BERGISCHE
UNIVERSITÄT
WUPPERTAL

Kosteneffiziente Antriebsarchitektur für kollaborative Automatisierung

Von der Fakultät für
Elektrotechnik, Informationstechnik und Medientechnik
der Bergischen Universität Wuppertal

zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
(Dr.-Ing.)

genehmigte Dissertation

von

Tobias Schmidt, M.Sc.

Referent: Univ.-Prof. em. Dr.-Ing. Joachim Holtz
Korreferent: Prof. Dr.-Ing. Jens Onno Krah

Tag der mündlichen Prüfung: 11. Oktober 2024

Vorwort

Diese Dissertation entstand im Rahmen meiner Tätigkeit als wissenschaftlicher Mitarbeiter bei Herrn Prof. Dr.-Ing. Jens Onno Krah am Institut für Automatisierungstechnik der Technischen Hochschule Köln in Kooperation mit der Firma SEW-EURODRIVE in Bruchsal. An dieser Stelle gilt mein Dank allen Personen, die mich fachlich und persönlich bei der Erstellung dieser Arbeit unterstützt haben.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. Jens Onno Krah für seine langjährige fachliche Begleitung und persönliche Unterstützung während meiner Zeit an der Technischen Hochschule Köln. Er hat durch seinen kontinuierlichen Rat wesentlich zum Gelingen dieser Arbeit beigetragen.

Ebenso möchte ich meinem Doktorvater, Herrn Univ.-Prof. em. Dr.-Ing. Joachim Holtz, meinen aufrichtigen Dank aussprechen. Als ehemaliger Lehrstuhlinhaber am Lehrstuhl für Elektrische Maschinen und Antriebe der Bergischen Universität Wuppertal und durch seine herausragende Forschungsarbeit in diesem Fachbereich hat er mir die Möglichkeit einer Promotion an der Bergischen Universität Wuppertal erst eröffnet.

Ein weiterer Dank geht an meine Kolleginnen und Kollegen sowie an die Studierenden des Labors für Regelungstechnik der Technischen Hochschule Köln. Insbesondere möchte ich mich bei Timo Wilkening, Joschka Laufs-Randerath und Christian Mühlfeld für die zahlreichen anregenden Diskussionen, die sorgfältigen Korrekturen und die schöne gemeinsame Zeit bedanken.

Mein herzlichster Dank gilt meiner Partnerin Luisa, die mir in den arbeitsintensiven Phasen dieser Arbeit, trotz ihrer eigenen privaten und beruflichen Herausforderungen, mit großem Rückhalt und viel Geduld zur Seite stand.

Zum Abschluss möchte ich mich bei meiner Familie bedanken, die mich während meiner gesamten akademischen Laufbahn tatkräftig unterstützt hat. Besonders meinen Eltern danke ich für ihre Ermutigung, ein Bachelorstudium zu beginnen, womit sie den Grundstein für diese Dissertation gelegt haben.

Bielefeld 2024

Tobias Schmidt

Kurzfassung

Eine kollaborative Automatisierung für die industrielle Fertigung erfordert eine direkte Zusammenarbeit zwischen Mensch und Roboter bzw. intelligenter Maschine. Solche intelligenten Fabriken setzen insbesondere autonome Systeme wie fahrerlose Transportsysteme oder autonome mobile Roboter ein, um zum einen ganze Produktionsprozesse ohne menschlichen Eingriff durchzuführen und zum anderen die Produktivität durch eine enge Zusammenarbeit zwischen Mensch und Roboter zu steigern. Dieser menschenzentrierte Ansatz sieht einen Kontakt mit dem Menschen vor und darf somit keine Gefahr darstellen.

Für diese kollaborative Automatisierung spielen funktional sichere Antriebe eine wichtige Rolle. Der klassische Ansatz, die Antriebselektronik durch eine zusätzliche antriebsinterne sicherheitsbezogene Logik zu ergänzen, ist insbesondere bei Antrieben kleiner Leistung nicht optimal. Dieser Ansatz benötigt nicht nur mehr Platz im ohnehin begrenzten Bauraum autonomer Fahrzeuge, sondern ist auch teurer aufgrund der Zertifizierung der sicherheitsrelevanten Komponenten im Antrieb. Zusätzlich ist dieser dezentrale Ansatz nicht ideal für eine zentrale Berechnung von Sicherheitsfunktionen für die Überwachung von Bewegungen im dreidimensionalen Raum für kollaborative Roboter.

Diese Arbeit stellt eine kompakte, funktional sichere und gleichzeitig kostengünstige Antriebarchitektur für eine kollaborative Automatisierung vor, bei der die Sicherheitsfunktionen redundant diversitär ausgeführt werden. Ein Kanal der Sicherheitsfunktionen ist in einem Mikrocontroller implementiert, der zweite in einem FPGA. Statt mit der in der funktional sicheren Automatisierung üblichen Aktualisierungsrate von zehn Millisekunden werden sicherheitsbezogene Feldbusse zyklisch jede Millisekunde oder schneller abgearbeitet, um die für kollaborative Anwendungen notwendigen schnellen Reaktionszeiten zu erreichen. Die Antriebsarchitektur nutzt dabei im Idealfall die bereits im Antrieb vorhandenen komplexen integrierten Schaltkreise, um die Sicherheitsfunktionen zu realisieren. Wie bei sicherheitsbezogenen Drehgebern soll die Diagnose der antriebsinternen Sicherheitsfunktionen in einer überlagerten sicherheitsbezogenen Logik durchgeführt werden. Durch diese externe Diagnose, die von einer Sicherheitssteuerung übernommen werden kann, und die redundant diversitäre Architektur kann auf eine Sicherheitszertifizierung des Antriebs verzichtet werden. Dadurch können Standardkomponenten verwendet werden, die den Ansatz nicht nur kostengünstiger machen, sondern auch den Austausch der Komponenten vereinfachen. Dies ist insbesondere bei der in den letzten Jahren aufgetretenen Bauteilknappheit in der Elektronikbranche von großem Vorteil.

Neben dem funktional sicheren Aspekt soll auch die Anforderung an die Leistungsfähigkeit des Antriebssystems berücksichtigt werden, um eine hochdynamische Regelung für autonome Fahrzeuge nach dem Stand der Technik zu gewährleisten.

Abstract

Collaborative automation for industrial manufacturing requires direct interaction between humans and robots or intelligent machines. Such smart factories will use autonomous systems, such as automated guided vehicles or autonomous mobile robots, to run entire production processes without human interaction and to increase productivity through close collaboration between humans and robots. This human-centered approach implies that contact with humans is intended and must not cause any danger.

Functionally safe drives are an important factor for collaborative automation. The common approach of expanding the drive electronics with additional drive-internal safety-related logic is not optimal, especially for low-power drives. This approach not only requires more space in the already limited construction space of autonomous vehicles but is also expensive due to the certification of the safety-related components in the drive. In addition, this decentralized approach is not ideal for a central calculation of safety functions for safe motion in three-dimensional space for collaborative robots.

This work presents a compact, functionally safe and also cost-effective drive architecture for collaborative automation with redundant diverse implemented safety functions. One channel of the safety functions is implemented in a microcontroller, the second in an FPGA. Instead of the typical update rate of ten milliseconds used in functionally safe automation, safety-related fieldbuses are processed cyclically every millisecond or faster in order to achieve the fast response times required for collaborative applications. Ideally, the drive architecture uses the complex integrated circuits already available in the drive to implement the safety functions. As with safety-related encoders, the diagnostics of the drive-internal safety functions should be performed in a higher-level safety-related logic. Due to this external diagnosis, which can be performed by a safety controller, and the redundant diverse architecture, safety certification of the drive is no longer necessary. As a result, standard components can be used, making the approach not only more cost-effective, but also simplifying the replacement of components. This is particularly advantageous considering the shortage of components in the electronics industry in recent years.

In addition to the functional safety aspect, the performance requirements of the drive system are also considered and a highly dynamic, state-of-the-art control architecture for autonomous vehicles is used.

Inhalt

Vorwort ... **III**
Kurzfassung ... **IV**
Abstract ... **V**
Inhalt ... **VI**
Abbildungsverzeichnis ... **VIII**
Tabellenverzeichnis ... **XI**
Abkürzungsverzeichnis ... **XII**
Symbole ... **XIV**
1 Einleitung ... **1**
1.1 Motivation ... 1
1.2 Zielsetzung ... 3
1.3 Gliederung der Arbeit ... 4
2 Grundlagen und Stand der Technik ... **6**
2.1 Servoantriebe ... 6
2.1.1 Steuerteil ... 8
2.1.2 Regelungsverfahren ... 10
2.1.3 Sensoren für Servoantriebe ... 12
2.1.4 Kommunikation über Feldbusse ... 16
2.1.5 Inbetriebnahme und Fehlerdiagnose ... 17
2.2 Sicherheitsbezogene Antriebstechnik ... 17
2.2.1 Normen ... 18
2.2.2 Entwurf eines sicherheitsbezogenen Teils einer Steuerung ... 19
2.2.3 Sicherheitsbezogene Software ... 21
2.2.4 Entwicklung sicherheitsbezogener Antriebsstrukturen ... 23
2.2.5 Sicherheitsbezogene Kommunikation ... 26
2.2.6 Sicherheitsbezogene Positionsmesssysteme ... 28
2.2.7 Mensch-Roboter-Kollaboration ... 30
2.2.8 Sicherheitsbezogener Motion-Controller für eine sichere Bewegungsüberwachung ... 31
2.2.9 Fehlertoleranz in der Maschinensicherheit ... 32
3 Hoch-performante Regelungsarchitektur ... **34**
3.1 Struktur des Antriebs ... 34
3.2 Feldorientierte Regelung ... 35
3.3 Ablauf der trägerbasierten Abtastregelung ... 37
3.4 Kaskaden-Regelkreisstruktur ... 38

3.5 Generierung der Positionssollwerte und Vorsteuersignale mit einer Interpolation 39
3.6 Feldbuskommunikation mit dem Motion-Controller 42
4 Sicherheitsbezogene Antriebsstruktur 44
4.1 Aufbau der Steuerelektronik 44
4.2 Sicherheitsfunktionen im Antrieb 46
4.2.1 Sicher abgeschaltetes Moment 47
4.2.2 Sichere Bremsansteuerung 52
4.2.3 Sicherer Stopp 56
4.3 Sicherheitsbezogene Kommunikation 61
4.4 Sicherheitsbezogene Strommessung 63
4.5 Sicherheitsbezogene Positionsmessung 67
4.5.1 Digitale Drehgeber 67
4.5.2 Gemischt kritische Resolver-Digital-Wandlung 69
4.6 Sicherheitsbezogene Ein- und Ausgänge mit IO-Link 72
4.7 Degradierter Betrieb 74
4.8 Antriebsinterne Diagnose 76
4.8.1 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache 76
4.8.2 Zusammenfassung sicherheitsrelevanter Logik und Diagnose im Antrieb 79
5 Validierung des Konzepts 84
5.1 Leistungsfähigkeit des Antriebssystems 86
5.2 Validierung der Diagnosetests 89
5.2.1 Validierung der Abschaltpfade 89
5.2.2 Validierung der Sinc-Filtertests 91
6 Fazit 93
Anhang 97
Literaturverzeichnis 102

Abbildungsverzeichnis

Abbildung 1: Aufbau und Struktur eines modernen elektrischen Servoantriebs. 7

Abbildung 2: Feldorientierte Regelung des permanenterregten Synchronmotors. 11

Abbildung 3: Zweikanalige Architektur für Kategorie 3 nach DIN EN ISO 13849. 20

Abbildung 4: Festverdrahtete Sicherheitslösung mit einem Sicherheitsschaltgerät. 24

Abbildung 5: Sicherheitsbezogene Antriebsstruktur mit einer Compound-SPS und antriebsintegrierter sicherheitsbezogener Logik. 26

Abbildung 6: Einsatz von Drehgebern als Subsystem bei einer Kategorie-3-Architektur. 29

Abbildung 7: Aufteilung der feldorientierten Motorregelungsstruktur im Steuerteil des Antriebs. 35

Abbildung 8: Typisches Verarbeitungsschema der trägerbasierten Abtastregelung bei 8 kHz Schaltfrequenz. 37

Abbildung 9: Kaskadenregelung des Servoantriebs mit Drehzahl-Beobachter, Smith-Prädiktor und Vorsteuersignalen. 38

Abbildung 10: Messung der Bandbreite des Lageregelkreises mit Polynominterpolation als Teilsystem. 39

Abbildung 11: Polynom 3. Ordnung durch die letzten vier Positionssollwerte: x^*_{k-3} ... x^*_k. 40

Abbildung 12: Blockschaltbild der Feininterpolation. 41

Abbildung 13: Synchronisation des PWM-Trägersignals im FPGA des Antriebs auf den Feldbus. 43

Abbildung 14: Aufbau der Steuerelektronik für eine sicherheitsbezogene Antriebsstruktur: a) klassischer Ansatz mit zwei zusätzlichen µCs, b) diversitäre redundante Struktur mit nur einem Standard-µC und einem Standard-FPGA. 45

Abbildung 15: Zweikanalige Sicherheitsfunktion für eine sichere Bewegungsüberwachung mit Kreuzvergleich in der Sicherheits-SPS. 46

Abbildung 16: Konzept der Sicherheitsfunktion STO im Antrieb. 47

Abbildung 17: Logische Verknüpfung der Impulssperre mit dem µC. 48

Abbildung 18: Implementierung der Diagnose im µC. a) Blockschaltbild und b) Zeitverlauf der Signale. 49

Abbildung 19: Logische Verknüpfung der Impulssperre mit dem FPGA. 50

Abbildung 20: Implementierung der Diagnose im FPGA. a) Blockschaltbild und b) Zeitverlauf der Signale. 51

Abbildung 21: Aufbau der Sicherheitsfunktion STO – zusammenfassende Darstellung mit Sicherheits-SPS und Antrieb. 52

Abbildung 22: Aufbau der Sicherheitsfunktion SBC. 53

Abbildung 23: Diagnose des 2. SBC-Funktionskanals. 54

Abbildung 24: Diagnose des 1. SBC-Funktionskanals. 56

Abbildung 25: Bremsmethode für einen PSM über die sicherheitsbezogene Logik mit Relais und Bremswiderständen. 57

Abbildung 26: Einphasiges Ersatzschaltbild des PSMs mit a) Relais und Bremswiderstand und b) dem Wechselrichter zum Bremsen. 57

Abbildung 27: Regelstruktur für das sensorlose Bremsen eines PSMs über das FPGA im Antrieb. 59

Abbildung 28: Polradspannung up, Klemmenspannung us und PWM-Tastgrad α während eines Bremsvorgangs mit vorgegebenem maximalen Bremsstrom is_cmd. 60

Abbildung 29: Blockschaltbild des Antriebs während eines Bremsvorgangs mit den drei unteren Transistoren. 60

Abbildung 30: Diversitäre Verarbeitung der beiden SPDUs im Antrieb mit dem µC und dem FPGA über jeweils eine Verbindung über ein sicherheitsbezogenes Feldbusprotokoll. 62

Abbildung 31: Digitales 12-Bit Datenwort nach dem Sinc³-Dezimierungsfilter in Abhängigkeit des Phasenstroms. 64

Abbildung 32: Blockschaltbild der sicherheitsbezogenen Strommessung und Übertragung zur überlagerten Sicherheits-SPS via Black-/Gray-Channel. 65

Abbildung 33: Zeitlicher Verlauf des Sinc³-Filtertests im 1. Kanal mit einem Testsignal über den sicherheitsbezogenen Feldbus. 66

Abbildung 34: Schematische Darstellung der Anbindung eines sicherheitsbezogenen Drehgebers über den Antrieb (FPGA und µC) an die übergeordnete Sicherheits-SPS. 68

Abbildung 35: Bereitstellung eines sicherheitsbezogenen Positionssignals über den Antrieb an eine übergeordnete Sicherheits-SPS. 70

Abbildung 36: Blockschaltbild des sicherheitsbezogenen volldigitalen RDCs mit einer diversitären redundanten Verarbeitung der Resolversignale im µC und FPGA. 71

Abbildung 37: Konfigurationen der IO-Link-Master für verschiedene Anwendungen zur Verwendung als sicherheitsbezogene digitale Ein- und Ausgänge am Antrieb. 74

Abbildung 38: Sicherheitsbezogene Antriebsstruktur mit externer qualifizierter Diagnose und Entscheider in der überlagerten Sicherheits-SPS. 76

Abbildung 39: Blockschaltbild der Spannungsversorgung für die Steuerelektronik im Antrieb. 77

Abbildung 40: Sicherheitsrelevante Funktionsblöcke des 1. Kanals implementiert im µC. 80

Abbildung 41: Sicherheitsrelevante Funktionsblöcke des 2. Kanals implementiert im FPGA. 82

Abbildung 42: Leiterplatte mit der Steuerelektronik des Antriebs. 85

Abbildung 43: Delta-Roboter als Technologiedemonstrator mit der verbauten Steuerelektronik auf der SPS-Messe 2022 in Nürnberg. 86

Abbildung 44: Gemessenes Bode-Diagramm des Stromregelkreises mit Smith-Prädiktor bei 8 kHz Schaltfrequenz. 87

Abbildung 45: Gemessenes Bode-Diagramm des Drehzahlregelkreises mit Drehzahl-Beobachter mit 400 Hz Bandbreite bei 8 kHz Schaltfrequenz. 88

Abbildung 46: Gemessenes Bode-Diagramm des Lageregelkreises mit Feininterpolation für das Antriebssystem. 89

Abbildung 47: Testung der Abschaltpfade für die Sicherheitsfunktionen STO und SBC 90

Abbildung 48: Test der Sinc³-Dezimierungsfilter für die sicherheitsbezogene Strommessung. 91

Abbildung 49: Gemischt-kritische Systemarchitektur für Mehrachs-Anwendungen. 98

Abbildung 50: Entwickelter 48-V-Doppelachs-Antrieb mit der externen Steuerelektronik verbunden über Flachbandkabel. 100

Abbildung 51: Verkettung der 2. Strom-SPDU mit dem FSoE-CRC und Anhängen an die FSoE-Slave-SPDU. 101

Tabellenverzeichnis

Tabelle 1: Vergleich von gängigen sicherheitsbezogenen Antriebsarchitekturen und dem vorgestellten Ansatz. 83

Tabelle 2: Punkteschema zur Bewertung der Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache [52]. 97

Tabelle 3: Erreichte Punktzahl für die Maßnahmen gegen CCF des vorgestellten Antriebssystems. 99

Abkürzungsverzeichnis

µC ..... Mikrocontroller
ADC ..... Analog-Digital-Wandler (engl.: analog-to-digital converter)
AMR ..... Autonome mobile Roboter
ASIC ..... Anwendungsspezifische integrierte Schaltung (engl.: application specific integrated circuit)
BEP ..... Bitfehlerwahrscheinlichkeit (engl.: bit error probability)
CCF ..... Ausfälle infolge einer gemeinsamen Ursache (engl. common cause failure)
CiA ..... CAN in Automation
CLB ..... Konfigurierbarer Logikblock (engl.: configurable logic block)
CNC ..... Rechnergestützte numerische Steuerung (engl.: computerized numerical control)
CPU ..... Zentrale Recheneinheit (engl.: central processing unit)
CRC ..... Zyklische Redundanzprüfung (engl.: cyclic redundancy check)
CSP ..... Zyklische synchrone Lageregelung (engl.: cyclic synchronous position)
DC Diagnosedeckungsgrad (engl.: diagnostic coverage), Verteilte Uhr (engl.: distributed clock)
DGUV ..... Deutsche Gesetzliche Unfallversicherung
DMA ..... Direkter Speicherzugriff (engl.: direct memory access)
DSP ..... Digitaler Signalprozessor
DTC ..... Direkte Drehmomentregelung (engl.: direct torque control)
EEPROM Elektrisch löschbarer programmierbarer Nur-Lese-Speicher (engl.: electrically erasable programmable read-only memory)
EMI ..... Elektromagnetische Störung (engl.: electromagnetic interference)
EMV ..... Elektromagnetische Verträglichkeit
ESC ..... EtherCAT-Slave-Controller
FFA ..... Beschleunigungsvorsteuerung (engl.: feed-forward acceleration)
FFV ..... Geschwindigkeitsvorsteuerung (engl.: feed-forward velocity)
FIT ..... Fehler pro Zeit (engl.: failure in time)
FMEA ..... Ausfallarten- und Effektanalyse (engl.: failure mode and effects analysis)
FOC ..... Feldorientierte Regelung (engl.: field oriented control)
FPGA ..... Feldprogrammierbares Logikgatter (engl.: field programmable gate array)
FPU ..... Fließkommaeinheit (engl.: floating-point unit)
FSoE ..... Failsafe over EtherCAT
FTF ..... Fahrerlose Transportfahrzeuge
HDSL ..... HIPERFACE DSL
I/O ..... Ein- und Ausgänge (engl.: input and output)
IC ..... Integrierter Schaltkreis (engl.: integrated circuit)
ID ..... Kennung (engl.: identifier)
IGBT ..... Bipolartransistor mit isolierter Gate-Elektrode (engl.: insulated-gate bipolar transistor)
IP-Core ..... Blöcke mit geistigem Eigentum (engl.: intellectual property core)
ISR ..... Interrupt Service Routine
LED ..... Leuchtdiode (engl.: light-emitting diode)
LVTTL ..... Niederspannung-Transistor-Transistor-Logik (engl.: low voltage transistor transistor logic)
MOSFET ... Metalloxid-Halbleiter-Feldeffekttransistor (engl.: metal oxide semiconductor field-effect transistor)
MRK ..... Mensch-Roboter-Kollaboration
$MTTF_D$ .. Mittlere Zeit bis zum gefahrbringenden Ausfall (engl.: mean time to dangerous failure)

OSR ..... Überabtastungsfaktor (engl.: over sampling ratio)
OSSD ..... Output Signal Switching Device
PDO ..... Prozessdatenobjekte
PELV ..... Schutzkleinspannung (engl.: protective extra low voltage)
PFH_D ... Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (engl.: probability of a dangerous failure per hour)
PL ..... Performance Level
PLL ..... Phasenregelschleife (engl.: phase locked loop)
PL_r ..... Erforderliches Performance Level (engl.: performance level required)
PLÜ ..... Programmlaufüberwachung
PSM ..... Permanenterregter Synchronmotor
PWM ..... Pulsweitenmodulation
QM ..... Qualitätsmanagement
RAM ..... Speicher mit wahlfreiem Zugriff (engl.: random-access memory)
RDC ..... Resolver-Digital-Wandler (engl.: resolver-to-digital converter)
RMS ..... Effektivwert (engl.: root mean square)
SAR .... Register mit schrittweiser Annäherung (engl.: successive-approximation register)
SBC ..... Sichere Bremsansteuerung (engl.: safe brake control)
SDO ..... Servicedatenobjekte
SELV ..... Sicherheitskleinspannung (engl.: safety extra low voltage)
SIL ..... Sicherheits-Integritätslevel (engl.: safety integrity level)
SLA ..... Sicher begrenzte Beschleunigung (engl.: safely-limited acceleration)
SLP ..... Sicher begrenzte Position (engl.: safely-limited position)
SLS ..... Sicher begrenzte Geschwindigkeit (engl.: safely-limited speed)
SLT ..... Sicher begrenztes Drehmoment (engl.: safely-limited torque)
SOS ..... Sicherer Betriebshalt (engl.: safe operating stop)
SPDU ..... Sichere Protokoll-Dateneinheit (engl.: safety protocol data unit)
SPI ..... Serielle Peripherieschnittstelle (engl.: serial peripheral interface)
SPS ..... Speicherprogrammierbare Steuerung
SRASW ..... Sicherheitsbezogene Anwendungssoftware (engl.: safety-related application software)
SRESW ..... Sicherheitsbezogene Embedded-Software (engl.: safety-related embedded software)
SRP/CS ... Sicherheitsbezogener Teil einer Steuerung (engl.: safety-related part of control system)
SS1 ..... Sicherer Stopp 1 (engl.: safe stop 1)
SS2 ..... Sicherer Stopp 2 (engl.: safe stop 2)
SSI ..... Synchron-serielle Schnittstelle (engl.: synchronous serial interface)
STO ..... Sicher abgeschaltetes Drehmoment (engl.: safe torque off)
SVM ..... Raumzeigermodulation (engl.: space vector modulation)
UART ..... Universeller asynchroner Empfänger/Sender (engl.: universal asynchronous receiver/transmitter)
USV ..... Unterbrechungsfreie Stromversorgung
VHDL ..... Very High Speed Integrated Circuit Hardware Description Language
VPN ..... Virtuelles privates Netzwerk
WLAN ..... Drahtloses Lokal-Netzwerk (engl.: wireless local area network)
ZVEI ..... Zentralverband Elektrotechnik und Elektronikindustrie e.V.
ΣΔ ..... Sigma-Delta

Symbole

Allgemeines

Für alle Variablen in dieser Arbeit gilt Folgendes: Kleinbuchstaben werden für Variablen verwendet, die eine Funktion der Zeit sind, z. B. i, u. Zeiger sind durch unterstrichene Symbole gekennzeichnet, z. B. $\underline{i}$, $\underline{u}$. Großbuchstaben werden für Variablen im sinusförmigen stationären Zustand und für konstante Größen verwendet, z. B. I, U. Dazu gehören auch die Effektivwerte (engl.: root mean square, RMS) der Wechselgrößen.

