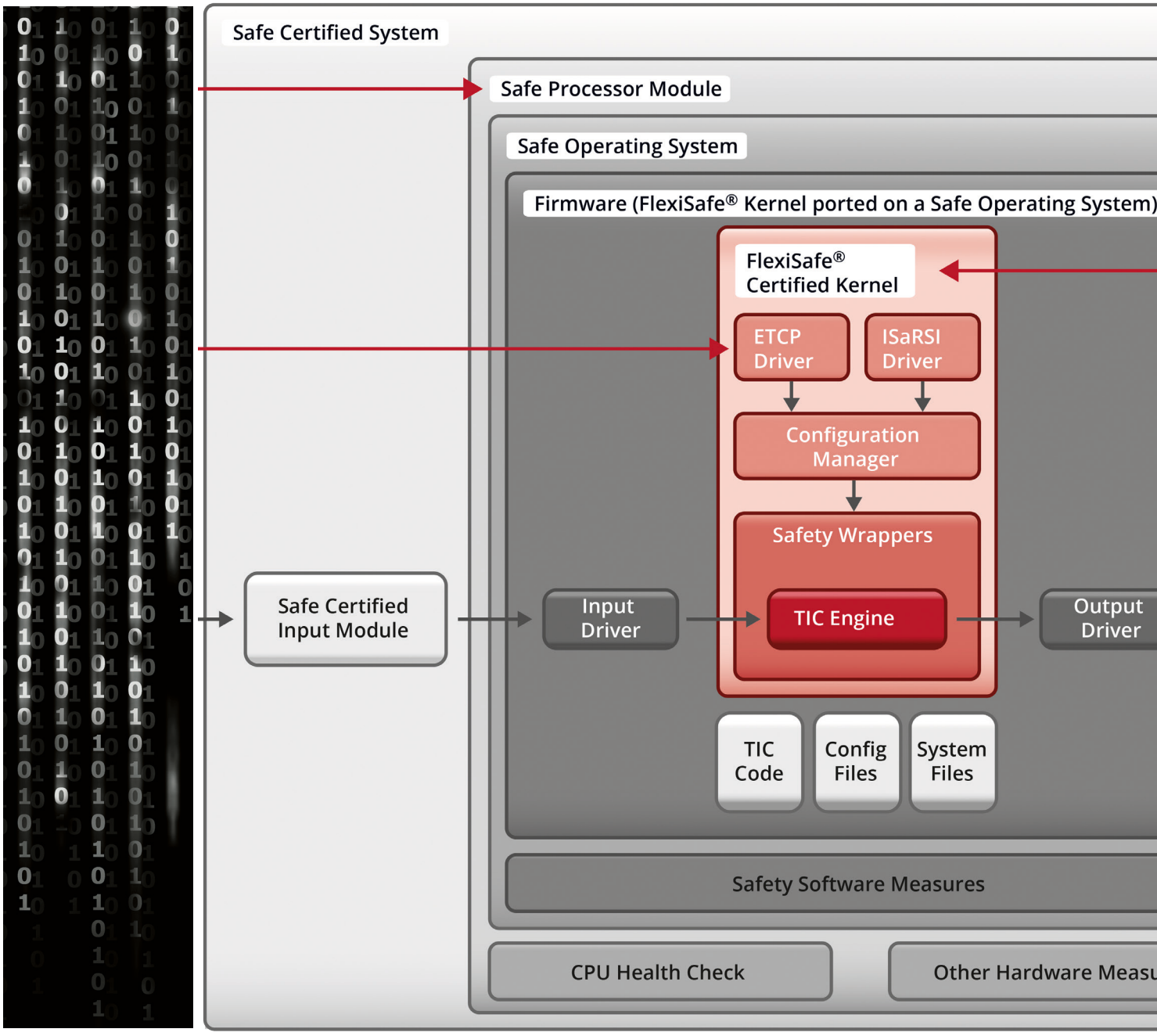
WHITEPAPER

iFSC - infoteam Functional Safety Control Concept



iFSC - infoteam Functional Safety Control Concept

1 Einleitung

Um ein sicheres Steuerungssystem zu entwickeln, bedarf es aufeinander abgestimmter, sicherer Systemkomponenten, die nicht nur einzeln für sich, sondern auch in ihrem Zusammenwirken in individuellen Anwendungsbereichen verifizierbar und validierbar sind.

