tabelle.

Für zukünftige Versionen sind Import-Funktionalitäten für gängige Datenformate geplant.

Die Spalte „_Modul“ stellt eine Besonderheit dar. Falls ein Eingangssignal bzw. das Ausgangssignal über einen Funktionsbaustein bzw. Modul verarbeitet wird, kann dieses Modul

hier angegeben werden. Nur Funktionsbausteine bzw. Module die bereits in der Tabelle „B3 Modularchitektur“ angelegt wurden können hier ausgewählt werden.

Ist ein Modul definiert, so wird für dieses Signal, in der Tabelle „B4 Matrix C+E“, in der eckigen Klammer nicht die Adresse z.B. [E8.4] sondern der Funktionsbausteinname z.B. [DOOR_SG1] dargestellt.

Die Spalte „_Aktiv in C+E“ kann dabei helfen, die Übersicht in der Tabelle „B4 Matrix C+E“ zu behalten. Bei der Aktualisierung der Tabelle „B4 Matrix C+E“ werden automatisch alle Eingangs- bzw. Ausgangssignale der Matrix hinzugefügt. Gibt es Signale, die für die Matrix nicht benötigt werden – da sie z. B. nur von einem Funktionsbaustein selbst verarbeitet werden – können sie hier deaktiviert werden. Deaktivierte Signale werden nun (bei einer Aktualisierung) der C+E-Matrix nicht hinzugefügt bzw. als entfernt markiert.

6.4 Tabellen für Maßnahmen und Anforderungen konfigurieren

Im SOFTEMA-Kochbuch 1 sind die „Registerkarte A3 Maßnahmen“ sowie die „Registerkarte A4 Anforderungen“ beschrieben. Die Inhalte dieser beiden Tabellen sind schon durch die Projektvorlage (Abschnitt 5.5) vorgegeben und die Tabelle A4 kann in SOFTEMA nicht mehr editiert werden. Es können aber einzelne Maßnahmen und Anforderungen deaktiviert werden (Spalte _Aktiv), wodurch sie dann bei der Projektierung und Validierung unberücksichtigt bleiben. In solchen Fällen sollte in die Kommentarspalte eine Begründung für die Deaktivierung eingetragen werden.

6.5 Modularchitektur eintragen

Im SOFTEMA-Kochbuch 1 ist die „Registerkarte B3 Modularchitektur“ beschrieben. Um das Projekt vollständig zu dokumentieren, sollten die verwendeten Funktionsbausteine mit all ihren Instanzen und ergänzenden Informationen eingetragen werden. Dies ist u. a. Teil des Konfigurationsmanagements. Für das spätere Editieren der Logikzellen in Tabelle „B4 Matrix C+E“ ist es mindestens erforderlich, den Instanzennamen und das sicherheitsbezogene Freigabesignal (nur ein Ausgang!) dieser Funktionsbausteine einzutragen (Spalten _Instanzname und _Ausgänge).

6.6 Tabelle „Personen“ über die Benutzerverwaltung ergänzen

Im SOFTEMA-Kochbuch 1 ist das Formular PROJEKTTEAM beschrieben (Abschnitt 8.1.14). Die bereits in der Vorlagedatei eingetragenen Personen können zu Projektbeginn oder auch später über die Benutzerverwaltung aktualisiert und ergänzt werden.

6.7 Tabelle „Dokumente“ ergänzen

Im SOFTEMA-Kochbuch 1 ist die „Registerkarte Dokumente“ beschrieben. Die bereits in der Vorlagedatei eingetragenen „Standarddokumente“ können zu Projektbeginn oder auch

später noch um projektspezifische Dokumente, Beschreibungen, Literatur usw. ergänzt werden.

7 Softwareentwurf

Nachdem alle für die Projektierung verfügbaren Informationen und Daten in die vorbereitete Projektvorlage eingetragen wurden, kann mit der SOFTEMA-Projektierung begonnen werden. Dieses Kapitel beschreibt die Schritte für den Softwareentwurf und die resultierende Softwarespezifikation sowie die Test- und Validierungspläne. Um vor diesen Schritten Spezifikationsfehler aufdecken zu können, sollten alle bisher ausgefüllten Tabellen schon mit der Registerkarten-Funktion „Formale Checks“ auf Korrektheit und Vollständigkeit geprüft werden (verfügbar in „A1 Sicherheitsfunktionen“ und „2.4 IO-Liste“). Ansonsten müsste die Softwarespezifikation später erneut aktualisiert werden.

Hinweis: Die in mehreren Registerkarten aufrufbaren Funktionen „Tabelle aktualisieren/neu erstellen“ und „Formale Checks“ werden in der aktuellen SOFTEMA-Version nicht automatisch bei Änderungen der Eingangsdaten durchgeführt, sondern müssen immer durch die SOFTEMA-Anwender(innen) manuell ausgelöst werden.

7.1 Tabelle „B4 Matrix C+E“ aktualisieren und ergänzen

Die Softwarespezifikation wird in Form der Tabellen „B4 Matrix C+E“ und „B4 Matrix kompakt“ dargestellt, wobei letztere vollständig durch SOFTEMA generiert wird (Abschnitt 7.2). Die „Registerkarte B4 Matrix C+E“ ist im SOFTEMA-Kochbuch 1 detailliert beschrieben.

Mit der Schaltfläche „Tabelle aktualisieren“ werden alle Eingangsdaten aus den Tabellen A1, A2.4 sowie B3 übernommen oder neue bzw. geänderte Eingangsdaten in der „B4 Matrix C+E“ aktualisiert. Sicherheitsfunktionen werden als Zeilen `Cx` und IO-Signale als Spalten `Ix` bzw. `Ox` eingetragen.

Wenn eine Zeile ergänzt oder aktualisiert wurde, dann muss die Zelle in der Spalte `_Test` angepasst werden. Diese Zelle gibt den Zustand/Cause des Systems an, aus dem diese Zeile getestet werden soll. Meistens ist dies der Cause `C0`, in dem alle Sicherheitsfunktionen entweder deaktiviert oder nicht angefordert sind. Aus diesem Zustand `C0` heraus wird üblicherweise eine Sicherheitsfunktion oder ein Testfall angefordert.

Wurden Eingangsdaten aktualisiert oder neu erstellt, werden in der Tabelle alle betroffenen Zeilen/Spalten *gelb* markiert. Der Anwender bzw. die Anwenderin muss diese dann manuell überprüfen, ergänzen und die Markierungen selber löschen.

Wurden dagegen Eingangsdaten gelöscht, werden nach Aktualisierung in der Tabelle die entsprechenden Zeilen-/Spaltenköpfe zur Löschung *rot* markiert. Die Anwenderin oder der Anwender muss diese dann manuell löschen.

Änderungen, die sich auf die Inhalte der Logikzellen auswirken (z. B. Löschen von Eingangsdaten), werden in den Logikzellen durch Hinweistexte gekennzeichnet. Als Abhilfe müssen diese Zellen erneut editiert werden.

7.1.1 Software für Sicherheitsfunktionen spezifizieren

Im rechten Bereich der Tabelle „B4 Matrix C+E“, in den Spalten Ox, können die Anwender und Anwenderinnen die booleschen Verknüpfungen für das Logikmodul zur Realisierung der Sicherheitsfunktionen spezifizieren. Diese Spezifikationen sind dann die Vorlage für die anschließende Codierung des Logikmoduls.