Symbole

a	Beschleunigung	R	Widerstand
C	Kondensator	r	Ruck
D	Diode	R_b	Bremswiderstand
e	Regelabweichung	R_bc	Bremschopper-Widerstand
E_0	Verstärkung	R_DSon	Drain-Source-Einschaltwiderstand
f_a	Abtastfrequenz	R_H	Pull-up-Widerstand
f_c	Trägerfrequenz	R_L	Pull-down-Widerstand
$f_{\Sigma\Delta}$	ΣΔ-Modulationsfrequenz	R_s	Statorwiderstand
i	Interpolationsindex	R_V	Vorwiderstand
i^*	Stromsollwert	t	Zeit
$\hat{i}$	Geschätzter Strom	T_a	Abtastzeit
i_α	Statorfeste Stromkomponente α	T_ca	Kompensationszeit Beschleunigung
i_β	Statorfeste Stromkomponente β	T_cv	Kompensationszeit Geschwindig.
i_d	Rotorfeste Stromkomponente d	t_k	Abtastzeitpunkt
i_q	Rotorfeste Stromkomponente q	T_t	Totzeit
i_s	Statorstrom	u_α	Statorfeste Spannungskomp. α
$i_\mathrm{u,v,w}$	Motorphasenströme	u_β	Statorfeste Spannungskomp. β
J	Trägheitsmoment	u_d	Rotorfeste Spannungskomp. d
K_e	Spannungskonstante	u_q	Rotorfeste Spannungskomp. q
K_T	Drehmomentkonstante	U_dc	Zwischenkreisspannung
L_s	Statorinduktivität	U_L	Spannung über Spule
M	Drehmoment	U_p	Polradspannung
m	Modulationsindex	U_R	Spannung über Widerstand
n	Drehzahl	U_Ref	Referenzspannung
p	Polpaarzahl	U_s	Statorspannung/Klemmenspannung

$U_{\sin}$	Sinusspannung (Resolver)	v	Geschwindigkeit
$U_{\cos}$	Kosinusspannung (Resolver)	V_{cc}	Versorgungsspannung
ü	Übersetzungsverhältnis	x	Position

Griechische Symbole

α	Winkelbeschleunigung	φ_{com}	Kommutierungsoffset
α	Tastgrad	φ_{el}	Elektrischer Winkel
$\hat{\alpha}$	Geschätzte Winkelbeschleunigung	φ_{m}	Mechanischer Winkel
ε	Abweichung	ω	Winkelgeschwindigkeit
ϑ	Temperatur	ω^*	Winkelgeschwindigkeit-Sollwert
τ	Einschaltdauer	$\hat{\omega}$	Geschätzte Winkelgeschwindigkeit
φ	Winkel	ω_{el}	Elektrische Kreisfrequenz
φ^*	Winkel-Sollwert	ω_{m}	Mechanische Kreisfrequenz

1 Einleitung

1.1 Motivation

Die elektrische Automatisierungsbranche ist einer der wichtigsten Industriezweige innerhalb des produzierenden Gewerbes. Als bedeutender Teilbereich der Elektroindustrie ist diese ein wichtiger Wirtschafts- und Arbeitsmarktfaktor in Deutschland und stellt eine innovative und wachstumsstarke Branche dar [1]. Zu dieser Branche gehört auch die elektrische Antriebstechnik, die heute bereits den Großteil aller Antriebsaufgaben im industriellen Bereich übernommen hat [2]. Zu den größten Herausforderungen der Branche zählen der demografische Wandel, der damit verbundene Fachkräftemangel sowie der neue weltweite Wettbewerb, der in den etablierten Markt vordringt [1]. Zusätzlich führen derzeit Lieferengpässe, insbesondere von Microchips und anderen Halbleiterbauelementen, zu Preissteigerungen und Produktionslücken [1]. Aus diesem Grund wählen Antriebshersteller Bauteile nach Verfügbarkeit und möglichen Alternativen von anderen Bauteileherstellern aus, sodass die Auswahl von Standardbauteilen ohne besondere Merkmale vorteilhaft ist. Die Bedeutung der elektrischen Antriebstechnik wird auch in den nächsten Jahren weiter zunehmen, vor allem in Hinblick auf die steigende Automatisierungsnachfrage, die Verringerung der Emissionen und die Erreichung der Klimaziele [2]. 80 % bis 90 % dieser elektrischen Antriebe sind heute regelbare Antriebe, die mit einem Servoregler oder Frequenzumrichter ausgestattet sind [2].

Der Innovationsdruck, der sowohl aus dem Wettbewerbsumfeld als auch aus den technischen Anforderungen resultiert, führt dazu, dass die Präzision, Geschwindigkeit und Effizienz industrieller Prozesse kontinuierlich steigen [3]. So werden Prozesse stetig optimiert und die Qualität der Produkte verbessert. Die damit einhergehende höhere Anforderung an die Leistungsfähigkeit (Performanz) von elektrischen Antrieben wird unter anderem durch eine hochdynamische Regelung des Antriebssystems erreicht. Der hochperformante Antrieb soll dabei das gewünschte Drehmoment innerhalb eines möglichst kurzen festgelegten Zeitrahmens präzise und ohne unerwünschtes Überschwingen für einen definierten Drehzahlbereich erzeugen [3].

Der digitale Wandel von automatisierten Fertigungsanalgen im Hinblick auf Industrie 4.0 stand durch den zunehmenden Einsatz von Informations- und Kommunikationstechnologie in den letzten Jahren im Vordergrund. In Zukunft sollen vernetzte und intelligente Fabriken für eine modulare und zunehmend flexiblere Produktion sorgen und durch Selbstoptimierung eine Senkung der Kosten erreichen [4]. Solche intelligenten Fabriken werden insbesondere autonome Systeme wie fahrerlose Transportfahrzeuge (FTF) oder Roboter einsetzen, um ganze Produktionsprozesse ohne menschlichen Eingriff durchzuführen. Die europäische Kommission spricht in einem Paper von der nächsten industriel-

len Revolution, der Industrie 5.0 [5]. Im Mittelpunkt der Industrie 5.0 sollen die Bedürfnisse und Interessen des Menschen stehen und nicht ausschließlich neue Technologien. Bei diesem menschenzentrierten Ansatz soll die Technologie dazu beitragen, den Produktionsprozess an den Arbeiter anzupassen und ihn bei seiner Arbeit zu unterstützen, anstatt die Fähigkeiten des Arbeiters an die Technologie anzupassen [5]. Außerdem besteht das Ziel darin, den Produktionsprozess der Industrie energie- und ressourceneffizienter zu gestalten, um eine nachhaltige Produktion aus wirtschaftlicher, ökologischer und gesellschaftlicher Perspektive zu erreichen [6]. Dieser menschenzentrierte Ansatz führt dazu, dass Roboter eng mit dem Menschen kollaborieren und ein Kontakt mit dem Menschen vorgesehen ist und keine Gefahr darstellen darf. Der Forschungsbeirat Industrie 4.0 kritisiert, dass der Begriff Industrie 5.0 mittlerweile immer häufiger verwendet wird, obwohl auch Industrie 4.0 bereits Kernthemen wie menschenzentrierte Ansätze und Entwicklung von künstlicher Intelligenz berücksichtigt [7]. Aus diesem Grund wird auf den Begriff Industrie 5.0 verzichtet und der Fokus dieser Arbeit auf die kollaborative Automatisierung und die Zusammenarbeit zwischen Mensch und Roboter gelegt.

Für solche Mensch-Roboter-Kollaborationen (MRK) werden neue verbesserte Sicherheitskonzepte im Hinblick auf die funktionale Sicherheit einer Maschine eine wichtige Rolle spielen, um die Sicherheit von Mensch, Maschine und Umwelt zu gewährleisten. Heutige Sicherheitslösungen sind oft zu langsam und haben daher auch eine zu hohe Reaktionszeit für kollaborierende Aufgaben [8]. Außerdem ist eine Überwachung der Roboterbewegung im dreidimensionalen Raum notwendig [9], was durch die in den dezentralen Antrieben verbaute funktional sichere Steuerelektronik allein nicht ohne großen Mehraufwand realisierbar ist. Hinzu kommt, dass funktional sichere Antriebssysteme aufgrund des Zertifizierungsaufwands der sicherheitsbezogenen Komponenten und der oft redundanten Strukturen zur Erreichung der Sicherheitsanforderungen noch deutlich teurer sind als rein funktionale Servoantriebe [10]. Zudem ist die eingesetzte Steuerelektronik, für die eine Sicherheitszertifizierung erforderlich ist, nicht ohne Weiteres austauschbar, was zu Problemen führen kann, wie Lieferengpässe in der Vergangenheit gezeigt haben. Für die Sicherheitsanwendung haben Antriebe eine komplette dezentrale sicherheitszertifizierte Logik, sodass bei jeder Änderung der Antriebsfunktionen eine neue Zertifizierung notwendig ist. Zusätzlich besitzt die übergeordnete Steuerung auch eine sicherheitszertifizierte Logik. Ein anderer Ansatz hat sich in den letzten Jahren bei sicherheitsbezogenen Drehgebern durchgesetzt. Durch eine externe Diagnose in einer übergeordneten sicherheitsbezogenen Logik kann auf eine vollständig zertifizierte Logik im Drehgeber verzichtet werden und der zusätzliche Aufwand im Drehgeber für die sicherheitsrelevante Anwendung ist vergleichsweise gering. Dieser Ansatz soll auch bei der sicherheitsbezogenen Antriebsarchitektur Anwendung finden.

1.2 Zielsetzung

Im Rahmen dieser Arbeit wird eine platzsparende, leistungsfähige und kostengünstige Antriebsarchitektur für autonome Fahrzeuge und kollaborierende Roboter vorgestellt. Dabei sollen nur wenige programmierbare Hardware-Bausteine verwendet werden, sodass für die Steuerelektronik nahezu eine Zwei-Chip-Lösung entsteht, bei der alle Funktionalitäten (z. B. Speicher) integriert sind. Um die Anforderungen an die Dynamik und die Präzision solcher Anwendungen zu erfüllen, wird eine hoch-performante Antriebsarchitektur nach dem Stand der Technik eingesetzt. Um die tatsächliche Leistungsfähigkeit des realen Antriebssystems, wie es in der späteren Anwendung zum Einsatz kommt, zu untersuchen, wird die in der Antriebstechnik üblicherweise verwendete Interpolation für den Lageregelkreis in die Untersuchung mit einbezogen. Das Ziel besteht darin, bewährte kostengünstige Komponenten und Standardtechnologien zu verwenden, die eine höhere Verfügbarkeit und Zuverlässigkeit bieten und in der Regel einen alternativen Lieferanten (Second Source) besitzen. Außerdem soll auf bewährte Feldbustechnologien gesetzt werden, die den Anforderungen heutiger Antriebssysteme an eine zyklische synchrone echtzeitfähige Datenübertragung gerecht werden. Zusätzlich sollen aber auch die Diagnose- und Inbetriebnahme-Möglichkeiten des Feldbussystems genutzt werden, um auf kostenintensive Speichermodule und Schnittstellen im Antrieb verzichten zu können.

Da das Antriebssystem für MRK eingesetzt werden soll, wird ein besonderer Fokus auf die funktional sichere Antriebsarchitektur gelegt. Die antriebsinternen Sicherheitsfunktionen beschränken sich auf grundlegende Funktionen zum zuverlässigen Stillsetzen des Motors und sind integraler Bestandteil des Antriebs, sodass keine zusätzliche Hardware, insbesondere in Form von Sicherheitsoptionskarten, erforderlich ist. Die Ansteuerung der Sicherheitsfunktionen erfolgt über ein sicherheitsbezogenes Feldbusprotokoll. Die komplexeren und rechenintensiveren Sicherheitsfunktionen zur Überwachung der Bewegung werden in einer übergeordneten zentralen Sicherheitssteuerung durchgeführt. Die dafür notwendigen Prozessgrößen, die im Antrieb gemessenen werden, werden ebenfalls über das sicherheitsbezogene Feldbusprotokoll an die Sicherheitssteuerung übertragen und nur dort verarbeitet und nicht, wie heute oft üblich, sowohl im Antrieb als auch in der Sicherheitssteuerung. Ähnlich wie bei sicherheitsbezogenen Drehgebern basiert das Konzept darauf, dass ein Großteil der Diagnose vom Antrieb extern in der übergeordneten Sicherheitssteuerung durchgeführt wird. In Kombination mit einer diversitären redundanten Antriebsarchitektur können kostengünstige Standardkomponenten anstelle von teuren sicherheitszertifizierten Komponenten eingesetzt werden. Dies führt zu einer kompakten sicherheitsbezogenen Antriebsarchitektur, bei der eine vollständig zertifizierte sicherheitsbezogene Logik im Antrieb nicht mehr erforderlich ist. Folgende zusätzliche Anforderungen werden an das Antriebssystem gestellt:

- Die sicherheitsbezogene Architektur entspricht den geltenden europäischen Normen für Maschinensicherheit und erreicht eine ausreichende Risikoreduzierung für eine MRK.
- Die Zykluszeit für die sicherheitsbezogene Feldbuskommunikation beträgt eine Millisekunde. Dadurch wird die Diagnose über die externe Sicherheitssteuerung und auch die Realisierung von sicheren Roboterbewegungen mit mehreren Achsen für MRK ermöglicht.

Durch die Antriebsarchitektur in Kombination mit einer zentralen übergeordneten Sicherheitssteuerung wird die für die funktionale Sicherheit benötigte sicherheitsbezogene Hardware im Antrieb und in der Sicherheitssteuerung durch sicherheitsbezogene Software in der Sicherheitssteuerung ersetzt [8]. Wie in [11] beschrieben, unterstützt diese sicherheitsbezogene Antriebsarchitektur die Verwendung von diversitären redundanten Sensorelementen anstelle von sicherheitszertifizierten Sensoren. Dieser Ansatz ermöglicht eine größere Freiheit beim Austausch von einzelnen Komponenten, ohne die funktionale Sicherheit des Systems zu beeinträchtigen.

1.3 Gliederung der Arbeit

Zu Beginn dieser Arbeit werden in Kapitel 2 die Grundlagen und der Stand der Technik heutiger Servoantriebe vorgestellt. Der Fokus wird auf die Architektur der Steuerelektronik und die Regelung von permanenterregten Synchronmotoren (PSM) gelegt. Zudem werden gängige Messverfahren zur Erfassung der Prozessgrößen wie Strom und Position vorgestellt sowie die heute übliche Kommunikation über Feldbusse mit einer übergeordneten Steuerung. Anschließend werden heutige sicherheitsbezogene Antriebsstrukturen dargestellt und näher untersucht. Dazu werden die dafür benötigten Normen näher betrachtet und verschiedene Kenngrößen präsentiert, die für den Entwurf eines sicherheitsbezogenen Antriebssystems von Bedeutung sind. Besonders wichtig ist der Aspekt der sicherheitsbezogenen Software für die Steuerelektronik im Antrieb und die sicherheitsbezogene Kommunikation mit einer übergeordneten Sicherheitssteuerung. In diesem Zusammenhang wird auch gezeigt, wie die MRK heute realisiert wird und wie sie in Zukunft gestaltet werden kann.

In Kapitel 3 wird die hoch-performante Architektur des Antriebs vorgestellt. Besonderer Fokus wird auf die Struktur der Steuerelektronik gelegt, die aus zwei programmierbaren Logikeinheiten besteht. In diesem Zusammenhang wird die Aufteilung der feldorientierten Regelalgorithmen auf diese beiden Komponenten erläutert. Darüber hinaus wird der zeitliche Verlauf der Abtastregelung näher untersucht, um eine geringe Zykluszeit der Regelkreise zu gewährleisten und somit eine höhere Dynamik zu erreichen. Ein wichtiger Aspekt hierbei ist die Bestimmung der Performanz des Lageregelkreises unter Berück-

sichtigung der Interpolation sowie der direkten Ableitung von Vorsteuersignalen für die Regelkreise aus der Interpolation.

Im vierten Kapitel wird die sicherheitsbezogene Antriebsarchitektur beschrieben. Dafür werden zunächst die Steuerelektronik und die antriebsinternen Sicherheitsfunktionen vorgestellt. Ein wichtiger Aspekt ist dabei ein Verfahren für ein geregeltes Stillsetzen des Motors durch den sicherheitsrelevanten Teil des Antriebs. Danach wird die sicherheitsbezogene Kommunikation mit der übergeordneten Sicherheitssteuerung erläutert und wie die Erfassung und Weiterleitung der sicherheitsrelevanten Strom- und Positionsmessdaten aus dem Antrieb zur Sicherheitssteuerung realisiert wird. Ein besonderer Fokus wird hierbei auf die Ermittlung eines sicherheitsbezogenen Positionswertes mit einem einzigen Resolver gelegt, bei der ein Teil der Auswertung weiterhin im Antrieb stattfindet. Im weiteren Verlauf wird gezeigt, wie mit dem Kommunikationsstandard IO-Link kostengünstig sicherheitsbezogene Ein- und Ausgänge für den Antrieb realisiert werden können und wie ein degradierter Betrieb nach [12] mit der vorgestellten Antriebsarchitektur umgesetzt werden kann. Zum Abschluss dieses Kapitels werden die verbleibenden antriebsinternen Diagnosemaßnahmen erläutert und gezeigt, wie mit der vorgestellten Architektur auf eine vollwertige zertifizierte Logik im Antrieb verzichtet werden kann.

Am Ende dieser Arbeit wird in Kapitel 5 die Validierung des Konzepts für die vorgestellte Antriebsstruktur anhand der entwickelten Hardware und einer Umsetzung an einem Industrieroboter gezeigt.

2 Grundlagen und Stand der Technik

2.1 Servoantriebe

Elektrische Antriebe gehören zu den wichtigsten Energiewandlern und wandeln in hochentwickelten Ländern etwa 60 % der erzeugten elektrischen Energie in mechanische Energie um [13]. Regelbare Antriebe setzen sich heute zur Effizienzsteigerung immer mehr durch. So nimmt der Anteil an geregelten Antrieben jährlich um etwa 5 % zu [14]. Unter geregelten Antrieben versteht man die Einhaltung vorgegebener Drehmomente, Drehzahlen oder Drehwinkel einer Maschine während ihrer Bewegungsabläufe unabhängig von Störeinflüssen. Diese Antriebe werden auch Servoantriebe genannt und bestehen aus einem Servomotor und einem leistungselektronischen Stellglied mit Leistungsteil und Steuerteil (auch Servoregler genannt), wie in Abbildung 1 dargestellt. Typische Anwendungen für Servoantriebe sind beispielsweise die Lageregelung von Robotern oder Bewegungsabläufe für Transportsysteme [14]. In der Automatisierungstechnik werden PSMs häufig als Servomotoren eingesetzt, da sie im Vergleich zu Asynchronmaschinen einen höheren Wirkungsgrad aufweisen und somit auf einen Lüfter verzichtet werden kann. [14]. Der PSM hat zusätzlich eine hohe Überbelastbarkeit, sodass durch kurzzeitige Stromerhöhung ein Spitzendrehmoment erzeugt werden kann, wodurch der Motor stark beschleunigt werden kann. Aus diesem Grund ist der PSM in Kombination mit einem Servoregler mit einer geeigneten Regelung für dynamische Prozesse wie Roboterantriebe geeignet [15]. Die Regelung eines Servoantriebs ist dabei meist in Form einer Kaskade mit Regelkreisen für Position, Drehzahl und Strom realisiert. Das Stellglied des Servoantriebs soll dabei für eine quasi-kontinuierliche Spannungsvorgabe mit minimaler Verzögerungszeit sorgen [14]. Um die zu regelnden Größen zu beeinflussen, sind Prozessgrößen durch Messwertgeber zu ermitteln. Für eine hohe Genauigkeit der Regelung besitzen die Sensoren eine hohe Auflösung und eine geringe Störanfälligkeit bzw. geringes Rauschen. Klassische Sensoren für Servoantriebe sind Drehgeber, Drehzahlgeber und Bauteile zur Messung des Motorstroms. In der Vergangenheit wurden analoge Signale als Steuersignale für den Antrieb verwendet, z. B. eine analoge Drehzahlvorgabe. Aufgrund der fortgeschrittenen Entwicklung und kostengünstigen Herstellung werden heutzutage jedoch meistens Mikroprozessoren zur Signalverarbeitung verwendet [13]. Bei größeren Maschinen oder Anlagen gibt es mehrere Servoantriebe, die ihre jeweilige Teilaufgabe dezentral ausführen. Die Sollwerte der einzelnen Antriebe werden dabei durch eine zentrale übergeordnete Steuerung berechnet bzw. vorgegeben. Die Aufgabe einer solchen Steuerung kann von einer rechnergestützten numerischen Steuerung (engl.: computerized numerical control, CNC) oder einer speicherprogrammierbaren Steuerung (SPS) übernommen werden. Für die Kommunikation zwischen Steuerung und Servoantrieben wird heute in der Regel ein Feldbus verwendet [14]. Die Mikroprozessortechnik in modernen

Servoantrieben vereinfacht die Anbindung solcher Feldbusse an eine übergeordnete Steuerung. So können neben Soll- und Istwert für die zu regelnde Größe auch Parameter für die Reglereinstellung des Servoantriebs über den Feldbus übertragen werden, wodurch eine Konfiguration über die Steuerung möglich ist [14].

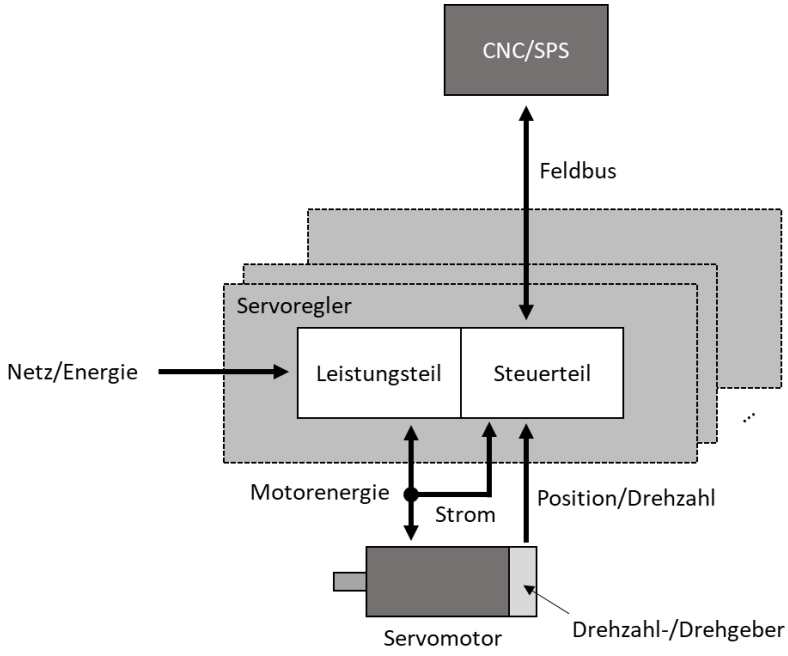


Abbildung 1: Aufbau und Struktur eines modernen elektrischen Servoantriebs.

Bevor etwa um 1960 leistungselektronische Halbleiterbauelemente aufkamen, wurden Stellglieder für drehzahlveränderliche Antriebe mit Maschinenumformer (Motor-Generator-System) oder mechanischen Verstellgetrieben realisiert. Auch durch eine elektrische Polumschaltung, d. h. eine Umschaltung der Polzahl des Stators eines Motors, war eine Veränderung der Drehzahl stufenweise möglich [14]. Moderne elektrische Servoantriebe sind hingegen mit leistungselektronischen Halbleiterbauelementen wie Bipolartransistoren mit isolierter Gate-Elektrode (engl.: insulated-gate bipolar transistor, IGBT) oder Metalloxid-Halbleiter-Feldeffekttransistoren (engl.: metal oxide semiconductor field-effect transistors, MOSFET) ausgestattet. Diese Leistungstransistoren werden nur im Schaltbetrieb genutzt, entweder in der Sättigung (maximal leitend) oder gesperrt (maximal isolierend), um die Verluste zu minimieren. Moderne leistungselektronische Stellglieder erreichen so Wirkungsgrade von über 90 % bei der Energieumwandlung mit geringen Oberschwingungen [14]. Typische Schaltfrequenzen heutiger Servoantriebe liegen zwischen 5 und 20 kHz [16]. Eine hohe Schaltfrequenz ermöglicht zwar eine schnelle Stromregelung und verringert den Stromrippel im Motorstrom, jedoch steigen dabei die Schaltverluste in den Leistungshalbleitern [16]. Bei niedriger Schaltfrequenz verhält es sich umgekehrt und der höhere Stromrippel führt zu zusätzlichen Wärmeverlusten im Motor.

Für die Ansteuerung der einzelnen Komponenten im Leistungsteil und die Signalverarbeitung der Sensoren werden Mikrocontroller (µC), digitale Signalprozessoren (DSP), feldprogrammierbare Logikgatter (engl.: field programmable gate array, FPGA) oder eine Kombination aus diesen eingesetzt. Die Sensorsignale können oftmals nicht direkt von den digitalen Prozessoren verarbeitet werden und es findet eine Vorverarbeitung der Signale mit Hilfe von Analog-Digital-Wandlern (engl.: analog-to-digital converter, ADC) statt. Der Servoregler und der Servomotor sind in heutigen Systemen nicht mehr unbedingt räumlich voneinander getrennt. Vor allem bei kleineren Leistungen (z. B. bei 48-V-Antrieben) sind Motor, Wechselrichter und Steuerelektronik in einem Gerät verbaut. Bei dieser kompakten Bauweise ist nur noch die Zuleitung für die Energieversorgung und die Anbindung an eine übergeordnete Steuerung notwendig [13].

2.1.1 Steuerteil

Vor dem Einzug der Digitalelektronik in der Signalverarbeitung wurden analoge Systeme für die Regelung von Antrieben genutzt. Obwohl eine analoge Regelstruktur bei der Schnelligkeit und der Bandbreite keinesfalls ein Nachteil gegenüber digitalen Systemen aufweist, ergeben sich für heutige Servoantriebe Anforderungen, die nicht mit analogen Strukturen realisiert werden können. So ist eine Konfiguration der Regler nur durch eine Änderung der Hardware möglich. Die geringe Rechenleistung lässt nur die Implementierung grundlegender Regelkreisstrukturen zu und ist für komplexere Regelalgorithmen, wie die feldorientierte Regelung (engl.: field oriented control, FOC) für den PSM, nicht geeignet. Außerdem werden viele passive Bauteile benötigt, was den Platzbedarf und die Komplexität der Hardware erhöhen [17]. Nachteil der digitalen Systeme ist die entstehende Totzeit durch die digitale Signalverarbeitung [16].

Seit der Einführung digitaler Regelsysteme in den 1970er Jahren ist es möglich, komplexe und rechenintensive Algorithmen für die Antriebsregelung zu entwerfen. Der Einsatz von DSPs und einfachen Mikroprozessoren war zunächst nur in hochpreisigen Servoantrieben üblich. Voll digitale Industrieantriebe waren jedoch erst ab Mitte der 1990er Jahre auf dem Markt verfügbar und bis dahin waren die meisten weiterhin mit analoger Technik ausgestattet. Der große Durchbruch voll digitaler Regelungen für Servoantriebe gelang erst Ende der 1990er Jahre mit der Verfügbarkeit von kostengünstigen µCs. Aufgrund der anfänglich geringen Performanz der µC wurde häufig eine Kombination aus µC und DSP verwendet. Der DSP war für die Ansteuerung der PWM-Signale und die Auswertung des Positionsfeedback geeignet, während der µC die rechenintensiven Aufgaben übernahm und als Schnittstelle für Feldbusse diente. Häufig wurde die Kombination aus beiden auch in einer anwendungsspezifischen integrierten Schaltung (engl.: application specific integrated circuit, ASIC) realisiert. Moderne µCs besitzen eine ausreichend hohe Performanz, was den DSP überflüssig macht. [17], [18]

Einer der wesentlichen Nachteile von µC-basierenden Servoantrieben ist die Einschränkung in Bezug auf die parallele Verarbeitung, wie sie bei einem Regelalgorithmus für Antriebe möglich wäre. Somit sind auch die Performanz und die erreichbare Bandbreite begrenzt. Durch den Einsatz eines FPGAs kann die Hardware-Architektur genau auf den zu implementierenden Regelalgorithmus angepasst werden, was zu einer schnelleren Signalverarbeitung führt [19]. Außerdem kann ein FPGA für verschiedene Anwendungen mit speziellen Anforderungen entworfen werden und ist im Gegensatz zu einem ASIC nicht nur auf eine bestimmte Aufgabe zugeschnitten. So haben Hersteller Systemfunktionen, die mit den damals zur Verfügung stehenden Standard-µCs nicht realisierbar waren, in einem zusätzlichen FPGA implementiert [20]. Das FPGA ist also für Systeme geeignet, bei denen sowohl eine einfache Berechnung als auch eine schnelle Verarbeitungszeit gefordert sind [17]. Dafür ist das FPGA aber für komplexere Algorithmen und die Kommunikation mit dem industriellen Umfeld über Feldbussysteme weniger geeignet als ein µC [17], [19]. Aufgrund der Vor- und Nachteile beider Systeme sind in modernen Servoantrieben oft sowohl ein µC als auch ein FPGA verbaut [20]. Die Aufgaben werden so verteilt, dass die Vorteile beider Komponenten genutzt werden können. Die Kommunikation zwischen µC und FPGA kann über einen parallelen oder seriellen Datenbus erfolgen.

