EUCHNER
More than safety.

EKS FSA an Siemens S7-300 – Betriebsartenwahl mit Touch-screen

Inhalt

Verwendete Bauteile / Module

EUCHNER

Beschreibung	Best.-Nr. / Artikelbezeichnung
EKS Profinet *FSA*	106306 / EKS-A-IIXA-G01-ST02/03/04
oder	
EKS Profibus *FSA*	100378 / EKS-A-IDXA-G01-ST09/03/04
EKS Schlüssel	077859 / EKS-A-K1RDWT32-EU 084735 / EKS-A-K1BKWT32-EU 091045 / EKS-A-K1BLWT32-EU 094839 / EKS-A-K1GNWT32-EU 094840 / EKS-A-K1YEWT32-EU

Tipp: Weitere Informationen und Downloads zu den o.g. EUCHNER-Produkten finden Sie unter www.EUCHNER.de. Geben Sie einfach die Bestellnummer in die Suche ein.

Andere

Beschreibung	Artikel
S7-300, CPU 315F-2 PN/DP	6ES7315-2FJ14-0AB0

Abkürzungen

Bezeichnung	Abkürzung
EKS *FSA* EKS	Das in dieser Applikation verwendete EKS mit *FSA* Funktionalität und Datenbusschnittstelle (siehe verwendete EUCHNER Bauteile)
SPS	Die konventionelle Steuerung, die verwendet wird und SPS-Funktionalität bietet. Die SPS hat Anschlüsse für die verwendeten Bussysteme
F-SPS	Die fehlersichere SPS, die in dieser Applikation verwendet wird. Die F-SPS hat einen gemeinsamen Datenbereich mit der SPS über Merkerworte
HMI	Die Schnittstelle von der Maschine zum Bediener (Human Machine Interface), gebildet aus eine Bildschirm mit einer Touchoberfläche oder Softkeys
MW	Merkerwort, ein 16 Bit Datenwort zum Austausch der Daten zwischen F-SPS und SPS
PL	Performance Level nach EN ISO 13849-1
PL_r	Performance Level required nach EN ISO 13849-1
SRASW	Sicherheitsbezogene Anwendungssoftware nach EN ISO 13849-1

Funktionsbeschreibung

Allgemein

Es soll eine Betriebsartenwahl an einer Maschine unter Nutzung des EKS *FSA* als Zugangssystem realisiert werden. Die Wahl der Betriebsart erfolgt über einen Touchscreen oder andere Bedienelemente, wie bspw. Softkeys in der HMI (Human Machine Interface). Die Bedienung ist somit über die Standard-Benutzerschnittstelle möglich, es muss kein Schlüsselschalter eingesetzt werden. Die Auswertung und die Umschaltung der Betriebsart ist über eine sichere SPS (F-SPS) realisiert. Die Datenverteilung erfolgt über eine Standard-SPS (SPS).

Beispiel einer Schlüsselstruktur

Die Daten auf dem Schlüssel sind bspw. wie folgt strukturiert. Andere Strukturen sind möglich.

Bytenr.	Beschreibung	Typ	Länge	Erläuterung
103 – 104	KEYCRC	CRC	2 Byte	Prüfsumme über einen bestimmten Teil des Schlüssels als Kopierschutz. Nähere Erläuterungen zur CRC siehe EKM Handbuch und Applikationsbeispiel AP000169-5-…
105 – 112	Verfallsdatum	Date	8 Byte	Verfallsdatum des Schlüssels
113 – 114	Berechtigungsstufe	Word	2 Byte	Autorisierungsstufe für Zugriff auf die Maschine.
115	Abteilung	Byte	1 Byte	Nummer, die eine begrenzte Menge an Maschinen oder Anlagen beschreibt.
116 – 123	KeyID	KeyID	8 Byte	Die KeyID ist eine von EUCHNER fest programmierte Nummer auf dem Schlüssel. Diese Nummer ist bei jedem Schlüssel unterschiedlich. Diese Nummer kann zur Werkeridentifizierung herangezogen werden.

Dies stellt nur ein sehr einfaches Beispiel dar. Der Datenbereich auf dem Schlüssel wird entsprechend den Anforderungen an den Zugang von Maschinen oder Anlagen strukturiert. Weitere Daten, wie bspw. Identifikationsdaten oder Daten für andere Bereiche oder Abteilungen können ebenfalls auf dem Schlüssel angelegt werden. Ergänzende Daten, die auf dem Schlüssel keinen Speicherplatz haben, können in der EKM Datenbank gespeichert werden. Nähere Hinweise zur Strukturierung des Datenbereichs auf dem EKS Schlüssel entnehmen Sie bitte der Applikation „Definition der Schlüsselstruktur auf einem EKS-Schlüssel“ (AP000169-1-…).

Ein wichtiges Feld, um ein Kopieren von Schlüsseln zu verhindern ist das Feld KEYCRC, mit dem eine Prüfsumme über den Schlüsselinhalt berechnet wird. Dieses Feld muss auch in der Steuerung berechnet und überwacht werden. Damit lässt sich ein wirkungsvoller Schutz gegen gefälschte oder kopierte Schlüssel aufbauen. Hierzu können Sie ein Beispiel in der Applikation AP000169-5… finden.

Die Definition der Schlüsselstruktur stellt den wichtigsten Schritt in der Anwendung des EKS dar. Hiermit wird der Leistungsumfang des EKS Schlüssels definiert.

Für diese Applikation hat das Feld „Berechtigungsstufe“ eine besondere Bedeutung. Mit diesem Feld werden bestimmte Betriebsarten für einzelne Nutzer freigegeben, womit die Forderung der Maschinenrichtlinie nach einer Beschränkung der Betriebsartenwahl auf bestimmte Personenkreise erfüllt werden kann.

Wertevorrat für die Berechtigungsstufe bei 5 Betriebsarten:

Binärwert	Hexadezimalwert
0000 1111 0000 1111	0F0FH
0000 1111 1111 0000	0FF0H
0011 0011 0011 0011	3333H
0011 0011 1100 1100	33CCH
0011 1100 0011 1100	3C3CH

Tabelle 1

Die Werte sind so gewählt, dass eine Hamming Distanz von 8 gegeben ist. Zusätzlich wird über die KEYCRC eine Verfälschung des Schlüssels verhindert. Mit dieser Kodierung könnten theoretisch maximal 31 verschiedene Betriebsarten angewählt werden. Der Wert Null darf nicht genutzt werden. Dieser Wert ist notwendig, um einen ausgesteckten Schlüssel zu erkennen. Da über den Bus eine Datenübertragung zwischen den verschiedenen Systemen gewährleistet sein muss, müssen die Codes für die Betriebsartenwahl entsprechend dem Wertevorrat gewählt werden. Diese Datenworte müssen deshalb auch innerhalb des Programms weiter verwendet werden.

Definition der Datenworte für die Stufe der Betriebsart

Um Fehler durch Überschreiben des Speichers in der SPS zu vermeiden, **muss** die Bedeutung der Betriebsartenwahl in den verschiedenen benutzten Speicherstellen den Wert wechseln. Hierzu wird in der Tabelle 2 bzw. Tabelle 4 festgelegt, was die Betriebsartenwahl in der jeweiligen Variablen bzw. im Datenwort für eine Bedeutung hat. Dies erfolgt mittels Konstanten.

Variable bzw. Datenwort	Definition Betriebsart	Hex	Bemerkung
Wertebereich für MW01 und ReadAuthorization, Schlüsselinhalt (entsprechend diesen Werten muss der Schlüssel beschrieben sein)	RE_MSO_0	0F0FH	Mode of Safe Operation 0: Manueller Betrieb
	RE_MSO_1	0FF0H	Mode of Safe Operation 1: Automatikbetrieb
	RE_MSO_2	3333H	Mode of Safe Operation 2: Einrichtbetrieb
	RE_MSO_3	33CCH	Mode of Safe Operation 3: Automatikbetrieb mit manuellem Eingriff
	RE_MSO_4	3C3CH	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme
Wertebereich für MW03 und SelectMSO	SE_MSO_0	0FF0H	Mode of Safe Operation 0: Manueller Betrieb
	SE_MSO_1	3333H	Mode of Safe Operation 1: Automatikbetrieb
	SE_MSO_2	33CCH	Mode of Safe Operation 2: Einrichtbetrieb
	SE_MSO_3	3C3CH	Mode of Safe Operation 3: Automatikbetrieb mit manuellem Eingriff
	SE_MSO_4	0F0FH	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme
Wertebereich für MW05 und CheckMSO	CH_MSO_0	3333H	Mode of Safe Operation 0: Manueller Betrieb
	CH_MSO_1	33CCH	Mode of Safe Operation 1: Automatikbetrieb
	CH_MSO_2	3C3CH	Mode of Safe Operation 2: Einrichtbetrieb
	CH_MSO_3	0F0FH	Mode of Safe Operation 3: Automatikbetrieb mit manuellem Eingriff
	CH_MSO_4	0FF0H	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme
Wertebereich für MW07 und SwitchMSO	SW_MSO_0	33CCH	Mode of Safe Operation 0: Manueller Betrieb
	SW_MSO_1	3C3CH	Mode of Safe Operation 1: Automatikbetrieb
	SW_MSO_2	0F0FH	Mode of Safe Operation 2: Einrichtbetrieb
	SW_MSO_3	0FF0H	Mode of Safe Operation 3: Automatikbetrieb mit manuellem Eingriff
	SW_MSO_4	3333H	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme

Tabelle 2

Die Werte stellen eine hierarchische Ordnung dar, bspw. ist MSO 1 und MSO 2 in MSO 3 enthalten.

Wichtig: Diese Werte müssen genutzt werden, um die Datenübertragung auf dem Bus zwischen SPS und HMI sicherzustellen.

Wertevorrat für die Berechtigungsstufe bei 3 Betriebsarten:

Wenn für eine Maschine oder Anlage nur bis zu 3 verschiedene Betriebsarten benötigt werden, kann anstelle des Datenworts auch ein Datenbyte verwendet werden, das die Hamming-Distanz 5 aufweist. Das Verfahren der ändernden Werte für die Bedeutung der Betriebsartenwahl muss auch hier angewendet werden.

Binärwert	Hexadezimalwert
00011111	1FH
11100011	E3H
11111100	FCH

Tabelle 3

Definition der Datenbytes für die Stufe der Betriebsart

WICHTIG: Die Definition der Datenbytes muss exakt dem Schema der Tabelle 4 entsprechen. Insbesondere müssen die Werte für den Automatikbetrieb entsprechend der Tabelle vergeben werden!

Variable bzw. Datenbyte	Definition Betriebsart	Hex	Bemerkung
Wertebereich für MB01 und ReadAuthorization	RA_MSO_1	1FH	Mode of Safe Operation 1: Automatikbetrieb
	RA_MSO_2	E3H	Mode of Safe Operation 2: Einrichtbetrieb
	RA_MSO_3	FCH	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme
Wertebereich für MB03 und SelectMSO	SE_MSO_1	E3H	Mode of Safe Operation 1: Automatikbetrieb
	SE_MSO_2	FCH	Mode of Safe Operation 2: Einrichtbetrieb
	SE_MSO_3	1FH	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme
Wertebereich für MB05 und CheckMSO	CH_MSO_1	1FH	Mode of Safe Operation 1: Automatikbetrieb
	CH_MSO_2	FCH	Mode of Safe Operation 2: Einrichtbetrieb
	CH_MSO_3	E3H	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme
Wertebereich für MB07 und SwitchMSO	SW_MSO_1	E3H	Mode of Safe Operation 1: Automatikbetrieb
	SW_MSO_2	1FH	Mode of Safe Operation 2: Einrichtbetrieb
	SW_MSO_3	FCH	Mode of Safe Operation Service: Betriebsart für Service und Inbetriebnahme

Tabelle 4

Die Werte stellen eine hierarchische Ordnung dar, bspw. ist MSO 1 und MSO 2 in MSO 3 enthalten.

Wichtig: Diese Werte müssen genutzt werden, um die Datenübertragung auf dem Bus zwischen SPS und HMI sicherzustellen.