Jeder Schnittpunkt einer Sicherheitsfunktion bzw. eines Testfalls mit einer Spalte Ox wird als Logikzelle bezeichnet. Das Editieren erfolgt für jede Logikzelle einzeln mit dem Logikeditor (siehe SOFTEMA-Kochbuch 1, Abschnitt „Der Logikeditor“). In den Logikzellen wird in der ersten Zeile eingetragen, wie diese Ausgangsvariable Ox bei Anforderung der betrachteten Sicherheitsfunktion/des Testfalls angesteuert werden soll.

Es gibt drei Steueralternativen, die auch die Hintergrundfarbe der Zelle und des Logikeditors bestimmen:

- OFF (roter Hintergrund) bedeutet: Ausgangsvariable wird mit 0/False angesteuert (typisch für verdrahtete Schütz- oder Ventilansteuerungen)
- NOP (weiß) bedeutet: Es gibt keine Ansteuerung dieser Ausgangsvariable.
- ON (grün) bedeutet: Ausgangsvariable wird mit 1/True angesteuert **(nur für Testfunktionen auswählbar)**

In den darunter folgenden Zeilen der Logikzelle werden die Schaltbedingungen eingetragen, nach denen die Ausgangsvariable Ox angesteuert werden soll.

7.1.2 Bildungsgesetz für die Softwarespezifikation

Das Bildungsgesetz für die Softwarespezifikation lautet:

Schritt 1: Für jede einzelne Sicherheitsfunktion, die bei einem Aktor einen Schaltvorgang auslöst, trägt man in die entsprechende Logikzelle der Tabelle diejenige logische Verknüpfung der Eingangsgrößen vom Logikmodul ein, die den Schaltvorgang auslöst. Der Schaltvorgang wird durch „OFF“ angegeben. Löst eine Sicherheitsfunktion bei einem Aktor keinen Schaltvorgang aus, ist dort ein „NOP“ einzutragen.

Ein Beispiel einer Logikzelle zeigt Abbildung 3 mit der Sicherheitsfunktion SF1 und wie sie auf den Ausgang QS_M1 wirkt:

In der Zelle steht in der ersten Zeile „OFF“ und darunter die Eingangsgröße „EMST_OK“. Dieser Eintrag ist wegen der negativen Logik der Eingangsgrößen so zu lesen: „Wenn die Variable EMST_OK = FALSE ist, dann soll Ausgang QS_M1 = FALSE sein“; d. h., der Ausgang wird OFF/Aus geschaltet.

In den Anweisungen der Abbildung 3 ist die Eingangsgröße „EMST_OK“ ergänzt worden: um einen Kommentar mit dem Zeilenbezeichner „IM1“ und dem Instanzennamen des entsprechenden Eingangs-Funktionsbausteines „Not_Halt_S1“ (aus „Registerkarte B3 Modularchitektur“). Diese Ergänzungen der Anweisungen sind konfigurierbar (siehe SOFTEMA-Kochbuch 1, Kapitel „Optionen“).

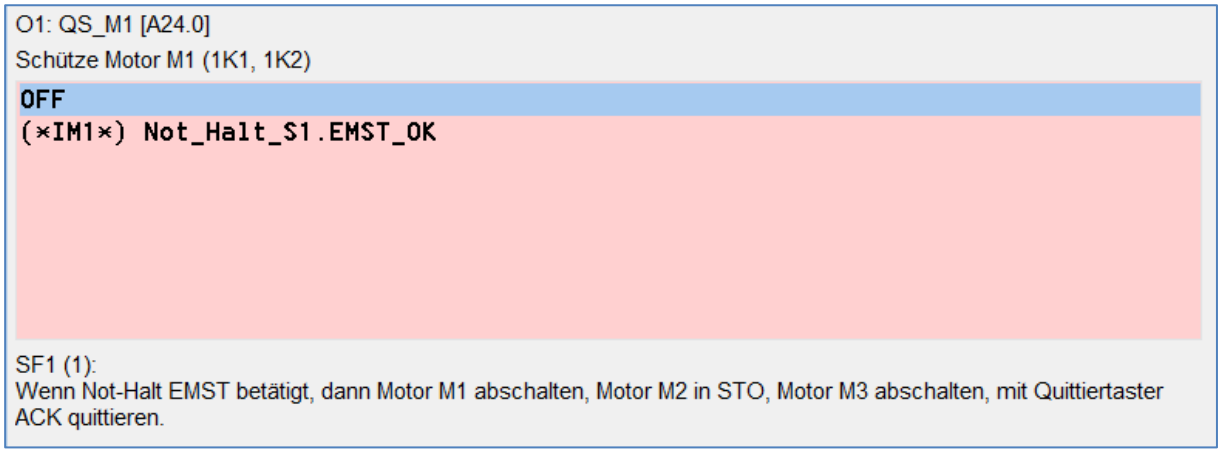


Abbildung 3: Beispiel 1 für die Spezifikation einer Logikzelle

In Abbildung 4 ist ein Beispiel einer Logikzelle für die Sicherheitsfunktion SF4 dargestellt, die wieder auf den Ausgang QS_M1 wirkt:

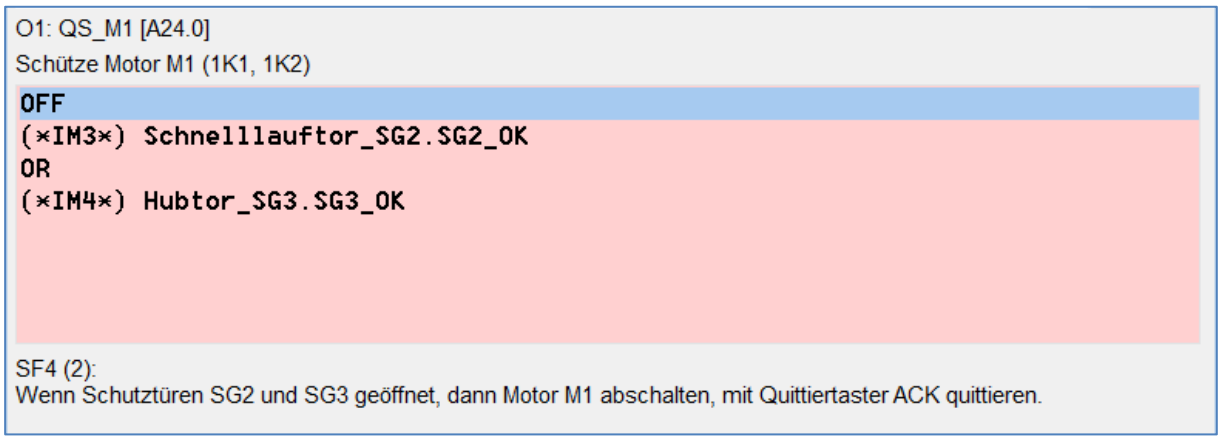


Abbildung 4: Beispiel 2 für die Spezifikation einer Logikzelle

Für Sicherheitsfunktion SF4 wird der Schaltvorgang OFF genau dann ausgelöst, wenn beide Schutztüren SG2 *und* SG3 offen sind. Deshalb muss wegen der negativen Logik der Eingangsgrößen die ODER-Verknüpfung „SG2_OK oder SG3_OK“ eingetragen werden. Das liest sich: „Wenn der Ausdruck (SG2 _OK OR SG3_OK) = FALSE ist, dann soll Ausgang QS_M1 = FALSE sein.“

In den Anweisungen der Abbildung 4 sind die Eingangsgrößen ergänzt worden: um einen Kommentar mit den Zeilenbezeichnern „IM3“ bzw. „IM4“ und den Instanzennamen der entsprechenden Eingangs-Funktionsbausteine „Schnelllauftor_SG2“ bzw. „Hubtor_SG3“.

Schritt 2: Die komplette logische Verknüpfung pro Aktor (also über alle Sicherheits-funktionen) ergibt sich dann aus der UND-Verknüpfung der in der Spalte des Aktors stehenden Anweisungen der Logikzellen.