Aufgrund dieser Kombination aus µC und FPGA im Steuerteil haben die Hersteller von µCs versucht, spezielle Peripherien für die Regelung von Servomotoren in ihren Produkten zu integrieren, die sonst im FPGA implementiert waren. Zum Beispiel wurden die Schnittstellen zu Positionssensoren wie EnDat und BiSS sowie die Auswertung von Sigma-Delta-ADCs (ΣΔ) zur Strommessung mittels Sinc-Filter im FPGA realisiert [20]. Viele µC können heute die ΣΔ-Signale auswerten [21]. Mit der µC Reihe C2000 bietet Texas Instruments mittlerweile konfigurierbare Logikblöcke (engl.: configurable logic block, CLB) an, mit denen FPGA-Funktionalitäten im µC implementiert werden können. So können in der C2000-Reihe auch die Schnittstellen für EnDat 2.2 und BiSS integriert und Zustandsautomaten umgesetzt werden [20], [22]. Auf der anderen Seite bieten FPGA-Hersteller schon seit längerer Zeit Hard- und Soft-Core-Prozessoren an, um die Funktionalität von µCs zu integrieren. Die Hard-Core-Prozessoren sind in einem eigenen Silizium im FPGA integriert und bieten eine hohe Taktrate bei geringer Flexibilität [19]. Intel® bietet FPGAs mit Arm Cortex Prozessoren an. Soft-Core-Prozessoren werden in den Logikblöcken im FPGA implementiert und bieten eine höhere Flexibilität bei der Konfiguration, haben jedoch geringere Taktraten [19]. Beispiele für Soft-Core-Prozessoren sind Nios® II von Intel®, MicroBlaze von Xilinx oder RISC-V.

Weder die Hersteller von µCs noch von FPGAs waren bisher in der Lage, die Komponenten des jeweils anderen vollständig zu ersetzen. Sowohl die Hard- und Soft-Core-Prozessoren als auch der in FPGAs integrierte On-Chip-Speicher wie Speicher mit wahlfreiem Zugriff (engl.: random-access memory, RAM) oder Flash-Speicher sind immer

noch deutlich teurer als bei herkömmlichen µCs. Moderne digitale Drehgeber-Protokolle wie EnDat 3 werden hingegen von µCs noch nicht unterstützt. Außerdem ist ein weiterer Nachteil solcher hochspezialisierten Halbleiterbausteine, dass meist keine alternativen Bauteile von anderen Herstellern zur Verfügung stehen [21].

2.1.2 Regelungsverfahren

Die Regelung in einem Antriebssystem sorgt dafür, dass die gewünschte Prozessgröße eingehalten wird. Bei Servoantrieben sind das meistens die Position oder die Drehzahl des Servomotors. Um einen vorgegebenen Verlauf der Sollwerte, die sogenannte Trajektorie, unabhängig von Maschinen- und Lastparametern oder externen Störeinflüssen genau einzuhalten, ist die Regelung des Motordrehmoments erforderlich. Die zwei gängigsten Regelungsverfahren für die Drehmomentregelung, die ebenfalls in industriellen Servoantrieben verwendet werden, sind die FOC und die direkte Drehmomentregelung (engl.: direct torque control, DTC) [14]. Es gibt verschiedene wissenschaftliche Arbeiten, die sich mit dem Vergleich der beiden Verfahren befassen. Beide Verfahren bieten Vor- und Nachteile [23], [24]. Im Rahmen dieser Arbeit wird jedoch nur die FOC betrachtet, da diese in Kombination mit einer Kaskadenregelstruktur in den meisten heute am Markt befindlichen Servoantrieben eingesetzt wird [25].

Da das Drehmoment des PSMs von den drei Strömen in den Statorwicklungen abhängig ist, diese aber in Bezug auf das Drehmoment in einem komplexen Zusammenhang stehen, werden für die FOC die drei Phasenströme in ein rotorfestes Koordinatensystem überführt [26]. Dadurch wird eine Entkopplung des drehmomentbildenden Stroms und des flussbildenden Stroms erreicht [27]. Für die mathematische Umrechnung von den drei Phasenströmen in die rotorfesten Komponenten i_d und i_q wird die Clarke- und Park-Transformation verwendet. Das rotorfeste Koordinatensystem rotiert mit dem Rotor des PSMs und dreht sich mit der elektrischen Kreisfrequenz ω_el in Bezug auf das statorfeste Koordinatensystem. Zur Bestimmung des Winkels zwischen statorfestem und rotorfestem Koordinatensystem ist die Messung des Rotorwinkels durch einen Drehgeber notwendig. Falls das Reluktanzmoment vernachlässigbar ist ($L_\mathrm{d} = L_\mathrm{q}$), sorgt nur der drehmomentbildende Strom i_q für ein Drehmoment (Synchronmoment), da es orthogonal zum Magnetfeld des Rotors steht. Aus diesem Grund wird der Strom i_d im Grunddrehzahlbereich zu null geregelt. Erst bei hohen Drehzahlen wird ein Feldschwächbetrieb des PSMs durch das Einprägen eines negativen i_d Stroms erreicht, sodass höhere Drehzahlen bei gleichbleibender Statorspannung möglich sind. Der Vorteil der FOC besteht darin, dass die rotorfesten Komponenten im stationären Zustand (bei konstanter Drehzahl und konstantem Drehmoment) Gleichgrößen sind, die sich einfacher regeln lassen als Wechselgrößen. [28]

Abbildung 2 zeigt die Struktur einer feldorientierten Stromregelung eines PSMs. Für die FOC werden der Winkel mithilfe eines Drehgebers sowie die drei Phasenströme gemessen. Daraus werden mittels Clarke- und Park-Transformation die rotorfesten Ist-Stromkomponenten berechnet. Für die Stromregelung werden typischerweise PI-Regler eingesetzt. Die rotorfesten Soll-Spannungen werden durch die inverse Park-Transformation in die statorfesten Koordinaten α und β umgewandelt. Diese beiden Sollwerte dienen als Eingangssignale für die Raumzeigermodulation (engl.: space vector modulation, SVM), welche die Ansteuersignale für die sechs Leistungshalbleiter im Wechselrichter generiert.

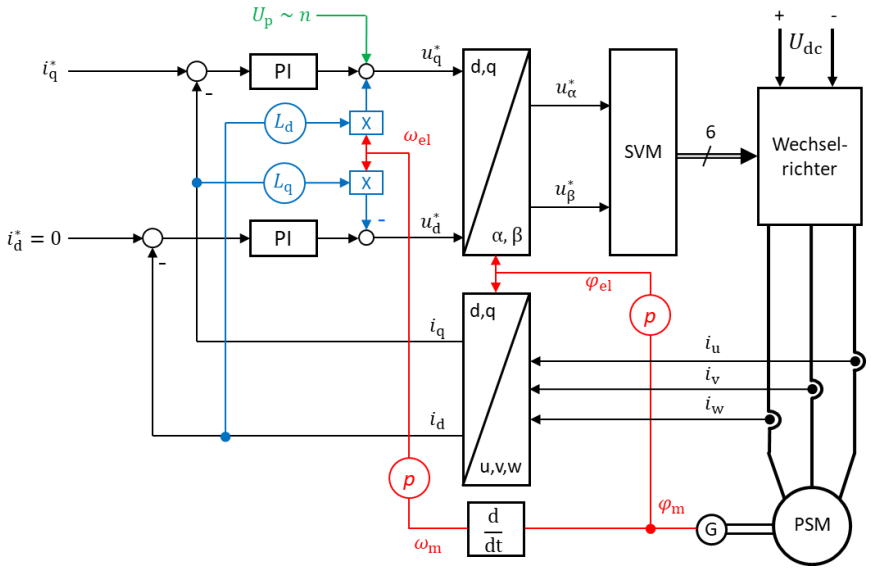


Abbildung 2: Feldorientierte Regelung des permanenterregten Synchronmotors.

Die SVM ist das gebräuchlichste on-line Pulsweitenmodulationsverfahren (PWM-Verfahren) für dreiphasige zweistufige Wechselrichter, da es einen geringen Stromrippel erzeugt und mit geringem Aufwand in einem DSP umgesetzt werden kann [29]. Eine effiziente Berechnung der Einschaltzeiten für die SVM wird in [30] vorgestellt. Alternativ zu den on-line Verfahren gibt es auch off-line berechnete Modulationsverfahren. Hierbei werden optimierte Pulsmuster für bestimmte Betriebspunkte im Voraus berechnet. Dadurch hat der Motorstrom zwar einen geringeren Oberschwingungsanteil, was die Verluste im Motor reduziert, allerdings sind diese optimierten Pulsmuster mit einem großen Rechenaufwand verbunden [31].

Die FOC wird meistens mit einer Kaskadenregelung kombiniert. Der innerste Regelkreis ist der Stromregelkreis, der die Spannungssollwerte für die SVM generiert. Der Stromsollwert wird vom Drehzahlregler und der Drehzahlsollwert vom Lageregler berechnet. Aus dem Positionsfeedback können die Istwerte für Lage- und Drehzahlregler bestimmt werden. Der Vorteil einer solchen Regelstruktur besteht darin, dass die einzelnen Sollwerte begrenzt werden können und damit an die elektrischen und mechanischen Grenzen des Systems angepasst werden können [32]. Die Bandbreite des Stromreglers limitiert die

Bandbreite der äußeren Regelkreise und ist ausschlaggebend für die Dynamik des Servoantriebs [25]. Typischerweise besitzen heutige Servoantriebe einen Stromregler mit einer Abtastzeit zwischen 31,25 µs und 125 µs [13]. Diese Aktualisierungsrate des Stromreglers entspricht meistens der doppelten PWM-Trägerfrequenz [25] und somit auch der doppelten Schaltfrequenz, sodass beide Schaltflanken berechnet werden können. Für den Drehzahl- und Lageregelkreis sind heute Abtastzeiten zwischen 125 µs für hochdynamische Anwendungen und 5 ms üblich [13]. Die Bandbreite der Regelkreise nimmt von innen nach außen ab. Typischerweise liegt die Bandbreite des Lageregelkreises heutiger Servoantriebe unterhalb von 150 Hz bei einer Abtastfrequenz von 16 kHz [33]. Ein weiterer Vorteil durch die Aufteilung der Regelkreise mit der Kaskadenstruktur besteht darin, dass bei den Regelkreisen nur eine Regelstrecke mit der entsprechenden Zeitkonstante und Störgröße zu kompensieren ist und nicht mehrere, wie es bei einem solchen Antriebssystem der Fall ist [14]. Vereinzelt werden auch moderne Regelungstechnikverfahren wie Beobachter eingesetzt, die meisten industriellen Servoantriebe werden jedoch als klassische Kaskadenregelung ohne diese Verfahren aufgebaut [13].

2.1.3 Sensoren für Servoantriebe

Für die Bewegungssteuerung (engl.: Motion-Control) mit Servoantrieben ist die Messung verschiedener elektrischer und mechanischer Regelgrößen erforderlich. Dazu zählen in erster Linie die Strommessung und die Messung der Rotorlage bzw. der Drehzahl und Position. Die Sensoren wandeln die physikalische Größe in ein entsprechendes analoges oder digitales Signal um. Im Folgenden sollen die Messverfahren für Strom und Position heutiger Servoantriebe vorgestellt werden.

Strommessung

Es gibt zwei gängige Methoden zur Messung des Stroms in Motoranwendungen. Die einfachste und kostengünstige Methode ist die Verwendung eines Shunt-Widerstandes in den Motorphasen [34]. Der Spannungsabfall am Widerstand wird ausgewertet. Da die Verluste minimiert werden sollen, wird der Wert des Widerstands möglichst klein gewählt, weshalb das Spannungssignal für eine direkte Verarbeitung zu klein ist [34]. Aus diesem Grund wird oft ein Signalverstärker benötigt, welcher gleichzeitig für eine galvanische Trennung zwischen Mess- und Signalpfad sorgt [35]. Ein Nachteil des Messverfahrens ist der Verlust im Shunt-Widerstand bei hohen Strömen.

Der Hall-Effekt-Sensor nutzt das Magnetfeld des stromdurchflossenen Leiters, das proportional zur Stromstärke des Motorstroms ist. Prinzipbedingt ist die Messung direkt galvanisch getrennt. Bei Hall-Sensoren wird zwischen Open-Loop- und Closed-Loop-Sensoren unterschieden. Während der Open-Loop-Sensor eine Spannung proportional zum Motorstrom ausgibt, wird beim Closed-Loop-Sensor ein zweiter Strom in gegenge-

setzter Richtung eingeprägt, der den Fluss im Magnetkern gegen null regelt. Dieser Strom ist proportional zu dem zu messenden Strom und kann über einen Widerstand als Ausgangsspannungssignal dargestellt werden. Der Closed-Loop-Hall-Sensor erzeugt eine Spannung mit hoher Genauigkeit und geringem Rauschen. [36]

Früher wurde für die Analog-Digital-Wandlung der analogen Ausgangssignale der Stromsensoren Register mit schrittweiser Annäherung (engl.: successive-approximation register, SAR) verwendet [35]. Für Servoantriebe hat sich in den letzten Jahren jedoch die ΣΔ-Technologie für die Messung der Motorströme durchgesetzt [36]. ΣΔ-ADCs haben eine deutlich höhere Auflösung als die herkömmlichen SAR-ADCs [37]. Der ΣΔ-Modulator erzeugt einen 1-Bit-Strom mit einer typischen Abtastfrequenz zwischen 10 MHz und 20 MHz. Da dieser Bitstrom nicht sofort weiterverarbeitet werden kann, ist zuerst die Umwandlung der Daten in ein digitales Wort notwendig. Dafür haben sich Sinc³-Dezimierungsfilter bewährt [36]. Diese Filter können vergleichsweise einfach in einem FPGA implementiert werden, sind heute aber auch als On-Chip-Peripherie in vielen µCs integriert.

Typischerweise wird der Motorstrom synchron zum PWM-Trägersignal abgetastet, um den kurzzeitigen Strommittelwert zu messen und nicht den durch das Schalten der Leistungshalbleiter entstehenden Stromrippel zu erfassen [35].

Weg- und Winkelmessung

Drehgeber messen den Winkel einer rotativen Achse in Bezug auf einen Referenzpunkt und wandeln die Information in ein elektrisches Signal um. Dieser mechanische Winkel wird mit φ_{m} bezeichnet. Wird speziell der Winkel eines Elektromotors gemessen, wird oft auch von einem Motor-Feedback-System gesprochen. Mit einem Drehgeber kann neben dem Winkel auch die Winkelgeschwindigkeit ω oder die Drehzahl n durch einfache Differentiation und die Winkelbeschleunigung α durch doppelte Differentiation bestimmt werden. In der Praxis wird zwischen Inkrementalgebern und Absolutwertgebern sowie Singleturn- und Multiturn-Drehgebern unterschieden. Während Singleturn-Drehgeber nur den Winkel innerhalb einer Motorumdrehung angeben, können Multiturn-Drehgeber auch die Anzahl der Motorumdrehungen messen. Bei Inkrementalgebern werden meistens zwei um 90° phasenverschobene Signale (z. B. Sin/Cos) eingesetzt, um neben der Winkeländerung auch die Drehrichtung zu bestimmen. Da der Inkrementalgeber nur Winkeländerungen anzeigt und keine absolute Winkelinformation liefert, ist beim Einschalten der Maschine immer eine Referenzfahrt durchzuführen. Dies ist auch der Nachteil eines Inkrementalgebers, da das Referenzieren bei Anwendungen mit mehreren Achsen zeitintensiv und komplex ist. Anders ist es bei den Absolutwertgebern, die unmittelbar nach dem Einschalten einen absoluten Winkel an die Steuerelektronik senden. Es gibt sowohl analoge als auch digitale Absolutwertgeber. Ein analoger Absolutwertgeber ist der Resolver.

Dieser hat eine hohe Temperaturverträglichkeit und ist mechanisch robust. Außerdem wird keine Elektronik im Resolver bzw. Motor benötigt, da die Auswertung komplett in der Steuerelektronik des Antriebs stattfindet. Aus diesen Gründen wird der Resolver häufig als Motor-Feedback für Servoantriebe verwendet. Digitale Absolutwertgeber haben heute meist einen µC integriert und kommunizieren über eine serielle Schnittstelle mit dem Antrieb. Unabhängig von der Art der Signale (analog oder digital) wird oft ein differentielles verdrilltes Leitungspaar (engl.: twisted pair) mit invertierten Signalen verwendet, um eingestreute elektromagnetische Störsignale bei der Übertragung zu unterdrücken. [38]

Heutige bidirektionale Schnittstellen basieren auf der von SICK STEGMANN entwickelten unidirektionalen synchron-seriellen Schnittstelle (engl.: synchronous serial interface, SSI) und werden als 4-Leiter- und 2-Leiter-Technologie angeboten [39]. Ein Überblick über die gängigen digitalen Schnittstellen für Drehgeber wird in [39] und [40] gegeben. Dazu zählen unter anderem die Drehgeber-Protokolle Endat 3, HIPERFACE DSL (HDSL) und SCS open link. Klassische Übertragungsraten heutiger digitaler Schnittstellen für Drehgeber liegen zwischen 10 und 25 Mbit/s [41]. Antriebshersteller sind heute dazu gezwungen, die Vielzahl unterschiedlicher Drehgeber-Schnittstellen zu unterstützen und je nach Kundenwunsch in den Antrieb zu integrieren. Abhilfe verschafft das in [41] vorgestellte Konzept für eine Multi-Drehgeber-Schnittstelle, mit der ein einheitlicher herstellerunabhängiger Zugriff auf verschiedene Drehgeber-Schnittstellen möglich ist.

Digitale Absolutwertgeber stellen heute nicht mehr nur die Winkelposition zur Verfügung, sondern bieten dem Antrieb über die Kommunikationsschnittstelle weitere Funktionen an. So kann die Temperatur vom Drehgeber selbst oder von den Motorwicklungen über das Drehgeber-Protokoll übertragen werden [38]. Außerdem besitzen die Drehbegeber einen nicht-flüchtigen Speicher, z. B. einen elektrisch löschbaren programmierbaren Nur-Lese-Speicher (engl.: electrically erasable programmable read-only memory, EEPROM), der das elektronische Typenschild zur Verfügung stellt. Dort können Motorparameter, Regelparameter, Informationen über den Drehgeber und anwendungsspezifische Daten hinterlegt werden, die eine Inbetriebnahme des Motors vereinfachen. Nach dem Einschalten können diese Informationen vom Antrieb aus dem Drehgeber gelesen und die Regelkreise so parametriert werden, dass ein optimaler Betrieb möglich ist [13]. Ein alternatives Konzept nutzt die Motorleitungen zum Auslesen eines elektronischen Typenschilds, das sich auch für Motoren eignet, die keinen digitalen Drehgeber integriert haben [42]. Durch ein offenes digitales Kommunikationsprotokoll können Motortypenschilder verschiedener Hersteller ausgelesen werden [42].

Resolver

Der elektromechanische Aufbau von Resolvern ist im Vergleich zu digitalen Positionsgebern einfach, da weder zusätzliche Lager noch Elektronik erforderlich sind, was zu einer geringen Ausfallrate führt. Aufgrund des Transformatorprinzips wird der Resolver auf der Primärseite mit einer Referenz-Wechselspannung u_{ref} erregt:

$$u_{\mathrm{ref}}(t) = E_0 \sin(2\pi f_{\mathrm{c}}\, t + \varphi_{\mathrm{c}}) \tag{1}$$

Diese sinusförmige Referenzspannung ist unabhängig vom mechanischen Winkel und wird üblicherweise synchron zur PWM der Leistungsstufe erzeugt. Typische Frequenzen sind 5 - 10 kHz [43]. Die beiden Ausgangswicklungen sind induktiv mit der Primärseite gekoppelt und mechanisch um 90° zueinander versetzt, sodass abhängig vom Übersetzungsverhältnis ü eine sinus- und eine kosinus-modulierte Ausgangsspannung erzeugt wird:

$$u_{\sin}(t) = \text{ü}\ u_{\mathrm{ref}}(t)\ \sin(\varphi_{\mathrm{m}}) \tag{2}$$
$$u_{\cos}(t) = \text{ü}\ u_{\mathrm{ref}}(t)\ \cos(\varphi_{\mathrm{m}}) \tag{3}$$

Die Berechnung des Positionssignals φ_{m} ist mathematisch eine arctan-Funktion mit den beiden Resolver-Ausgangsspannungen $U_{\sin}$ und $U_{\cos}$ als Eingangssignale:

$$\varphi_{\mathrm{m}} = \arctan\frac{U_{\sin}}{U_{\cos}} \tag{4}$$

Die Berechnung des digitalen Positionssignals φ_{m} aus den analogen Spannungen wird auch als Resolver-Digital-Wandlung bezeichnet. Eine solche Berechnung ist jedoch nicht ohne Einschränkungen möglich, insbesondere dann, wenn die Ausgangssignale aufgrund des Referenzsignals nahe null sind. Bei der Verwendung von arctan ist das Positionssignal prinzipbedingt stark verrauscht. Aus diesem Grund sind Nachlaufschleifen (engl. Tracking-Loops) bei solchen Resolver-Digital-Wandlern (engl.: resolver-to-digital converters, RDC) üblich. Ein Vorteil der Tracking-Loop ist, dass das Positionssignal mit einem Tiefpass 2. Ordnung gefiltert wird, ohne dass bei konstanter Geschwindigkeit eine Phasenverschiebung auftritt. Eine solche Tracking-Loop kann mit einem speziellen integrierten Schaltkreis (engl.: integrated circuit, IC) [44] oder mit SAR-ADCs [45] realisiert werden. Aufgrund der Kosten, der begrenzten Konfigurationsflexibilität, der erforderlichen Leiterplattenfläche und der Anfälligkeit gegenüber elektromagnetischen Störungen (engl.: electromagnetic interferences, EMI) beim Schaltvorgang der Leistungsstufe werden diese RDC-Konzepte nicht mehr eingesetzt. Heutige RDC-Konzepte verwenden fortschrittliche ADCs und eine digitale Signalverarbeitung für die Filterung und Weiterverarbeitung. In [43] werden ΣΔ-ADCs mit einer effektiven Auflösung von 16 Bit verwendet. Anstelle einer µC-basierten Verarbeitung wird ein quasi-zeitkontinuierlicher FPGA-Algorithmus implementiert. Dieser Ansatz bietet volle Konfigurationsflexibilität in Kom-

bination mit vollständig digital implementierten Filtern, die unempfindlich gegenüber EMI von Antrieben sind. Diese schnell abgetastete (16 MHz) nahezu volldigitale RDC-Technologie entspricht dem Stand der Technik [46].

2.1.4 Kommunikation über Feldbusse

Bei Maschinen und Anlagen, bei denen Antriebe einzelne Teilaufgaben ausführen, wie die Bewegung der verschiedenen Gelenke eines Roboterarms, spielt die Kommunikation mit der übergeordneten Steuerung eine wichtige Rolle. Dafür besitzt heute jeder moderne Antrieb eine Feldbusschnittstelle. Die Trajektorie für die einzelnen Antriebe wird zentral in der Steuerung berechnet. Typischerweise wird die Trajektorie mit einer Zykluszeit zwischen 250 µs und 1 ms generiert und über den Feldbus an den Antrieb übertragen. Um die verschiedenen Zykluszeiten von der Erzeugung der Trajektorie und den Regelkreisen im Antrieb aufeinander anzupassen, wird üblicherweise eine Feininterpolation genutzt. Diese berechnet Zwischensollwerte in der Trajektorie im Abstand der Zykluszeit der Regelkreise im Antrieb. [16]

Ursprünglich bestand die Idee darin, durch die Einführung von Feldbussen bei großen Anlagen den Verkabelungsaufwand durch die Parallelverdrahtung und somit auch die Kosten möglichst gering zu halten. Feldbussysteme für Antriebe erfordern jedoch zusätzliche Eigenschaften wie ein hohe Echtzeitanforderung und eine Synchronisation mehrerer Antriebe im Mikrosekundenbereich [47]. Die zyklische synchrone Datenübertragung der Prozessdaten zu den Antrieben ist erforderlich, um die gewünschten Bewegungsverläufe exakt zu erreichen. Zu den Prozessdaten gehören Soll- und Istwerte für den Positions-, Drehzahl, oder Drehmomentregler. Zusätzlich werden auch azyklisch Informationen über Feldbusse übertragen. Diese beinhalten größtenteils Steuerbefehle und Statusinformationen, die z. B. für das Ein- oder Ausschalten des Antriebs genutzt werden. Es ist aber auch möglich, Parameter für die Regelkreise oder Fehler- und Diagnoseinformationen über den Feldbus zu senden. Für diesen Informationsaustausch wurden Antriebsprofile für Feldbussysteme entwickelt und in der IEC 61800-7-1 standardisiert, um eine herstellerunabhängige Kommunikation und einen einheitlichen Zugriff auf Antriebsparameter zu ermöglichen [14].

Heute gibt es etwa 50 verschiedene Feldbusse, wobei in den letzten Jahren insbesondere offene Feldbusse, die eine Kommunikation herstellerunabhängiger Komponenten über den Feldbus ermöglichen, und echtzeitfähige Ethernet Feldbusse (Industrial Ethernet) in der Antriebstechnik an Bedeutung gewonnen haben [13]. Es gibt verschiedene Vorteile von Industrial Ethernet, aber hauptsächlich ist es durch den Ethernet-Standard eine performante, bewährte und kostengünstige Technologie, die sich schon länger bei der Vernetzung von Büroumgebungen durchgesetzt hat [48]. Außerdem hat sich durch die Entwicklung des Internets ein universeller Standard für die Hardware-Komponenten bei

ethernet-basierten Kommunikationssystemen ergeben [48]. Zu den Industrial-Ethernet-Protokollen zählen unter anderem EtherCAT, PROFINET IRT, EtherNet/IP und SERCOS III. Bei Herstellern von Servoantrieben ist EtherCAT der am häufigsten verwendete Feldbus [48].

2.1.5 Inbetriebnahme und Fehlerdiagnose

Die Inbetriebnahme eines Servoantriebs sollte schnell und ohne zusätzlichen Aufwand durchzuführen sein. Moderne Servoantriebe haben jedoch oft mehrere hundert einstellbare Parameter, was die optimale Einstellung dieser Parameter zu einer komplexen Aufgabe macht [13]. Aus diesem Grund bieten viele Hersteller Inbetriebnahme-Tools an, die eine Inbetriebnahme nach Anleitung mit Oszilloskopfunktionen und Frequenzanalysen ermöglichen. Aber auch ein automatisches Einstellen der Reglerparameter über ein sogenanntes Autotuning ist mit diesen Werkzeugen möglich [32]. Für die Inbetriebnahme wird häufig ein Rechner über eine entsprechende Schnittstelle an den Antrieb angeschlossen, worüber auch die Firmware des Servoantriebs aktualisiert werden kann. Wenn die Inbetriebnahme abgeschlossen und die optimalen Parameter eingestellt sind, werden diese häufig in einem EEPROM im Antrieb abgespeichert und beim nächsten Neustart daraus ausgelesen [13]. Zusätzlich gibt es oft noch ein steckbares Speichermodul, sodass ein defektes Gerät ohne erneute Inbetriebnahme ausgetauscht werden kann [13]. Das neue Gerät erhält das alte Speichermodul mit allen relevanten Parametern und ggf. der Firmware. Diese Steckmodule sind zwar vergleichsweise teuer, werden aber immer noch eingesetzt. Alternative Konzepte nutzen den Feldbus zur Übertragung von Parametern bei jedem Neustart. Bei den Servoreglern der Baureihe AX5000 der Firma Beckhoff Automation werden die Parameter nicht mehr im Antrieb gespeichert, sondern nur zentral in der Steuerung [49].