Blockschaltbild und Beschreibung

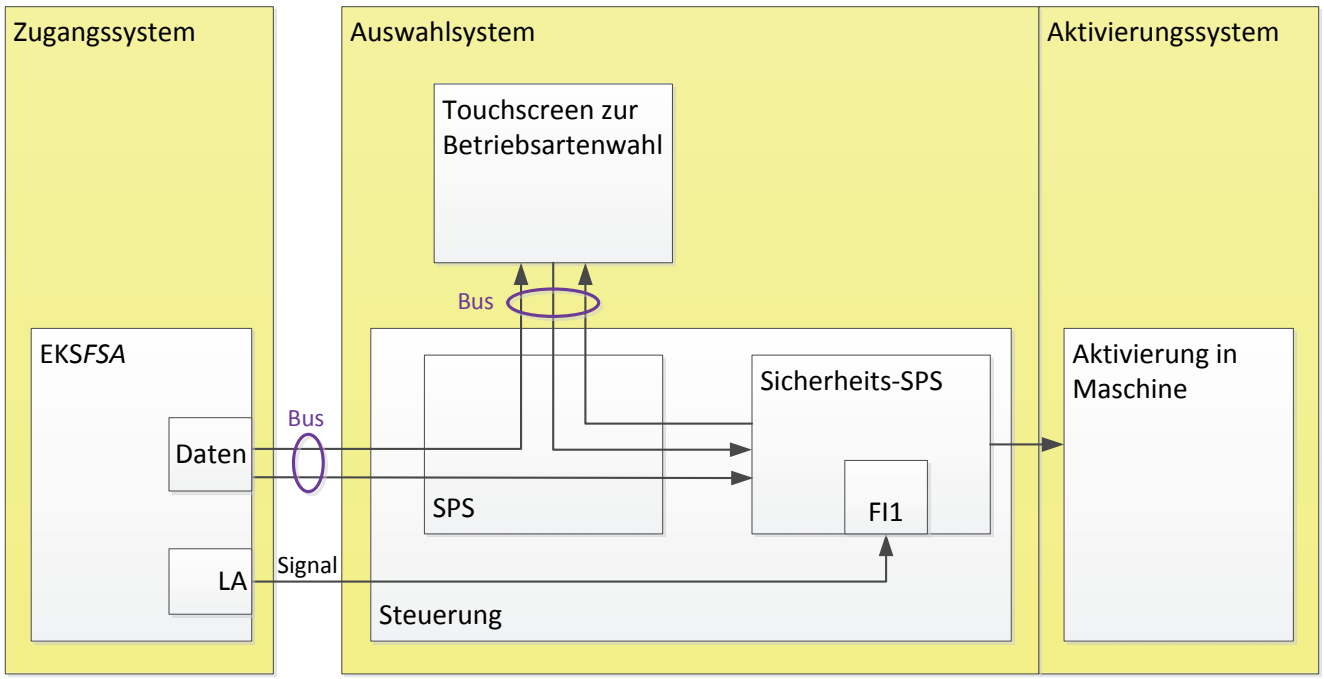


Bild 1

Das EKS *FSA* wird über den Bus an die SPS angeschlossen. Die Daten werden ausschließlich an die SPS gesendet. Die SPS sendet die Daten intern über Merkerworte (MW..) weiter an die Sicherheits-SPS (F-SPS). Die Kommunikation zur HMI kann beliebig erfolgen, typisch über einen Bus. Der Schaltkanal LA des EKS *FSA* muss an einen sicheren Eingang der F-SPS angeschlossen werden. Im Beispiel wird FI1 benutzt. Die sichere SPS ist zuständig für die Umschaltung der Betriebsart. Dies können zum einen interne Signale an die SPS sein, vor allem wird aber auch die Sicherheitstechnik für die gewählte Betriebsart über Ausgänge eingeschaltet. Es ist zu beachten, dass dieser Teil der Betriebsartenwahl ebenfalls sicherheitsrelevant ist und somit den erforderlichen Performance Level (PL_r) der Betriebsartenwahl erfüllen muss.

Generelle Hinweise zur Programmierung

Die Abläufe in den 4 verschiedenen Geräten sind so aufgebaut, dass die F-SPS aufgrund der Daten, die durch die verschiedenen Geräte generiert und durchgereicht werden, möglichst viele Fehler automatisch erkennt.

Die Darstellung in den untenstehenden Diagrammen ist ein logischer Ablauf, der in einer SPS und einer F-SPS mit einer zyklischen Bearbeitung nicht automatisch eingehalten wird. Die Programmierung muss deshalb so erfolgen, dass jeder Schritt nur ein einziges Mal durchlaufen wird. Das kann bspw. in Form einer einfachen Statusmaschine erfolgen, die so programmiert ist, dass pro SPS-Zyklus nur ein einziger der einzelnen Schritte aus den untenstehenden Diagrammen bearbeitet wird. Erst wenn der einzelne Schritt fertig bearbeitet ist, wird auf den nächsten Schritt umgeschaltet.

Vor jedem Einzelschritt muss in der SPS, der HMI sowie in der F-SPS eine Abfrage entsprechend Bild 3 bzw. Bild 8 programmiert werden, damit der Zustand des EKS immer richtig erkannt wird und in den Ausgangszustand zurück geschaltet wird, falls bspw. während der Programmabarbeitung der Schlüssel herausgezogen wird. Mit diesen Abfragen vor jedem Schritt wird zum einen überwacht, dass alle Steuerungsteile parallel ablaufen und dass aus einem eventuell auftretenden Fehler zurück geschaltet wird, wenn die Softwareteile wieder ordnungsgemäß durchlaufen werden.

Wenn ein Ablauf komplett durchlaufen wurde, muss anschließend zumindest die Routine „Stecken vor jedem Schritt“ oder „Ausstecken vor jedem Schritt“ durchlaufen werden.

Stecken eines EKS Schlüssels

Der gesamte Ablauf wird im Flussdiagramm Bild 2.1 bis Bild 2.3 dargestellt. Übergabevariablen sind rot dargestellt.

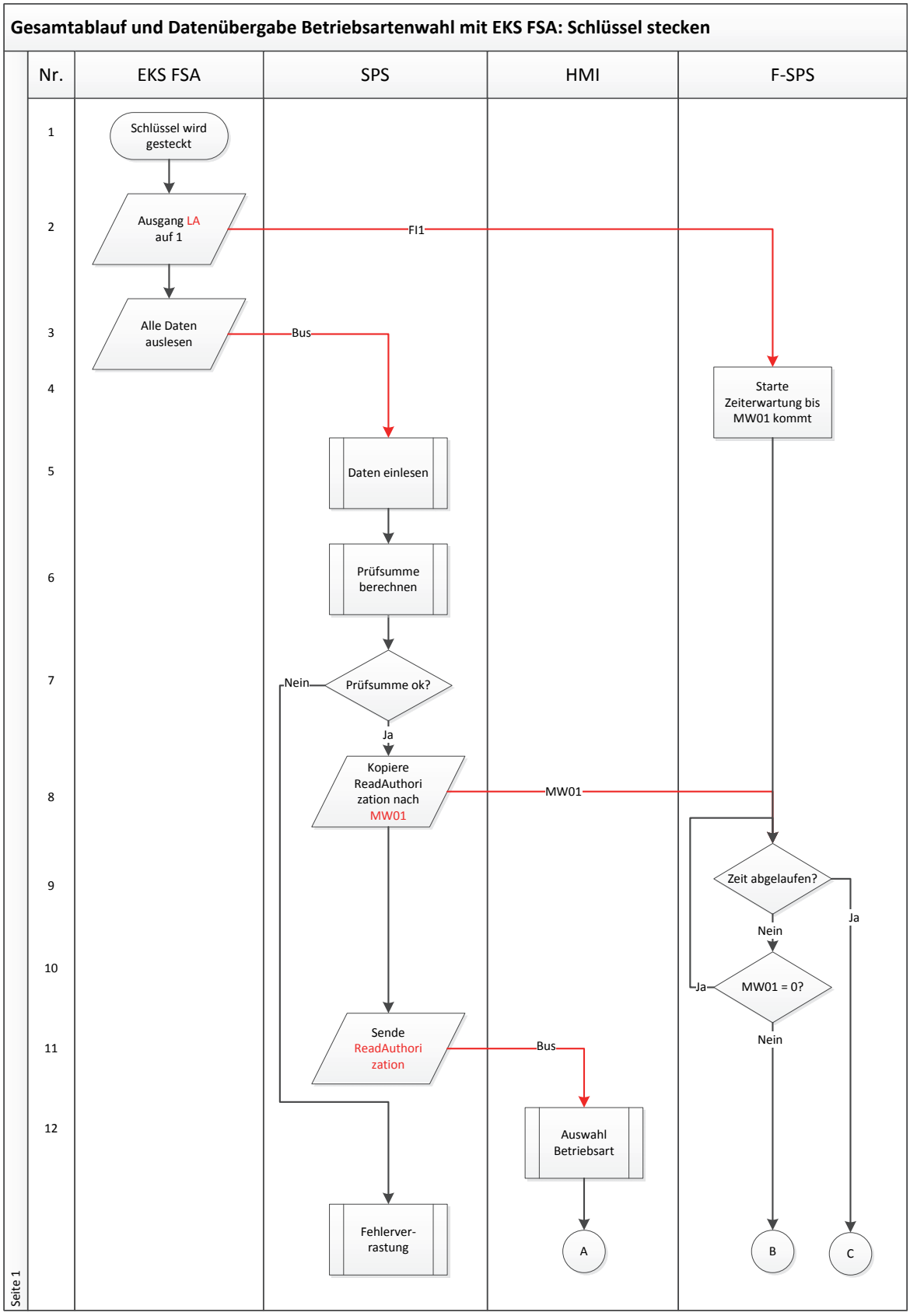


Bild 2.1

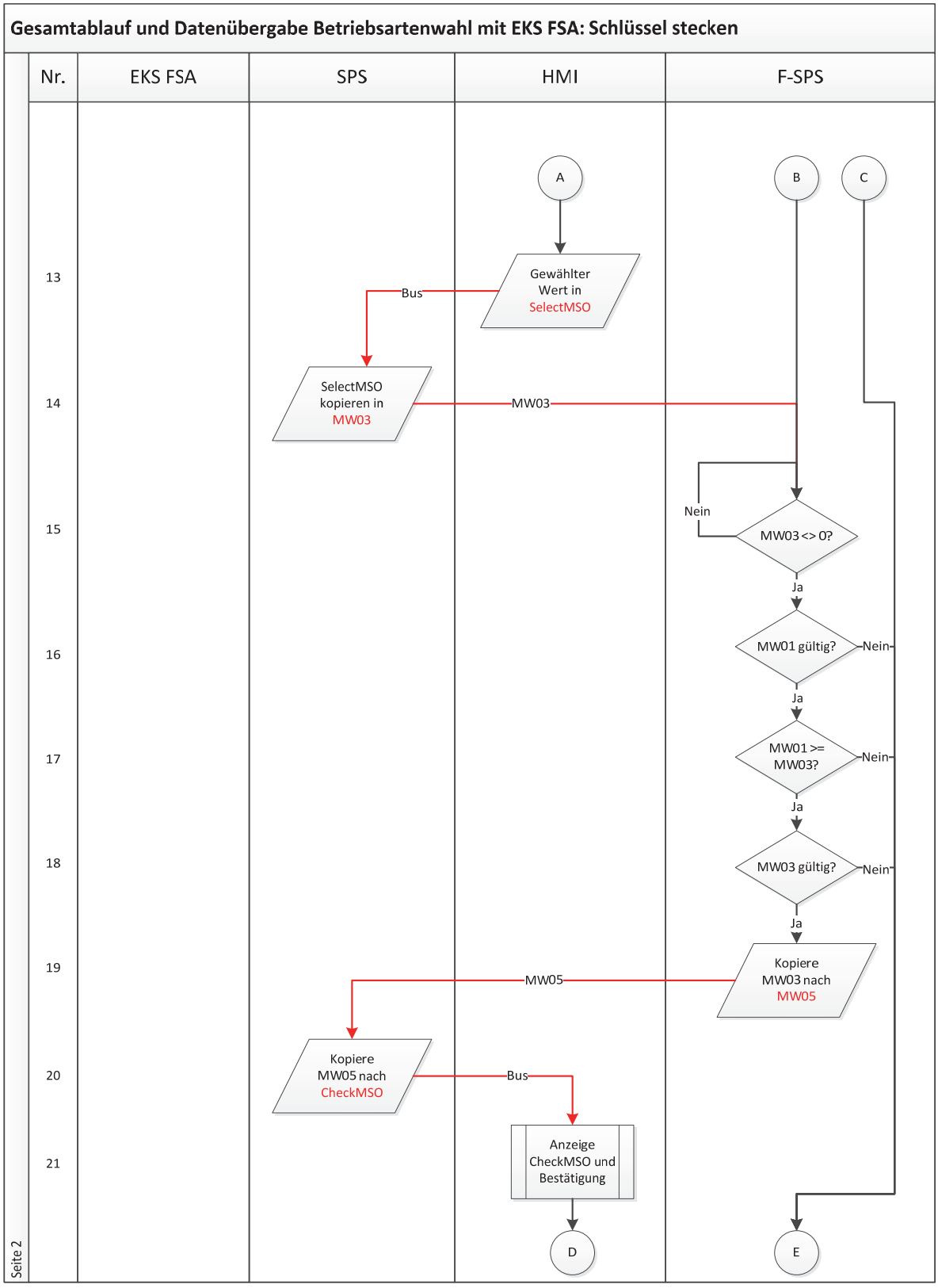

Gesamtablauf und Datenübergabe Betriebsartenwahl mit EKS FSA: Schlüssel stecken
Nr.
EKS FSA
SPS
HMI
F-SPS
13
14
15
16
17
18
19
20
21
A
B
C
Gewählter Wert in SelectMSO
Bus
SelectMSO kopieren in MW03
MW03
Nein
MW03 <> 0?
Ja
MW01 gültig?
Nein
Ja
MW01 >= MW03?
Nein
Ja
MW03 gültig?
Nein
Ja
Kopiere MW03 nach MW05
MW05
Kopiere MW05 nach CheckMSO
Bus
Anzeige CheckMSO und Bestätigung
D
E
Seite 2