Abbildung 5 zeigt einen Ausschnitt der resultierenden Spezifikation für das exemplarische Logikmodul als Kombination der Schaltanweisungen aus Abbildung 3 und Abbildung 4.

```
(* Schütze Motor M1 (1K1, 1K2) [A24.0]*)
QS_M1 :=        (*Betriebsart B0: Alle*)
                        (*PRIO1*)
                        (*IM1*) Not_Halt_S1.EMST_OK
                        AND
                        (
                        (*Betriebsart B1: Automatik*)
                                (*PRIO2*)
                                ((*IM3*) Schnelllauftor_SG2.SG2_OK
                                OR
                                 (*IM4*) Hubtor_SG3.SG3_OK
                                )
                        );
```

Abbildung 5: Beispiel 3 für die resultierende Spezifikation für einen Aktor

Hinweis: Die generische Struktur der Spezifikation für das Logikmodul wird im IFA-Report 2/2016 [4], Abschnitt 6.6 und in Abbildung 16 beschrieben. Dort ist die boolesche Verknüpfung von mehreren Schaltbedingungen unterschiedlicher Prioritäten und Betriebsarten dargestellt. Wenn allerdings Schaltbedingungen einer Betriebsart mit einer UND-Funktion zusammengefasst werden (wie die blauen Blöcke in Abbildung 16 dort), muss der Ausgang dieser UND-Funktion bei inaktiver Betriebsart auch deaktiviert (= FALSE) werden. Dazu wird z. B. das Freigabesignal der Betriebsart (in positiver Logik) mit in der UND-Funktion verknüpft.

7.1.3 Testfälle ergänzen

Während die Sicherheitsfunktionen nur von SOFTEMA in der Matrix aktualisiert werden, müssen die Testfälle dagegen über das Kontextmenü ZEILE EINFÜGEN → TESTZEILE UNTERHALB EINFÜGEN an einer passenden Stelle manuell eingetragen und dann editiert werden. In solch einer Testzeile müssen alle Zellen manuell editiert werden, einschließlich einer eindeutigen Bezeichnung TFn in der Spalte _SF-Nr (n = fortlaufende Nummer der Testfälle) und der Priorität des Testfalls in Spalte _Prio. In den Spalten Ix kann eine Konstellation der Eingangssignale eingestellt werden und in den Spalten Ox wird im Logikeditor das zu erwartende Schaltverhalten OFF/ON/NOP (ohne weitere Schaltbedingungen!) eingetragen. In der Spalte _SF-Name ist dieser Testfall dann zu beschreiben.

7.2 Tabelle „B4 Matrix kompakt“ aktualisieren

Diese Tabelle stellt eine kompakte, quasi transponierte Form der „B4 Matrix C+E“ dar, d. h. die Rollen der Zeilen und Spalten sind vertauscht. Die Zeilen beschreiben in kompakter Form jeweils einen Aktor/Ausgang und dessen Ansteuerungen durch Eingänge und Sicherheitsfunktionen. Für das Testen des Anwendungsprogramms oder bei sehr großen Datenmengen ist dies eine praktische Form der Darstellung. Die Tabelle kann über das Menü DRUCKEN einzeln gedruckt werden.

Die „Registerkarte B4 Matrix kompakt“ ist im SOFTEMA-Kochbuch 1 detailliert beschrieben. Der Anwender oder die Anwenderin kann die Tabelle über die Schaltflächen löschen, neu erstellen oder aktualisieren (z. B. bei Modifikationen). Aktualisierte Zellen werden markiert; diese Markierung wird aber bei der darauffolgenden Aktualisierung evtl. wieder überschrieben/gelöscht.

7.3 Verifikations- und Validierungspläne

Mit dem Entwurf der vorgenannten Tabellen für die Spezifikation des Logikmoduls sind auch gleichzeitig die Zellen für die nach der Codierung erforderliche Verifikation und Validierung (kurz: V&V) in den Spalten _Verifikation und _Validierung entstanden. In diesen Spalten wird die erfolgte V&V durch Auswahl der Texte „not OK“ bzw. „OK“ gekennzeichnet.

Hinweis: Tabellenblätter, die über die Spalte _Sperre verfügen, können nur verifiziert und validiert werden, wenn die Sperre gesetzt wurde.

Möchte man darüber hinaus noch für jede der Zeilen in den Tabellen „B4 Matrix …“ eine V&V-Information/-Kriterium eintragen, dann sollten schon in der Projektvorlagedatei solche Spalten mit „projektspezifischen Spaltenbezeichnern mittels vordefinierter Präfixe“ (siehe SOFTEMA-Kochbuch 1) wie z. B. eine Spalte #CO_ValiKriterium rechts neben der Spalte _Validierung ergänzt worden sein.

Für die Anwendung der Matrix gilt also grundsätzlich:

- Programmierende Personen lesen pro Aktor die zugehörige Spalte der C&E-Matrix bzgl. der Eintragungen der Logikzellen, um daraus die Logik zu codieren.
- Testende Personen lesen die Zeilen der Matrix, um einzelne Sicherheitsfunktionen zu testen.

8 Codierung des Anwendungsprogramms

In dem nächsten Schritt der Projektierung muss die Spezifikation der Tabelle „B4 Matrix C+E“ in den Code des Logikmoduls für das Anwendungsprogramm umgesetzt werden. Dabei sind mehrere zugelassene Programmiersprachen, die von den Entwicklungsumgebungen der Steuerungen angeboten werden, möglich. Als Beispielsprache in diesem Leitfaden wird „Strukturierter Text (ST)“ verwendet. Dies ist auch dadurch begründet, dass der Logikeditor in der Spezifikation einen dem ST entsprechenden Spezifikationstext erzeugt (siehe dazu auch 7.1.2 Bildungsgesetz für die Softwarespezifikation).

Hinweis: Es wäre möglich, den Code des Logikmoduls aus den Logikzellen automatisch zu generieren – das ist auch für eine spätere SOFTEMA-Version geplant.

8.1 Maßnahmen im Rahmen der Toolqualifizierung

In SOFTEMA müssen Nutzende Maßnahmen ergreifen, um die wahrscheinlich enthaltenen Fehler und damit möglicherweise fehlerhafte Spezifikationen aufdecken zu können. Dazu zählen

- Review der mit SOFTEMA erzeugten Spezifikationen insbesondere in den Tabellen „B3 Modularchitektur“, „B4 Matrix C+E“ und „B4 Matrix kompakt“. Die Spezifikationen werden dabei mit den vorgegebenen Sicherheitsanforderungen verglichen.
- Modultest der mit diesen Spezifikationen codierten Programmteile, um sicherzustellen, dass die vorgegebenen Sicherheitsanforderungen erfüllt werden.
- (Erweiterter) Funktionstest des vollständigen Anwendungsprogramms, um sicherzustellen, dass die vorgegebenen Sicherheitsanforderungen erfüllt werden.

Im Rahmen der Verifikationen (Kapitel 9) und Validierungen (Kapitel 10) werden vorgenannte Maßnahmen durchgeführt und bestätigt.

9 Verifikation des codierten Programms

In diesem Kapitel werden die Schritte zur Verifikation des codierten Programms gegen die Spezifikationen und Projektdaten dargestellt. Nach einer Verifikation sind die Protokollfelder mit Datum, Name und Signatur der verifizierten Programmversion auszufüllen bzw. zu aktualisieren.

Die Personen, die Verifikationen durchführen, sollten unabhängig von den Personen sein, die die verifizierten Daten erstellt haben. Eine Orientierung, welche Unabhängigkeitsgrade eingehalten werden sollten, findet sich im IFA-Report 2/2016 [4], Abschnitt 5.15.