Obwohl heutige Feldbussysteme die Fehlerdiagnose unterstützen und vereinfachen, nutzen einige Hersteller einen Fehlerspeicher [50], um antriebsinterne Fehler zu hinterlegen, die dann von entsprechendem Servicepersonal ausgelesen werden können. Daraus kann der Hersteller möglicherweise erkennen, aus welchem Grund ein Gerät ausgefallen ist und ob es repariert werden kann. Das Auslesen von Fehlermeldungen durch Personal ist deutlich aufwendiger als das zentrale Sammeln und Abspeichern dieser Informationen in der Steuerung. Außerdem ermöglicht ein Feldbus eine Zustandserfassung der Maschine (engl.: condition monitoring) und eine vorausschauende Wartung (engl.: predicitve maintance), wodurch kritische Ereignisse frühzeitig erkannt werden und nötige Wartungsmaßnahmen vorausschauend getroffen werden können.

2.2 Sicherheitsbezogene Antriebstechnik

Das Ziel sicherheitsbezogener Antriebstechnik besteht darin, das entstehende Risiko durch die Verwendung von Antrieben in Maschinen für Mensch und Umwelt zu minimie-

ren, da durch Antriebe gefahrbringende Bewegungen an Maschinen entstehen können [51]. Dafür können zunächst Risiken durch eine geeignete Konstruktion der Maschine beseitigt oder reduziert werden [52]. Falls dies nicht umsetzbar oder ausreichend ist, sind zusätzliche Schutzmaßnahmen erforderlich. Zu diesen Maßnahmen zählen auch Sicherheitsfunktionen, die das Risiko der Maschine auf ein akzeptables Maß reduzieren sollen. Die Sicherheitsfunktionen werden ganz oder in Teilen auch vom Servoantrieb ausgeführt, weshalb eine Betrachtung des Antriebs hinsichtlich sicherheitsbezogener Aspekte von Bedeutung ist. Die Begriffe „sicherheitsbezogen“ und „sicherheitsrelevant“ beziehen sich in dieser Arbeit immer auf die funktionale Sicherheit eines Systems (im Englischen mit dem Begriff „safety“ gleichzusetzen) und sind nicht mit dem Begriff Sicherheit in Bezug auf den Schutz einer Maschine vor unbefugtem Zugriff durch Menschen zu verwechseln (im Englischen mit dem Begriff „security“ gleichzusetzen).

2.2.1 Normen

Alle Maschinen, die seit dem 1. Januar 1995 innerhalb des europäischen Wirtschaftsraumes eingeführt werden, unterliegen den Anforderungen der Maschinenrichtlinie [52]. Die EG-Maschinenrichtlinie 2006/42/EG ist die aktuell gültige Maschinenrichtlinie in Europa, in der auch Sicherheitsanforderungen an Maschinen gestellt werden und Hersteller dazu verpflichten eine Risikobeurteilung durchzuführen [52]. Dort sind auch harmonisierte Normen aufgelistet, mit deren Einhaltung die technischen Anforderungen an die EU-Richtlinien erfüllt werden [53]. Die Anwendung harmonisierter Normen ist zwar freiwillig, andernfalls sind aber alternative Lösungen zur Erfüllung der Anforderungen erforderlich [53].

Die DIN EN ISO 12100 [54] ist die grundlegende Norm für Maschinensicherheit und legt grundsätzliche Begriffe und Methoden fest. Außerdem werden hier Vorgehensweisen für die Risikobeurteilung und Risikominderung erläutert [54]. Die Einhaltung dieser Norm allein reicht jedoch nicht aus, um die Sicherheitsanforderungen in der Richtlinie zu gewährleisten. Daher gibt es darauf aufbauend die Normreihe DIN EN 61508 mit ihrer Sektornorm IEC 62061 für die Maschinenindustrie sowie die DIN EN ISO 13849 ebenfalls für die Maschinenindustrie. Die Basisnorm DIN EN 61508 ist keine harmonisierte Norm und befasst sich unabhängig von dem Anwendungsgebiet mit der funktionalen Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen Systemen. Die Sektornorm IEC 62061, speziell für die Maschinenindustrie, wurde 2021 in einer neuen Ausgabe veröffentlicht und gilt seit 2022 als harmonisierte Norm. Diese Anwendungsnorm richtet sich an Hersteller von Steuerungssystemen und enthält Anforderungen für den Entwurf eines sicherheitsbezogenen Steuerungssystems [55]. Die neue Ausgabe begrenzt sich nicht mehr nur auf elektrische, elektronische und programmierbare elektronische Systeme, sondern kann für alle Arten von Technologien verwendet werden (z. B.

hydraulisch, pneumatisch und mechanisch). Die DIN EN 61508 und die IEC 62061 verwenden als Klassifizierungsschema das Sicherheits-Integritätslevel (engl.: safety integrity level, SIL). Speziell für elektrische Leistungsantriebe mit einstellbarer Drehzahl gibt es noch die DIN EN 61800-5-2, die Anforderungen an den Entwurf von sicherheitsbezogenen Leistungsantrieben vorgibt. Diese bezieht sich auch auf die im Rahmen der DIN EN 61508 vorgegebenen Anforderungen [56]. Hier sind unter anderem auch verschiedene Sicherheitsfunktionen definiert, die für Servoantriebe relevant sind.

Die DIN EN ISO 13849 hingegen benutzt als Klassifizierungsschema das Performance Level (PL) und stellt einen Leitfaden für die Gestaltung sicherheitsbezogener Teile einer Steuerung (engl.: safety related part of control system, SRP/CS) bereit [57]. Diese Norm ersetzt die frühere Basisnorm EN 954-1 und verwendet weiterhin den dort festgelegten Begriff der Kategorien [52].

Obwohl die Methoden der beiden harmonisierten Normen IEC 62061 und DIN EN ISO 13849 unterschiedlich sind, führen beide zu einer vergleichbaren Risikominderung in der Maschinensicherheit [52]. Aus Sicht der Anwender in der Praxis bietet die DIN EN ISO 13849 aber einen vereinfachten Quantifizierungsansatz bei Verwendung der vorgesehenen Architekturen im Vergleich zur IEC 62061 [52].

2.2.2 Entwurf eines sicherheitsbezogenen Teils einer Steuerung

Nach der Risikobeurteilung sind für den SRP/CS entsprechende Schutzmaßnahmen in Form von Sicherheitsfunktionen festzulegen, falls die Gefährdung durch konstruktive Maßnahmen nicht völlig ausgeschlossen werden kann [52]. Die Sicherheitsfunktion wird dabei von einem Sensor (Eingang), einer Logik (Signalverarbeitung) und einem Aktor (Ausgang) durchgeführt [51]. Servoregler übernehmen dabei häufig den Teil des Sensors und/oder Aktors und ggf. die Aufgabe der Logikeinheit. Die Sicherheitsfunktion soll in Abhängigkeit vom Risiko eine bestimmte Qualität erreichen, um die erforderliche Risikoreduzierung einzuhalten [52]. Dazu wird in der DIN EN ISO 13849 das PL verwendet. Je nach Risiko der Gefährdung ist ein erforderliches PL einzuhalten (engl.: performance level required, PL_r). Zur Bestimmung dieses PL_r ist in der Norm ein vereinfachter Riskograph unter Verwendung bestimmter Kriterien vorgesehen.

Bei der Realisierung des SRP/CS spielen verschiedene Kriterien eine Rolle, um am Ende das PL_r zu erreichen und die geforderte Risikoreduzierung zu erzielen. Zu diesen Kriterien gehören die Qualität der Bauteile, deren Kombination und gegenseitige Beeinflussung, die Wirksamkeit der Diagnose und die Systemtoleranz gegenüber Fehlern. Diese Kriterien dienen der Bestimmung der durchschnittlichen Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (engl.: probability of a dangerous failure per hour, PFH_D). Auf Basis der PFH_D kann das erreichte PL der entworfenen Struktur des SRP/CS bestimmt werden. Die Bestimmung der PFH_D kann auf unterschiedliche Weisen durchge-

führt werden. In der DIN EN ISO 13849 ist ein vereinfachtes Verfahren durch die Anwendung eines Säulendiagramms vorgesehen. [52]

Die Kategorien bilden die grundlegende Struktur des SRP/CS und haben Auswirkung auf die Widerstandsfähigkeit gegen Fehler und somit auch auf die mögliche Risikoreduzierung [52]. Durch die Anforderungen an moderne Leistungsantriebe für sicherheitsbezogene Anwendungen werden meist zweikanalige Strukturen realisiert, die die Anforderungen einer Kategorie-3- oder Kategorie-4-Architektur nach DIN EN ISO 13849 erfüllen [51]. Eine solche Architektur für Kategorie 3 ist in Abbildung 3 dargestellt. Ein einzelner Fehler führt hierbei nicht zum Verlust der Sicherheitsfunktion, da der andere Kanal diese noch ausführen kann (Einfehlertoleranz).

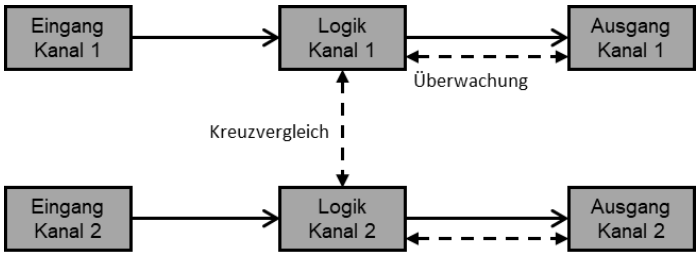


Abbildung 3: Zweikanalige Architektur für Kategorie 3 nach DIN EN ISO 13849.

Die Bauteilzuverlässigkeit hat ebenso wie die Kategorie einen Einfluss auf das PL, weshalb eine Betrachtung jedes sicherheitsrelevanten Bauteils, das an der Ausführung einer Sicherheitsfunktion beteiligt ist, notwendig ist. Die entsprechende Kenngröße nach DIN EN ISO 13849 ist die mittlere Zeit bis zum gefahrbringenden Ausfall (engl. mean time to dangerous failure, $MTTF_D$). Ein genauer Weg zur Bestimmung der $MTTF_D$ aller Bauteile kann über eine Ausfallarten- und Effektanalyse (engl.: failure mode and effects analysis, FMEA) durchgeführt werden, allerdings gibt es auch verschiedene Tabellen oder Angaben von Herstellern mit entsprechenden Werten. Aus den $MTTF_D$-Werten der einzelnen Bauteile kann ein $MTTF_D$-Wert des Kanals bestimmt werden, der in die drei Klassen niedrig, mittel und hoch eingeteilt wird. [52]

Ein weiterer Kennwert zur Bestimmung des PL ist der Diagnosedeckungsgrad (engl.: diagnostic coverage, DC), der die Wirksamkeit von Test- und Überwachungsmaßnahmen im SRP/CS angibt. Der durchschnittliche Diagnosedeckungsgrad DC_{avg} (engl.: average), welcher beim Säulendiagramm Anwendung findet, definiert den DC des gesamten SRP/CS und wird aus dem DC und der $MTTF_D$ der einzelnen Blöcke berechnet. Auch hier findet bei einem vereinfachten begründeten Schätzverfahren eine Klassifizierung in keinen, niedrigen, mittleren und hohen DC_{avg} statt. Für Kategorie 3 ist mindestens ein niedriger DC_{avg} erforderlich. Die Test- und Überwachungsmaßnahmen dienen dazu, gefahrbringende Ausfälle rechtzeitig zu erkennen und das System in einen sicheren Zustand zu überführen. Zu diesen Maßnahmen zählen beispielsweise die zyklische Testung von Eingängen (Dynamisierung), die Plausibilität von Ein- und Ausgängen durch Rücklesen

und Kreuzvergleich, eine Programmlaufüberwachung (PLÜ) der Logik, Speicher-Tests sowie Tests der zentralen Recheneinheit (engl.: central processing unit, CPU). Die Testhäufigkeit spielt eine wichtige Rolle, da nicht nur zufällige Bauteilfehler, sondern auch systematische Fehler wie fehlerhafte Software mit den Maßnahmen aufgedeckt werden können. Bei einem zweikanaligen Kategorie-3-System ist die Aufdeckung des Nichtausführens der Sicherheitsfunktion erst vor dem Ausfall des zweiten Kanals durch einen Test erforderlich, da bei einem gefahrbringenden Ausfall der zweite Kanal weiterhin die Sicherheitsfunktion ausführen kann. [52]

Der letzte Parameter zur Bestimmung des PL bezieht sich auf Ausfälle infolge einer gemeinsamen Ursache (engl. common cause failure, CCF). Für ein Kategorie-3-System bedeutet das, dass ein Fehler einen gefahrbringenden Ausfall in beiden Kanälen verursacht und somit die Einfehlertoleranz des zweikanaligen Systems nicht gewährleistet ist. Um diesem Effekt entgegenzuwirken, beinhaltet die DIN EN ISO 13849 ein Punkteschema zur Bewertung von Gegenmaßnahmen (vgl. Tabelle 2 im Anhang). Wird eine Punktzahl von mindestens 65 Punkten für den SRP/CS erreicht, gelten die Maßnahmen gegen CCF als ausreichend. [52]

In der Praxis wird eine Sicherheitsfunktion meist nicht nur von einem SRP/CS, sondern in Teilen von verschiedenen SRP/CS als Subsysteme ausgeführt. Diese Subsysteme, bestehend aus Eingang, Logik und Ausgang (vgl. Abbildung 3), können hintereinandergeschaltet werden, um eine Sicherheitsfunktion auszuführen. Für das Gesamtsystem kann anhand der PL der Subsysteme ein Gesamt-PL bestimmt werden, obwohl die Subsysteme unterschiedliche Kategorien besitzen können. Beispielsweise kann für eine Sicherheitsfunktion ein Drehgeber zur Positionserfassung zum Einsatz kommen, welcher von einer Logik ausgewertet wird, und über einen Antrieb kann der sichere Zustand herbeigeführt werden. In diesem Fall besteht das Gesamtsystem für die Ausführung der Sicherheitsfunktion aus drei Subsystemen. Alle drei Subsysteme können einzeln als SRP/CS betrachtet werden und benötigen ein PL und eine Kategorie, die nach den genannten Kriterien bestimmt werden können. [52]

2.2.3 Sicherheitsbezogene Software

Mit dem zunehmenden Einsatz von programmierbaren Bauteilen wie µCs und FPGAs in sicherheitsbezogenen Anwendungen nahm auch die Bedeutung bei der Entwicklung von Software zu. Vor allem spielen Softwarefehler dabei eine große Rolle, denn nach [58] beinhaltet eine hochwertige Software durchschnittlich etwa zwei bis drei Fehler pro 1000 Programmzeilen. Diese Softwarefehler können in ungünstigen Situationen zu gefährlichen Ausfällen führen, weshalb in den Normen DIN EN ISO 13849 und DIN EN 61508 Anforderungen an die Entwicklung sicherheitsbezogener Software gestellt werden. Dabei wird zwischen sicherheitsbezogener Anwendungssoftware (engl.: safety-related applica-

tion software, SRASW) und sicherheitsbezogener Embedded-Software (engl.: safety-related embedded software, SRESW) unterschieden. SRASW wird von Anwendern bei der Entwicklung von Sicherheitsfunktionen in einer SPS verwendet und soll an dieser Stelle nicht weiter betrachtet werden. Die sicherheitsbezogene Firmware in einem Servoantrieb dagegen zählt zu SRESW.

Komplexe elektronische Komponenten von Servoantrieben wie Mikroprozessoren und ASICs können nicht als bewährte Komponenten nach DIN EN ISO 13849-2 betrachtet werden. Obwohl solche Komponenten bereits seit mehreren Jahren für die funktionale Sicherheit eingesetzt werden, gelten sie aufgrund von Softwarefehlern und vergleichsweise kurzen Firmware-Update-Zyklen nicht als bewährt [59]. Die Ausfallraten elektronischer Komponenten sind vergleichsweise gering, z. B. 31,4 Ausfälle pro Zeit (in 10^9 h) (engl.: failure in time, FIT) für ein MAX® 10 FPGA von Intel® [60]. Dies entspricht einer mittleren Zeit bis zu einem Ausfall (nicht zu verwechseln mit $MTTF_D$) von etwa 3653 Jahren. Andere Ursachen für gefährliche Ausfälle sind jedoch viel wahrscheinlicher als der dauerhafte Ausfall eines Bauteils. Um diese Ausfälle rechtzeitig zu erkennen und den Antrieb in einen sicheren Zustand zu bringen, sind zusätzliche Maßnahmen erforderlich.

In der DIN EN ISO 13849 sind verschiedene Anforderungen an SRESW gestellt, um eine Fehlervermeidung sowohl bei der Entwicklung der Software als auch während des Betriebs zu gewährleisten. Zu den hier relevanten Anforderungen für PL d und PL e zählen die Beherrschung von systematischen Ausfällen und die Abgrenzung von nicht sicherheitsbezogener Software. Ersteres bezieht sich z. B. auf die Überführung des SRP/CS in einen sicheren Zustand bei Spannungsausfall und Über- oder Unterspannung. Ebenfalls wird eine Überwachung des Programmablaufs und des Takts der Prozessoren gefordert, um fehlerhafte Programmabläufe aufzudecken. Dies kann durch eine zeitliche PLÜ mit einem externen Hardware-Watchdog oder einer zeitlich-logischen PLÜ mit gegenseitiger Überwachung der beiden Kanäle realisiert werden [61]. Der zweite oben genannte Punkt bezieht sich auf die Kapselung der sicherheitsbezogenen Software, um Einflüsse durch die nicht sicherheitsbezogene Software zu vermeiden (Rückwirkungsfreiheit) [61]. Nach DIN EN ISO 13849-1 sind für PL e zusätzlich die Anforderungen der DIN EN 61508 zu berücksichtigen, es sei denn, das zweikanalige System nach Kategorie 3 ist diversitär ausgelegt, dann genügen die oben genannten Anforderungen [57]. Diese Diversität der beiden Kanäle wird z. B. durch unterschiedliche Embedded-Software auf unterschiedlicher Hardware erreicht [52].

Werden Standardkomponenten, also Bauteile ohne Sicherheitsbewertung durch den Hersteller, verwendet, ist die Einhaltung der zuvor genannten und weiteren SRESW-Anforderungen nicht notwendig, falls für das SRP/CS nur PL c oder PL d erforderlich ist und eine diversitäre Technologie in Kategorie 2 oder 3 verwendet wird. Außerdem ist eine entsprechende Fehlererkennung für den DC über die SRASW zu realisieren. Den-

noch sind weiterhin ab Kategorie 1 bewährte Sicherheitsprinzipien anzuwenden. Da in der DIN EN ISO 13849-2 aber keine bewährten Sicherheitsprinzipien für programmierbare Systeme vorgegeben werden, können dafür z. B. die Maßnahmen zur Beherrschung von systematischen Fehlern oder Selbsttests von Mikroprozessoren, wie sie bereits bei den Maßnahmen zur Abschätzung des DC aufgelistet sind, verwendet werden. [52]

Letztere Maßnahmen umfassen z. B. CPU-Tests, Speichertests und Peripherietests, die die fehlerfreie Funktion und die Anbindung des Prozessors an weitere Komponenten des SRP/CS überprüfen [62]. Es können auch andere geeignete Maßnahmen zur Fehlererkennung getroffen werden, die jedoch im Falle des Auftretens eines gefährlichen Fehlers das System in einen sicheren Zustand überführen [59]. Klassische Ausfälle bei komplexer Elektronik sind Stuck-at-Fehler wie statische Signale, Kurzschlüsse oder Unterbrechungen [59].

2.2.4 Entwicklung sicherheitsbezogener Antriebsstrukturen

Als die Firma Pilz 1987 ihr erstes Sicherheitsschaltgerät PNOZ auf den Markt brachte, wurden Sicherheitslösungen fest verdrahtet [63]. Dieses Sicherheitsschaltgerät kann Not-Halt-Schalter, Schutztüren und Lichtschranken überwachen und Fehler bei der Verdrahtung erkennen (z. B. Erd- oder Querschluss) [64]. Abbildung 4 zeigt eine solche festverdrahtete Sicherheitslösung für drei Servoantriebe. Über den zweikanaligen Not-Halt-Schalter kann die Energiezufuhr der Servoantriebe zweikanalig über Netzschütze abgeschaltet werden. Um gefährliche Fehler, wie das Nicht-Öffnen beider Kontakte im Not-Halt-Schalter oder das Nicht-Öffnen der Kontakte beider Schütze, zu verhindern, ist der Ausfall eines Kanals durch zusätzliche Diagnosemaßnahmen aufzudecken. Dazu wird über das Sicherheitsschaltgerät zum einen überprüft, ob beide Kontakte im Not-Halt-Schalter geöffnet oder geschlossen sind und zum anderen kann der Schaltzustand der Schütze über einen weiteren zwangsgeführten Öffnerkontakt ausgewertet werden. Der Not-Halt-Schalter und die Netzschütze sind bewährte Standardkomponenten nach DIN EN ISO 13849-2 [65] und werden in der Regel nicht für die funktionale Sicherheit zertifiziert. Stattdessen wird ihre Ausfallrate nach der Qualitätsmanagement(QM)-Norm ISO 9001 [66] gemessen. Durch die bekannte Ausfallrate, die Redundanz und den DC ist aber ein Einsatz in Sicherheitslösungen möglich. Die in Abbildung 4 gezeigte Sicherheitslösung kann für die Sicherheitsfunktion sicher abgeschaltetes Drehmoment (engl.: safe torque off, STO) nach DIN EN 61800-5-2 verwendet werden, da durch das Abschalten der Energieversorgung verhindert wird, dass dem Motor eine krafterzeugende Energie zugeführt wird.

Während die Servoregler aus Abbildung 4 nur die funktionalen Anforderungen für die Lage- oder Drehzahlregelung übernehmen, sind zusätzliche Komponenten wie Netzschütze zur Realisierung der Sicherheitsfunktion erforderlich. Da Kategorie 3 Redundanz

erfordert, verdoppeln sich die Komponenten und der Verdrahtungsaufwand noch einmal. Dies macht die gesamte Sicherheitslösung teuer und unflexibel.

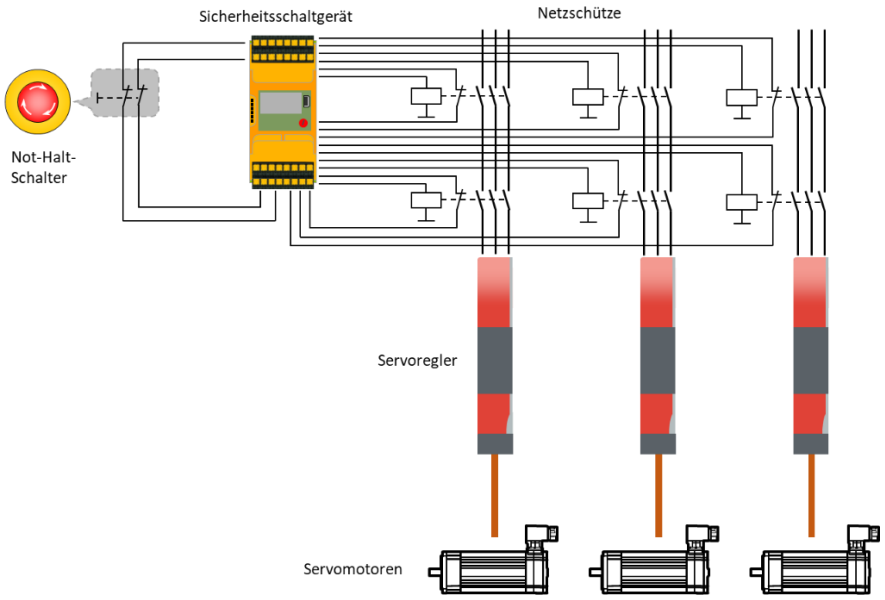


Abbildung 4: Festverdrahtete Sicherheitslösung mit einem Sicherheitsschaltgerät.

Mit dem Aufkommen von sicherheitsbezogenen Feldbussystemen wurde die parallele Verdrahtung weitestgehend verdrängt. Zunächst wurde die Sicherheits-SPS mit einem proprietären Sicherheitsfeldbus ausgestattet [67]. Diese herstellerspezifischen nicht offenen Feldbussysteme können jedoch nur sicherheitsbezogene Daten übertragen, weshalb ein paralleler Feldbus für die Kommunikation zu einer Standard-SPS notwendig ist [67]. Für die Synchronisierung zwischen Sicherheits-SPS und Standard-SPS wird ein zusätzliches physisches Netzwerk benötigt [68]. Zeitgleich rückte die Umsetzung der Sicherheitsfunktionen näher Richtung Servoregler. Zum einen ist die Realisierung mit Netzschützen nicht nur teuer und aufwändig, sondern das Laden des Zwischenkreises führt bei dieser Lösung beim Wiedereinschalten zu zusätzlichen Ausfallzeiten [51]. Zum anderen wird für weitere Sicherheitsfunktionen eine Überwachung von Position und Drehzahl verwendet, weshalb für die komplexe Berechnung Mikroprozessoren benötigt werden [51]. Dies wird auch heute noch in sogenannten Sicherheitsoptionskarten realisiert (im weiteren Verlauf nur noch als Optionskarte bezeichnet). Diese können in den Servoregler eingesteckt werden und sind meist mit zwei zusätzlichen µCs für die sicherheitsbezogene Überwachung für Kategorie 3 ausgestattet [69]. Verschiedene Hersteller wie beispielsweise SEW-EURODRIVE und Bosch Rexroth haben die Sicherheitsfunktion STO im Servoregler in Form einer Impulssperre integriert, welche über einen sicherheitsbezogenen 24-V-Eingang angesteuert werden kann [69], [70].

Um eine Überwachung von Drehzahl und Position zu realisieren, können zwei Drehgeber an die Optionskarte angeschlossen werden [69]. Der erste wird in der Regel im Motor integriert, während der zweite an der Last befestigt wird [39]. Die Anzahl der Drehgeber

ist vom erforderlichen PL bzw. vom Sicherheitskonzept des Drehgebers abhängig [51]. Außerdem besitzt die Optionskarte eine Schnittstelle für den Sicherheitsfeldbus sowie verschiedene Eingänge (inklusive Testausgänge zur Diagnose) für Lichtschranken, Not-Halt-Schalter oder Ausgänge zur Ansteuerung von STO im Servoregler. Obwohl diese Sicherheitslösung immer noch viele Komponenten durch die parallele Struktur auf Antriebs- und Steuerungsebene benötigt, sind solche Strukturen auch heute noch üblich [69], [71], [72], jedoch mit einem gemeinsamen Kommunikationskanal für die nicht sicherheitsbezogenen und die sicherheitsbezogenen Informationen.

Aufgrund der steigenden Nachfrage an sicherheitsbezogener Antriebstechnik, insbesondere nach komplexeren Sicherheitsfunktionen für eine sichere Bewegungsüberwachung, aber auch aufgrund des Platzbedarfs und der Kosten einer zusätzlichen Optionskarte, bieten viele Hersteller seit einigen Jahren ihre Servoregler mit integrierter sicherheitsbezogener Logik an [73], [74], [75]. Ebenso benötigen zwei Steuerungen (Standard- und Sicherheits-SPS) mehr Platz und meist zwei unterschiedliche Programmierumgebungen für Motion-Control und SRASW. Daher bieten verschiedene Hersteller eine sogenannte Compound-SPS an, die eine Standard- und eine Sicherheits-SPS kombiniert und mit einer Entwicklungsumgebung programmiert werden kann [76], [77]. Abbildung 5 zeigt eine solche Antriebsstruktur mit einer Compound-SPS und Servoreglern mit integrierter sicherheitsbezogener Logik. Ein einziger Standard-Feldbus mit sicherheitsbezogenem Protokoll dient der Datenübertragung zwischen SPS und Antrieben. Über diesen können auch die Sicherheitsfunktionen wie STO im Servoregler angesteuert werden. Die Compound-SPS bietet außerdem mehrere sicherheitsbezogene digitale Ein- und Ausgänge (engl.: input and output, I/O) zum Anschluss von Lichtschranken und Not-Halt-Schaltern. Durch die Verwendung eines sicherheitsbezogenen Drehgebers anstelle von zwei Standard-Drehgebern wird eine Sicherheitslösung ohne parallele Komponenten für Standard- und sicherheitsbezogene Anwendung erreicht.