Die infoteam Software AG zeigt mit dem iFSC-Konzept einen ganzheitlichen Ansatz zur Realisierung sicherer Funktionen und zur Entwicklung sicherer Steuerungssysteme nach individuellen Kundenanforderungen auf – effizient und risikoarm:

- vom normenkonformen Entwicklungsprozess,
- über die sicheren Systemkomponenten,
- und die sicheren Engineering-Tools,
- bis hin zur Programmierung und Parametrierung sicherer Anwendungen.

Die im Folgenden beschriebenen Elemente des Konzeptes sind im Detail nicht zwingend festgeschrieben und können den besonderen Rahmenbedingungen und Anforderungen der Projekte entsprechend angepasst oder ausgetauscht werden.

2 iFSM - infoteam Functional Safety Management-Prozess

Der Weg zum zertifizierten System führt über einen sicheren Entwicklungsprozess. Der nach IEC 61508 bis SIL 3 vom TÜV Süd zertifizierte Projektleitfaden iFSM unterstützt bei der normenkonformen Dokumentation und Durchführung von Projekten nach den Vorgaben des Functional Safety Management (siehe Abb. 1).

Ein aufwendiges Einarbeiten aller Projektbeteiligten in die Norm ist bei der Verwendung des iFSM nicht mehr notwendig. Alle relevanten Norminhalte sind verständlich aufbereitet und auf die einzelnen Rollen und Phasen einer Entwicklung nach der IEC 61508 zugeschnitten.

Das Entwicklungsteam kann sich somit vollständig auf die Umsetzung der Funktionalität konzentrieren, anstatt das korrekte Vorgehen zur normenkonformen Dokumentation ermitteln zu müssen. Der Fokus der Arbeit des Entwicklungsteams liegt somit voll auf der Umsetzung der Funktionalität anstatt auf der Ermittlung des Vorgehens zur normenkonformen Dokumentation.

Der Projektleitfaden iFSM stellt sicher, dass alle notwendigen Schritte erledigt wurden und die Zertifizierung gelingt.

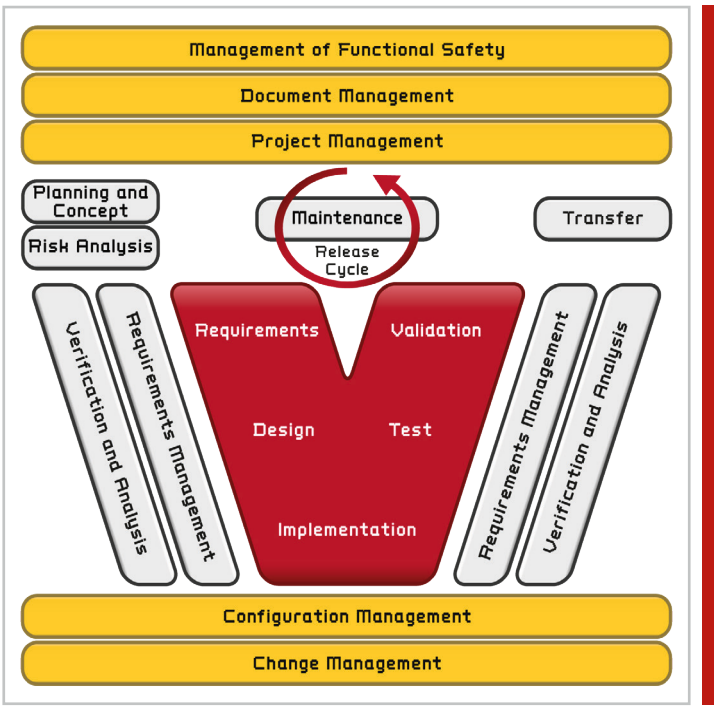


Abbildung 1:
Der zertifizierte iFSM-Prozess

3 Sichere Systemkomponenten

3.1 Laufzeitsystem FlexiSafe®

Mit FlexiSafe® steht ein nach IEC 61508:SIL 3, EN ISO 13849:PLe und DIN EN ISO 50128:SIL 4 zertifiziertes Softwaresystem zur Verfügung, das speziell auf die Anforderungen bezüglich funktionaler Sicherheit zugeschnitten ist. FlexiSafe® besteht aus einem Engineering- und Programmiersystem nach IEC 61131 und IEC 61499 sowie einer Firmware für Safety-Controller. Einzigartig ist dabei die Verfügbarkeit aller in der IEC 61131 definierten Programmiersprachen.