Die unten beschriebenen Verifikationen werden in der Regel als Sichtprüfungen durchgeführt und enthalten jeweils zwei Fragestellungen, die durch ein „OK“ in der Verifikationsspalte zu bestätigen sind:

- Sind die Inhalte der Tabelle – vor der Codierung – korrekt und vollständig erstellt worden?
- Sind die Inhalte der Tabelle im Code korrekt und vollständig umgesetzt worden?

9.1 Maßnahmen im Rahmen der Toolqualifizierung

In SOFTEMA müssen Nutzende Maßnahmen ergreifen, um die in SOFTEMA wahrscheinlich enthaltenen Fehler und damit eine möglicherweise fehlerhafte Spezifikation aufdecken zu können. Dazu zählen die im Folgenden beschriebenen Verifikationen.

9.2 Verifikation in der Tabelle „A2.4 IO-Liste“

In der Spalte _SW-Verif. wird bestätigt, dass einerseits die Signale korrekt mit Variablensymbol, Adresse und Bezeichnung eingetragen sind und andererseits die Variablen auch richtig im Programm bzw. mit den zugehörigen Funktionsbausteinen verschaltet sind.

In der Spalte _DIAG-Test wird bestätigt, dass Zustands- und Fehlerinformationen über z. B. Eingangs-/Ausgangsbaugruppen richtig mit den zugehörigen Funktionsbausteinen verschaltet sind.

9.3 Verifikation in der Tabelle „A3 Maßnahmen“

In der Spalte _Verifikation wird bestätigt, dass die Maßnahmen umgesetzt wurden, die für Spezifikation und Codierung des Programms gefordert sind. Maßnahmen, die erst spätere Aktivitäten im Projekt betreffen (Inbetriebnahme, Prüfung etc.), können erst später verifiziert und bestätigt werden.

9.4 Verifikation in der Tabelle „B3 Modularchitektur“

In der Spalte _Verifikation wird bestätigt, dass alle Eintragungen für das Modul in der Zeile vorhanden und korrekt sind. Dazu gehören die für die Spezifikation geforderten Inhalte sowie die zusätzlich von der Projektleitung gewünschten Inhalte (siehe Abschnitt 6.5).

9.5 Verifikation in der Tabelle „B4 Matrix C+E“

In der Spalte _Verifikation wird bestätigt, dass alle Eintragungen in der Zeile vorhanden sind und die Logikzellen korrekt und vollständig ausgefüllt sind. Die Schaltanweisungen müssen dazu auch mit der Definition der zugehörigen Sicherheitsfunktion bzw. des Testfalls verglichen werden.

9.6 Verifikation in der Tabelle „B4 Matrix kompakt“

In der Spalte _Verifikation wird bestätigt, dass alle Eintragungen in der Zeile vorhanden sind und die Zellen korrekt und vollständig ausgefüllt sind. Das Summenfeld am unteren Tabellenrand wird in der aktuellen SOFTEMA-Version nicht automatisch in die Tabelle „Codereview“ gespiegelt. Es könnte dort aber als zusätzlicher manueller Verifikationspunkt eingetragen werden (siehe Abschnitt 5.5.10).

9.7 Verifikation in der Tabelle „Codereview“

In dieser Tabelle werden die Summenzellen aller vorher genannten Verifikationen (Ausnahme: Verifikation in „B4 Matrix kompakt“) zusammengefasst dargestellt. Diese Zellen in der Spalte _Verifikation können nicht manuell eingetragen werden. Der Erfüllungsgrad dieser Verifikationen wird in Prozent angegeben.

Zusätzlich können weitere Verifikationspunkte in der Projektvorlage ergänzt worden sein (siehe Abschnitt 5.5.10). Die zugehörigen Zellen in der Spalte _Verifikation müssen manuell befüllt werden („OK“, „not OK“), um diese Verifikationspunkte zu beurteilen.

10 Validierung des Anwendungsprogramms

In diesem Kapitel werden die Schritte zur Validierung des codierten Programms sowie aller vorhergehenden Schritte und Maßnahmen im V-Modell beschrieben. Nach einer Validierung sind die Protokollfelder mit Datum, Name und Signatur der validierten Programmversion auszufüllen bzw. zu aktualisieren.

Die Personen, die Validierungen durchführen, sollten unabhängig von den Personen sein, die die validierten Daten erstellt haben. Eine Orientierung, welche Unabhängigkeitsgrade eingehalten werden sollten, findet sich im IFA-Report 2/2016 [4], Abschnitt 5.15.

10.1 Maßnahmen im Rahmen der Toolqualifizierung

SOFTEMA Nutzende müssen Maßnahmen ergreifen, um die in SOFTEMA wahrscheinlich enthaltenen Fehler und damit eine möglicherweise fehlerhafte Spezifikation aufdecken zu können. Dazu zählen die im Folgenden beschriebenen Validierungen, insbesondere der Spezifikationen, da diese als Codierungsvorlage dienen.

10.2 Validierung in der Tabelle „A2.4 IO-Liste“

In der Spalte _Validierung wird mittels IO-Check bestätigt, dass die Signale korrekt verdrahtet sind bzw. bei Datenaustausch über Netzwerk die Kommunikation korrekt konfiguriert ist.

10.3 Validierung in der Tabelle „B4 Matrix C+E“

In der Spalte _Validierung wird mittels Blackbox-Test des Logikmoduls und des Programms (zusätzlich Simulation bei höheren PL) bestätigt, dass die spezifizierten Schaltanweisungen für die Sicherheitsfunktionen korrekt ausführt werden.

10.4 Validierung in der Tabelle „B4 Matrix kompakt“

In der Spalte _Validierung wird mittels Blackbox-Test des Logikmoduls und des Programms (zusätzlich Simulation bei höheren PL) bestätigt, dass die spezifizierten Schaltanweisungen mit Wirkung auf die Aktoren korrekt ausführt werden. Das Summenfeld am unteren Tabellenrand wird in der aktuellen SOFTEMA-Version nicht automatisch in die Tabelle „Validierung“ gespiegelt. Es könnte dort aber als zusätzlicher manueller Validierungspunkt eingetragen werden (siehe Abschnitt 5.5.11).

10.5 Validierung in der Tabelle „A1 Sicherheitsfunktionen“

In der Spalte _Validierung wird mittels Funktionstests (erweiterter Funktionstest bei höheren PL) bestätigt, dass das Programm in der Steuerung die Sicherheitsfunktionen – wie in allen Parametern spezifiziert – korrekt ausführt.

10.6 Validierung in der Tabelle „A4 Anforderungen“

In der Spalte _Validierung wird bestätigt, dass die normativen Anforderungen umgesetzt wurden, die für die Softwareentwicklung gefordert sind. Anforderungen, die spätere Aktivitäten im Projekt betreffen (Dokumentation, Prüfung etc.), können erst nachträglich validiert und in dieser Tabelle bestätigt werden.

10.7 Validierung in der Tabelle „Validierung“

In dieser Tabelle werden die Summenzellen aller vorher genannten Validierungen (Ausnahme: Validierung in „B4 Matrix kompakt“) zusammengefasst dargestellt. Diese Zellen in der Spalte _Validierung können nicht manuell eingetragen werden. Der Erfüllungsgrad dieser Validierungen wird in Prozent angegeben.

Zusätzlich können weitere Validierungspunkte in der Projektvorlage ergänzt worden sein (siehe Abschnitt 5.5.11). Die zugehörigen Zellen in der Spalte _Validierung müssen manuell befüllt werden („OK“, „not OK“), um diese Validierungspunkte zu beurteilen.