Der Nachteil der heutigen sicherheitsbezogenen Antriebsstrukturen, ob mit einer Optionskarte oder integrierter sicherheitsbezogener Logik, ist die zweifach vorhandene zertifizierte sicherheitsbezogene Logik sowohl dezentral im Antrieb als auch in der Sicherheits-SPS. Darüber hinaus ist im Antrieb nur eine sichere Bewegungsüberwachung einer einzelnen Achse realisierbar und daher nicht für Mehrachsanwendungen wie beispielsweise Knickarmroboter geeignet [60].

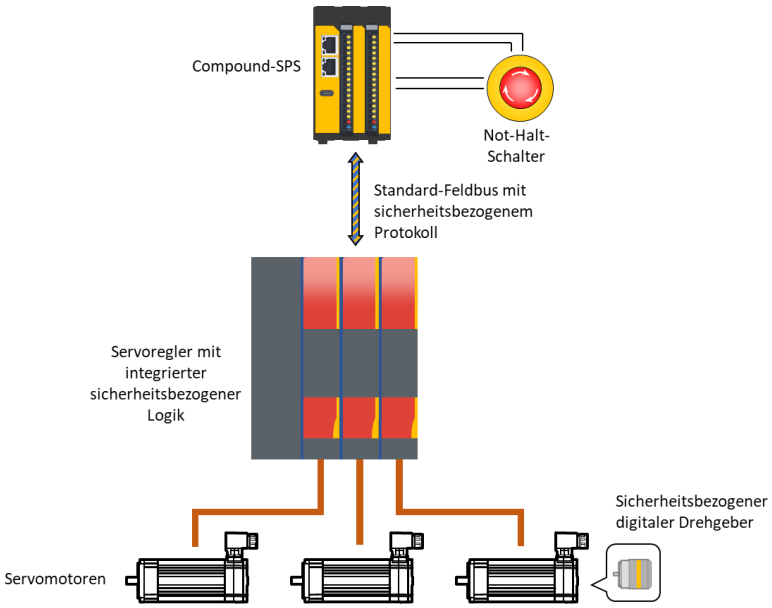


Abbildung 5: Sicherheitsbezogene Antriebsstruktur mit einer Compound-SPS und antriebsintegrierter sicherheitsbezogener Logik.

2.2.5 Sicherheitsbezogene Kommunikation

Wenn für eine Sicherheitsfunktion eine Kommunikation zwischen verschiedenen Subsystemen erforderlich ist, wie bei der Kommunikation über einen Feldbus zwischen Servoregler und Sicherheits-SPS, ist eine Abschätzung der möglichen Ausfälle bei der Datenübertragung erforderlich. Die DIN EN 61508-2 nennt zwei Lösungsansätze zur Übertragung sicherheitsbezogener Nachrichten über einen Kommunikationskanal. Zum einen den sogenannten weißen Kanal (engl.: white channel) und zum anderen den sogenannten schwarzen Kanal (engl.: black channel). An dieser Stelle verweist die DIN EN 61508-2 auch auf die DIN EN IEC 61784-3, die die Übertragung von sicherheitsbezogenen Nachrichten mit Feldbustechnologie beschreibt und ebenfalls auf dem Black-Channel-Ansatz basiert.

Bei einer White-Channel-Kommunikation werden die Daten von Komponenten verarbeitet, die bekannt sind, d. h. ihre Ausfallarten wurden ermittelt und entsprechende Maßnahmen getroffen, sodass die Sicherheitsanforderungen erfüllt sind. Jede beteiligte Komponente (z. B. Protokoll, Dienste und Netzwerkkomponenten) erhält ein SIL bzw. ein PL, wodurch dieser Ansatz aufwändig und teuer im Hinblick auf die Umstellung auf neue Technologien ist [78]. Außerdem wird weiterhin ein paralleler Feldbus für die Standard-Kommunikation benötigt, da nur sicherheitsbezogene Daten übertragen werden.

Mit dem Industrial-Ethernet haben sich ethernet-basierte Kommunikationssysteme in der Fertigungs- und Maschinenautomatisierung durchgesetzt. Der Nachteil bei der Verwendung von ethernet-basierten Technologien liegt in der unbekannten Zuverlässigkeit der Komponenten und Software [78]. Da diese Komponenten nicht nach DIN EN 61508 entworfen sind, wird dieser Kommunikationskanal als Black-Channel bezeichnet [79]. Um

einen Black-Channel dennoch für die Übertragung von sicherheitsrelevanten Daten zu nutzen, werden eingebaute Mechanismen zur Erkennung von Übertragungsfehlern genutzt [78]. Zu diesen Maßnahmen, welche in einer Sicherungsschicht im SRP/CS umgesetzt werden, gehören beispielsweise laufende Nummern, Zeitmarken, Kennungen (engl.: identifier, ID) für Sender und Empfänger sowie die Datensicherung mittels zyklischer Redundanzprüfung (engl.: cyclic redundancy check, CRC) [80]. Einige dieser Maßnahmen werden in die sicherheitsbezogene Nachricht eingefügt und gemeinsam als sichere Protokoll-Dateneinheit (engl.: safety protocol data unit, SPDU) über den Black-Channel versendet. Durch den Black-Channel-Ansatz können sicherheitsbezogene Daten und nicht sicherheitsbezogene Daten über denselben Feldbus übertragen werden, ohne Eigenschaften über den zugrunde liegenden Kommunikationskanal zu berücksichtigen. Beispiele für Feldbusse, die auf dem Black-Channel-Ansatz basieren, sind EtherCAT mit der sicherheitsbezogenen Protokollschicht Failsafe over EtherCAT (FSoE) oder PROFINET mit PROFIsafe.

Zur Bestimmung der PFH_D ist die Restfehlerwahrscheinlichkeit die entscheidende Kenngröße bei der sicherheitsbezogenen Kommunikation [81]. Die Restfehlerwahrscheinlichkeit gibt die Wahrscheinlichkeit für unerkannte fehlerhafte Daten bei der Übertragung an [81]. Die Maßnahmen des Black-Channel-Ansatzes sollen dabei eine hohe Wahrscheinlichkeit zur Erkennung solcher Fehler gewährleisten. Die Bitfehlerwahrscheinlichkeit (engl.: bit error probability, BEP) des Black-Channel ist nach DIN EN IEC 61784-3 [82] auf 10^{-2} festgelegt und wird unter Verwendung eines Modells zur Berechnung der Restfehlerwahrscheinlichkeit benötigt [81]. Diese spezifizierte BEP bedeutet, dass durchschnittlich jedes 100. Bit fehlerhaft sein kann und durch das sicherheitsbezogene Protokoll aufzudecken ist [83]. Die Verwendung dieses Modells wird jedoch seit einiger Zeit als unzureichend erachtet, da bestimmte Fehlerarten nicht berücksichtigt werden [81]. Vor allem durch die Verwendung von Security-Methoden wie beispielsweise Verschlüsselung im zugrunde liegenden Kommunikationskanal treten veränderte Fehlermuster auf, weshalb ein weiteres Kanalmodell eingeführt werden soll [81], [83]. An den Black-Channel werden weiterhin keine Eigenschaften über den zugrunde liegenden Kommunikationskanal gestellt, jedoch soll das sicherheitsbezogene Protokoll höhere Anforderungen an die BEP erfüllen (z. B. 0,5 statt bisher 10^{-2}) [81], [83]. Durch verbesserte Modelle zur Berechnung der Restfehlerwahrscheinlichkeit sollen auch Verschlüsselung und Komprimierung der Daten berücksichtigt werden [81], [83]. Die sicherheitsbezogenen Protokolle mit den aktuellen Anforderungen an die BEP werden daher als „grauer Kanal“ (engl.: gray channel) bezeichnet [8]. Bei dem Gray-Channel-Ansatz sind dann jedoch Annahmen über den zugrunde liegenden Kommunikationskanal zu treffen, da die Daten zur Übertragung nicht verändert werden dürfen. Folgende Annahmen sind zu treffen [8]:

- Keine Verschlüsselung (z. B. virtuelles privates Netzwerk, VPN)
- Keine Komprimierung (z. B. ZIP)
- Keine Modulation (z. B. drahtloses Lokal-Netzwerk, engl.: wireless local area network, WLAN)

Die neue Version der DIN EN IEC 61784-3 plant diese Einschränkungen bezüglich des Gray-Channel-Ansatzes zu berücksichtigen [83].

2.2.6 Sicherheitsbezogene Positionsmesssysteme

Für die sichere Bewegungsüberwachung von Maschinen werden Sicherheitsfunktionen zur Begrenzung der Position, Drehzahl und Beschleunigung eingesetzt [84]. Zur Erfassung dieser Prozessgrößen können Drehgeber verwendet werden. Die DIN EN 61800-5-2 gibt hierfür die entsprechenden Sicherheitsfunktionen sicher begrenzte Position (engl.: safely-limited position, SLP), sicher begrenzte Geschwindigkeit (engl.: safely-limited speed, SLS) und sicher begrenzte Beschleunigung (engl.: safely-limited acceleration, SLA) an. Da der Drehgeber an der Sicherheitsfunktion beteiligt ist, wird er als Subsystem betrachtet und die Anforderungen der DIN EN ISO 13849 sind zu erfüllen. Seit Juli 2019 gibt es einen dritten Teil der Normreihe DIN EN 61800-5, der sich speziell mit den Anforderungen an die funktionale Sicherheit von Drehgebern befasst [85].

Die Anforderungen an den Drehgeber hängen zum einen von der Sicherheitsfunktion ab und zum anderen von dem PL_r des Systems [51]. Zur Umsetzung der Anforderungen an den Drehgeber als Subsystem bei einer Kategorie-3-Architektur gibt es in der Praxis verschiedene Möglichkeiten. Eine weit verbreitete Methode ist der Einsatz inkrementeller Drehgeber mit analogen Sin/Cos-Signalen [39]. Alternativ dazu werden auch je nach Anforderung ein oder mehrere Absolutwertgeber mit oder ohne sicherheitsbezogener Feldbusschnittstelle und seit einigen Jahren zunehmend auch sicherheitsbezogene Absolutwertgeber eingesetzt.

Abbildung 6 zeigt diese verschiedenen Möglichkeiten zur Realisierung eines Subsystems mit Drehgebern für eine Kategorie-3-Architektur mit anschließender Auswertung durch eine übergeordnete zweikanalige Logik. Abbildung 6a) zeigt die Umsetzung des Subsystems mit zwei konventionellen inkrementellen Sin/Cos-Drehgebern, sodass durchgängig eine zweikanalige Struktur gegeben ist, um die Einfehlertoleranz für Kategorie 3 einzuhalten [84]. Zusätzlich sind Maßnahmen zu treffen, um einen ausreichenden DC für Kategorie 3 zu erreichen. Alternativ kann für dieses Subsystem auch ein digitaler Absolutwertgeber mit zwei diversitären Messverfahren (z. B. magnetisch und optisch) verwendet werden [86].

Wird ein sicherheitsbezogener Drehgeber verwendet, wie in Abbildung 6b) dargestellt, ist keine Sicherheitsbewertung vom Anwender notwendig, da der Hersteller bereits PL,

PFH_D und Kategorie des Subsystems angibt [52]. Ein solches Subsystem wird als gekapseltes Subsystem bezeichnet. Damit ein gekapseltes Subsystem die sicherheitstechnischen Kennwerte erfüllt, sind die vom Hersteller angegebenen Einsatzbedingungen einzuhalten [52]. Neben der Einhaltung von Temperaturangaben sind auch Maßnahmen zur Fehlererkennung für den erforderlichen DC nach Herstellerangaben extern im Servoregler umzusetzen [51]. Die beiden im Drehgeber erzeugten unabhängigen Positionswerte werden via Black-/Gray-Channel an die übergeordnete Logik übertragen und dort plausibilisiert (Vergleich der beiden Positionswerte), sodass intern im Drehgeber keine vollwertige zertifizierte Logik benötigt wird [39]. Aus diesem Grund ist der zusätzliche Rechenaufwand im Drehgeber im Vergleich zu nicht sicherheitsbezogenen Drehgebern gering [46]. Zusätzlich zu den sicherheitsbezogenen Positionssignalen wird ein Positionssignal mit hoher Auflösung und hoher Aktualisierungsrate für die Antriebsregelung im Servoregler erzeugt [46]. Die zwei Positionssignale für die sicherheitsbezogene Logik haben meist eine niedrigere Auflösung und eine geringere Aktualisierungsrate [46].

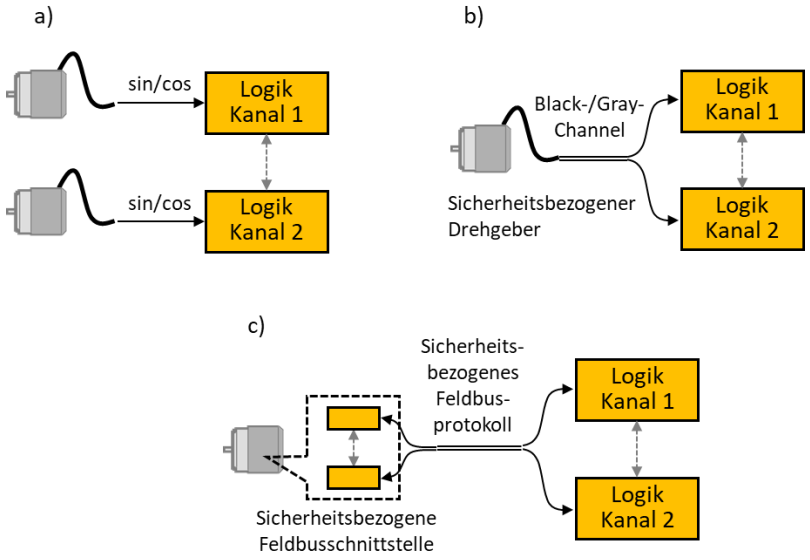


Abbildung 6: Einsatz von Drehgebern als Subsystem bei einer Kategorie-3-Architektur.

Eine dritte Möglichkeit für eine sicherheitsbezogene Positionsmessung ist die Verwendung eines Drehgebers mit integrierter sicherheitsbezogener Feldbusschnittstelle, wie in Abbildung 6c) dargestellt. Bei diesen Drehgebern werden die beiden unabhängig erzeugten Positionswerte, anders als bei den zuvor beschriebenen Drehgebern, bereits im Drehgeber plausibilisiert, sodass nur ein Positionswert über den Feldbus mit sicherheitsbezogenem Protokoll übertragen wird [39]. Aus diesem Grund sind solche Drehgeber mit einer vollwertigen zertifizierten Logik ausgestattet und es sind die Anforderungen an SRESW zu erfüllen, weshalb Drehgeber mit sicherheitsbezogener Feldbusschnittstelle teurer sind als die sicherheitsbezogenen Drehgeber mit externer Diagnose [39].

Im Servoregler können lediglich die Position und die Geschwindigkeit einer Achse überwacht und sicher begrenzt werden. Um dennoch eine sichere Bewegungsüberwachung einer gesamten Maschine mit mehreren Achsen zu realisieren, setzen Hersteller von Maschinen bzw. Servoreglern heute verschiedene Vorgehensweisen ein. Ein redundantes Positionssignal wird üblicherweise von einer zweikanaligen Logik im Antrieb ausgewertet. Das plausibilisierte sicherheitsbezogene Positionssignal kann über einen Feldbus mit sicherheitsbezogenem Protokoll an die Maschinensteuerung übertragen werden, um dort die Überwachung im dreidimensionalen Raum umzusetzen [87]. Dieser Zwischenschritt im Servoregler verursacht eine zusätzliche Zeitverzögerung des sicherheitsbezogenen Positionssignals [46] und hat einen negativen Einfluss auf die Abschaltzeit bei einer Grenzwertüberschreitung. Eine alternative Methode besteht darin, zusätzlich zu den Motor-Feedback-Systemen Drehgeber mit sicherheitsbezogenem Feldbusprotokoll einzusetzen, welche die Positionswerte direkt an die Maschinensteuerung übertragen. Dennoch ist weiterhin ein zweiter Drehgeber im System erforderlich, um ein Positionssignal für die Antriebsregelung bereitzustellen.

2.2.7 Mensch-Roboter-Kollaboration

Seit vielen Jahren werden Roboter in der Industrie für Produktionszwecke eingesetzt, um Aufgaben vom Menschen zu übernehmen. Dabei sind die Arbeitsbereiche von Menschen und Robotern auch heute üblicherweise räumlich getrennt. Diese Trennung wird entweder durch trennende Schutzeinrichtungen (z. B. Zäune) oder nichttrennende Schutzeinrichtungen (z. B. Lichtgitter) erreicht [88]. Sobald ein Mensch den Arbeitsbereich des Roboters betritt, wird dieser sofort angehalten und fährt erst nach dem Verlassen des Bereiches und nach einer Quittierung wieder an.

Bei der MRK arbeiten Roboter und Mensch zeitgleich in einem gemeinsamen Arbeitsbereich, um die Vorteile beider in den Herstellungsprozess zu integrieren und die Produktivität zu steigern [89]. Die Sicherheit wird bisher durch eine räumliche bzw. zeitliche Trennung der Arbeitsbereiche gewährleistet. Bei der Kollaboration ist auch ein Kontakt zwischen Mensch und Roboter möglich, weshalb auch Maßnahmen vom SRP/CS in Form von Geschwindigkeitsüberwachung und Kraftbegrenzung zu treffen sind [88]. Technische Spezifikationen und Sicherheitsanforderungen für solche kollaborierende Industrierobotersysteme werden in der DIN ISO/TS 15066 [90] festgelegt. Bei der Geschwindigkeitsüberwachung wird die Geschwindigkeit des Roboters entsprechend dem Abstand zum Menschen reduziert. Bei der Kraftbegrenzung wird die Kraft des Roboters reduziert, um sicherzustellen, dass keine schweren Verletzungen bei einer Kollision entstehen können [88]. Neben den klassischen Not-Aus- und Not-Halt-Funktionen sollte das SRP/CS für MRK nach [9] für eine sichere Bewegungsüberwachung über folgende Sicherheitsfunktionen verfügen:

- Sichere Überwachung und Begrenzung des Drehmoments bzw. der Kraft: Für die Umsetzung können entsprechende Kraft- und Drehmomentsensoren eingesetzt werden. Alternativ kann das Drehmoment über die Motorströme ermittelt werden.
- Sichere Überwachung und Begrenzung der Geschwindigkeit und sichere Überwachung der Position: Zur Messung der Geschwindigkeit und Position können sicherheitsbezogene Positionsmesssysteme eingesetzt werden.

Heutige kollaborierende Roboter (sogenannte Cobots) bestehen in der Regel aus einem oder zwei Armen mit mehreren Freiheitsgraden [89] und besitzen zusätzliche passive Schutzmaßnahmen wie gepolsterte Arme, um Verletzungen zu minimieren [9]. Außerdem sind Cobots heute bis zu viermal langsamer als herkömmliche Industrieroboter und können aufgrund ihrer dauerhaften Kraftbegrenzung deutlich weniger Gewicht heben [91]. Diese Eigenschaften wirken sich negativ auf die Einsatzmöglichkeiten und die Produktivität eines Cobots aus.

Bei FTFs und autonomen mobilen Robotern (AMR) zeichnet sich eine Entwicklung für den Einsatz als autonome Systeme für MRK ab. In der Vergangenheit waren FTFs spurgeführt (z. B. mit einer magnetischen Leitlinie) [92] und aufgrund ihres geringen Transportgewichtes und ihrer niedrigen Geschwindigkeit war keine aufwendige Sicherheitslösung integriert [93]. Außerdem wurde bei einer Objekterkennung auf dem Fahrweg direkt abgebremst. Heutige FTFs und AMRs zeichnen sich durch eine freie Navigation in ihrer Umgebung aus und verzichten dabei auf eine Spurführung. Dafür ist das FTF oder der AMR ebenfalls mit einer sicheren Bewegungsüberwachung auszustatten und es werden zusätzliche Sensoren benötigt (z. B. Laserscanner, Radarsensoren und Kamerasysteme), um Hindernisse in der Umgebung zu erkennen und rechtzeitig auszuweichen [94].

Typischerweise liegt die heutige Zykluszeit für die Kommunikation von sicherheitsbezogenen Daten über den Feldbus im Bereich von 10 ms oder mehr [60]. Für MRK sind diese Zykluszeiten nicht geeignet. Bei zu großen Zykluszeiten kann der Roboter gefahrbringende Kräfte oder Geschwindigkeiten entwickeln, bevor dieser entsprechend auf den Kontakt mit dem Menschen reagieren kann.

2.2.8 Sicherheitsbezogener Motion-Controller für eine sichere Bewegungsüberwachung

In [77] wird ein Konzept für einen sicherheitsbezogenen Motion-Controller zur sicheren Bewegungsüberwachungen von mehrachsigen Antriebsstrukturen vorgestellt. Die Sicherheits-SPS übernimmt dort die Aufgabe der sicherheitsbezogenen Logik nach DIN EN ISO 13849-1. Sensor und Aktor der Sicherheitsfunktionen befinden sich weiterhin im Antrieb. Die Eingangs- und Ausgangsdaten für die Sicherheitsfunktionen werden über ein sicherheitsbezogenes Feldbusprotokoll zwischen Steuerung und Antrieb ausgetauscht. Durch die zentrale Auswertung aller sicherheitsrelevanten Eingangsdaten wird eine siche-

re mehrachsige Bewegungsüberwachung für MRK ermöglicht. Für die zentrale Berechnung aller Sicherheitsfunktionen wird in der übergeordneten Steuerung allerdings eine hohe sicherheitsbezogene Rechenleistung benötigt. In [77] wird dafür eine Compound-SPS basierend auf einem Quad-Core-Prozessor vorgestellt. Auf einer Hardware können gleichzeitig sowohl die nicht sicherheitsbezogene Motorsteuerung der Antriebe als auch die Verarbeitung der sicherheitsrelevanten Algorithmen mit hoher Rechenleistung implementiert werden. Ein mehrachsiges System mit einem solchen sicherheitsbezogenen Motion-Controller nach [77] für eine zentrale Berechnung der Sicherheitsfunktionen ist in Abbildung 49 im Anhang dargestellt. Neben der zentralen Berechnung für die sichere Bewegungsüberwachung kann auch eine zentrale Diagnose der Sicherheitsfunktionen über die Sicherheits-SPS erfolgen. Dafür sind weitere Diagnoseinformationen aus den Antrieben nötig, welche ebenfalls über den sicherheitsbezogenen Feldbus zur Sicherheits-SPS übertragen werden können. Dieser Ansatz ermöglicht es, die Komplexität der sicherheitsbezogenen Architektur im Antrieb zu reduzieren und somit einen kosteneffizienten und kompakten Antrieb zu entwerfen, wie er in dieser Arbeit vorgestellt wird. Die Sicherheitsfunktionen können in der Sicherheits-SPS in Software frei konfigurierbar umgesetzt werden und somit Hardware im Antrieb ersetzen [77]. Durch die hohe Rechenleistung und die damit einhergehende schnelle Verarbeitung der sicherheitsbezogenen Anwendung kann eine kurze Zykluszeit von 1 ms für den sicherheitsbezogenen Feldbus erreicht werden.

2.2.9 Fehlertoleranz in der Maschinensicherheit

Bei den meisten Antrieben, die für die funktionale Sicherheit verwendet werden, geht der sichere Zustand heute mit dem Abschalten der Energie einher. Somit kann die Maschine keine Kraft mehr erzeugen. Durch das Stoppen und Abschalten der Energie der Maschine entsteht jedoch jedes Mal ein ungewollter Maschinenstillstand, der wiederum zu einem ungewollten Produktionsstopp führen kann. Da aber eine hohe Verfügbarkeit und Produktivität der Maschine gefordert sind, sind Alternativen zum sofortigen Abschalten einer Maschine erforderlich, ohne dabei den Schutz von Personen und Anlage zu vernachlässigen. Dazu hat der Zentralverband Elektrotechnik und Elektronikindustrie e.V. (ZVEI) ein Whitepaper [12] veröffentlicht, um eine Alternative zum sofortigen Abschalten vorzustellen.

Wenn ein Antrieb eine Fehlertoleranz aufweist, kann die Funktion des Antriebs weiterhin aufrechterhalten werden, auch wenn Ausfälle bestimmter Komponenten oder Fehlerfälle in Sicherheitsfunktionen bereits erkannt wurden. In diesem sogenannten degradierten Betrieb kann der Antrieb weiterhin betrieben werden, obwohl ein Fehler in einer Sicherheitsfunktion aufgetreten ist. Im degradierten Betrieb ist es möglich, einen laufenden Produktionsschritt trotz eines Fehlerfalls zu beenden, ohne dabei einen Produktionsstopp der

ganzen Anlage auszulösen. Zusätzlich zu der Fehlertoleranz des Antriebs ist aber auch eine Bewertung der Fehler erforderlich. In Abhängigkeit des Fehlers wird entschieden, ob ein degradierter Betrieb überhaupt möglich ist oder ob ein sofortiges Stoppen der Maschine erforderlich ist. Ein nicht tolerierbarer Fehler ist beispielsweise der Ausfall des FPGAs oder µCs im Antrieb, da ohne Steuerelektronik kein Betrieb mehr möglich ist. Ein tolerierbarer Fehler dagegen ist zum Beispiel der Ausfall eines Kanals der Sicherheitsfunktion STO bei einer Kategorie-3-Architektur. Die Bewertung der Fehler wird durch einen Entscheider getroffen, der den Antrieb entweder in den degradierten Zustand versetzt oder in den abgeschalteten sicheren Zustand überführt. Um diese Bewertung durchführen zu können, ist eine hinreichende Diagnose des Antriebssystems erforderlich. In [95] wird diese qualifizierte Diagnose als Diagnose^{+} bezeichnet. [12]

In Teil 2 des Whitepapers [95] werden die Anforderungen an die sicherheitsbezogene Logik für den degradierten Betrieb detaillierter spezifiziert. Diese übernimmt die Rolle des Entscheiders und kann anhand der Diagnoseinformationen entweder den degradierten Zustand oder den sicheren Zustand aktivieren. Der Entscheider besitzt dabei mindestens das gleiche PL wie die Sicherheitsfunktion.

3 Hoch-performante Regelungsarchitektur

In diesem Kapitel wird eine hoch-performante Regelungsarchitektur für Servoantriebe vorgestellt. Der Steuerteil des Servoreglers wird dabei aufgrund der genannten Vorteile aus einer Kombination von µC und FPGA bestehen. Es soll eine kostengünstige Architektur entstehen, basierend auf einem Standard-µC und einem Standard-FPGA, die ohne Probleme durch andere Produkte ggf. von anderen Herstellern ersetzt werden können. Außerdem wird eine kaskadenförmige Regelkreisstruktur mit der FOC verwendet.