Bild 2.2

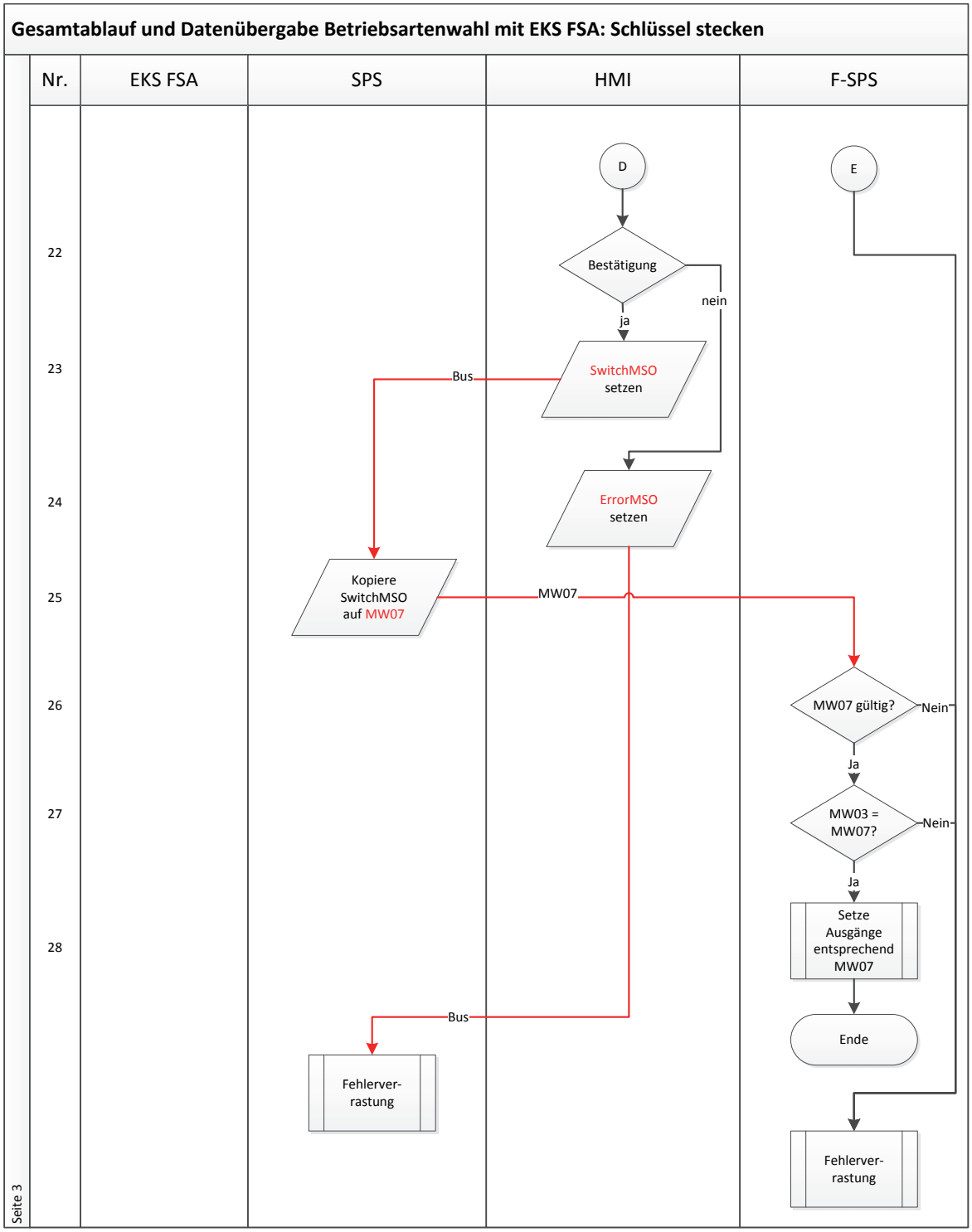

Gesamtablauf und Datenübergabe Betriebsartenwahl mit EKS FSA: Schlüssel stecken
Nr.
EKS FSA
SPS
HMI
F-SPS
22
23
24
25
26
27
28
D
Bestätigung
nein
ja
SwitchMSO setzen
Bus
ErrorMSO setzen
Kopiere SwitchMSO auf MW07
MW07
Bus
Fehlerver-rastung
E
MW07 gültig?
Nein
Ja
MW03 = MW07?
Nein
Ja
Setze Ausgänge entsprechend MW07
Ende
Fehlerver-rastung
Seite 3

Bild 2.3

Schritt	System	Beschreibung
1	EKS *FSA*	Durch einen Benutzer wird ein Schlüssel eingesteckt.
2	EKS *FSA*	Wenn ein Schlüssel gesteckt wird, wird der Ausgang LA auf 1 gesetzt, sofern der Schlüssel ein gültiger Schlüssel ist. Der Inhalt des Schlüssels wird dabei nicht beachtet.
3	EKS *FSA*	Das EKS *FSA* liest den Schlüssel aus. Dabei wird das Format des Schlüssels erkannt und nur wenn alles korrekt ist, werden die Daten gesendet.
4	F-SPS	In der sicheren SPS wird eine Zeiterwartung (ca. 1s) gestartet, bis nach Setzen des sicheren Eingangs FI1 die zugehörigen Daten von der SPS gesendet werden. Vor Ablauf der Zeit müssen alle weiteren Daten vom EKS *FSA* eingelesen worden sein und über die verschiedenen Systeme an die F-SPS gemeldet worden sein.
5	SPS	Alle Schlüsseldaten werden von der SPS im festgelegten Eingangsbereich eingelesen und werden von dort in einen globalen Datenbaustein umkopiert.
6	SPS	Es wird die Prüfsumme des Schlüsselinhalts berechnet. Anschließend wird als Bit zurückgegeben, ob die Prüfsumme ok ist. (Siehe hierzu Applikation AP000169-5…)
7	SPS	Prüfen, ob die Prüfsummenberechnung dasselbe Ergebnis ergeben hat, wie auf dem Schlüssel geschrieben ist. (Siehe hierzu Applikation AP000169-5…)
8	SPS	Die Daten aus dem Bereich des Datenbausteins, an der Stelle der Zugangsberechtigung werden unverändert in das Merkerwort MW01 umkopiert, damit die F-SPS die Daten bekommt. Zu beachten ist, dass hier die Definition des Wertebereichs für MW01 sowie ReadAuthorization aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Die Daten müssen in in dieser Form bereits auf dem Schlüssel stehen.
9	F-SPS	Prüfen, ob die Zeit abgelaufen ist. Damit wird überwacht, ob sowohl das EKS, als auch die SPS korrekt arbeitet.
10	F-SPS	Es wird abgefragt, ob von der SPS neue Daten gekommen sind. Das ist dadurch gekennzeichnet, dass im MW01 ein beliebiger Wert ungleich 0 erscheint.
11	SPS	Die SPS sendet über das Bussystem den Inhalt von ReadAuthorization an die HMI. Zu beachten ist, dass hier die Definition des Wertebereichs für MW01 sowie ReadAuthorization aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Die Daten müssen in in dieser Form bereits auf dem Schlüssel stehen.
12	HMI	In der HMI wird ein Bild aufgebaut oder zugänglich gemacht, in dem die Betriebsart angewählt werden kann. Es wird über einen Touchscreen oder über Softkeys eine Betriebsart angewählt. Die maximal eingebbare Betriebsart darf dabei nicht höher als die Zugangsberechtigung auf dem EKS Schlüssel entsprechend MW01 bzw. ReadAuthorization sein.
13	HMI	Die HMI sendet über den Bus die vom Anwender gewählte Betriebsart. Zu beachten ist, dass hier die Definition des Wertebereichs für MW03 sowie SelectMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss.
14	SPS	Die gewählte Betriebsart wird aus dem Eingangsbereich des Busanschluss unverändert in das Merkerwort MW03 kopiert, um es an die F-SPS zu übergeben.
15	F-SPS	Es wird abgefragt, ob von der SPS neue Daten gekommen sind. Das ist dadurch gekennzeichnet, dass im MW03 ein beliebiger Wert ungleich 0 erscheint.
16	F-SPS	Im MW01 muss einer der zulässigen Codes stehen. Falls ein unzulässiger Code erscheint, muss in den Fehler verzweigt werden. Zu beachten ist, dass hier die Definition des Wertebereichs für MW01 sowie die für SelectMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Eine Ablaufbeschreibung, die diesen Schritt im Detail beinhaltet, finden Sie in Bild 4
17	F-SPS	Die gewählte Betriebsart muss innerhalb des zulässigen Bereichs sein. Zu beachten ist, dass hier die Definition des Wertebereichs für MW01 sowie readAuthorization und MW03 sowie SelectMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Eine Ablaufbeschreibung, die diesen Schritt im Detail beinhaltet, finden Sie in Bild 4
18	F-SPS	Im MW03 muss einer der zulässigen Codes stehen. Falls ein unzulässiger Code erscheint, muss in den Fehler verzweigt werden. Zu beachten ist, dass hier die Definition des Wertebereichs für MW03 sowie SelectMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Eine Ablaufbeschreibung, die diesen Schritt im Detail beinhaltet, finden Sie in Bild 5

19	F-SPS	Nur wenn die Prüfung ergeben hat, dass alles ok ist, wird die Rückmeldung in MW05 gegeben. Zu beachten ist, dass hier die Definition des Wertebereichs für MW05 sowie CheckMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Eine Ablaufbeschreibung, die diesen Schritt im Detail beinhaltet, finden Sie in Bild 5
20	SPS	Das Merkerwort MW05 von der SPS wird unverändert in den Ausgangsbereich für die HMI umkopiert, damit es in der HMI gelesen werden kann.
21	HMI	In der HMI muss die in MW05 zurück gemeldete Betriebsart angezeigt werden, damit der Benutzer diese bestätigen kann. Es wird abgefragt, ob alles ok ist (Abfrage ob die angezeigte Betriebsart der zuvor gewählten entspricht, bspw. Ja und Nein). Hierzu muss in der HMI ein neues Eingabefeld erzeugt werden, es darf nicht das bereits zuvor verwendete Eingabefeld aus Schritt 12 verwendet werden. Die Bestätigung muss auf dem Touchscreen sowohl in der X- als auch in der Y-Koordinate an einer anderen Stelle als zuvor die Betriebsart in Schritt 12 eingegeben werden. Die Bestätigung darf nicht an derselben Stelle auf dem Touchscreen erfolgen, an der auch die gewählte Betriebsart bestätigt wurde.
22	HMI	Der Benutzer muss die Betriebsart, die angezeigt wird, bestätigen.
23	HMI	Nachdem die Betriebsart bestätigt wurde, wird der Wert für die gewählte Betriebsart auf SwitchMSO geschrieben und über den Bus an die SPS gesendet. Zu beachten ist, dass hier die Definition des Wertebereichs für MW07 sowie SwitchMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss.
24	HMI	Als negative Bestätigung wird von der HMI gekennzeichnet, dass ein Fehler aufgetreten ist. Diese Information wird über den Bus gesendet.
25	SPS	Die gewählte Betriebsart wird aus dem Eingangsbereich des Busanschluss in das Merkerwort MW07 kopiert um es an die F-SPS zu übergeben.
26	F-SPS	Im MW07 muss einer der zulässigen Codes stehen. Falls ein unzulässiger Code erscheint, muss in den Fehler verzweigt werden. Zu beachten ist, dass hier die Definition des Wertebereichs für MW07 sowie SelectMSO aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Eine Ablaufbeschreibung, die diesen Schritt im Detail beinhaltet, finden Sie in Bild 6
27	F-SPS	Es wird verglichen, ob die ursprünglich gewählte Betriebsart MW03 auch der bestätigten Betriebsart MW07 entspricht. Eine Ablaufbeschreibung, die diesen Schritt im Detail beinhaltet, finden Sie in Bild 6
28	F-SPS	Bei Entsprechung wird auf die neue Betriebsart aus MW07 umgeschaltet.