FlexiSafe® basiert auf der Technologie des infoteam-Partners ISaGRAF und kann auf jedes „Safe Operating System" portiert werden. Fertige Portierungen liegen u. a. bereits für QNX, Wind River VxWorks Cert und PikeOS von SYSGO vor.

3.2 Betriebssystem

Der QNX® Neutrino® RTOS Safe Kernel erfüllt die Anforderungen des Standards IEC 61508 bis SIL 3. Er stellt damit eine zertifizierte Plattform für sicherheitskritische Systeme mit hohen Anforderungen an die funktionale Sicherheit dar.

Der QNX® Neutrino® RTOS Safe Kernel läuft auf x86-, Power- sowie ARM-Plattformen inklusive Multicore-Unterstützung durch SMP und bringt dabei einige wichtige Eigenschaften mit, die beim Aufbau eines sicherheitskritischen Systems essenziell sind, u. a.:

- Definierter Design Safe State: wenn der Kernel ein Problem feststellt, das er nicht lösen kann, wechselt er in einen definierten sicheren Zustand.
- Isolation: alle Applikations- und Systemprozesse sind voneinander und vom Kernel isoliert.
- Vorhersagbares Scheduling: mittels Thread-Prioritäten wird vorhersagbares Zeitverhalten gewährleistet, ebenso wie durch Mechanismen zur Vermeidung der Nichtverfügbarkeit wichtiger Ressourcen.

3.3 Hardware

Der neue CompactPCI-PlusIO-SBC F75P wurde speziell für sicherheitskritische Anwendungen entwickelt und holt funktionale Sicherheit durch redundant vorhandene Intel-Atom-Prozessoren auf die Board-Ebene.

Zwei der insgesamt drei Intel-Atom-E680T-Prozessoren sind redundant aufgebaut und bilden die sichere Steuerungseinheit der F75P. Der dritte Intel Atom übernimmt die Steuerung der Ein- und Ausgabe.

Einige der Eigenschaften der F75P im Überblick:

- 2x Intel® E680T, 1,6 GHz für Zweifach-Redundanz
- 1x Intel® E680T, 1,6 GHz, 1 GB DDR2 als I/O-Prozessor
- Unabhängiger Supervisor für jeden Funktionsblock
- Fail-Safe- und Fail-Silent-Architektur
- Event-Logging
- Entwickelt gemäß DIN EN 50129, DIN EN 50128 und IEC 61508
- -40 bis +85 °C Betriebstemperatur
- Volle EN 50155-Konformität

3.4 Architektur

Das iFSC-Referenzsystem (siehe Abb. 2) basiert auf den bereits genannten Komponenten:

- Hardware von MEN Mikro Elektronik GmbH
- QNX® Neutrino® RTOS Safe Kernel
- Firmware FlexiSafe® von ISaGRAF

infoteam führt alle oben genannten Systemarchitekturkomponenten zu kundenspezifischen Lösungen zusammen.

Die FlexiSafe® Firmware ermöglicht dabei auch die Einbindung verschiedenster Kommunikation-Stacks und anderen Subsystemen.