3.1 Struktur des Antriebs

Die Struktur der Steuerelektronik im Antrieb besteht aus zwei Logikeinheiten, einem FPGA und einem µC. Die Logikeinheiten haben Eingangs- und Ausgangssignale, um mit der Peripherie zu kommunizieren. Für die Kommunikation zwischen dem FPGA und dem µC wird eine serielle Schnittstelle verwendet. Die serielle Peripherieschnittstelle (engl.: serial peripheral interface, SPI) ist eine weitverbreitete serielle Kommunikationsschnittstelle nach dem Master-Slave-Prinzip. Für eine synchrone Kommunikation gibt es einen seriellen Takt, ein MISO-Signal (Master In Slave Out) und ein MOSI-Signal (Master Out Slave In). Durch diese zwei Datenleitungen ist die SPI vollduplexfähig. Bei einer Octo-SPI stehen acht statt zwei Datenleitungen zur Verfügung. Jedoch kann hier zu einem Zeitpunkt nur lesend oder schreibend zugegriffen werden. Daher ist die Octo-SPI nur halbduplexfähig. Die Kommunikation kann nur vom Master gestartet werden. Für einen effizienten Datenaustausch zwischen dem FPGA und dem µC im Antriebssystem wird eine Octo-SPI verwendet. Mit geeigneten ICs und einem entsprechenden Layout sind hohe Taktfrequenzen möglich. Bei Flash-Speichern beispielsweise sind mehr als 100 MHz typisch [96]. Für die Octo-SPI werden nur elf Signale bzw. Leiterbahnen zwischen µC und FPGA benötigt, deutlich weniger als ein paralleles Bussystem mit seinem Adressbus, Datenbus und Steuersignalen [21].

Der µC wird mit einem Octo-SPI-Master ausgestattet. Für das FPGA wird der Slave in VHDL implementiert. Wenn der SPI-Master mit direktem Speicherzugriff (engl.: direct memory access, DMA) kombiniert wird, ist der µC während der Datenübertragung für andere Aufgaben verfügbar. Wird ein µC mit On-Chip-Speicher eingesetzt, ergibt sich annähernd eine Zwei-Chip-Lösung für den Steuerteil des Antriebs. Ein DMA-Datentransfer zum und vom On-Chip-Speicher des µCs ermöglicht dem Prozessor den Zugriff auf die Prozessdaten für die Motorsteuerung. [21]

3.2 Feldorientierte Regelung

Abbildung 7 zeigt das Blockschaltbild der FOC. Die violette vertikale Linie symbolisiert die Octo-SPI als Signalschnittstelle, welche den µC von dem FPGA trennt. In den meisten Servoanwendungen wird keine Entkopplung (Blau in Abbildung 7) und insbesondere keine Vorsteuerung der Polradspannung (Grün in Abbildung 7) verwendet [21].

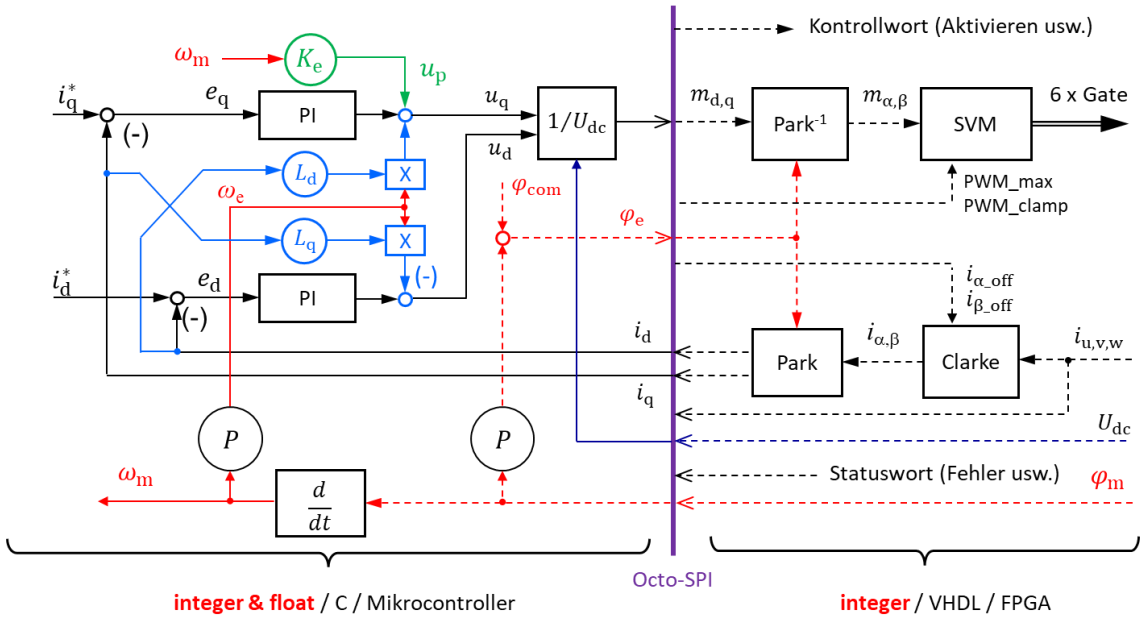


Abbildung 7: Aufteilung der feldorientierten Motorregelungsstruktur im Steuerteil des Antriebs.

Besonders auf der linken Seite des Blockschaltbilds ist die Flexibilität eines µCs mit einer Fließkommaeinheit (engl.: floating-point unit, FPU) nützlich, um alternative Regelungsstrukturen zu implementieren. Üblicherweise sind die zyklisch abgetasteten Stromsignale $i_{u,v,w}$ und die PWM-Stellsignale $m_{d,q}$ 16-Bit ganzzahlige Signale (short integer). Das Gebersignal φ_m wird als hochauflösendes ganzzahliges Wort bereitgestellt. Bei dem digitalen Drehgeber-Protokoll EnDat 3 werden bis zu 48 Bit Auflösung erreicht [40].

Um unerwünschte Verzögerungszeiten zu minimieren, werden alle zyklischen Prozessdaten mit einem Octo-SPI-Lese-Burst vom FPGA zum µC und einem Schreib-Burst in umgekehrter Richtung übertragen. Bei einem Burst-Modus wird der Lese- bzw. Schreibvorgang beschleunigt, indem mehrere Datenpakete hintereinander übertragen werden und die Adresse automatisch hochgezählt wird, ohne zusätzliche Befehle zu übertragen [96]. Für den µC werden die Prozessdaten in organisierten Lese- und Schreibstrukturen abgelegt. Im FPGA kann der Octo-SPI-Slave beispielsweise als Avalon®-Master konfiguriert werden, sodass über die Avalon®-Schnittstelle die Daten innerhalb des FPGAs direkt in die entsprechenden Register geschrieben bzw. aus den Registern gelesen werden können [97].

Die Verwendung von Fließkommasignalen für Regelungsalgorithmen ist von großem Vorteil. Bei geeigneter Skalierung in SI-Einheiten werden Ströme direkt in Ampere und Spannungen in Volt angegeben. Auf diese Weise werden auch die Regelkreisverstärkungen sofort in SI-Einheiten angegeben. Die Einheit der proportionalen Verstärkung des Stromregelkreises wird somit zu V/A. Bei Fließkommasignalen gibt es keine Probleme mit Überläufen oder Rundungsfehlern und auch die Integration von modellbasierten Algorithmen ist problemlos möglich.

Im Allgemeinen ist es für kostengünstige Lösungen vorteilhaft, nur ganzzahlige (integer) Mathematik in einem FPGA zu verwenden und für µCs, die eine FPU enthalten, auch Fließkommasignale zu nutzen. Eine FPGA-Implementierung von Algorithmen ist in der Regel schneller aufgrund ihrer Fähigkeit, Vorgänge parallel zu verarbeiten, während eine prozessorbasierte Implementierung viel flexibler ist. Aus diesem Grund werden die Clarke- und Park-Transformationen in VHDL mit ganzzahliger Mathematik im FPGA realisiert. Da die gemessenen Stromsignale bei Verwendung eines ΣΔ-Modulators mit anschließendem Sinc³-Dezimierungsfilter nur eine Genauigkeit von bis zu maximal 16 Bit erreichen [35], ist es nicht sinnvoll, diese Algorithmen mit Fließkomma-Mathematik zu berechnen. Die Offsetkompensation der ADCs kann ebenfalls mit den Berechnungen im FPGA durchgeführt werden. Das FPGA stellt dem µC die feldorientierten Stromsignale i_d und i_q als skalierte ganzzahlige 16-Bit Signale zur Weiterverarbeitung zur Verfügung. Systematische Verstärkungsfehler der ADCs können zusammen mit der Skalierung auf ein Fließkommasignal in Ampere ohne zusätzlichen Rechenaufwand vom µC berücksichtigt werden. Ähnliche Überlegungen gelten für die inverse Park-Transformation und die SVM. Die SVM ist in VHDL implementiert und kann mit geringem Rechenaufwand wie in [30] umgesetzt werden. Das Trägersignal für die SVM kann auf einen externen Takt eines Feldbusses synchronisiert werden. Außerdem kann eine kurzzeitige diskontinuierliche SVM realisiert werden. Die Dauer dieses „Klemmens“ (engl.: clamping) der drei Motorphasen bei einem hohen Modulationsgrad an die positive oder negative Zwischenkreisspannung, um Schaltverluste zu reduzieren, kann dabei eingestellt werden. Der µC gibt die mit der Zwischenkreisspannung U_dc skalierten Modulationsindizes m_d und m_q als ganzzahlige 16-Bit Signale an das FPGA weiter.

Zusätzlich werden noch Kontroll- und Statusinformationen zwischen dem FPGA und dem µC ausgetauscht, um beispielsweise Befehle zum Aktivieren der PWM oder Rückmeldungen über Fehler wie Überstrom oder Überspannung zu übergeben. Der elektrische Winkel φ_e für die Park-Transformation wird auf Grundlage des mechanischen Winkels, der Polpaarzahl des Motors und des Kommutierungsoffsets im µC berechnet.

3.3 Ablauf der trägerbasierten Abtastregelung

Abbildung 8 zeigt typische Rechenzeiten bei einer trägerbasierten Abtastregelung mit 8 kHz Schaltfrequenz. Die Rechenzeit des µCs ist abhängig von der Anwendung und der Leistungsfähigkeit des eingesetzten Prozessors. Die dargestellten Rechenzeiten dienen daher lediglich der Veranschaulichung. Gleiches gilt für die Rechenzeit der Sinc-Filter, welche abhängig von den Einstellungen der Filter ist, sowie für die herstellerspezifische Zeit für die Bereitstellung der digitalen Position des Drehgebers.

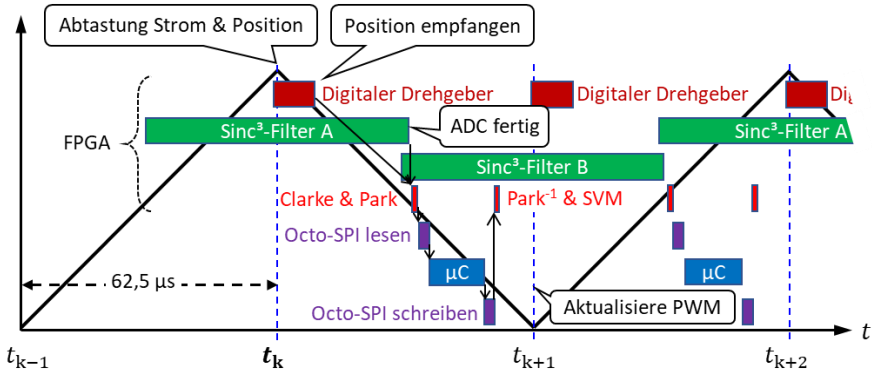


Abbildung 8: Typisches Verarbeitungsschema der trägerbasierten Abtastregelung bei 8 kHz Schaltfrequenz.

Clarke-Transformation, Park-Transformation, Inverse Park-Transformation und SVM können in deutlich weniger als einer Mikrosekunde vom FPGA verarbeitet werden. An jeder Ecke des 8-kHz-Trägersignals werden die Position und die Ströme abgetastet. Für die Strommessung werden ΣΔ-Modulatoren mit anschließenden Sinc³-Dezimierungsfiltern verwendet. Die Sinc³-Filter benötigen 64 µs Rechenzeit bei einem Überabtastungsfaktor (engl.: over sampling ratio, OSR) von 256 und einer ΣΔ-Modulationsfrequenz von 12 MHz. Da dies mehr als die Regelzykluszeit von 62,5 µs ist, sind zwei parallele Sinc³-Filter (A und B) implementiert, wie in Abbildung 8 dargestellt. Das gespeicherte Positionssignal (engl.: latch) wird beispielsweise bei EnDat 3 ca. 10 µs nach der Anfrage zum Abtastzeitpunkt empfangen. Sobald die Strom- und Positionssignale vorhanden sind, wird ein Interrupt ausgelöst, der den Regelalgorithmus im µC startet. Der µC liest die aktuellen Strom- und Positionssignale über die Octo-SPI ein. Anschließend berechnet der µC die Regelalgorithmen und schreibt über die Octo-SPI die neuen Modulationsindizes für die SVM in das FPGA. Mit dem Burst-Modus beim Lese- und Schreibzugriff über die Octo-SPI werden nur wenige Mikrosekunden benötigt. Die drei neuen PWM-Schwellenwerte werden wieder an den Ecken des Trägersignals aktualisiert. Somit haben die abgetasteten Positions- und Stromdaten zum Zeitpunkt t_k direkten Einfluss auf die Schwellwerte zum nächsten Abtastzeitpunkt t_{k+1} und es kann sowohl die steigende als auch die fallende Schaltflanke beeinflusst werden.

Die vorgestellte Architektur für die Antriebsregelung ist in der Lage, PI-Regelkreise für die FOC unter Verwendung von Fließkomma-Mathematik mit hohen Aktualisierungsraten von bis zu 50 kHz im Stromregelkreis zu berechnen. Es sind auch komplexere Regelungsverfahren wie prädiktive Algorithmen möglich, die jedoch mehr Rechenzeit oder einen schnelleren Prozessor erfordern. Für erweiterte Funktionalitäten der Antriebsstruktur können von Herstellern vorgefertigte kundenbasierte Blöcke mit geistigem Eigentum (engl.: intellectual property cores, IP-Cores) verwendet werden.

3.4 Kaskaden-Regelkreisstruktur

Typischerweise werden Servoregler in einer kaskadierten Regelstruktur aufgebaut, in der der innerste Regelkreis das Drehmoment bzw. den Strom, der zweite Regelkreis die Drehzahl und der äußere Regelkreis die Position regelt. Für eine hoch-performante Regelungsarchitektur wird die Kaskaden-Regelkreisstruktur um einen Smith-Prädiktor, einen Drehzahl-Beobachter und eine Vorsteuerung erweitert, wie in Abbildung 9 dargestellt.

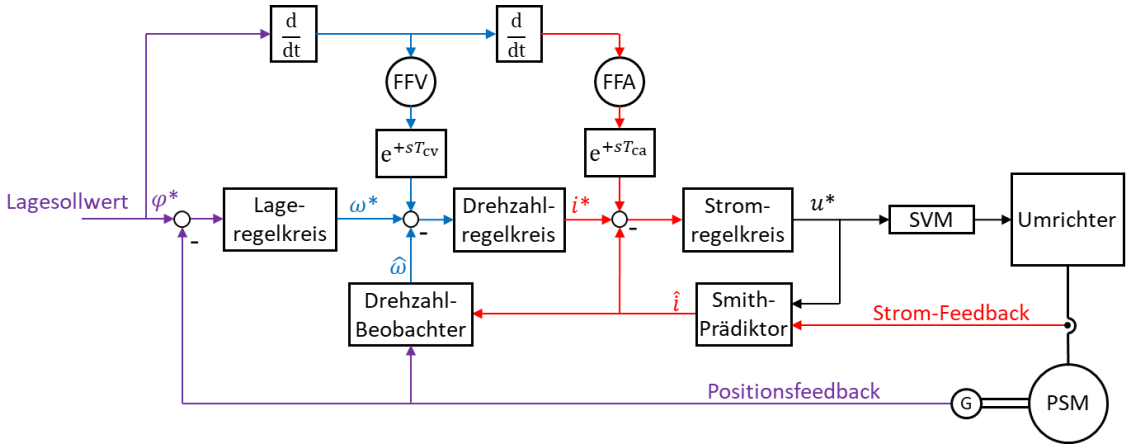


Abbildung 9: Kaskadenregelung des Servoantriebs mit Drehzahl-Beobachter, Smith-Prädiktor und Vorsteuersignalen.

Der Stromregelkreis ist der innerste Regelkreis und arbeitet mit einer Zykluszeit von 62,5 µs. Dieser ist wie in [25] mit einem Smith-Prädiktor ausgestattet, um die systembedingte Totzeit eines abgetasteten Stromistwertes zu kompensieren. Dadurch wird eine höhere Phasenreserve erreicht und es kann eine größere Proportionalverstärkung des Stromregelkreises eingestellt werden, was wiederum die Dynamik des Systems verbessert [98]. Üblicherweise werden für den Stromregelkreis zwei PI-Regler verwendet. Zur Strommessung können drei Open-Loop Hallsensoren in Verbindung mit ΣΔ-Modulatoren 2. Ordnung und Sinc³-Dezimierungsfiltern eingesetzt werden [36].

Der PI-Drehzahlregler ist dem Stromregelkreis überlagert. Das Positionsfeedback des Motors wird zur Erzeugung eines Drehzahlsignals verwendet. Aufgrund der Auflösung und der elastischen Befestigung des Drehgebers an der Motorwelle kann die Drehzahl jedoch nur näherungsweise über das Positionsfeedback bestimmt werden. Zusätzlich ent-

stehen durch die Abtastung des Positionswertes und die numerische Differentiation zur Berechnung der Drehzahl eine Phasenverschiebung bzw. Totzeit. Um dieser Problematik entgegenzuwirken, wird ein Drehzahl-Beobachter nach [99] eingesetzt, wodurch die Performanz des Servoantriebs erhöht wird.

Der äußere Lageregelkreis verwendet einen gewöhnlichen P-Regler. Um die Performanz des Systems zu erhöhen, werden eine Geschwindigkeitsvorsteuerung (engl.: feed-forward velocity, FFV) und eine Beschleunigungsvorsteuerung (engl.: feed-forward acceleration, FFA) verwendet. Abbildung 9 zeigt, dass eine einfache Ableitung der Position nach der Zeit zu einer FFV und eine doppelte Ableitung zu einer FFA führt, welche proportional zum Drehmoment bzw. Strom ist. Diese Signale werden zur Bildung der Regler-Sollwerte verwendet und wirken somit beschleunigend auf die Regelkreise. Über die Parameter FFV und FFA kann die Verstärkung der jeweiligen Vorsteuersignale eingestellt werden. Mit den Kompensationszeiten T_{cv} und T_{ca} können die Vorsteuersignale um bestimmte Zeiten voreilend eingestellt und damit die Vorsteuersollwerte gezielt beeinflusst werden [32].

3.5 Generierung der Positionssollwerte und Vorsteuersignale mit einer Interpolation

Um die reale Leistungsfähigkeit des vorgestellten Antriebs zu ermitteln, wird der Antrieb als abgeschlossenes Teilsystem betrachtet und die Bandbreite des Lageregelkreises untersucht. Dazu hat sich in der Praxis das Bode-Diagramm als nützlich erwiesen, welches den Frequenzgang eines Systems darstellt. In Abbildung 10 werden dafür sinusförmige Positionssollwerte x_{k}^{*} erzeugt und zyklisch vorgegeben (zyklische synchrone Lageregelung, engl.: cyclic synchronous position, CSP). Dies entspricht einem Motorwinkel-Sollwert φ_{k}^{*} für den Lageregelkreis.

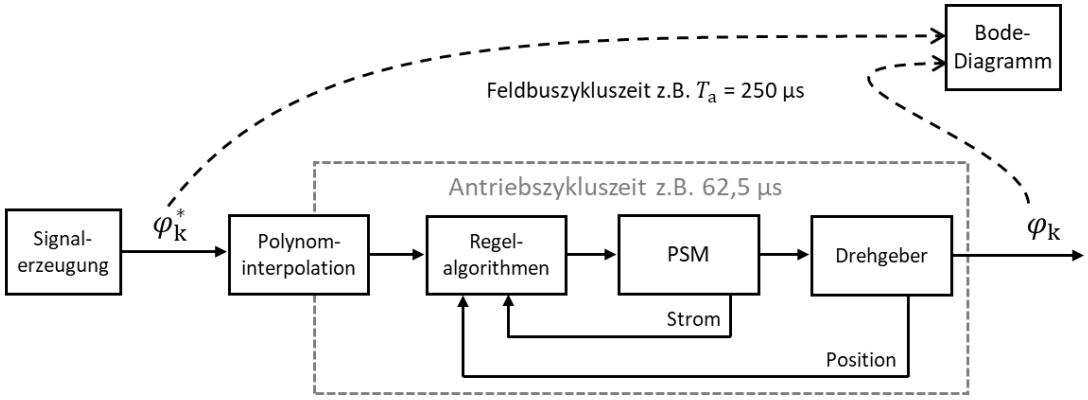


Abbildung 10: Messung der Bandbreite des Lageregelkreises mit Polynominterpolation als Teilsystem.

Der Block „Regelalgorithmen“ in Abbildung 10 ist als kaskadierte Regelkreisstruktur ausgelegt und wird mit 62,5 µs aktualisiert. Die Polynominterpolation im µC erzeugt aus

dem Positionssollwert, der mit der Zykluszeit des Feldbusses bereitgestellt wird, einen Lageregler-Sollwert für den Antrieb mit der entsprechenden Antriebszykluszeit. Für die Messung des Positionsistwertes für das Bode-Diagramm wird ein Drehgeber verwendet. Die PWM im Antrieb wird für die weitere Betrachtung auf 8 kHz festgelegt. Die zyklischen synchronen Positionssollwerte werden vom Motion-Controller so erzeugt, dass sie mindestens dreimal differenzierbar sind. Physikalisch entspricht dies den zugehörigen Verläufen von Geschwindigkeit, Beschleunigung und Ruck. Der berechnete Positionssollwert x_{k}^{*} wird zyklisch und digital als abgetastetes Signal übertragen. Die Zykluszeit definiert die mögliche Signalbandbreite. Typisch sind $T_{\mathrm{a}} = 250\ \mu s$ für hochdynamische CNC-Maschinen und 1 ms für Robotik-Anwendungen. Wird für die Übertragung des Positionssollwertes über den Feldbus eine Datenwortbreite von mindestens 48 Bit für eine ganzzahlige Darstellung oder eine 64-Bit-Fließkommadarstellung gewählt, ist das Quantisierungsrauschen vernachlässigbar.

Abbildung 11 zeigt, wie ein Polynom 3. Ordnung für die Feininterpolation zwischen den letzten vier übertragenen Positionssollwerten verwendet wird.

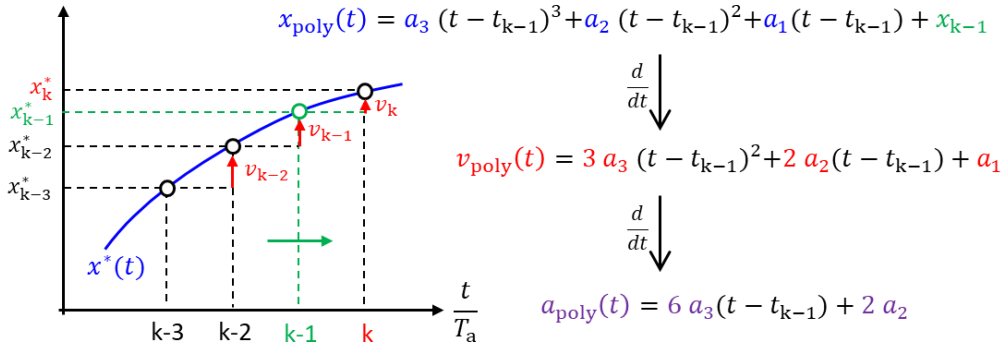


Abbildung 11: Polynom 3. Ordnung durch die letzten vier Positionssollwerte: $x_{\mathrm{k-3}}^{*}$ ... x_{k}^{*}.

Dieses Polynom kann ebenso wie der vom Motion-Controller erzeugte Sollverlauf dreimal differenziert werden. Damit können die Koeffizienten des Polynoms mit minimalem Aufwand auch zur Berechnung feininterpolierter Vorsteuersignale für Geschwindigkeit und Beschleunigung verwendet werden [100]. Basiert der generierte Sollwertverlauf ebenfalls auf einem Polynom maximal 3. Ordnung, funktioniert die Interpolation fehlerfrei und auch die aus dem Sollwertverlauf berechneten Ableitungen sind exakt.

Abbildung 12 zeigt die schematische Darstellung zur Erzeugung des Positionssollwertes und der Vorsteuersignale für den Antrieb durch Interpolation aus dem Positionsverlauf der übergeordneten Steuerung. Bei der Interpolation können die Kompensationszeiten T_{cv} und T_{ca} gewählt werden. Wie in Abbildung 12 dargestellt, wird das Differenzsignal v_{k} im Antrieb mit der Aktualisierungsrate des Feldbusses gebildet. Diese Positionsdifferenzsignale der letzten drei Zyklen, zusammengefasst als Vektor V_{k}, sind die Eingangsgrößen für ein Intervall der Feininterpolation. Für eine Feininterpolation wird dieser Vektor V_{k} (kon-

stant innerhalb eines Feininterpolationsintervalls) mit einer Matrix multipliziert. Der Interpolationsindex i kann in einem Bereich zwischen 0 und N-1 liegen, wobei N der Interpolationsfaktor ist und das Verhältnis zwischen der Bus- und der Regelkreiszykluszeit des Antriebs angibt. Für 250 µs CNC-Zykluszeit und 62,5 µs Regelkreiszykluszeit ist N = 4. Der in Abbildung 12 gezeigte Feininterpolationsblock beinhaltet diese Multiplikation des Vektors V_k mit der i-ten Matrix. Die so ermittelten Signale für Geschwindigkeit v_ki und Beschleunigung a_ki können direkt als Vorsteuersignale verwendet werden. Die Summe der Signale Δx_ki und x_k^* wird mit voller Datenwortbreite berechnet, um den feininterpolierten Positionssollwert x_ki zu erhalten. Die genaue Berechnung der Feininterpolation ist in [21] beschrieben.

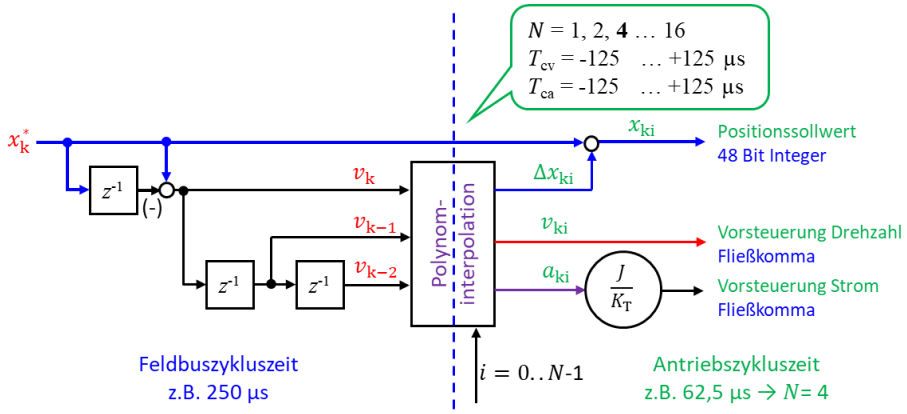


Abbildung 12: Blockschaltbild der Feininterpolation.