11 Prüfung der Projektdatei

In diesem Kapitel wird dargestellt, wie Personen mit den Rollen Prüfen1/Prüfen2 ein Projekt in SOFTEMA prüfen können. Die Prüfung können interne und/oder externe Personen vornehmen, daher sind zwei Rollen und entsprechende Eingabezellen vorgesehen.

Die Personen, die Prüfungen durchführen, sollten unabhängig von den Personen sein, die die geprüften Daten erstellt haben. Eine Orientierung, welche Unabhängigkeitsgrade eingehalten werden sollten, findet sich im IFA-Report 2/2016 [4], Abschnitt 5.15.

11.1 Sichtprüfung in den Tabellen

In den Rollen Prüfen1/Prüfen2 können alle Tabellen betrachtet, aber größtenteils nicht editiert werden. Bei dieser Sichtprüfung können also die Vollständigkeit, Widerspruchsfreiheit und Plausibilität der Tabellen festgestellt werden. In den Tabellen „C1 Codereview“ und „D1 Validierung“ kann man sich einen schnellen Überblick über diese Aktivitäten schaffen. Durch Doppelklick auf die Tabellenbezeichnungen in der Spalte _Referenzblatt und dann zurück mit dem Befehl der Werkzeugleiste VORHERIGE SEITE kann man schnell durch die Verifikation bzw. Validierung der Tabellen navigieren.

Folgende für eine Prüfung wichtige Funktionen können ebenfalls durch die Rollen Prüfen1/Prüfen2 ausgeführt werden:

- die Funktion FORMALE CHECKS in verschiedenen Registerkarten
- Druckfunktionen einschließlich Zusammenfassung (Kapitel 12)
- Öffnen von verlinkten Dokumenten, z. B. in der Tabelle „Dokumente“

11.2 Kommentierung in den Tabellen

Zu den Feldern, die von Prüfen1/Prüfen2 editiert werden können, zählt die Spalte _Kommentar_Prüfen. In der aktuellen SOFTEMA-Version ist nur diese eine Spalte für beide Rollen gemeinsam vorgesehen. Diese Kommentare können von allen anderen Rollen nur gelesen werden.

11.3 Protokollfelder

Die Protokollfelder für Prüfen1/Prüfen2 unterhalb der Verifikations-/Validierungsspalten können ebenfalls und ausschließlich durch diese Rollen editiert werden. Dort kann ein Datum und der Name der prüfenden Person ausgewählt werden, um den Prüfvorgang zu dokumentieren.

12 Druckfunktionen

Dieses Kapitel beschreibt die verschiedenen Möglichkeiten, die Tabelleninhalte in SOFTEMA zu drucken bzw. in eine PDF-Datei zu exportieren.

12.1 Druckeinrichtung

Der Menübefehl DATEI → DRUCKEINRICHTUNG öffnet einen Dialog (Abbildung 6), in dem sich der für SOFTEMA aktive Drucker auswählen und konfigurieren lässt.

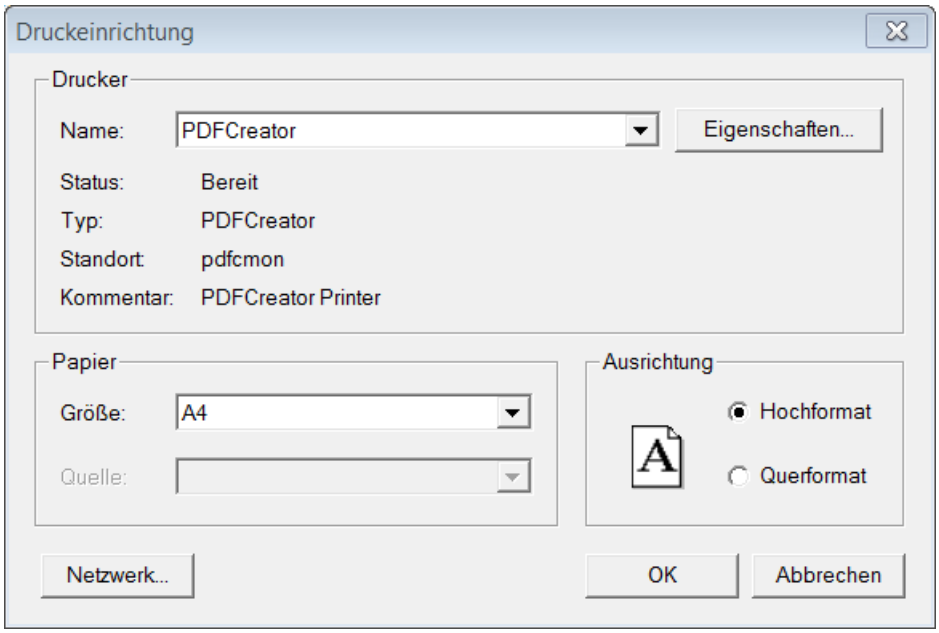


Abbildung 6: Dialog für Druckeinrichtung

12.2 Tabellen drucken

Der Menübefehl DRUCKEN → TABELLE DRUCKEN dient zum Drucken der aktuell dargestellten Tabelle. Es öffnet sich zunächst ein Dialog für die Druckeinstellungen (Abbildung 7). Nach dem Bestätigen der Druckeinstellungen mit Schaltfläche OK wird eine Druckvorschau angezeigt. In dieser Vorschau kann dann gedruckt werden.

Die Option `IniFile_PrintSettings` (siehe INI-Datei) weist den Namen der Datei zu, in der die Druckeinstellungen (Registerkarte EINSTELLUNGEN in Abbildung 7) gespeichert werden können. Die Druckeinstellungen werden beim Öffnen des Dialogs automatisch aus dieser Datei geladen.

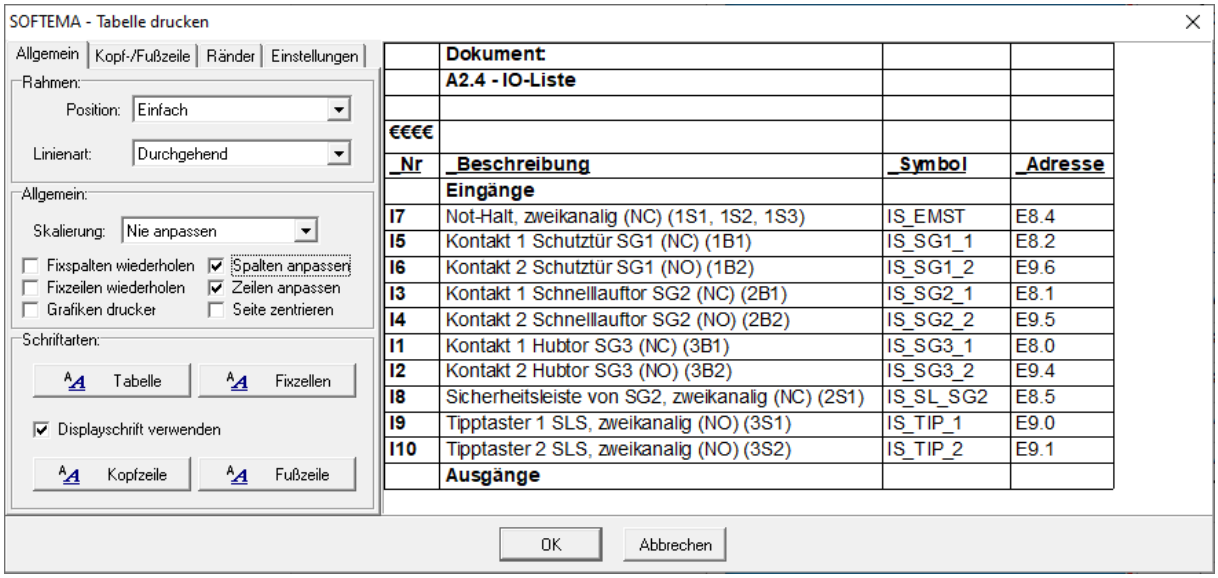


Abbildung 7: Dialog für Druckeinstellungen

12.3 Zusammenfassung erstellen

Der Menübefehl DRUCKEN → ZUSAMMENFASSUNG dient zum Erstellen einer vollständigen Projektzusammenfassung mit Inhalten *aller* Tabellen des Projektes. Zunächst öffnet sich ein Dialog für die Optionen (Abbildung 8). Hier kann die Ausgabe direkt auf den Drucker, in eine Datei oder in eine Vorschau (Standardeinstellung) gesteuert werden.