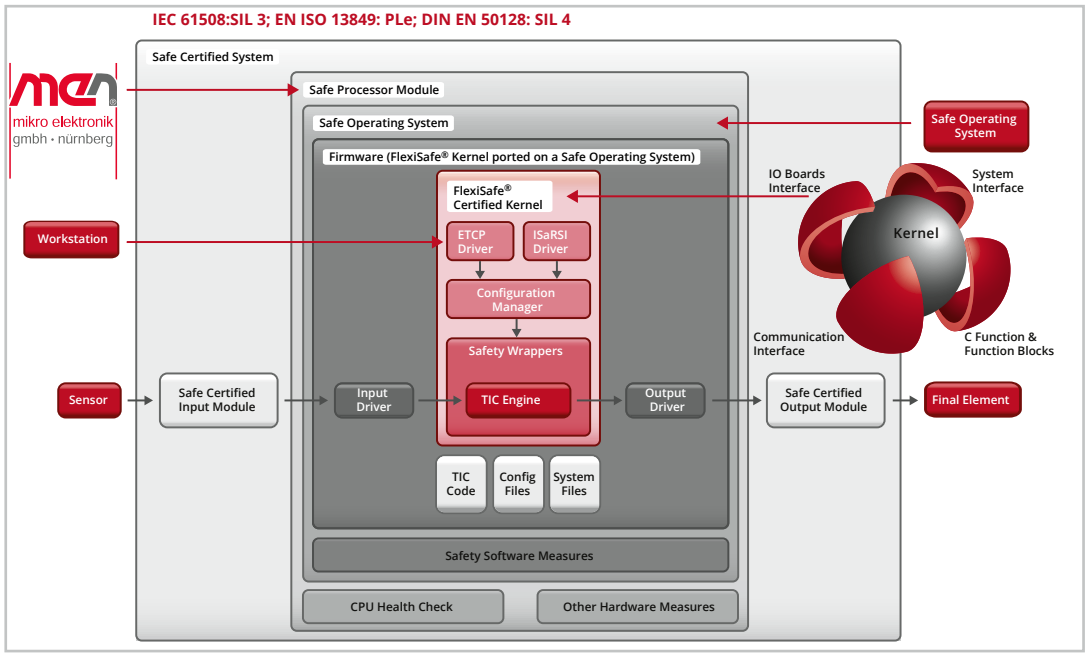


Abbildung 2:
Architektur des iFSC-Referenzsystems

4 Sichere Engineering-Tools

4.1 Programmierumgebung

Die Safety-Programmierumgebung FlexiSafe® von ISaGRAF (siehe Abb. 3) ermöglicht die Erstellung von Anwenderapplikationen in allen IEC-Sprachen und als Sequential Function Chart (SFC). Dabei erlaubt FlexiSafe® die Projektierung sicherer wie auch nicht sicherer Funktionen in einem Tool. Mit dem nachfolgend beschriebenen Cause and Effect Editor steht in der FlexiSafe®-Programmierumgebung ein speziell für die Projektierung von Sicherheitsfunktionen etabliertes Verfahren zur Verfügung.

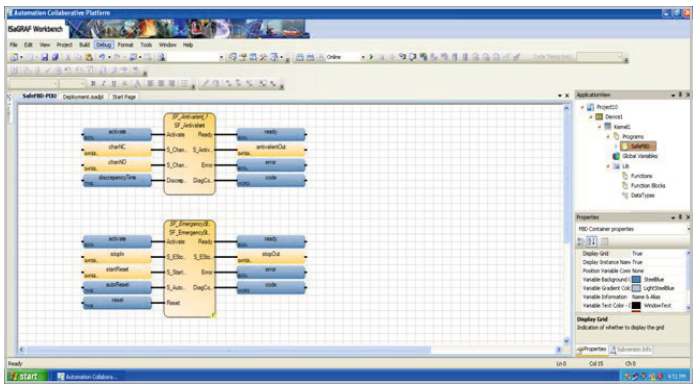


Abbildung 3:
Safety-Programmierumgebung FlexiSafe®

4.2 Cause and Effect Editor

Für die besonders übersichtliche und effiziente Projektierung von Sicherheitsfunktionen dient der in FlexiSafe® integrierte C&E-Editor (siehe Abb. 4).

Der besondere Vorteil bei der Erstellung von Applikationen mit dem C&E-Editor liegt in der deutlich vereinfachten Führung des Sicherheitsnachweises. Damit reduziert sich nicht nur der Aufwand für die Erstellung und Pflege, sondern auch für die Abnahme der sicheren Anwendung.

Die für eine sichere Inbetriebnahme notwendigen Funktionen wie Bypass oder Force sind im C&E-Editor ebenfalls integriert.

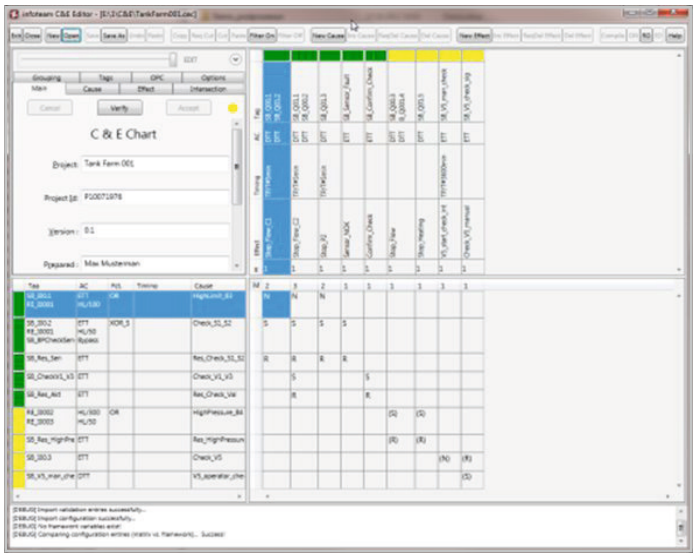


Abbildung 4:
Cause and Effect Editor

5 Anwendungsbeispiele für sichere Funktionen

Im Folgenden sind Beispiele sicherer Funktionen dargestellt, die sich mit dem sicheren Engineering-Tool FlexiSafe® realisieren lassen.