Für jeden Interpolationsschritt wird eine Matrix mit ihren neun konstanten Koeffizienten verwendet. Diese Matrizen können im Voraus während des Programmstarts offline berechnet werden, um Rechenzeit zu sparen.

Wenn die Trajektorie $x^*(t)$ nicht ein Polynom von maximal 3. Ordnung ist, können Interpolationsfehler auftreten. Dies ist bei einem sinusförmigen Verlauf der Fall, wie er für das Bode-Diagramm verwendet wird. Die daraus resultierenden Abweichungen für das Bode-Diagramm werden ebenfalls in [21] dargelegt.

Durch die hier erläuterte Vorgehensweise zeigt das Bode-Diagramm die Leistungsfähigkeit des realen Antriebssystems, wie es in der Anwendung zum Einsatz kommt. Zusätzlich zum Lageregelkreis wird die Vorgabe des Positionssollwerts mit der Feldbuszykluszeit sowie die Interpolation dieses Sollwerts für die Antriebszykluszeit berücksichtigt. Eine Validierung der Leistungsfähigkeit der vorgestellten Antriebsarchitektur wird in Kapitel 5 durchgeführt.

3.6 Feldbuskommunikation mit dem Motion-Controller

Die Anforderungen für einen Feldbus in der Automatisierungstechnik umfassen eine harte Echtzeitfähigkeit mit deterministischen Antwortzeiten. In der Regel sind viele Teilnehmer vorhanden, wobei jeder Teilnehmer nur wenige zyklische Prozessdaten besitzt [101]. Dies trifft auch auf mehrachsige Motion-Control-Anwendungen zu. Ebenfalls spielt dort die Synchronisation der Antriebe mit dem Motion-Controller eine wichtige Rolle, damit die Antriebe, die vom Motion-Controller erzeugten abgetasteten Sollwerte synchron verarbeiten können und die gewünschte Trajektorie entsteht. Zur Synchronisation der Feldbus-Teilnehmer gibt es unterschiedliche Verfahren. EtherCAT beispielsweise basiert auf dem Mechanismus der verteilten Uhren (engl.: distributed clock, DC) [101].

Um auch die Prozessdaten der Antriebsregelung, wie den Positionsistwert oder Stromistwert, synchron abzutasten und über den Feldbus dem Motion-Controller bereitzustellen, wird das PWM-Trägersignal ebenfalls zum Feldbus synchronisiert. Dafür kann in der Steuerelektronik des Antriebs ein Algorithmus ähnlich einer Phasenregelschleife (engl.: phase locked loop, PLL) implementiert werden. Abbildung 13 zeigt die Synchronisation des PWM-Trägersignals im FPGA des Antriebs auf den Feldbus. Der SPS-Task wird zyklisch z. B. jede 250 µs ausgeführt. Am Ende der Task werden die Ausgangsdaten in den Ausgangspuffer geschrieben. Der Feldbus sendet die Ausgangsdaten an den Antrieb, liest die Eingangsdaten zurück und schreibt diese in den Eingangspuffer. Im nächsten SPS-Task werden die Eingangsdaten von dort eingelesen und verarbeitet. Im µC des Antriebs ist ein Zähler mit der Antriebszykluszeit von z. B. 62,5 µs implementiert, welcher auf den Synchronisationsmechanismus des Feldbusses synchronisiert wird. Anhand dieses Zählers wird auch der Startzeitpunkt der Interrupt Service Routine (ISR) im µC festgelegt, in der auch die Regelalgorithmen berechnet und das Lesen und Schreiben über die Octo-SPI ausgeführt werden. Um den entstehenden Jitter bei der Feldbusübertragung zu kompensieren, werden die Ausgangsdaten nicht direkt mit der ersten ISR aus dem Feldbus-Slave ausgelesen. Der Feldbus-Slave kann ebenfalls im µC des Antriebs integriert werden. Mit den nächsten vier ISRs werden auf Basis des empfangenen Positionssollwertes die interpolierten Positionssollwerte berechnet und von den Regelkreisen verarbeitet. Die entsprechenden Modulationindizes werden über die Octo-SPI an das FPGA gesendet und dort von der SVM für die Ansteuerung der Leistungshalbleiter genutzt. Das PWM-Trägersignal im FPGA wird dabei über die Octo-SPI mit Hilfe eines PLL-Algorithmus auf den Zähler im µC synchronisiert. Der im FPGA zum Synchronisationsmechanismus abgetastete Positionsistwert wird mit der nächsten ISR über die Octo-SPI vom µC eingelesen und an den Feldbus-Slave übergeben. Mit dem nächsten Feldbus-Frame wird dieser zur SPS übertragen und kann in dem nächsten SPS-Task verarbeitet werden. Beim Ausfall der Feldbus-Verbindung kann sich der µC zwar nicht mehr auf den Feldbus synchro-

nisieren, aber dennoch bleiben der µC und das FPGA synchronisiert und die Algorithmen im µC und FPGA können weiterhin ordnungsgemäß ausgeführt werden.

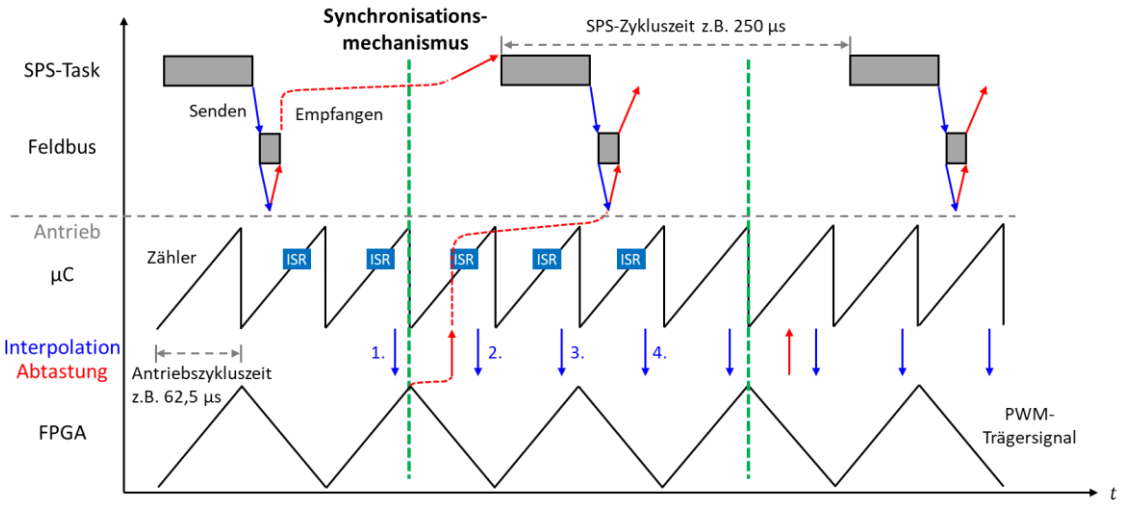


Abbildung 13: Synchronisation des PWM-Trägersignals im FPGA des Antriebs auf den Feldbus.

Verschiedene Hersteller bieten Kommunikationsprotokolle an, um den in der Automatisierungstechnik gängigen CANopen-Standard mit Objektverzeichnis und Mapping von Prozessdatenobjekten (PDO) und Servicedatenobjekten (SDO) nutzen zu können. Dadurch kann auch das für Antriebe und Motion-Control spezifizierte Geräteprofil „CAN in Automation“ (CiA) 402 verwendet werden.

Der Feldbus soll auch für eine zentrale Fehlerdiagnose und Inbetriebnahme über die SPS genutzt werden, sodass für das vorgestellte Konzept im Antrieb keine zusätzlichen teuren Schnittstellen und Fehlerspeicher mehr verbaut sind. Ebenso kann anstelle eines steckbaren Speichermoduls für die optimal eingestellten Parameter der Antriebsregelung der Feldbus für die Übertragung der Parameter bei einem Neustart oder Austausch des Antriebs verwendet werden. Dafür gibt es beispielsweise die in der Entwicklungsumgebung CODESYS Development System bereitgestellte Startparameter-Liste. In dieser Liste können alle notwendigen Parameter gespeichert und beim Hochfahren des Antriebs an diesen übermittelt werden. Diese Liste kann exportiert und importiert werden, sodass alle Parameter jederzeit zentral in der Steuerung abgerufen und gespeichert werden können.

4 Sicherheitsbezogene Antriebsstruktur

In diesem Kapitel wird ein Konzept für eine sicherheitsbezogene Antriebsstruktur für die kollaborierende Automatisierung mit AMRs oder FTFs vorgestellt. Die antriebsinternen Sicherheitsfunktionen werden über einen sicherheitsbezogenen Feldbus angesteuert und reduzieren sich auf STO, sichere Bremsansteuerung (engl.: safe brake control, SBC) und optional sicherer Stopp 1 (engl.: safe stop 1, SS1) für ein sicheres Stillsetzen des Motors. Das Konzept nutzt für den Großteil der antriebsinternen Sicherheitsfunktionen bereits vorhandene Strukturen des Antriebs, sodass der zusätzliche Aufwand und die Kosten gering sind. Die Auswertung aller Eingangssignale für die sichere Bewegungsüberwachung erfolgt in einer übergeordneten Sicherheits-SPS. Die Strom- und Positions-SPDUs der Antriebe werden über einen sicherheitsbezogenen Feldbus nach dem Black-/Gray-Channel-Prinzip an die Sicherheits-SPS übertragen. Ähnlich wie bei sicherheitsbezogenen Drehgebern basiert das Konzept darauf, dass ein Großteil der Diagnose vom Antrieb extern in der übergeordneten Sicherheits-SPS erfolgt. Dadurch wird keine vollständig zertifizierte sicherheitsbezogene Logik im Antrieb benötigt. In Kombination mit einer diversitären redundanten Architektur können kostengünstige Standardkomponenten anstelle von teureren sicherheitszertifizierten Komponenten eingesetzt werden. Dieser Ansatz ermöglicht eine größere Freiheit beim Austausch von Komponenten, ohne die funktionale Sicherheit des Systems zu beeinträchtigen [11].

4.1 Aufbau der Steuerelektronik

Abbildung 14a) zeigt eine typische Hardware-Struktur für eine Motorregelung bestehend aus einem FPGA und einem µC. Für die komplexeren Sicherheitsfunktionen nach IEC 61800-5-2 und die sicherheitsbezogene Feldbusschnittstelle werden zwei zusätzliche getrennte µCs als lokale sicherheitsbezogene Logik im Antrieb für Kategorie 3 eingesetzt. Als Testmechanismus zur Fehleraufdeckung wird zyklisch ein Kreuzvergleich zwischen den beiden sicherheitsbezogenen Kanälen durchgeführt. Abbildung 14b) zeigt den alternativen Ansatz der Steuerelektronik für die sicherheitsbezogene Antriebsstruktur. Da die sicherheitsbezogenen µCs in der Regel nicht die höchste Rechenleistung benötigen, wird bei diesem Konzept ein Teil der Algorithmen dieser beiden µCs von dem ursprünglich nicht sicherheitsbezogenen µC und dem nicht sicherheitsbezogenen FPGA übernommen. Diese Struktur, die zwei zusätzliche µCs für den sicherheitsbezogenen Teil des Antriebs einspart, erfordert keine zusätzliche Entwicklungsumgebung [60] und führt zu einer diversitären Redundanz durch die verschiedenen Komponenten und die unterschiedliche Embedded-Programmierung in „C“ und „VHDL“. Durch den Wegfall der beiden µCs ergibt sich eine Platz- und Kostenersparnis.

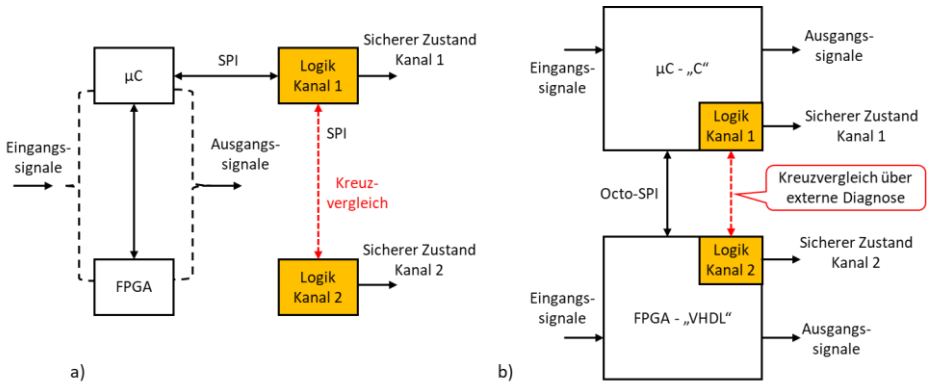


Abbildung 14: Aufbau der Steuerelektronik für eine sicherheitsbezogene Antriebsstruktur: a) klassischer Ansatz mit zwei zusätzlichen µCs, b) diversitäre redundante Struktur mit nur einem Standard-µC und einem Standard-FPGA.

Wie bei den sicherheitsbezogenen Drehgebern wird der Großteil der Diagnose des Antriebs von einer übergeordneten sicherheitsbezogenen Logik durchgeführt. Bestimmte Diagnosemaßnahmen zur Fehleraufdeckung, wie die Überwachung von Temperatur, Spannung und Takt, können jedoch nicht vollständig extern durchgeführt werden und sind daher teilweise im Antrieb zu implementieren. Die übergeordnete Logik kann eine Sicherheits-SPS mit einer sicherheitsbezogenen Feldbusschnittstelle wie FSoE/EtherCAT oder PROFIsafe/PROFINET sein. Durch die diversitäre redundante Kategorie-3-Architektur kann mit Standardkomponenten maximal PL d erreicht werden, ohne dass die Anforderungen an SRESW, wie beispielsweise die Rückwirkungsfreiheit in einem gemischt-kritischen System (System mit sicherheitsbezogenen und nicht sicherheitsbezogenen Komponenten), zwingend zu erfüllen sind. Dennoch sind geeignete Maßnahmen zur Fehlererkennung und Fehlerreaktion zu treffen, um systematische Ausfälle frühzeitig zu erkennen. Dadurch entsteht eine redundante Struktur mit Standardkomponenten und ausreichendem DC, ähnlich wie bei der festverdrahteten Lösung mit Not-Halt-Schalter und Schützen.

Abbildung 15 zeigt eine vereinfachte zweikanalige Struktur für Sicherheitsfunktionen, bestehend aus drei Subsystemen, vergleichbar mit einer Kategorie-3-Architektur nach DIN EN ISO 13849-1. Für eine sichere Bewegungsüberwachung kann als Eingang bzw. Sensor eine Positionsmessung oder eine Strommessung dienen. Die Übertragung der Drehgeber- oder Strom-SPDUs erfolgt über einen Feldbus zur Sicherheits-SPS. Der Kreuzvergleich zur Plausibilitätsprüfung der Daten findet nicht mehr im Antrieb statt, sondern ausschließlich in der Sicherheits-SPS. Für die Sicherheits-SPS sind die Sicherheitsfunktionen STO und SBC im Antrieb digitale Ausgänge, die in einem 1. Kanal im µC und in einem 2. Kanal im FPGA über den sicherheitsbezogenen Feldbus aktiviert werden können [60]. Zur Diagnose werden bestimmte Daten über den Feldbus zurückgelesen und in der Sicherheits-SPS ausgewertet.

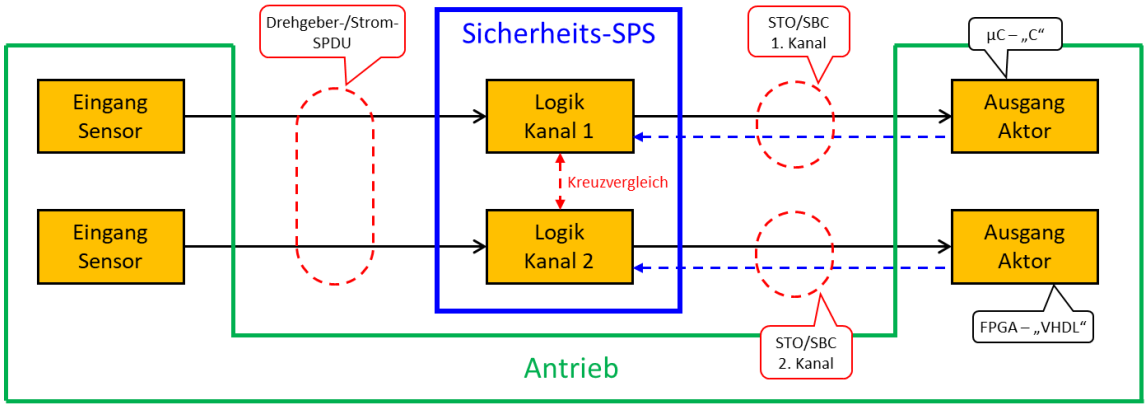


Abbildung 15: Zweikanalige Sicherheitsfunktion für eine sichere Bewegungsüberwachung mit Kreuzvergleich in der Sicherheits-SPS.

4.2 Sicherheitsfunktionen im Antrieb

Das zuverlässige Anhalten einer Maschine ist eine der am häufigsten verwendeten Sicherheitsfunktionen. DIN EN 61800-5-2 [56] definiert drei Stoppfunktionen, die den drei in der DIN EN 60204-1 [102] spezifizierten Stoppkategorien 0, 1 und 2 entsprechen: STO, SS1 und sicherer Stopp 2 (engl.: safe stop 2, SS2). Während STO nur die Energiezufuhr abschaltet, beinhalten die beiden anderen Stoppfunktionen auch eine aktive Verzögerung des Motors. Bei SS1 wird die Sicherheitsfunktion STO bei Motorstillstand aktiviert, während sich der Antrieb bei SS2 im sicheren Betriebshalt (engl.: safe operating stop, SOS) befindet. Bei SOS befindet sich der Antrieb noch im geregelten Betrieb und es findet eine Überwachung eines definierten Positionsbereichs statt, welcher nicht verlassen werden darf. Wird dieser Bereich überschritten, wird auch hier STO aktiviert. Für die Sicherheitsfunktion SOS wird ein sicherheitsbezogenes Positionssignal benötigt. Da das hier vorgestellte Konzept keine Verarbeitung der sicherheitsrelevanten Positionssignale im Antrieb vorsieht, kann eine Überwachung des Positionsbereichs für die Sicherheitsfunktion SOS und somit auch für SS2 nur außerhalb des Antriebs stattfinden und soll daher in diesem Kapitel nicht weiter betrachtet werden.

In manchen Fällen reicht ein kontrolliertes Abbremsen und eine anschließende Abschaltung der Energiezufuhr des Motors über STO nicht aus. Denn in bestimmten Anwendungen würde nach dem Abschalten über STO eine an einem Roboterarm hängende Last herunterfallen und ggf. einer Person Schaden zuführen. SBC kann eine im Motor integrierte Haltebremse ansteuern und somit das Herunterfallen verhindern. Bei der Ausführung der Sicherheitsfunktion SS1 kann SBC beispielsweise gleichzeitig mit STO ausgelöst werden, wenn die Drehzahl einen gewissen unteren Schwellwert erreicht hat.

4.2.1 Sicher abgeschaltetes Moment

In der Vergangenheit wurde STO oftmals durch ein Netzschütz oder Motorschütz realisiert, um die Energiezufuhr zum Motor zu unterbrechen. Aufgrund der zusätzlichen Hardware-Komponenten wird typischerweise eine Impulssperre für die Umsetzung der Sicherheitsfunktion verwendet. Wenn durch einen geeigneten IC verhindert werden kann, dass die Leistungshalbleiter mit einem Pulsmuster angesteuert werden, kann kein Drehfeld mehr im Motor erzeugt werden, wodurch auch kein Drehmoment mehr entstehen kann [51]. Abbildung 16 zeigt das Konzept der STO-Sicherheitsfunktion im Antrieb mit der Verwendung von Optokoppler-Gate-Treibern. Für die Erfüllung der Zweikanaligkeit für Kategorie 3 werden die Transistoren in eine High-Side- und Low-Side-Gruppe aufgeteilt. Um im Motor die Erzeugung eines Drehmoments zu verhindern, genügt die Abschaltung einer Transistor-Gruppe, da für einen Stromfluss das Einschalten der High-Side und der Low-Side erforderlich ist. Die drei oberen Gate-Treiber werden von dem µC über nSTO_high und die drei unteren von dem FPGA über nSTO_low angesteuert. Wird das nSTO-Signal bzw. die Versorgungsspannung an der Anode der Optokoppler abgeschaltet, kann kein Pulsmuster mehr übertragen werden, auch wenn das FPGA weiterhin PWM-Signale erzeugt. Die Optokoppler-Gate-Treiber sorgen zusätzlich für eine galvanische Trennung zwischen den Steuersignalen und der Leistungsseite. Die sechs digitalen PWM-Ausgänge vom FPGA arbeiten als Open-Drain-Schalter und schalten jeweils die Kathoden der Optokoppler auf Logisch „Low“, um den zugehörigen Leistungstransistor einzuschalten. Sechs Vorwiderstände, jeweils in Reihe zu den Anoden der Leuchtdioden (engl.: light-emitting diode, LED), begrenzen den Strom durch die LEDs der Gate-Treiber.

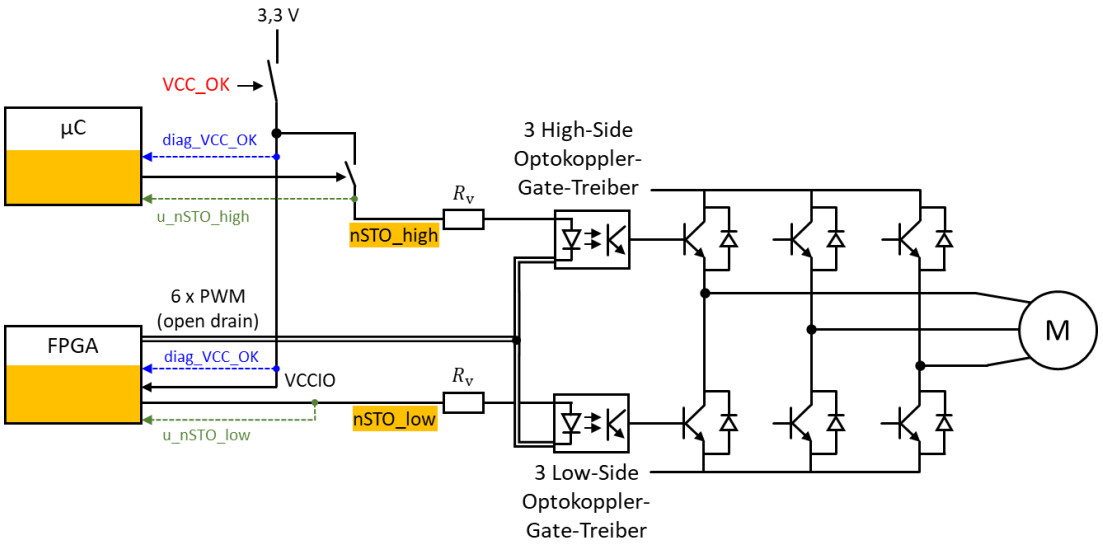


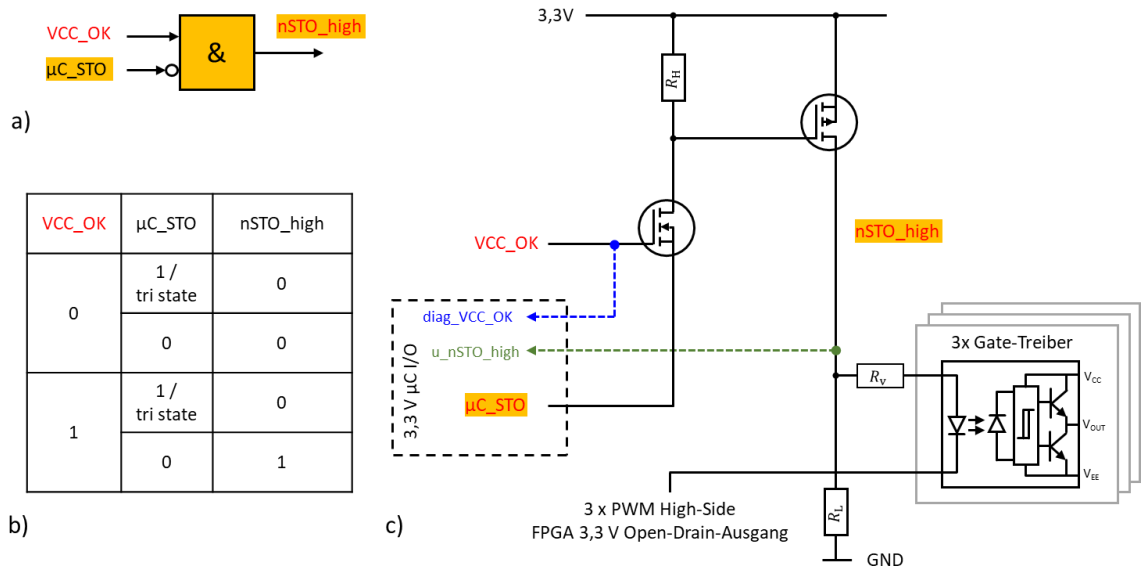
Abbildung 16: Konzept der Sicherheitsfunktion STO im Antrieb.

Die zweikanalige Abschaltung mit Hilfe der Impulssperre kann unter Umständen versagen, weshalb eine Fehlererkennung durch geeignete Diagnosemaßnahmen erforderlich

ist. Diese Diagnose kann innerhalb des Antriebs oder durch eine externe Überwachungseinheit ausgeführt werden. Die Diagnose wird in diesem Fall in die übergeordnete Sicherheits-SPS ausgelagert. Dazu ist die Übertragung von Rückmeldesignalen der Abschaltpfade an die Sicherheits-SPS notwendig. In Abbildung 16 sind diese Signale in grün eingezeichnet und lesen die Spannung der Abschaltpfade zurück. Der µC liest die Spannung des High-Side nSTO-Signals über u_nSTO_high und das FPGA die Spannung der Low-Side über u_nSTO_low zurück. Um das gewünschte PL zu erreichen, sind die Abschaltpfade der Sicherheitsfunktion in regelmäßigen Zeitabständen zu testen und über die Diagnosesignale auszuwerten. Durch die Tests können mögliche Fehler im Abschaltpfad rechtzeitig aufgedeckt werden, bevor die Sicherheitsfunktion das nächste Mal angefordert wird. Unabhängig von µC und FPGA können ein Reset-Signal sowie eine Baugruppe zur Spannungsüberwachung die Spannungsversorgung für alle Anoden der Optokoppler mit dem Signal VCC_OK abschalten. Diese Spannungsüberwachung ist ein Teil der antriebsinternen Diagnose. Zur Überwachung dieses Spannungssignals wird VCC_OK von beiden Kanälen über diag_VCC_OK zurückgelesen. Die Implementierung der beiden Funktionskanäle für STO und das Rücklesen zur Diagnose wird im Folgenden detailliert betrachtet.

1. STO-Funktionskanal im µC

Der erste Funktionskanal der Sicherheitsfunktion STO wird im µC realisiert. Abbildung 17a) zeigt die logische Verknüpfung der beiden Signale mit einem „UND“-Gatter. Abbildung 17b) stellt die logischen Zusammenhänge der Signale in einer Tabelle dar und Abbildung 17c) veranschaulicht die zugehörige Schaltung mit zwei MOSFETs.



VCC_OK	µC_STO	nSTO_high
0	1 / tri state	0
	0	0
1	1 / tri state	0
	0	1

Abbildung 17: Logische Verknüpfung der Impulssperre mit dem µC.