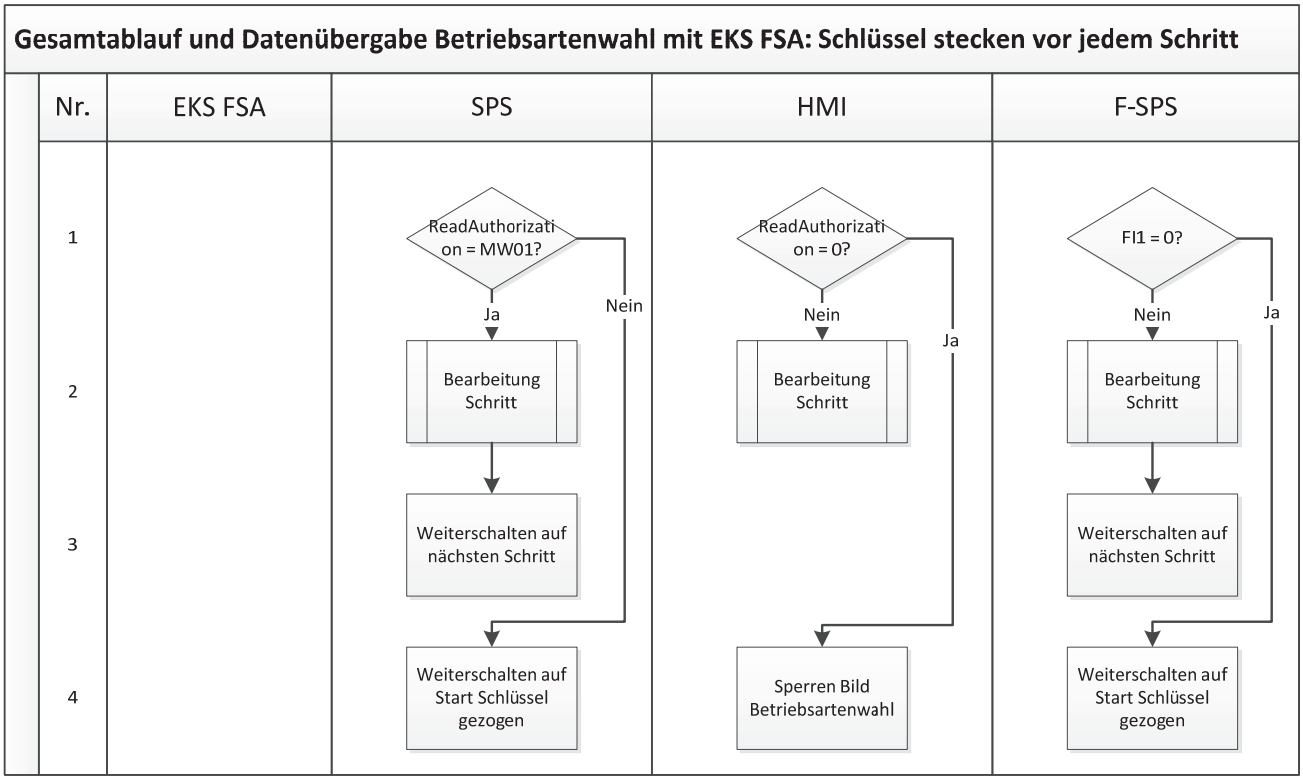


Bild 3

Durch den synchronen Ablauf in den Systemen SPS, HMI und F-SPS können Unterschiede in den Systemen (Kanälen) aufgedeckt werden. Deshalb muss vor jedem einzelnen Schritt im Ablaufdiagramm aus Bildern 2 der Ablauf aus Bild 3 programmiert bzw. aufgerufen werden.
Diese Ablaufschritte müssen auch vor der Fehlerroutine durchlaufen werden. Damit wird sichergestellt, dass das System sich durch Ziehen des Schlüssels wieder fangen kann, wenn eine Störung nicht dauerhaft besteht (bspw. durch den Benutzer ausgelöst wurde).

Schritt	System	Beschreibung
1	SPS	Es wird geprüft, ob die Daten im Eingangsbereich unverändert gegenüber den letzten an die F-SPS weitergegebenen Daten sind. Zu beachten ist, dass hier die Definition für MW01 sowie ReadAuthorization aus Tabelle 2 oder Tabelle 4 genutzt werden muss. Da dieselben Werte für die Variablen verwendet werden, kann ein direkter Vergleich erfolgen.
1	HMI	Es wird geprüft, ob seitens der SPS immer noch eine Freigabe für das Bild „Eingabe der Betriebsart“ besteht.
1	F-SPS	Es wird geprüft, ob das EKS *FSA* immer noch anzeigt, dass ein Schlüssel gesteckt ist.
2	SPS HMI F-SPS	Der gerade abzuarbeitende Schritt aus dem Ablaufdiagramm in Bild 2 wird bearbeitet.
3	SPS F-SPS	Es wird im Status auf den nächsten Schritt aus dem Ablaufdiagramm in Bild 2 weiter geschaltet.
4	SPS	Es wird auf den Start der Routine „Schlüssel wird ausgesteckt“ umgeschaltet.
4	HMI	Der Zugang zum Bild Betriebsartenwahl wird gesperrt.
4	F-SPS	Es wird auf den Start der Routine „Schlüssel wird ausgesteckt“ umgeschaltet.

Unterprogramm bei Schlüssel stecken: Schritt 16 und Schritt 17 (MW01 gültig und MW01 >= MW03)

Nr.	F-SPS

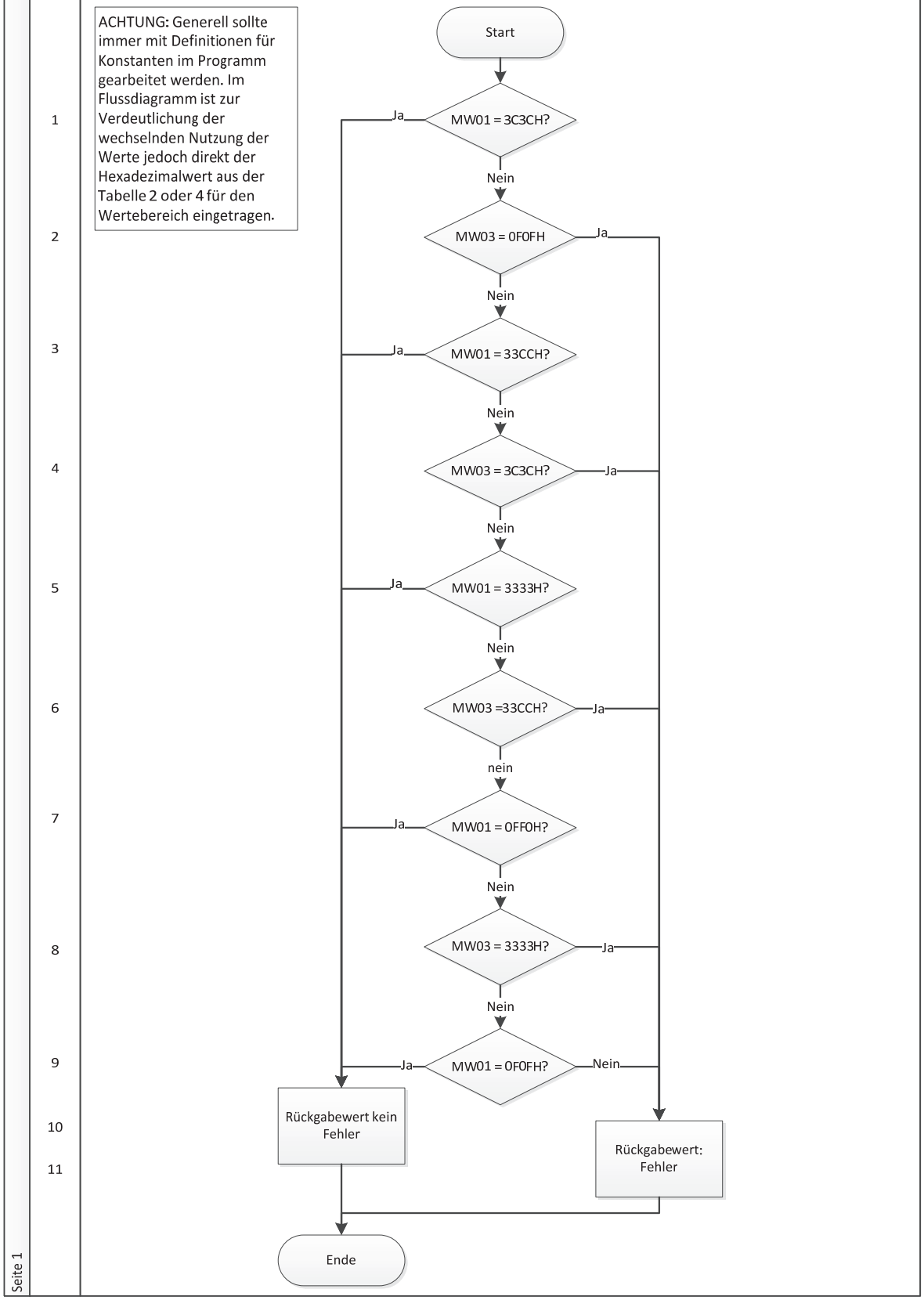
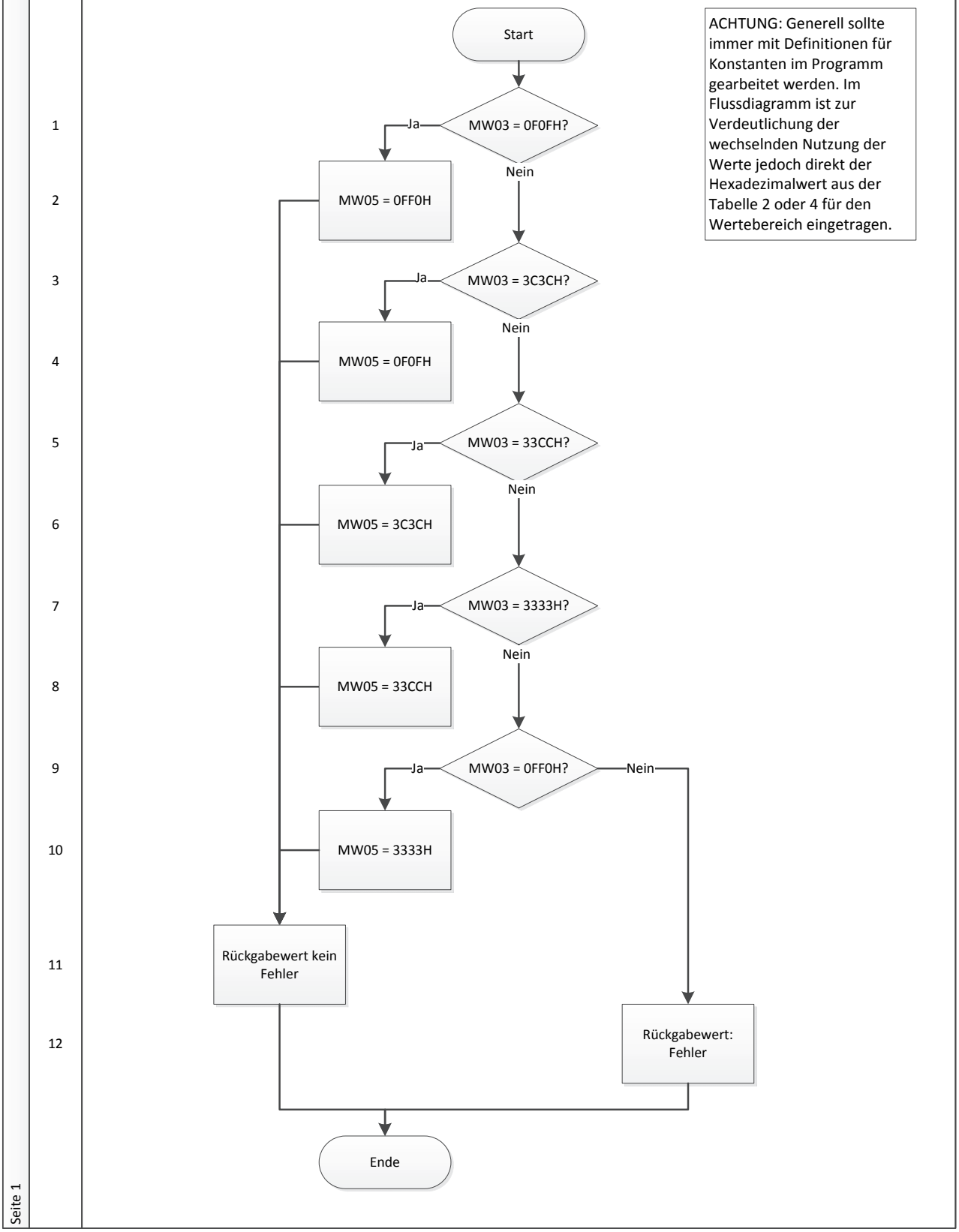