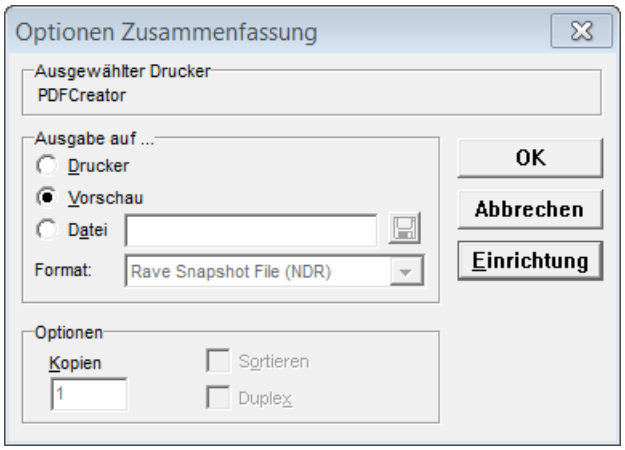


Abbildung 8: Optionen für die zu erstellende Zusammenfassung

Danach wird die Zusammenfassung anhand der aktuellen Tabelleninhalte generiert. In der Vorschau (Abbildung 9) kann dann die Zusammenfassung betrachtet, gedruckt oder als PDF gespeichert werden.

Das Projekt muss vorher gespeichert werden, wobei die Prüfsumme neu berechnet wird. Diese Prüfsumme wird auf jeder Seite der Zusammenfassung in der Kopfzeile dargestellt. Anhand dieser Prüfsumme und des Datums der letzten Änderung lässt sich überprüfen, ob eine vorliegende Zusammenfassung und ein geladenes Projekt übereinstimmen.

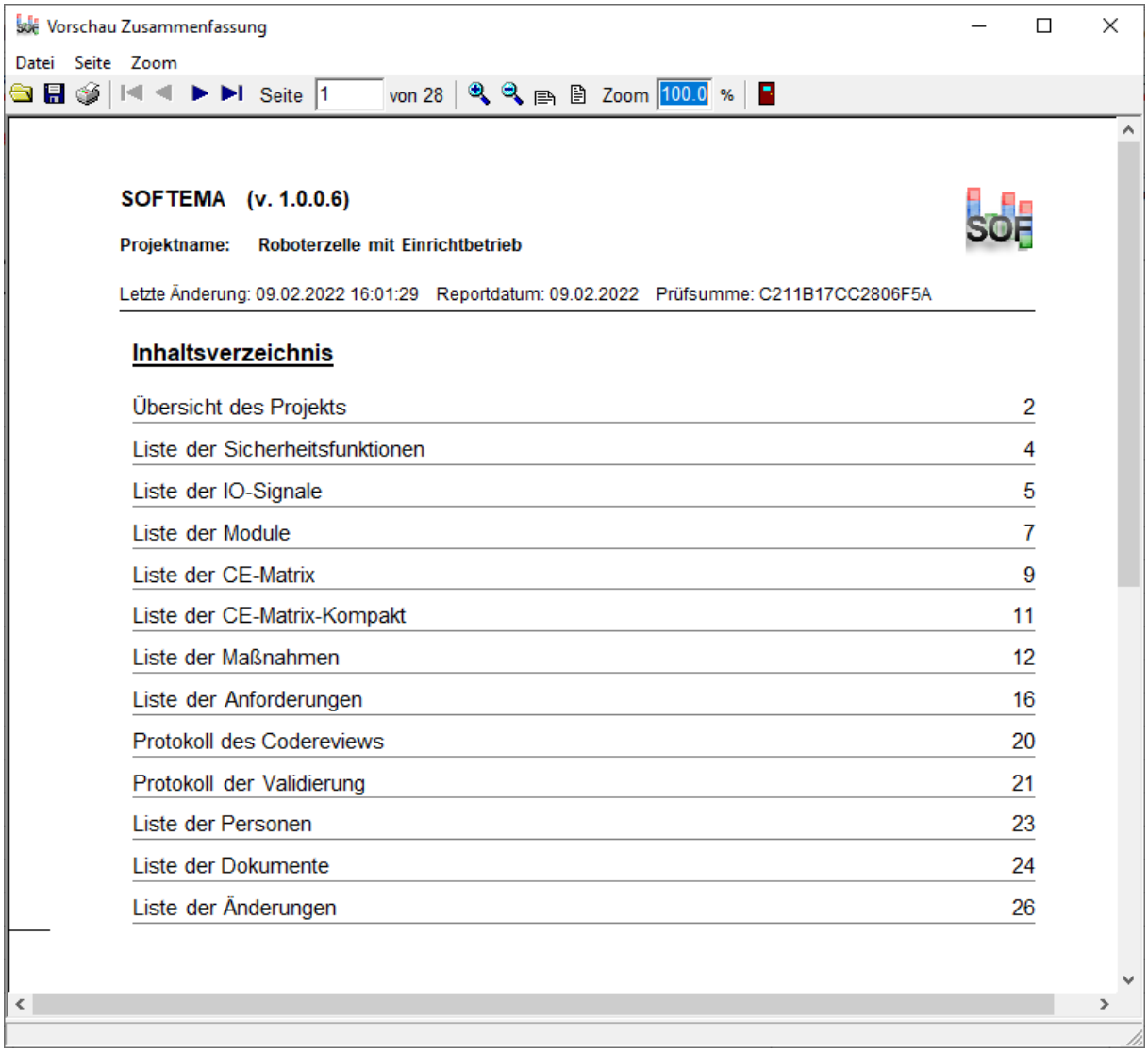
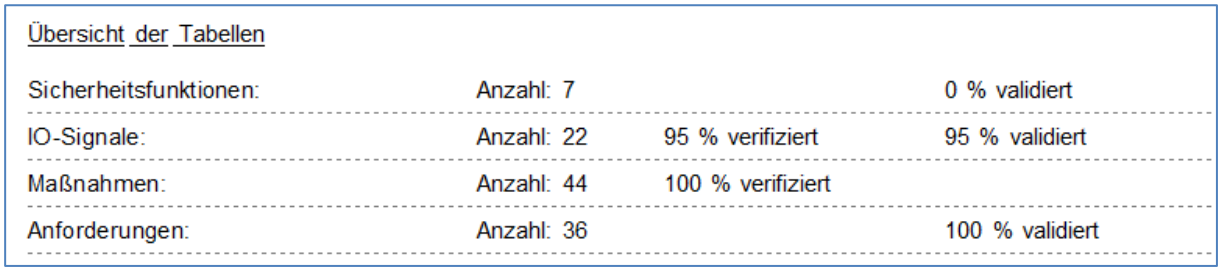


Abbildung 9: Vorschau der Zusammenfassung (1. Seite: Inhaltsverzeichnis)

Ab der zweiten Seite der Zusammenfassung sind oben die Informationen der Tabelle „Projekt“ und darunter die Übersicht der Tabellen (Abbildung 10) dargestellt. Diese Übersicht benennt für jede Tabelle die Anzahl der Inhaltszeilen (z. B. Anzahl der Sicherheitsfunktionen oder Anzahl der Maßnahmen) und den Erfüllungsgrad der Verifikationen/Validierungen von 0 % bis 100 %.