Diese Beispiele dienen lediglich dem besseren Verständnis der Engineering-methoden und erheben keinen Anspruch auf Vollständigkeit.

5.1 Prozesstechnik - Überlaufschutz z. B. Berstschutz einer Tankfarm

Für einen Druckbehälter soll ein Berstschutz erstellt werden. In dem Druck-behälter findet eine exotherme Reaktion statt, die durch Zufluss von Stoff 1 gesteuert werden kann. Wird die Zufuhr von Stoff 1 gestoppt, kommt die Reaktion zum Erliegen. Durch Rücksetzmechanismen kann das System wie-der in den produzierenden Betriebszustand gebracht werden (siehe Abb. 5).

Die Erstellung der Applikation wurde im C&E-Editor durchgeführt, um die Einfachheit und Transparenz dieser Programmiermethode aufzuzeigen. Vertiefende Informationen speziell zum C&E-Editor stellen wir in unserem Whitepaper „Engineering von Sicherheitsfunktionen mit Cause and Effect Charts“ bereit.

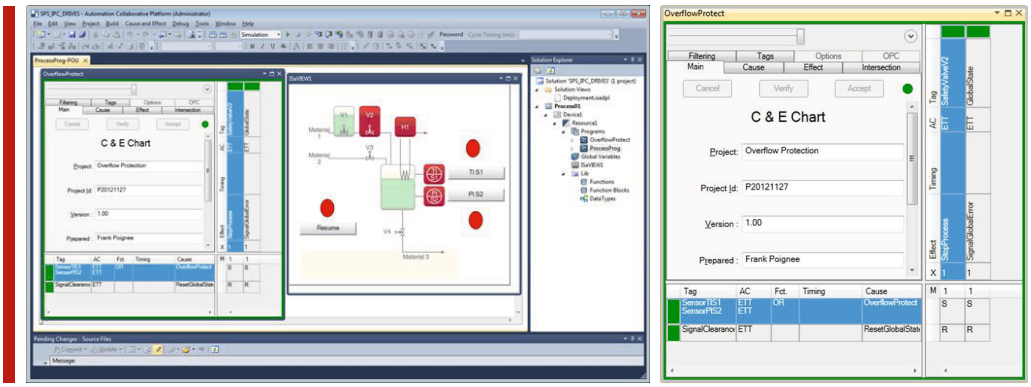


Abbildung 5:
Projektierung Berstschutz mit Cause and Effect Editor in FlexiSafe®

5.2 Bahntechnik - Sicherheitsfahrschaltung

Die Sicherheitsfahrschaltung (kurz: Sifa) auf dem Führerstand besteht aus einer oder mehreren Bedieneinrichtungen, welche dauernd betätigt und in bestimmten Zeitabständen kurz losgelassen und erneut gedrückt werden müssen. Bei Nichtbetätigung wird, wenn optische und akustische Warnungen unbeachtet bleiben, die Zwangsbremsung eingeleitet.

Die Umsetzung der Sifa-Funktion wurde auch hier mithilfe des C&E-Editors realisiert (siehe Abb. 6). Eine Darstellung in Funktionsblöcken (FBD) ist ebenso möglich.

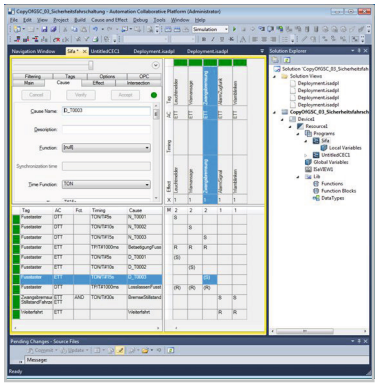


Abbildung 6:
Umsetzung der Sifa-Funktion
im C&E-Editor

5.3 Antriebstechnik –Sicherer Stopp

Bei einem Eingriff in die Maschine, hier das Öffnen der Schutztüre/Klappe, wird die Funktion „Sicherer Stopp“ ausgeführt. Diese Funktion fährt den Antrieb geregelt herunter und leitet in der Folge den sicheren Betriebshalt ein. Im sicheren Betriebshalt wird die erreichte Stopp-Position überwacht und das Verlassen des Positionsfensters verhindert (siehe Abb. 7). Die Regelfunktionen des Antriebs bleiben vollständig erhalten, sodass bei Verlassen des überwachten Positionsfensters der Antrieb sicher abgeschaltet wird.