Bild 4

Schritt	System	Beschreibung
1	F-SPS	Es wird geprüft, ob im MW01 (zulässige Betriebsart) die höchste Berechtigungsstufe (MSO 4) gespeichert ist. Im MW01 wird dies durch den Wert 3C3CH dargestellt. Falls JA, ist jede gewählte Betriebsart gültig sofern das übertragene Datenwort in MW03 einen gültigen Wert aufweist (Prüfung in Schritt 18) und es kann ohne Fehlermeldung weiter gearbeitet werden.
2	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die höchste Berechtigungsstufe (MSO 4) gespeichert ist. Im MW03 wird dies durch den Wert 0F0FH dargestellt. Falls JA, wurde eine nicht zulässige Betriebsart angewählt, denn im MW01 fehlt die Berechtigung für diese Betriebsart.
3	F-SPS	Es wird geprüft, ob im MW01 (zulässige Betriebsart) die zweithöchste Berechtigungsstufe (MSO 3) gespeichert ist. Im MW01 wird dies durch den Wert 33CCH dargestellt. Falls JA, ist jede gewählte Betriebsart gültig sofern das übertragene Datenwort in MW03 einen gültigen Wert aufweist (Prüfung in Schritt 18) und es kann ohne Fehlermeldung weiter gearbeitet werden.
4	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die zweithöchste Berechtigungsstufe (MSO 3) gespeichert ist. Im MW03 wird dies durch den Wert 3C3CH dargestellt. Falls JA, wurde eine nicht zulässige Betriebsart angewählt, denn im MW01 fehlt die Berechtigung für diese Betriebsart.
5	F-SPS	Es wird geprüft, ob im MW01 (zulässige Betriebsart) die dritthöchste Berechtigungsstufe (MSO 2) gespeichert ist. Im MW01 wird dies durch den Wert 3333H dargestellt. Falls JA, ist jede gewählte Betriebsart gültig sofern das übertragene Datenwort in MW03 einen gültigen Wert aufweist (Prüfung in Schritt 18) und es kann ohne Fehlermeldung weiter gearbeitet werden.
6	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die dritthöchste Berechtigungsstufe (MSO 2) gespeichert ist. Im MW03 wird dies durch den Wert 33CCH dargestellt. Falls JA, wurde eine nicht zulässige Betriebsart angewählt, denn im MW01 fehlt die Berechtigung für diese Betriebsart.
7	F-SPS	Es wird geprüft, ob im MW01 (zulässige Betriebsart) die vorletzte Berechtigungsstufe (MSO 1) gespeichert ist. Im MW01 wird dies durch den Wert 0FF0H dargestellt. Falls JA, ist jede gewählte Betriebsart gültig sofern das übertragene Datenwort in MW03 einen gültigen Wert aufweist (Prüfung in Schritt 18) und es kann ohne Fehlermeldung weiter gearbeitet werden.
8	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die vorletzte Berechtigungsstufe (MSO 1) gespeichert ist. Im MW03 wird dies durch den Wert 3333H dargestellt. Falls JA, wurde eine nicht zulässige Betriebsart angewählt, denn im MW01 fehlt die Berechtigung für diese Betriebsart.
9	F-SPS	Es wird geprüft, ob im MW01 (zulässige Betriebsart) die letzte Berechtigungsstufe (MSO 0) gespeichert ist. Im MW01 wird dies durch den Wert 0F0FH dargestellt. Falls JA, ist die gewählte Betriebsart gültig sofern das übertragene Datenwort in MW03 einen gültigen Wert aufweist (Prüfung in Schritt 18) und es kann ohne Fehlermeldung weiter gearbeitet werden. Falls Nein, ist MW01 ungültig.
10	F-SPS	Es wird zurück gemeldet, dass kein Fehler aufgetreten ist.
11	F-SPS	Es wird zurück gemeldet, dass ein Fehler aufgetreten ist.

Unterprogramm bei Schlüssel stecken: Schritt 18 und Schritt 19 (MW03 gültig und Kopiere MW03 nach MW05)

Nr.	F-SPS



Seite 1

Bild 5

Schritt	System	Beschreibung
1	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die Berechtigungsstufe MSO 4 gespeichert ist. Im MW03 wird dies durch den Wert 0F0FH dargestellt. Falls JA, kann in MW05 der zugehörige Wert eingespeichert werden. Falls NEIN, wird weiter geprüft.
2	F-SPS	Es wird in MW05 (zu prüfende Betriebsart) der Wert für die Berechtigungsstufe MSO 4 gespeichert. In MW05 wird das durch den Wert 0FF0H dargestellt.
3	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die Berechtigungsstufe MSO 3 gespeichert ist. Im MW03 wird dies durch den Wert 3C3CH dargestellt. Falls JA, kann in MW05 der zugehörige Wert eingespeichert werden. Falls NEIN, wird weiter geprüft.
4	F-SPS	Es wird in MW05 (zu prüfende Betriebsart) der Wert für die Berechtigungsstufe MSO 3 gespeichert. In MW05 wird das durch den Wert 0F0FH dargestellt.
5	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die Berechtigungsstufe MSO 2 gespeichert ist. Im MW03 wird dies durch den Wert 33CCH dargestellt. Falls JA, kann in MW05 der zugehörige Wert eingespeichert werden. Falls NEIN, wird weiter geprüft.
6	F-SPS	Es wird in MW05 (zu prüfende Betriebsart) der Wert für die Berechtigungsstufe MSO 2 gespeichert. In MW05 wird das durch den Wert 3C3CH dargestellt.
7	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die Berechtigungsstufe MSO 1 gespeichert ist. Im MW03 wird dies durch den Wert 3333H dargestellt. Falls JA, kann in MW05 der zugehörige Wert eingespeichert werden. Falls NEIN, wird weiter geprüft.
8	F-SPS	Es wird in MW05 (zu prüfende Betriebsart) der Wert für die Berechtigungsstufe MSO 1 gespeichert. In MW05 wird das durch den Wert 33CCH dargestellt.
9	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die Berechtigungsstufe MSO 0 gespeichert ist. Im MW03 wird dies durch den Wert 0FF0H dargestellt. Falls JA, kann in MW05 der zugehörige Wert eingespeichert werden. Falls NEIN, wird ein Fehler zurück gemeldet.
10	F-SPS	Es wird in MW05 (zu prüfende Betriebsart) der Wert für die Berechtigungsstufe MSO 0 gespeichert. In MW05 wird das durch den Wert 3333H dargestellt.
11	F-SPS	Es wird zurück gemeldet, dass kein Fehler aufgetreten ist.
12	F-SPS	Es wird zurück gemeldet, dass ein Fehler aufgetreten ist.

Unterprogramm bei Schlüssel stecken: Schritt 26 und Schritt 27 (MW07 gültig und MW03 = MW07?)