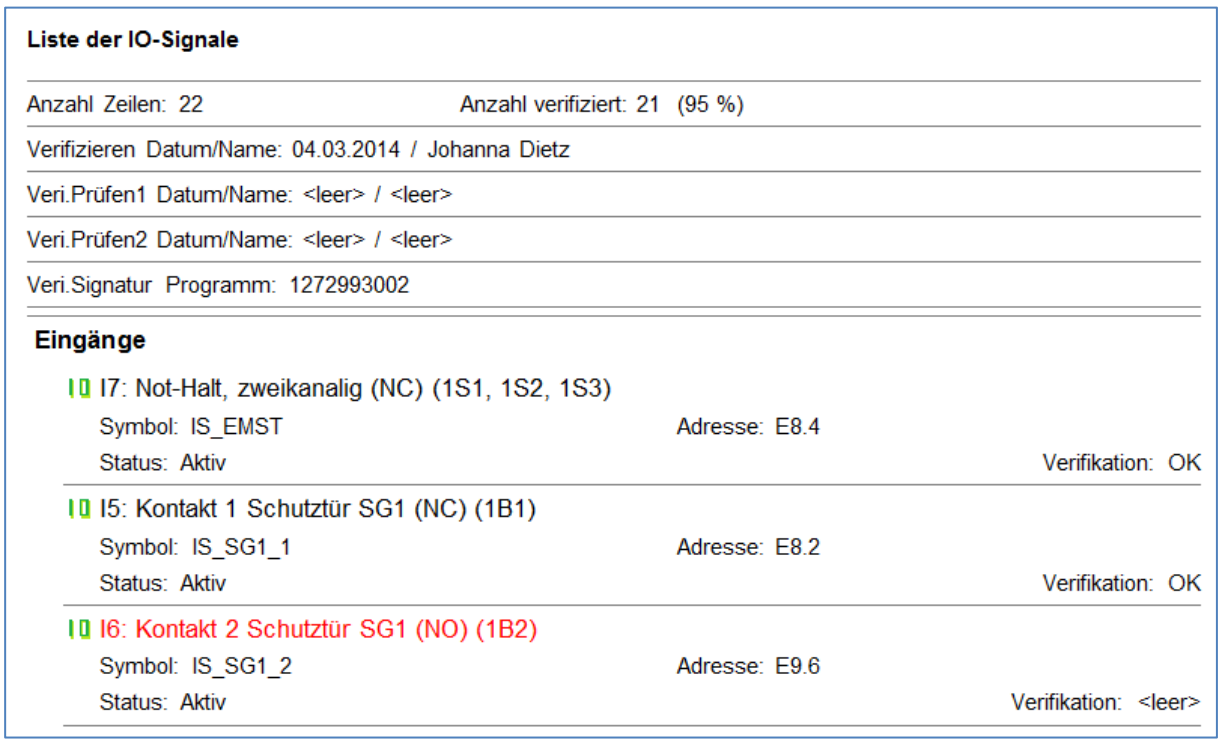


Übersicht der Tabellen

Sicherheitsfunktionen:	Anzahl: 7		0 % validiert
IO-Signale:	Anzahl: 22	95 % verifiziert	95 % validiert
Maßnahmen:	Anzahl: 44	100 % verifiziert	
Anforderungen:	Anzahl: 36		100 % validiert

Abbildung 10: Vorschau der Zusammenfassung (ab 2. Seite: Übersicht der Tabellen)

Auf den folgenden Seiten der Zusammenfassung werden alle Tabellen mit einer Übersicht und darunter den Details aller Inhaltszeilen dargestellt, hier beispielhaft den beginnenden Teil der „Liste der IO-Signale“ (Abbildung 11).



Liste der IO-Signale

Anzahl Zeilen: 22 Anzahl verifiziert: 21 (95 %)

Verifizieren Datum/Name: 04.03.2014 / Johanna Dietz

Veri.Prüfen1 Datum/Name: <leer> / <leer>

Veri.Prüfen2 Datum/Name: <leer> / <leer>

Veri.Signatur Programm: 1272993002

Eingänge

I7: Not-Halt, zweikanalig (NC) (1S1, 1S2, 1S3)
Symbol: IS_EMST Adresse: E8.4
Status: Aktiv Verifikation: OK

I5: Kontakt 1 Schutztür SG1 (NC) (1B1)
Symbol: IS_SG1_1 Adresse: E8.2
Status: Aktiv Verifikation: OK

I6: Kontakt 2 Schutztür SG1 (NO) (1B2)
Symbol: IS_SG1_2 Adresse: E9.6
Status: Aktiv Verifikation: <leer>

Abbildung 11: Vorschau der Zusammenfassung (Liste der IO-Signale)

In der Übersicht werden dargestellt:

- die Anzahl aller Zeilen und die Anzahl verifizierter Zeilen und darunter
- Datum und Namen aller bei der Verifikation bzw. der Validierung beteiligten Personen

In den Details werden die Bezeichnungen wie folgt dargestellt:

- in roter Farbe, wenn bei einer Inhaltszeile die Verifikation bzw. Validierung fehlt oder „not OK“ ist (letzter Eingang in Abbildung 11)
- durchgestrichen, wenn eine Inhaltszeile „nicht aktiv“ ist (letzte Maßnahme in Abbildung 12)

Entwicklung eigener Funktionsbausteine:

ME R19: Eigene wiederverwendbare Funktionsbausteine werden separat nach V-Modell entwickelt und dokumentiert.

Status: Aktiv Verifikation: OK

ME R20: Die komplette Testung der Bausteine geschieht in der Simulation.

Status: Aktiv Verifikation: OK

ME R21: Für eigene Funktionsbausteine muss ein Bibliotheksmagagement gepflegt werden.

Status: Aktiv Verifikation: OK

ME ~~R22: Eigene Funktionsbausteine mit Codeschutz versehen.~~

Status: Nicht Aktiv Verifikation: <leer>

Abbildung 12: Vorschau der Zusammenfassung (Liste der Maßnahmen)

13 Dokumentation zum Anwendungsprogramm

Die Dokumentation für ein mit SOFTEMA projektiertes Anwendungsprogramm sollte aus folgenden Teilen bestehen:

- der SOFTEMA-Projektdatei zusammen mit den zugehörigen INI-Dateien und weiteren Konfigurationsdateien
- der Zusammenfassung und den Tabellenausdrucken bzw. PDF-Dateien (siehe Kapitel 12)
- den Dokumenten, die in der Projektdatei verlinkt wurden (besonders in Tabelle „Dokumente“)
- den Dokumenten, die in Tabelle „Validierung“ benannt sind

Wenn die oben genannten Dateien und Dokumente in einem Projektverzeichnis mit Unterverzeichnissen abgelegt wurden, dann ist eine Archivierung dieses Projektverzeichnisses mit einem externen Tool in ein Archiv-Dateiformat (z. B. ZIP, RAR, TAR) recht einfach. Solch eine Archiv-Datei kann dann an andere Personen weitergegeben werden, die z. B. dieses Projekt prüfen wollen.

In der aktuellen SOFTEMA-Version sind noch keine eingebauten Funktionen zum Archivieren verfügbar.