Überwiegend sind die sicheren Funktionen in den jeweiligen Antrieben realisiert und werden von der Steuerung angestoßen. In FlexiSafe® sind die PLC- Open-Safety-Bausteine als Bibliothek integriert.

Weitere zertifizierbare Bibliotheken kann der Anwender selbstständig erstellen. So lassen sich wiederkehrende Anforderungen zusammenfassen und können dem Endkunden als vordefinierte Funktionsbausteine zur Verfügung gestellt werden.

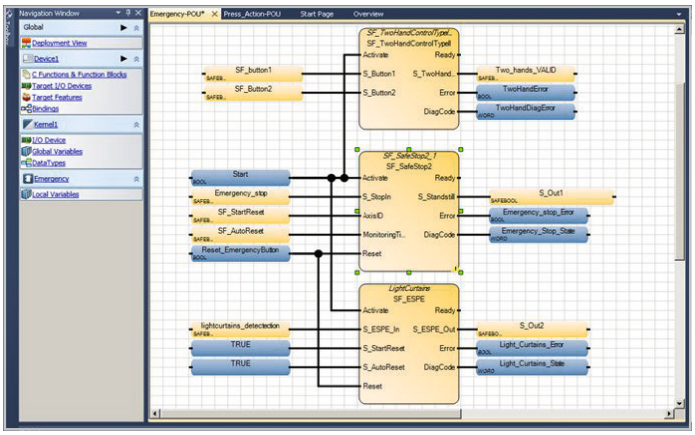


Abbildung 7:
Beispiel „Sicherer Stopp“

6 Vorteile des infoteam Functional Safety Control Concepts

Das iFSC-Concept für die Realisierung eines sicheren Steuerungssystems einzusetzen, hat vielfältige Vorteile:

Vorteil 1: Geringeres Entwicklungsrisiko, denn

- der iFSM-Prozess ist vom TÜV Süd zertifiziert und
- die Systemkomponenten sind betriebsbewährt und validiert.

Vorteil 2: Zeit- und Kostenersparnis, weil

- keine aufwendige Einarbeitung in die Details der Norm IEC 61508 notwendig ist und
- die Systemkomponenten aufeinander abgestimmt sind.

Vorteil 3: Effiziente Erstellung sicherer Applikationssoftware

- mit dem C&E-Editor
- mit allen IEC 61131-3 Sprachen und dem SFC.

7 Glossar

C&E	Cause and Effect
FBD	Function Block Diagram
iFSC	infoteam Functional Safety Control
PLe	Performance Level
SFC	Sequential Function Chart
Sifa	Sicherheitsfahrschaltung
SIL	Sicherheitsintegritätslevel
SMP	Symmetrischer Multiprozessor

Über die infoteam Software Gruppe

Die infoteam Software Gruppe realisiert seit fast 40 Jahren spezifische Softwarelösungen für ihre Kunden aus den Märkten Industry, Infrastructure, Life Science und Public Service. Das Kerngeschäft bilden die Teil- oder Gesamtentwicklung von Steuerungs- und Embedded-Software, Middleware und Anwendungssoftware – agil, modern und nach aktuellen Security-Anforderungen. Spezialdisziplinen sind u. a. normativ regulierte Software für den Einsatz in Medizin- und Laborgeräten (IVDR, MDR, FDA, ISO 13485, IEC 62304 etc.) sowie funktional sichere Software bis zur höchsten Sicherheitsstufe (IEC 61508, DIN EN 50128 etc.). Abgerundet wird das Leistungsportfolio durch langjährige Erfahrungen in den Bereichen Datenanalyse, KI und maschinelles Lernen.

Die infoteam Software Gruppe beschäftigt mehr als 300 Mitarbeiter und verfügt über Standorte und Tochtergesellschaften in Deutschland, Tschechien, der Schweiz und China. Stammsitz der Muttergesellschaft infoteam Software AG ist Bubenreuth bei Erlangen.

www.infoteam.de

Kontakt

infoteam Software AG
Am Bauhof 9 | 91088 Bubenreuth | Deutschland
Telefon: +49 9131 78 00-0
Telefax: +49 9131 78 00-50
info@infoteam.de | www.infoteam.de