Nr. | F-SPS

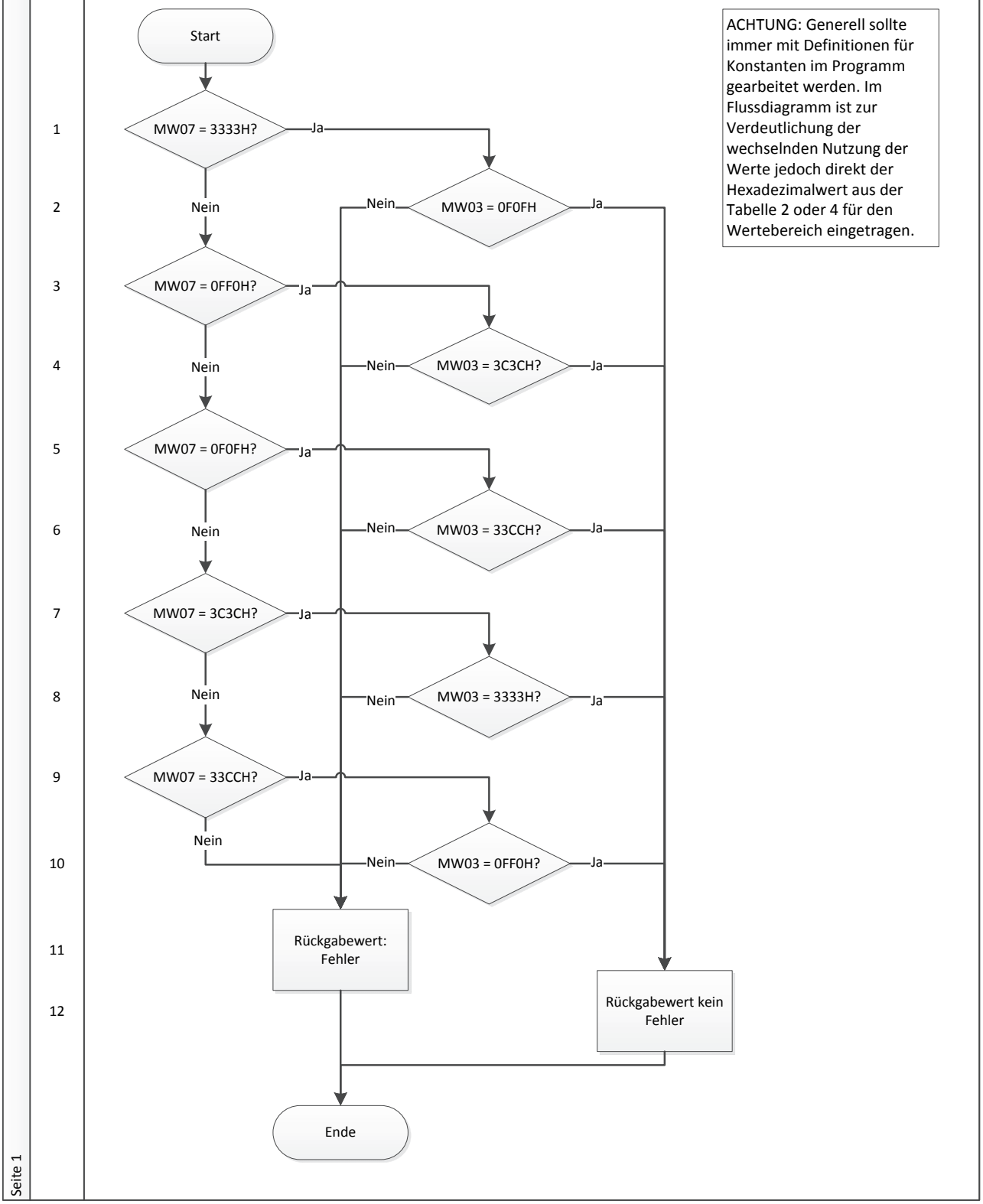


Bild 6

Schritt	System	Beschreibung
1	F-SPS	Es wird geprüft, ob im MW07 (bestätigte Betriebsart) die höchste Berechtigungsstufe (MSO 4) gespeichert ist. Im MW07 wird dies durch den Wert 3333H dargestellt. Falls JA, kann geprüft werden, ob das auch die zuvor gewählte Betriebsart ist.
2	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die höchste Berechtigungsstufe (MSO 4) gespeichert ist. Im MW03 wird dies durch den Wert 0F0FH dargestellt. Falls JA, kann auf diese Betriebsart umgeschaltet werden.
3	F-SPS	Es wird geprüft, ob im MW07 (bestätigte Betriebsart) die zweithöchste Berechtigungsstufe (MSO 3) gespeichert ist. Im MW07 wird dies durch den Wert 0FF0H dargestellt. Falls JA, kann geprüft werden, ob das auch die zuvor gewählte Betriebsart ist.
4	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die zweithöchste Berechtigungsstufe (MSO 3) gespeichert ist. Im MW03 wird dies durch den Wert 3C3CH dargestellt. Falls JA, kann auf diese Betriebsart umgeschaltet werden.
5	F-SPS	Es wird geprüft, ob im MW07 (bestätigte Betriebsart) die dritthöchste Berechtigungsstufe (MSO 2) gespeichert ist. Im MW07 wird dies durch den Wert 0FF0H dargestellt. Falls JA, kann geprüft werden, ob das auch die zuvor gewählte Betriebsart ist.
6	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die dritthöchste Berechtigungsstufe (MSO 2) gespeichert ist. Im MW03 wird dies durch den Wert 33CCH dargestellt. Falls JA, kann auf diese Betriebsart umgeschaltet werden.
7	F-SPS	Es wird geprüft, ob im MW07 (bestätigte Betriebsart) die vorletzte Berechtigungsstufe (MSO 1) gespeichert ist. Im MW07 wird dies durch den Wert 3C3CH dargestellt. Falls JA, kann geprüft werden, ob das auch die zuvor gewählte Betriebsart ist.
8	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die vorletzte Berechtigungsstufe (MSO 1) gespeichert ist. Im MW03 wird dies durch den Wert 3333H dargestellt. Falls JA, kann auf diese Betriebsart umgeschaltet werden.
9	F-SPS	Es wird geprüft, ob im MW07 (bestätigte Betriebsart) die letzte Berechtigungsstufe (MSO 0) gespeichert ist. Im MW07 wird dies durch den Wert 33CCH dargestellt. Falls JA, kann geprüft werden, ob das auch die zuvor gewählte Betriebsart ist.
10	F-SPS	Es wird geprüft, ob im MW03 (gewählte Betriebsart) die letzte Berechtigungsstufe (MSO 0) gespeichert ist. Im MW03 wird dies durch den Wert 0FF0H dargestellt. Falls JA, kann auf diese Betriebsart umgeschaltet werden.
11	F-SPS	Es wird zurück gemeldet, dass kein Fehler aufgetreten ist.
12	F-SPS	Es wird zurück gemeldet, dass ein Fehler aufgetreten ist.

Ausstecken eines EKS Schlüssels

Der gesamte Ablauf wird im Flussdiagramm Bild 7.1 bis Bild 7.2 dargestellt. Übergabevariablen sind rot dargestellt.

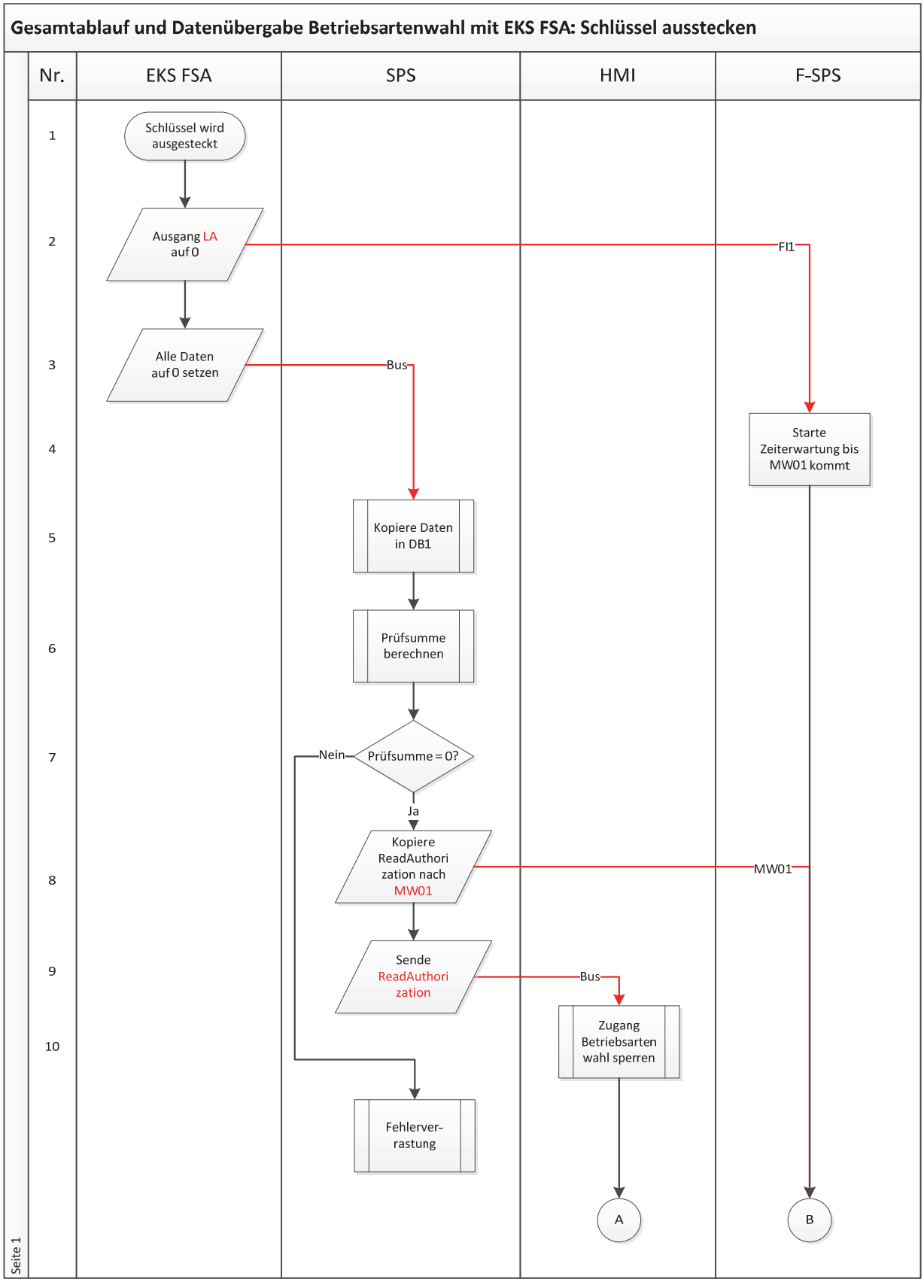


Bild 7.1

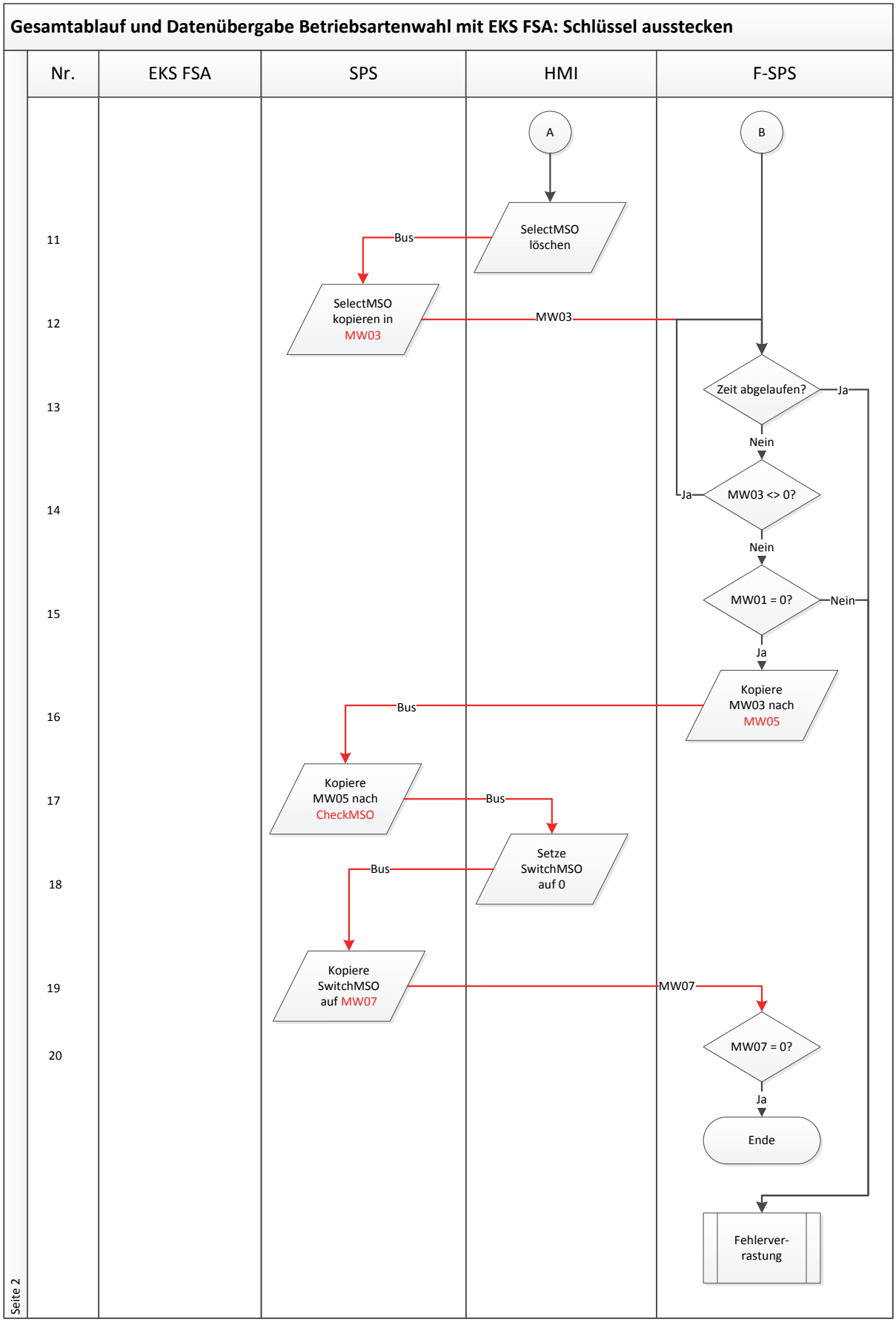


Bild 7.2

Beschreibung:

Schritt	System	Beschreibung
1	EKS *FSA*	Durch einen Benutzer wird ein Schlüssel ausgesteckt.
2	EKS *FSA*	Wenn ein Schlüssel ausgesteckt wird, wird der Ausgang LA auf 0 gesetzt.
3	EKS *FSA*	Das EKS *FSA* sendet ohne Schlüssel als Daten nur noch Nullen über den Bus.
4	F-SPS	In der sicheren SPS wird eine Zeiterwartung (ca. 1s) gestartet, bis nach Löschen des sicheren Eingangs FI1 die zugehörigen Daten (Nullen) von der SPS gesendet werden.
5	SPS	Alle Schlüsseldaten werden von der SPS im festgelegten Eingangsbereich eingelesen und werden von dort in einen globalen Datenbaustein umkopiert.
6	SPS	Es wird die Prüfsumme des Schlüsselinhalts berechnet. Anschließend wird als Bit zurückgegeben, ob die Prüfsumme 0 ergeben hat. (Siehe hierzu Applikation AP000169-5…)
7	SPS	Die Prüfsummenberechnung muss 0 ergeben.
8	SPS	Die Daten aus dem Bereich des Datenbausteins, an der Stelle der Zugangsberechtigung werden in das Merkerwort MW01 umkopiert, damit die F-SPS die Daten bekommt.
9	SPS	Die SPS sendet über das Bussystem den Inhalt von ReadAuthorization an die HMI.
10	HMI	Die HMI muss aufgrund der fehlenden Zugangsberechtigung das Bild zur Betriebsartenwahl sperren, so dass keine Änderungen mehr eingegeben werden können. Die derzeit angewählte Betriebsart bleibt aktiviert und muss weiterhin angezeigt werden.
11	HMI	Als Rückmeldung gibt die HMI als neue gewählte Betriebsart die Null zurück.
12	SPS	Die Daten von der HMI werden in das Merkerwort MW03 umkopiert, damit sie für die F-SPS zugängig sind.
13	F-SPS	Es wird maximal die eingestellt Zeit abgewartet.
14	F-SPS	Es wird geprüft, ob von HMI und SPS als Daten Nullen im Merkerwort MW03 gesendet wurden. Damit wird der korrekte Ablauf durch die SPS und die HMI geprüft.
15	F-SPS	Es wird geprüft, ob im Merkerwort MW01 auch eine Null gemeldet wird.
16	F-SPS	Um weiterhin den Weg durch die SPS und HMI abzuprüfen, wird als Rückantwort das MW05 auf Null gesetzt.
17	SPS	Die SPS kopiert das Datenwort MW05 direkt um in den Ausgangsbereich und sendet die Daten an die HMI weiter.
18	HMI	Die HMI sendet als quittierte Betriebsart die Null zurück.
19	SPS	Die Daten von der HMI werden in das Merkerwort MW07 umkopiert, damit sie für die F-SPS zugängig sind.
20	F-SPS	Die F-SPS prüft, ob in diesem Merkerwort MW07 die Null zurückgegeben wurde.