Darüber hinaus sind alle Dokumente zu archivieren, die von der Entwicklungsumgebung des Anwendungsprogramms erzeugt werden können (z. B. Listing des Codes, Symboltabellen, Querverweislisten).

Die archivierten Dokumente müssen einer Version des lauffähigen Anwendungsprogramms zugeordnet werden können.

14 Modifikation des Anwendungsprogramms

Dieses Kapitel widmet sich der Frage, wie Modifikationen des Anwendungsprogramms in SOFTEMA unterstützt werden können. Je nach Art der Modifikation müssen die Phasen des V-Modells teilweise oder ganz erneut durchlaufen werden. In der Tabelle „Projekt“ sollten auch die Projektversion und der Projektstatus angepasst werden. Hinweise zu den Modifikationen können in den Kommentarfeldern, in projektspezifischen Spalten oder auch in der Tabelle „Änderungen“ hinterlegt werden. Die Projektgruppe sollte für die Handhabung von Modifikationen einen Prozess definiert haben.

14.1 Modifikation von Projektdaten

Ändern sich Sicherheitsanforderungen, Sicherheitsfunktionen oder die Steuerungshardware oder werden Programmfehler behoben, kommt es zu geänderten oder neuen Daten in den Zeilen der Tabellen A1, A2.4 und A3:

- Zu ändernde Zeilen müssen entsperrt werden, woraufhin die Verifikation-/Validierungszellen gelöscht werden. Geänderte Zellen sollten manuell markiert werden, um die Aufmerksamkeit auf diese Änderungen zu lenken (Abbildung 13, Eingang I13, Spalte _Adresse)
- Neue Zeilen werden automatisch markiert und die Verifikation/Validierungszellen sind zunächst leer (Abbildung 13, Eingang I15).

_Nr	_Beschreibung	_Symbol	_Adresse	_Datentyp	_Modul	_Aktiv_in_C+E	_Aktiv	_Sperre	_SW-Verif.	_IO-Test	_DIAG-Test
	Eingänge										
I7	Not-Halt, zweikanalig (NC) (1S1, 1S2, 1S3)	IS_EMST	E8.4	BOOL	ESTOP_S1	Aktiv	Aktiv	x	OK	OK	OK
I5	Kontakt 1 Schutztür SG1 (NC) (1B1)	IS_SG1_1	E8.2	BOOL		Aktiv	Aktiv	x	OK	OK	OK
I6	Kontakt 2 Schutztür SG1 (NO) (1B2)	IS_SG1_2	E9.6	BOOL		Aktiv	Aktiv	x	OK	OK	OK
I3	Kontakt 1 Schnellauftor SG2 (NC) (2B1)	IS_SG2_1	E8.1	BOOL		Aktiv	Aktiv	x	OK	OK	OK

Abbildung 13: Geänderte/neue Zeilen bei Modifikationen

Damit wird in den Tabellen gekennzeichnet, welche Zeilen nach einer Modifikation erneut zu verifizieren/validieren sind.

Alle Modifikationen sollten in der Tabelle „Änderungen“ dokumentiert werden.

14.2 Aktualisierung der Spezifikationstabellen

Nachdem die Projektdaten aktualisiert wurden, sind die Spezifikationen in den Tabellen „B4 Matrix C+E“ und „B4 Matrix kompakt“ nicht mehr aktuell. Daher muss nun die Aktualisierung dieser Tabellen manuell ausgelöst werden (Abschnitte 7.1 und 7.2). Die aktualisierten Zellen werden dabei markiert und die Logikzellen müssen daraufhin ggf. auch geändert werden. Dies ist nur möglich, wenn die betroffenen Zeilen entsperrt werden, womit dann auch die Verifikations-/Validierungszellen gelöscht werden.

Möglicherweise sind aufgrund der Modifikationen zusätzliche Testfälle erforderlich.

Alle Anpassungen sollten in der Tabelle „Änderungen“ dokumentiert werden.

14.3 Verifikation, Validierung und Prüfung der Modifikationen

Nach der Codierung der Modifikationen erfolgen die stellenweise notwendigen Verifikationen (Kapitel 9), Validierungen (Kapitel 10) und Prüfungen (Kapitel 11). Dabei sind auch die Protokollfelder mit Datum, Name und Signatur der modifizierten Programmversion zu aktualisieren.

Nach dem erfolgreichen Abschluss der Modifikation ist die Markierung der bearbeiteten Zellen wieder zu entfernen.

14.4 Dokumentation der Modifikationen

Weil sich das Anwendungsprogramm geändert hat, muss auch wieder eine vollständige Dokumentation dieser neuen Programmversion erstellt und archiviert werden (Kapitel 12 und 13).

Anhang A: Literatur

[1] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (12/2008); sowie Änderung 1 der DIN EN ISO 13849-1 (2016). Beuth, Berlin 2008/2016

[2] DIN EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (09/2013). Beuth, Berlin 2013

[3] Becker, N.; Eggeling, M.: Abschlussbericht zum DGUV Projekt Nr. FF-FP0319: Normgerechte Entwicklung und Dokumentation von sicherheitsbezogener Anwendersoftware im Maschinenbau. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2013. http://www.dguv.de/webcode/dp54444

[4] Huelke, M.; Becker, N.; Eggeling, M.: Sicherheitsbezogene Anwendungssoftware von Maschinen – Die Matrixmethode des IFA (IFA-Report 2/2016). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2016. http://www.dguv.de/webcode/d1023063

[5] Software-Assistent SOFTEMA. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. http://www.dguv.de/ifa, Webcode d1082520

[6] Software-Assistent SISTEMA. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. http://www.dguv.de/ifa, Webcode d11223

[7] Definition von Sicherheitsfunktionen – Was ist wichtig? (SISTEMA-Kochbuch 6). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015. http://www.dguv.de/ifa, Webcode d109240

[8] Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M. et al.: Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849 (IFA-Report 2/2017). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2017. http://www.dguv.de/ifa, Webcode d1099283

Anhang B: Abkürzungsverzeichnis

Tabelle 2 enthält die in diesem Kochbuch verwendeten Abkürzungen.

Tabelle 2: In diesem Kochbuch verwendete Abkürzungen

Abkürzung	Bezeichnung
C&E-Matrix	Cause and effect matrix; Synonym: cause and effect table; Ursache-Wirkungs-Diagramm
INI-Datei	Initialisierungsdatei; normale Textdatei mit der Dateiendung *.ini*
I/O	Input/Output; Eingang/Ausgang einer SPS
NOP	No operation; Nulloperation: ist ein Befehl in der C&E-Matrix, der nichts bewirkt
OFF	Aus; ein Befehl in der C&E-Matrix, der die Ausgangsvariable mit 0/False ansteuert
ON	Ein; ein Befehl in der C&E-Matrix, der die Ausgangsvariable mit 1/True ansteuert
PL	Performance Level
PL_r	Required Performance Level; erforderlicher Performance Level
SF	Safety function; Sicherheitsfunktion
SFK	Sicherheitsfunktions-Kennzeichen: eindeutige Bezeichnung der SF im Projekt
SISTEMA	Softwareassistent des IFA „Sicherheit von Steuerungen an Maschinen“
SOFTEMA	Softwareassistent des IFA „Sichere Software an Maschinen“
SPS(en)	Speicherprogrammierbare Steuerung(en)
SSPS(en)	Sicherheits-Speicherprogrammierbare Steuerung(en)
SRASW	Safety-related application software; sicherheitsbezogene Anwender-Software
SRESW	Safety-related embedded software; sicherheitsbezogene eingebettete Software
ST	SPS-Sprache: Strukturierter Text; englisch: Structured Text
TF	Testfall