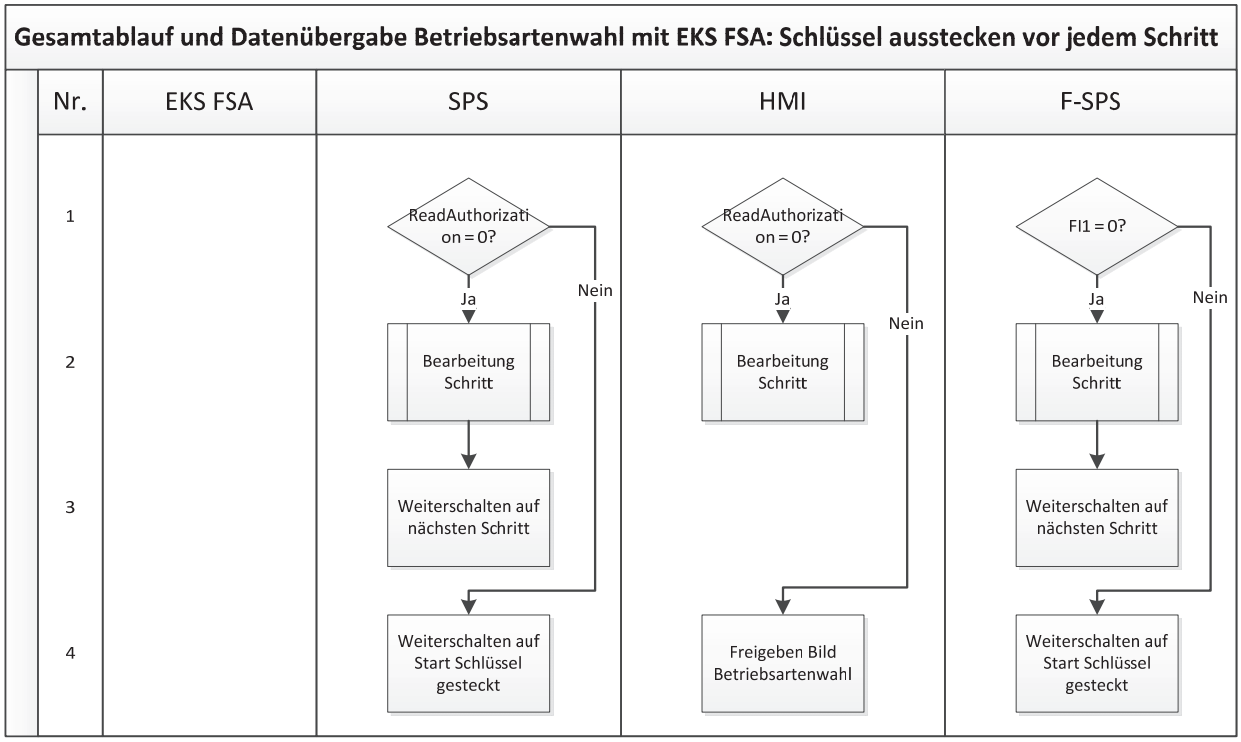


Bild 8

Durch den synchronen Ablauf in den Systemen SPS, HMI und F-SPS können Unterschiede in den Systemen (Kanälen) aufgedeckt werden. Das stellt eine Fehlererkennung im Sinne der EN ISO 13849-1 dar. Deshalb muss vor jedem einzelnen Schritt im Ablaufdiagramm aus Bild 7 der Ablauf aus Bild 8 programmiert bzw. aufgerufen werden.
Diese Ablaufschritte müssen auch vor der Fehlerroutine durchlaufen werden. Damit wird sichergestellt, dass das System sich durch Stecken des Schlüssels wieder fangen kann, wenn eine Störung nicht dauerhaft besteht (bspw. durch den Benutzer ausgelöst wurde).

Schritt	System	Beschreibung
1	SPS	Es wird geprüft, ob die Daten im Eingangsbereich weiterhin Nullen sind.
1	HMI	Es wird geprüft, ob seitens der SPS immer noch eine Sperrung für das Bild „Eingabe der Betriebsart“ besteht.
1	F-SPS	Es wird geprüft, ob das EKS *FSA* immer noch anzeigt, das kein Schlüssel gesteckt ist.
2	SPS HMI F-SPS	Der gerade abzuarbeitende Schritt aus dem Ablaufdiagramm in Bild 4 wird bearbeitet.
3	SPS F-SPS	Es wird im Status auf den nächsten Schritt aus dem Ablaufdiagramm in Bild 4 weiter geschaltet.
4	SPS	Es wird auf den Start der Routine „Schlüssel wird gesteckt“ umgeschaltet.
4	HMI	Der Zugang zum Bild Betriebsartenwahl wird freigegeben.
4	F-SPS	Es wird auf den Start der Routine „Schlüssel wird gesteckt“ umgeschaltet.

Prinzipielles Schaltbild

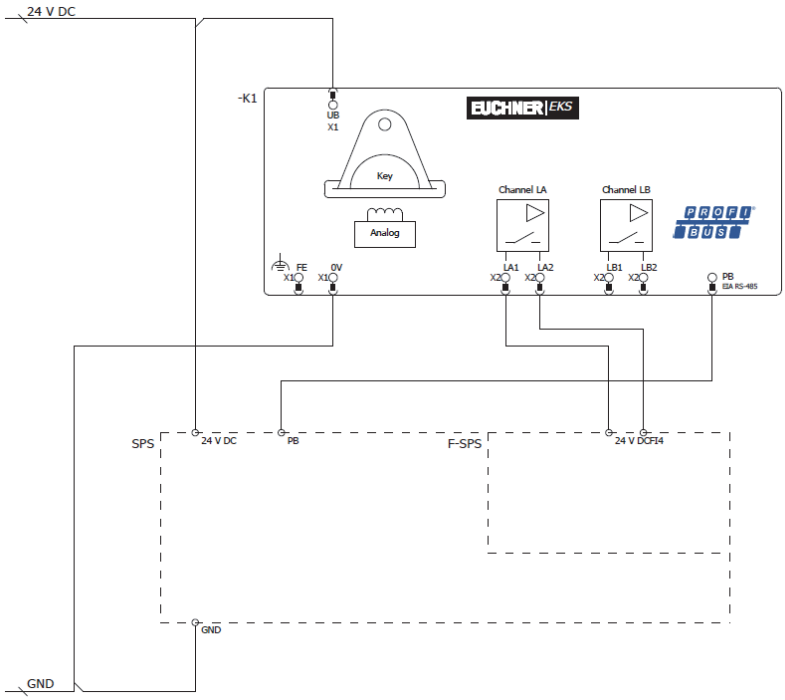


Bild 9

Daten in der Steuerung

Globaler Datenbaustein

Es wird ein globaler Datenbaustein angelegt, in dem der Inhalt des Schlüssel steht, wenn ein Schlüssel gesteckt ist. Wenn kein Schlüssel gesteckt ist, wird der Inhalt des Datenbausteins durch die EKS-Sendung auf Null gesetzt. Damit können alle Routinen und Speicherbereiche auf ordnungsgemäßen Ablauf geprüft werden.
Im Datenbaustein für das Lesen sind die Daten strukturiert angelegt, wobei alle Daten mit mehr als einem Byte als Einzelbytes angelegt sind, um das geradzahlige Alignement in der Steuerung zu umgehen.

DB1, ReadBufferEKS
Der in Bild 10 abgebildete Datenbaustein passt zum Beispiel AP000169-3… , in dem das EKS mit Profibus verwendet wird.
Mit einem Profinet EKS muss der Datenbaustein DB1 etwas anders aufgebaut werden. Die Bytes 1 bis 3 werden bei Profinet nicht genutzt (ReadKeyCount, ReadStartAddress, ReadNumberBytes). Die entsprechenden Zeilen werden im DB1 für das EKS Profinet weggelassen.

Adresse	Name	Typ	Anfangswert	Kommentar
0.0		STRUCT		
+0.0	ReadEKSStatus	BYTE	B#16#0	Statusbyte vom EKS
+1.0	ReadKeyCount	BYTE	B#16#0	Zähler für gesteckte Schlüssel
+2.0	ReadStartAddress	BYTE	B#16#0	Erstes gelesenes Byte
+3.0	ReadNumberBytes	BYTE	B#16#0	Anzahl der gelesenen Bytes
+4.0	ReadCRC_00	BYTE	B#16#0	CRC Byte 0
+5.0	ReadCRC_01	BYTE	B#16#0	CRC Byte 1
+6.0	ReadDate_00	BYTE	B#16#0	Datum Byte 0
+7.0	ReadDate_01	BYTE	B#16#0	Datum Byte 1
+8.0	ReadDate_02	BYTE	B#16#0	Datum Byte 2
+9.0	ReadDate_03	BYTE	B#16#0	Datum Byte 3
+10.0	ReadDate_04	BYTE	B#16#0	Datum Byte 4
+11.0	ReadDate_05	BYTE	B#16#0	Datum Byte 5
+12.0	ReadDate_06	BYTE	B#16#0	Datum Byte 6
+13.0	ReadDate_07	BYTE	B#16#0	Datum Byte 7
+14.0	ReadAuthorization_00	BYTE	B#16#0	Berechtigungsstufe Byte 0
+15.0	ReadAuthorization_01	BYTE	B#16#0	Berechtigungsstufe Byte 1
+16.0	ReadDepartment	BYTE	B#16#0	Abteilungsnummer
+17.0	ReadKeyID_00	BYTE	B#16#0	KeyID Byte 0
+18.0	ReadKeyID_01	BYTE	B#16#0	KeyID Byte 1
+19.0	ReadKeyID_02	BYTE	B#16#0	KeyID Byte 2
+20.0	ReadKeyID_03	BYTE	B#16#0	KeyID Byte 3
+21.0	ReadKeyID_04	BYTE	B#16#0	KeyID Byte 4
+22.0	ReadKeyID_05	BYTE	B#16#0	KeyID Byte 5
+23.0	ReadKeyID_06	BYTE	B#16#0	KeyID Byte 6
+24.0	ReadKeyID_07	BYTE	B#16#0	KeyID Byte 7
+26.0	Buffer	ARRAY[0..5]		Empfangspuffer auf 32 Byte füllen
*1.0		BYTE		
=32.0		END_STRUCT		

Bild 10

Sicherheitstechnische Beschreibung

EKS FSA

Im ersten Kanal des EKS *FSA* werden die Daten und damit die Zugangsberechtigung aus dem gesteckten Schlüssel ausgelesen. Das Ergebnis wird über den Bus als Zugangsberechtigung an die SPS gemeldet. Die SPS gibt die Daten unverändert an die sichere SPS und an die HMI weiter. Somit wird in der HMI geprüft, dass nur innerhalb des Wertebereichs eine Betriebsart gewählt wird und in der sicheren SPS wird geprüft, ob der Wertebereich eingehalten wurde.

Im zweiten Kanal des EKS *FSA* wird geprüft, ob ein gültiger Schlüssel gesteckt ist. Das Ergebnis wird auf dem Ausgang LA ausgegeben, der an die F-SPS angeschlossen ist. Der Ausgang des zweiten Kanals wird nur dann eingeschaltet, wenn auch im ersten Kanal ein gültiger Schlüssel erkannt wird. Die F-SPS erlaubt nur ein Umschalten der Betriebsart, wenn dieser Eingang eingeschaltet ist und überprüft, ob überhaupt eine Umschaltung zulässig ist.

Beim Entfernen des Schlüssels werden vom EKS *FSA* als Daten nur noch Nullen gesendet. Somit wird auch die Berechtigungsstufe auf 0 gesetzt. Diese wird an die HMI übermittelt, so dass die HMI die Betriebsartenwahl abschaltet. Als Quittung wird der Rückgabewert von der HMI ebenfalls auf 0 gesetzt. Dies wird an die F-SPS übermittelt. Der Ausgang des zweiten Kanal des EKS *FSA* wird ebenfalls zurückgesetzt. Auf diesem Weg prüft die F-SPS, dass die Null an alle beteiligten Steuerungen übermittelt wurde.
Eine Datenverfälschung auf den Übertragungsstrecken (Bussystemen) oder im Speicher der verschiedenen Systeme ist möglich. Durch die gewählten Codes mit einem Datenwort mit 16 Bit und einer Hamming-Distanz von 8 ergibt sich nach GS-ET-26 eine Restfehlerwahrscheinlichkeit von

$$R(p) \approx 1{,}2 \cdot 10^{-12}$$

Bei Verwendung eines 8-Bit Codes mit Hamming-Distanz 5 ergibt sich als Restfehlerwahrscheinlichkeit

$$R(p) \approx 5{,}43 \cdot 10^{-9}$$

Aufgrund dieser geringen Restfehlerwahrscheinlichkeit wird sichergestellt, dass durch das EKS *FSA* keine falsche Betriebsart angewählt werden kann. Diese Restfehlerwahrscheinlichkeit wird nicht in die Bestimmung der PFH_d des gesamten Systems eingerechnet. Das EKS *FSA* dient nur als Zugangssystem zur Betriebsartenwahl und geht damit nicht in die Berechnung des Performance Level ein.

SPS mit Touchscreen

In der HMI wird nur dann, wenn an den Eingängen vom EKS *FSA* eine Berechtigung vorliegt, auf den Bildschirm mit der Betriebsartenwahl umgeschaltet.
Freigegeben werden nur die Tasten auf dem Touchscreen, die entsprechend dem gesteckten Schlüssel berechtigt anwählbar sind. Die gewählte Betriebsart wird an die SPS und von dort an die sichere SPS übermittelt. Von der sicheren SPS kommt eine Quittung mit der gewählten Betriebsart zurück, die angezeigt werden muss. Diese muss vom Bediener quittiert werden. Das Verfahren entspricht einer sicheren Parametereingabe nach Abschnitt 4.6.4 EN ISO 13849-1:2008.
Um die Integrität der Daten sicherzustellen, die zu diesem Zweck ausgetauscht werden müssen, sind mehrere Maßnahmen implementiert.

- Kontrolle alle Daten auf Gültigkeit in der F-SPS
- Beherrschung von Datenverfälschungen durch die hohe Hamming Distanz
- Plausibilitätsprüfungen der Abläufe, um Fehler in Hard- und Software aufzudecken
- Wechsel der Bedeutung der Datenworte in den verschiedenen Stufen der Anwahl, um Überschreiben des Speichers oder fälschliches Speichern von Daten zu verhindern

Die Betriebsart bleibt eingestellt, wenn der Schlüssel gezogen wird und das entsprechende Bild in der HMI nicht mehr dargestellt wird.
Die Ausfallswahrscheinlichkeit von HMI und SPS muss nicht in die Berechnung der Ausfallwahrscheinlichkeit der Sicherheitsfunktion einbezogen werden, da HMI und SPS nur zur Eingabe von Daten entsprechend dem von der EN ISO 13849-1 vorgegebenen Verfahren dienen.

F-SPS

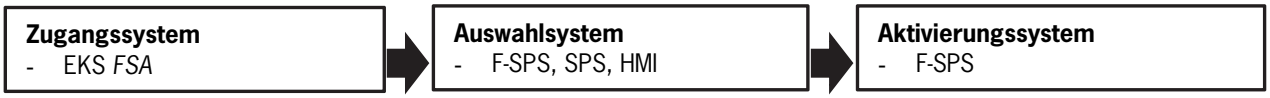
In der F-SPS wird die Auswahl der Betriebsart als 1 aus N System realisiert (Nur eine einzige Betriebsart kann gewählt werden).
Die F-SPS kann die Bedingungen eines PL e Systems nach EN ISO 13849-1 erfüllen, vorausgesetzt, der PL der F-SPS lässt dies zu und alle Maßnahmen innerhalb der Softwareerstellung werden beachtet. Weitere Hinweise hierzu siehe im nächsten Abschnitt.
Die F-SPS dient zur Fehleraufdeckung in allen beteiligten Geräten und Komponenten. Der Ablauf zur Auswahl der Betriebsart muss in der F-SPS implementiert werden.
Die Ausfallswahrscheinlichkeit der F-SPS geht als eigentliche Umschaltung der Betriebsart in die Berechnung des PL ein.

Software

Die Software in der F-SPS ist sicherheitsrelevant. Zur Erstellung und Beurteilung der Software in der F-SPS müssen die Methoden und Maßnahmen, die im Abschnitt 4.6.3 der EN ISO 13849-1:2008 für SRASW beschrieben sind, herangezogen werden. Die Software muss entsprechend Abschnitt 9.5 der EN ISO 13849-2:2013 validiert werden.
Die Erstellung der Software in SPS und HMI muss dem Abschnitt 4.6.4 der EN ISO 13849-1:2008 entsprechen. Die in dieser Applikation vorgestellte Methodik erfüllt diese Anforderungen, jedoch muss auch die Programmierung dementsprechend umgesetzt werden. Die Software muss nach Abschnitt 4.6.4 verifiziert werden.

Zusammenfassung

Die sicherheitstechnische Beurteilung einer Betriebsartenwahl umfasst 3 Blöcke:



Die Sicherheitsfunktion zur Betriebsartenwahl heißt: Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen. Mit einer Betriebsartenwahl wird zwischen verschiedenen Sicherheitssystemen umgeschaltet, bspw. geschlossene Schutztür bei Automatikbetrieb und Zustimmtaster zusammen mit begrenzter Geschwindigkeit bei offener Schutztür.

Das Zugangssystem dient dazu, den Forderungen der Maschinenrichtlinie nachzukommen, den Zugriff auf bestimmte Personenkreise zu beschränken.
Das Auswahlsystem ist die Auswahl des Benutzers, welche Betriebsart benötigt wird. In diesem Beispiel erfolgt die Eingabe des Benutzers über den Touchscreen.
Das Aktivierungssystem schaltet die sicherheitstechnische Sensorik und Aktorik entsprechend der gewählten Betriebsart zu bzw. weg. Bspw. kann beim Einrichten ein Zustimmtaster aktiviert, jedoch bestimmte Vorschubbewegungen unterbunden werden.
Tipp: Nähere Informationen zu sicherheitsbezogenen Betriebsarten finden Sie in der DGUV-Information FB HM-073.

Das Zugangssystem muss nicht mit einem PL bewertet werden, ist jedoch ein Teil des Sicherheitssystems. Die Zugangsbeschränkung muss mindestens gleichwertig zu der eines mechanischen Schlüssels sein. Diese Sicherheit wird aufgrund der Kodierung des Schlüssels und der zweikanaligen Struktur erreicht. Darüber hinaus bietet das EKS *FSA* eine Personalisierung, da die Zuordnung des Schlüssels zu einer Person möglich ist. Zudem ist ein hoher Schutz gegen Kopieren eines Schlüssels gegeben.
In dieser Applikation dient das EKS *FSA* unter anderem dazu eine Fehlerüberprüfung in der F-SPS anzutriggern, um das EKS *FSA*, die SPS und das HMI auf korrekte Funktion zu überwachen.

Das System aus SPS, HMI und F-SPS bildet in diesem Beispiel das Auswahlsystem, welches sicherheitstechnisch beurteilt werden muss. Bei Umsetzung der Betriebsartenwahl entsprechend dieser Applikation kann das Auswahlsystem der Betriebsart sicherheitstechnisch einem Schlüsselschalter gleichgestellt werden. Ein PL kann dem Auswahlsystem in diesem Beispiel nicht zugeordnet werden, da es sich bei der Auswahl der Betriebsart um eine Parametrisierung basiernd auf Softwaremaßnahmen nach Abschnitt 4.6.4 der EN ISO 13849-1:2008 (Softwarebasierende Parametrisierung) handelt.
Das Aktivierungssystem muss den PL$_r$ aus der Risikobeurteilung der Maschine für die Umschaltung der Betriebsart erfüllen. Bei ausschließlicher Verwendung der F-SPS als Aktivierungssystem ergibt sich der PL der F-SPS (PL e). Beachtet werden muss, dass die Software nach 4.6.3 der EN ISO 13849-1:2008 erstellt und nach 9.5 der EN ISO 13849-2:2013 validiert werden muss. Falls weitere, der F-SPS nachgeschaltete Systeme (z.B. Schütze und Ventile) einen Beitrag zur Umschaltung der Betriebsart leisten, müssen diese in die Beurteilung des PL mit einbezogen werden.

Damit kann die Sicherheitsfunktion „Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen“ mit einem Performance Level bis zu PL e ausgeführt werden.

Sicherheitstechnisches Blockdiagramm:

Wichtiger Hinweis – Bitte unbedingt sorgfältig beachten!

Dieses Dokument richtet sich an einen Konstrukteur, der die entsprechenden Kenntnisse in der Sicherheitstechnik hat und die Kenntnis der einschlägigen Normen besitzt, z. B. durch eine Ausbildung zum Sicherheitsingenieur. Nur mit entsprechender Qualifikation kann das vorgestellte Beispiel in eine vollständige Sicherheitskette integriert werden.

Das Beispiel stellt nur einen Ausschnitt aus einer vollständigen Sicherheitskette dar und erfüllt für sich allein genommen keine Sicherheitsfunktion. Zur Erfüllung einer Sicherheitsfunktion muss beispielsweise zusätzlich die Abschaltung der Energie der Gefährdungsstelle sowie auch die Software innerhalb der Sicherheitsauswertung betrachtet werden.

Die vorgestellten Applikationen stellen lediglich Beispiele zur Lösung bestimmter Sicherheitsaufgaben zur Absicherung von Schutztüren dar. Bedingt durch applikationsabhängige und individuelle Schutzziele innerhalb einer Maschine/Anlage können die Beispiele nicht erschöpfend sein.

Falls Fragen zu diesem Beispiel offen bleiben, wenden Sie sich bitte direkt an uns.

Nach der Maschinenrichtlinie 2006/42/EG ist der Konstrukteur einer Maschine bzw. Anlage verpflichtet, eine Risikobeurteilung durchzuführen und Maßnahmen zur Minderung des Risikos zu ergreifen. Er muss sich hierbei an die einschlägigen nationalen und internationalen Sicherheitsnormen halten. Normen stellen in der Regel den aktuellen Stand der Technik dar. Der Konstrukteur sollte sich daher laufend über Änderungen in den Normen informieren und seine Überlegungen darauf abstimmen, relevant sind u.a. die EN ISO 13849 und EN 62061. Diese Applikation ist immer nur als Unterstützung für die Überlegungen zu Sicherheitsmaßnahmen zu sehen.

Der Konstrukteur einer Maschine/Anlage ist verpflichtet die Sicherheitstechnik selbst zu beurteilen. Die Beispiele dürfen nicht zu einer Beurteilung herangezogen werden, da hier nur ein kleiner Ausschnitt einer vollständigen Sicherheitsfunktion sicherheitstechnisch betrachtet wurde.

Um die Applikationen der Sicherheitsschalter an Schutztüren richtig einsetzen zu können, ist es unerlässlich, dass die Normen EN ISO 13849-1, EN ISO 14119 und alle relevanten C-Normen für den jeweiligen Maschinentyp beachtet werden. Dieses Dokument ersetzt keinesfalls eine eigene Risikoanalyse und kann auch nicht als Basis für eine Fehlerbeurteilung herangezogen werden.

Insbesondere bei einem Fehlerausschluss ist zu beachten, dass dieser nur vom Konstrukteur einer Maschine bzw. Anlage durchgeführt werden kann und dass hierzu eine Begründung notwendig ist. Ein genereller Fehlerausschluss ist nicht möglich. Nähere Auskünfte zum Fehlerausschluss gibt die EN ISO 13849-2.

Änderungen an Produkten oder innerhalb der Baugruppen von dritten Anbietern, die in diesem Beispiel verwendet werden, können dazu führen, dass die Funktion nicht mehr gewährleistet ist oder die sicherheitstechnische Beurteilung angepasst werden muss. In jedem Fall sind die Angaben in den Betriebsanleitungen sowohl seitens EUCHNER, als auch seitens der dritten Anbieter zugrunde zu legen, bevor diese Applikation in eine gesamte Sicherheitsfunktion integriert wird. Sollten hierbei Widersprüche zwischen Betriebsanleitungen und diesem Dokument auftreten, setzen Sie sich bitte mit uns direkt in Verbindung.

Verwendung von Marken- und Firmennamen

Alle aufgeführten Marken- und Firmennamen sind Eigentum des jeweiligen Herstellers. Deren Verwendung dient ausschließlich zur eindeutigen Identifikation kompatibler Peripheriegeräte und Betriebsumgebungen im Zusammenhang mit unseren Produkten.

EUCHNER GmbH + Co. KG · Kohlhammerstraße 16 · 70771 Leinfelden-Echterdingen
Telefon: +49 711 75 97 -0 · Telefax: +49 711 75 97 -303 · info@euchner.de · www.euchner.de