Nur wenn das Signal VCC_OK „High“ ist und gleichzeitig µC_STO „Low“ ist, ergibt sich eine positive Gate-Source-Spannung an dem N-Kanal-MOSFET. Dieser wiederum schaltet eine negative Gate-Source-Spannung auf den P-Kanal-MOSFET, die diesen einschaltet und das Signal nSTO_high auf 3,3 V schaltet. Nur dann wird die Anode der LED des Optokopplers mit Spannung versorgt und die PWM-Signale werden von den Gate-Treibern an die High-Side-Leistungstransistoren weitergeleitet.

Abbildung 18 veranschaulicht die Implementierung der Diagnosemaßnahme im µC. Wie Abbildung 18a) zeigt, kann die übergeordnete Sicherheits-SPS über ein Bit der sicherheitsbezogenen Daten des sicherheitsbezogenen Feldbusses das Signal FS_nSTO_high auf „Low“ oder „High“ setzen. In einem weiteren Bit wird ein Testsignal übertragen, welches bei steigender Flanke ein Monoflop aktiviert. Dieses Monoflop setzt den Ausgang µC_STO für 100 ns auf „High“, wodurch das Signal nSTO_high für diese Zeit auf „Low“ geschaltet wird. Die Abtastung von u_nSTO_high erfolgt wie in Abbildung 18b) dargestellt entsprechend etwa 80 ns nach dem Abschalten bzw. dem Aktualisieren der sicherheitsbezogenen Daten. Die Zeiten ergeben sich durch die sequenzielle Abarbeitung des Codes im µC. Bei einem erfolgreichen Test wechselt das Signal diag_STO_high für einen Zyklus des sicherheitsbezogenen Feldbusses auf „Low“.

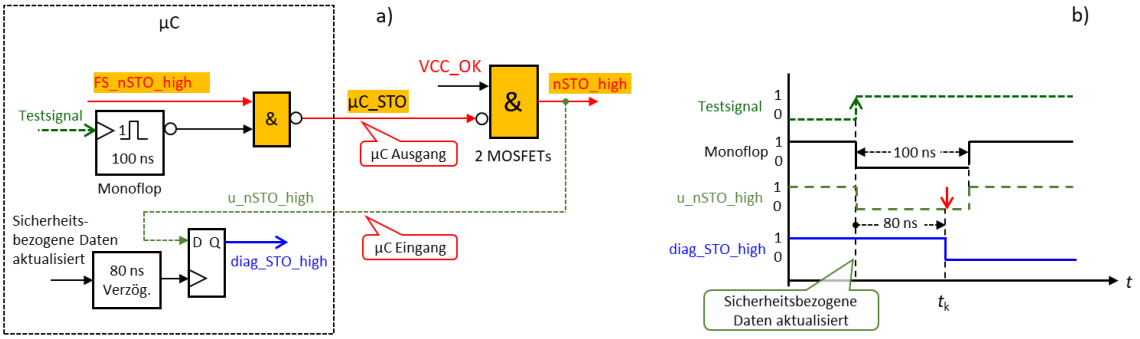


Abbildung 18: Implementierung der Diagnose im µC. a) Blockschaltbild und b) Zeitverlauf der Signale.

Der Optokoppler-Gate-Treiber sowie der Gate-Widerstand mit der Gate-Source-Kapazität wirken als Tiefpass, wodurch der angesteuerte Leistungstransistor von dem kurzen Testimpuls nicht beeinflusst wird.

2. STO-Funktionskanal im FPGA

Der zweite Funktionskanal der STO-Sicherheitsfunktion wird mit dem FPGA realisiert. Auch hier kann die übergeordnete Sicherheits-SPS über ein Bit der sicherheitsbezogenen Daten STO auslösen. Abbildung 19 zeigt die Realisierung der Impulssperre mit dem FPGA. In Abbildung 19a) ist das Blockschaltbild der logischen „UND“-Verknüpfung durch das Schalten der Spannungsversorgung der FPGA-I/O-Bank dargestellt. Der FPGA-I/O-Buffer kann das Signal nSTO_low nur dann einschalten, wenn die Signale VCC_OK und FPGA_nSTO „High“ sind. Der Zustand des Ausgangsignals kann direkt

über denselben I/O-Buffer zurückgelesen werden. Da jeder FPGA-Ausgang bei 3,3 V Niederspannung-Transistor-Transistor-Logik (engl.: low voltage transistor transistor logic, LVTTL) nur einen begrenzten Strom treiben kann [103], sind drei Ausgänge der entsprechenden I/O-Bank parallelgeschaltet, um die LEDs der drei Low-Side-Optokoppler mit ausreichend Strom zu versorgen. Abbildung 19b) veranschaulicht die Aufteilung des FPGAs in neun unabhängige I/O-Bänke [103]. Die I/Os jeder Bank werden je nach Spezifikation der angeschlossenen Peripherie mit den jeweils erforderlichen Versorgungsspannungen V_{CCIO} versorgt. Ohne diese I/O-Spannungsversorgung kann die FPGA-Logik die Leistungstransistoren über die Gate-Treiber nicht einschalten. Abbildung 19c) zeigt das zugehörige Schaltbild. Wenn das Signal VCC_OK „High“ ist, ergibt sich eine positive Gate-Source-Spannung an dem N-Kanal-MOSFET. Dieser wiederum schaltet eine negative Gate-Source-Spannung auf den P-Kanal-MOSFET, die diesen einschaltet und so die Versorgungsspannung der 2. FPGA-I/O-Bank V_{CCIO2} auf 3,3 V schaltet. Nur bei eingeschalteter I/O-Versorgungsspannung kann das Signal nSTO_low auf „High“ geschaltet werden und die PWM-Signale können über die drei Gate-Treiber-LEDs an die Low-Side-Leistungstransistoren weitergeleitet werden.

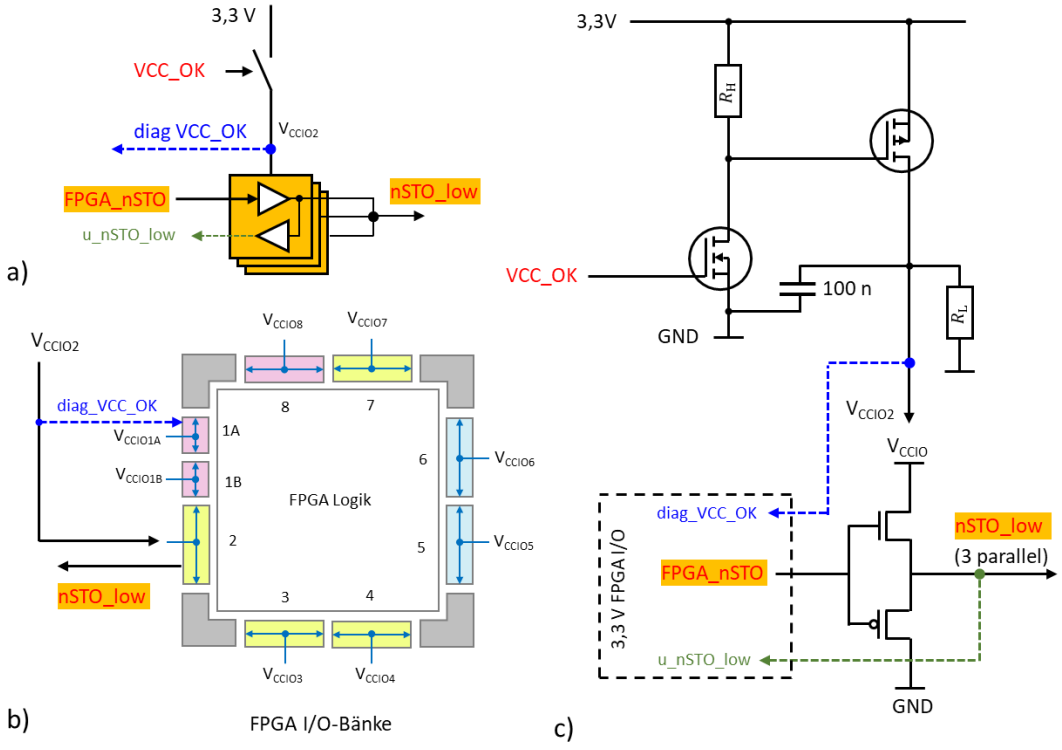


Abbildung 19: Logische Verknüpfung der Impulssperre mit dem FPGA.

Über diag_VCC_OK kann der Zustand der I/O-Versorgungsspannung zurückgelesen werden. Dazu wird die Spannungsversorgung von der 2. I/O-Bank V_{CCIO2} über eine andere nicht abschaltbare 3,3-V-I/O-Bank eingelesen, wie in Abbildung 19b) dargestellt. Bei jedem Booten (Hochfahren) des Antriebs kann ein Test durchgeführt werden, welcher

überprüft, ob sich die I/O-Versorgungsspannung über die Spannungsüberwachungsbausteine abschalten lässt.

Abbildung 20 zeigt die Implementierung der Diagnosemaßnahme im FPGA. Wie Abbildung 20a) darlegt, kann auch hier wieder die übergeordnete Sicherheits-SPS über ein Bit der sicherheitsbezogenen Daten das Signal FS_nSTO_low auf „Low“ oder „High“ setzen. Wie auch im µC wird in einem weiteren Bit ein Testsignal übertragen, um einen zyklischen Test anzufordern. Bei steigender Flanke wird das Monoflop aktiviert und die interne FPGA-Logik setzt die drei 3,3-V-Ausgänge über den I/O-Buffer für 100 ns auf „Low“. Über den I/O-Buffer wird der Ausgang dann über die Spannung u_nSTO_low zurückgelesen. Die Abtastung von u_nSTO_low erfolgt wie in Abbildung 20b) dargestellt entsprechend etwa 80 ns nach dem Abschalten bzw. dem Aktualisieren der sicherheitsbezogenen Daten kurz vor dem Wiedereinschalten. Die Zeiten können durch die Verwendung des Systemtakts im FPGA realisiert werden. Bei einem erfolgreichen Test wechselt das Signal diag_STO_low für einen Zyklus des sicherheitsbezogenen Feldbusses auf „Low“. Zur Diagnose wird dieses Signal zur übergeordneten Sicherheits-SPS geschickt.

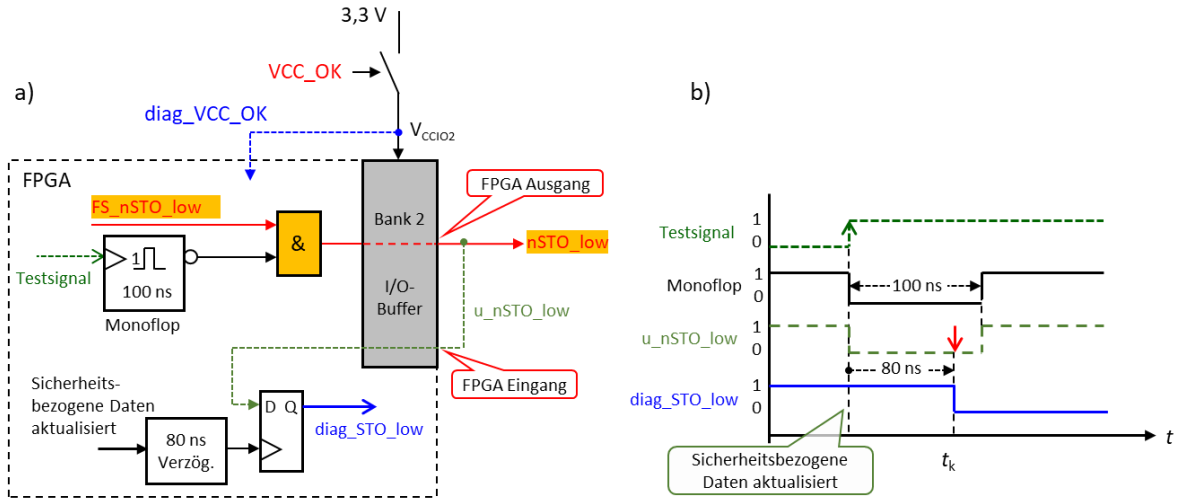


Abbildung 20: Implementierung der Diagnose im FPGA. a) Blockschaltbild und b) Zeitverlauf der Signale.

In Abbildung 21 ist der Aufbau der Sicherheitsfunktion STO mit Diagnose und übergeordneter zentraler Sicherheits-SPS zusammenfassend dargestellt. Die Sicherheits-SPS steuert die Versorgungsspannung der Gate-Treiber-Anoden über ein sicherheitsbezogenes Feldbusprotokoll an (Digitaler Ausgang), um eine zweikanalige Impulssperre zu realisieren. Die sicherheitsbezogenen Daten, die vom Antrieb zurück zur Steuerung gesendet werden (Digitaler Eingang), können für das zweikanalige Rücklesen der STO-Zustände genutzt werden. Die zyklischen Tests zur Abschaltung der STO-Ausgänge werden von der übergeordneten Sicherheits-SPS angestoßen. Für ein eindeutiges Testergebnis sollten beide Kanäle zu unterschiedlichen Zeitpunkten getestet werden. Nach Anstoßen des Testsignals hat die Sicherheits-SPS die Erwartungshaltung nach einer definierten Anzahl an Zyklen den Zustand des entsprechenden Diagnosesignals als „Low“ zurückzulesen. Ist

dies nicht der Fall, war der Test nicht erfolgreich und es sind entsprechende Maßnahmen, wie das Herbeiführen des sicheren Zustands, von der Sicherheits-SPS durchzuführen.

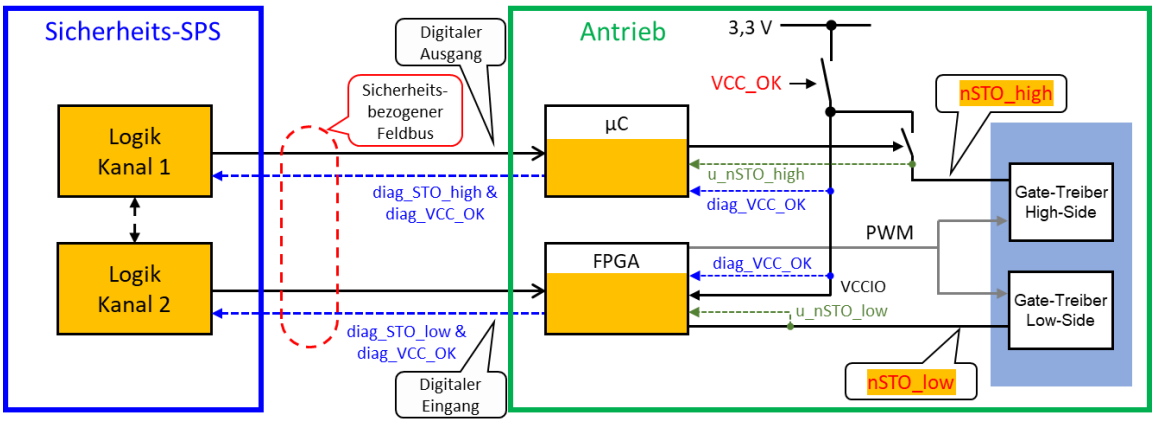


Abbildung 21: Aufbau der Sicherheitsfunktion STO – zusammenfassende Darstellung mit Sicherheits-SPS und Antrieb.

Das Rücklesen der sicherheitsbezogenen Ausgangssignale im Antrieb ist vergleichbar mit der konventionellen Kategorie-3-Architektur mit Schützen und zwangsgeführten Öffnerkontakten.

4.2.2 Sichere Bremsansteuerung

Wenn auf den Motor externe Kräfte, wie beispielsweise die Schwerkraft auf eine hängende Last wirken, kann mit der Sicherheitsfunktion SBC eine Haltebremse angesteuert werden. Haltebremsen sind meist so aufgebaut, dass Strom durch eine Spule der Bremse gegen eine Federkraft arbeitet und zufällt, sobald der Stromfluss unterbrochen wird. Wann SBC ausgelöst wird, um die Bremse im Motor einfallen zu lassen, ist abhängig von der Anwendung. Bei Erkennung eines Fehlers kann die Bremse auch für einen Not-Halt eingesetzt werden, jedoch ist der Verschleiß der Haltebremse nur für eine begrenzte Anzahl von Notbremsungen bei Nenndrehzahl akzeptabel und sollte daher vermieden werden.

Abbildung 22 zeigt den gesamten Aufbau der Sicherheitsfunktion SBC mit einer übergeordneten Sicherheits-SPS, einem Antrieb mit diversitärer Architektur und einer extern angeschlossenen Haltebremse. Die angeschlossene Motorhaltebremse kann zweikanalig abgeschaltet werden. Die Sicherheits-SPS kann die Spannung positiv und negativ schaltend über je einen galvanisch getrennten MOSFET abschalten. Die galvanische Trennung kann dabei durch einen Optokoppler erreicht werden. Die Verknüpfung der Signale VCC_OK und µC_SBC bzw. FPGA_SBC ist als logische „UND“-Verknüpfung dargestellt. Nur wenn beide Signale „High“ sind, kann nSBC_high den oberen und nSBC_low den unteren Optokoppler einschalten. Genau wie bei der Sicherheitsfunktion STO kann diese Verknüpfung im Kanal des µCs mit zwei MOSFETs realisiert werden und im Kanal des FPGAs durch das Abschalten der Versorgungsspannung einer I/O-Bank. Die Sicherheits-SPS kann die beiden MOSFETs T_High und T_Low über das sicherheitsbezogene

Feldbusprotokoll ansteuern. Die Umsetzung der einzelnen Kanäle und ein Testverfahren zur Diagnose werden nun vorgestellt. Es wird zunächst auf den zweiten Funktionskanal im FPGA eingegangen, da dies für das Verständnis des ersten Kanals notwendig ist.

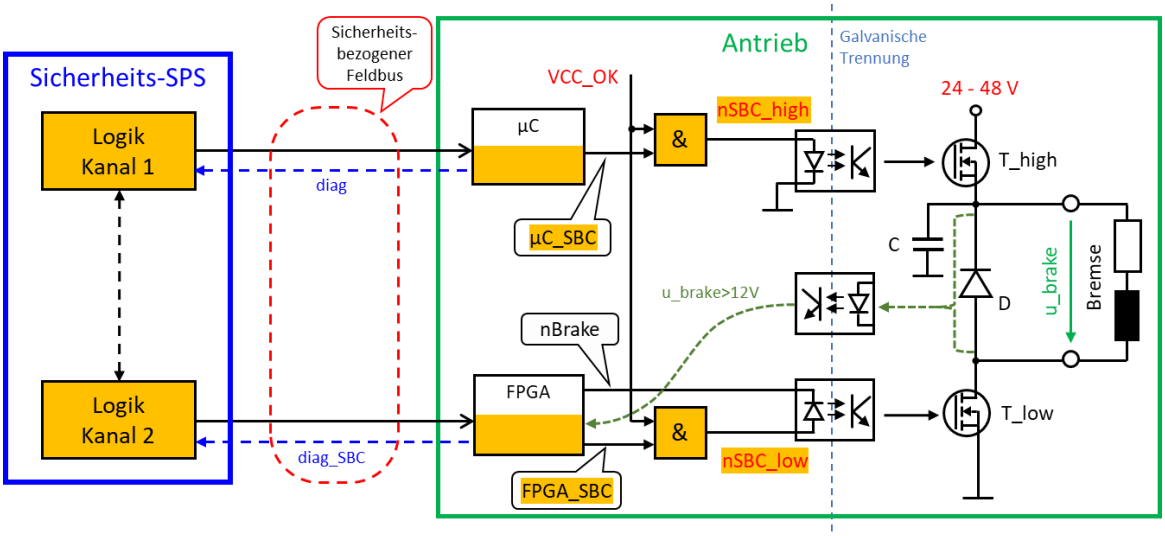


Abbildung 22: Aufbau der Sicherheitsfunktion SBC.

2. SBC-Funktionskanal im FPGA

Der untere MOSFET T_low dient als 2. Funktionskanal und wird über das FPGA angesteuert. Dieser Funktionskanal wird für die folgenden drei Aufgaben verwendet:

1. Funktional sicheres Abschalten über den sicherheitsbezogenen Feldbus mit dem Signal nSBC_low
2. Nicht sicherheitsrelevantes Abschalten des Lüftstroms der Bremse mit dem Signal n_sf_Brake (vgl. Abbildung 23)
3. Stromreduktion nach dem Lüftvorgang durch eine PWM

Der Transistor T_low wird nur dann geschaltet, wenn nSBC_low „High“ ist (Anode des Optokopplers) und die logische „NAND“-Verknüpfung (nicht UND) aus dem PWM-Signal und n_sf_Brake „Low“ wird (Kathode des Optokopplers). Wird die Bremse von der nicht sicherheitsbezogenen Antriebssteuerung über n_sf_Brake zum Lüften freigegeben, wird mit dem MOSFET T_low zunächst für kurze Zeit die volle Spannung ohne PWM eingeschaltet, um die Lüftung der Haltebremse zu beschleunigen. Danach wird mit dem MOSFET T_low, der Freilaufdiode D und dem PWM-Signal ein Tiefsetzsteller mit nicht lückendem Betrieb gebildet, sodass der Strom durch die Spule der Bremse nicht auf null sinkt und die Bremse weiterhin gelüftet bleibt. Der Tastgrad der PWM wird so eingestellt, dass im zeitlichen Mittel die gewünschte Haltespannung an der Bremse liegt.

Abbildung 23 zeigt einen Zeitverlauf zur Diagnose des 2. SBC-Funktionskanals. Ganz oben ist der Verlauf des Signals nSBC_low in Rot dargestellt. Zyklisch, mit einem Testintervall von einer Sekunde, wird ein Testimpuls mit einer Dauer von einer Millisekunde ausgelöst. Die Testimpulsdauer entspricht dabei der Zeit zwischen zwei von der Sicherheits-SPS empfangenen SPDUs. Nach dem Lüftvorgang wird die PWM zur Verringerung

der Verlustleistung genutzt. Erzeugt wird diese PWM von einem dreieckförmigen Trägersignal synchron zur PWM der Motorsteuerung. Nach dem Aktivieren von n_sf_Brake bis zum Beginn des Testpulses zum Zeitpunkt t_k wird T_low entsprechend der PWM geschaltet. Die analoge Spannung u_brake verläuft ähnlich, jedoch etwas phasenverschoben aufgrund der Schaltverzögerung der Bauelemente. Die Spannung u_brake wird, wie in Abbildung 23 gezeigt, mit einem Optokoppler zurückgelesen. Dabei ist die LED des Optokopplers mit einem Vorwiderstand R_v in Reihe geschaltet, um den Strom durch die LED zu begrenzen. Der Widerstand wird dabei so gewählt, dass die LED ab einer Spannung unter 12 V kein Licht mehr emittiert und somit der Pull-Down-Widerstand am Ausgang des Optokopplers das Signal u_brake>12V auf „Low“ zieht.

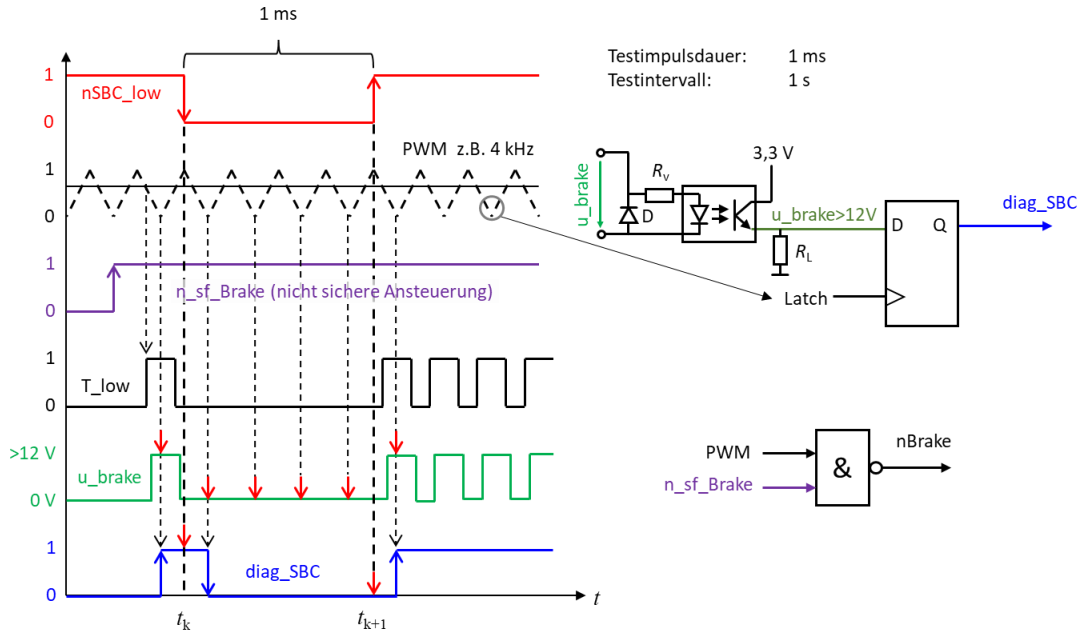


Abbildung 23: Diagnose des 2. SBC-Funktionskanals.

Ist der Schalter T_low eingeschaltet, liegt die volle Bremsspannung an der Diode an und das Signal u_brake>12V ist „High“. Wenn der Schalter ausgeschaltet ist, fällt nur die Spannung an der Diode in Durchlassrichtung ab (etwa 0,7 V). Somit entspricht u_brake der negativen Diodenspannung und das Signal u_brake>12V ist „Low“. Immer wenn das Trägersignal der PWM am unteren Umkehrpunkt ist, wird eine steigende Flanke im Signal Latch erzeugt. Mit dieser Flanke wird das D-Flipflop getriggert und das Signal u_brake>12V wird in diag_SBC gelatcht. Dadurch erfolgt die Abtastung immer in der Mitte der PWM-Pulse zu Zeiten, in denen der Transistor T_low durch die PWM prinzipbedingt eingeschaltet ist. Bei ordnungsgemäßer Funktion ist das Signal diag_SBC nach einem Testimpuls, gestartet zum Zeitpunkt t_k bei t_{k+1} „Low“, da die Spannung u_brake zum Zeitpunkt des vorhergehenden Latch-Signals kleiner als 12 V war.

1. SBC-Funktionskanal im µC

Der obere MOSFET T_high ist ausschließlich für die Sicherheitsfunktion SBC vorgesehen und wird über den µC angesteuert. Die Ansteuerung erfolgt mit der Sicherheits-SPS über das sicherheitsbezogene Feldbusprotokoll. Da die Haltebremse elektrisch betrachtet eine RL-Reihenschaltung ist, fällt die Spannung bei ausgeschaltetem Schalter T_high exponentiell mit der Zeitkonstante $\tau = L/R$ ab. Die Zeitkonstante τ ist deutlich größer als die sicherheitsbezogene Zykluszeit. Aus diesem Grund kann der MOSFET T_high mit einem Testimpuls, generiert in der Sicherheits-SPS, diagnostiziert werden, ohne dass die Bremse dabei einfällt. Bei der Sicherheitsfunktion STO ist das Abschalten für einen ganzen Zyklus zu lange und der Leistungstransistor würde über den Optokoppler-Gate-Treiber abgeschaltet. Aus diesem Grund wurde der beschriebene Monoflop verwendet, um die Abschaltdauer auf 100 ns zu verkürzen. Der Transistor T_high wird bei gelüfteter Bremse zyklisch mit einem Testintervall von 1 s für eine Testimpulsdauer von 1 ms abgeschaltet. Durch die Induktivität der Bremse ändert sich der Strom durch die Wicklung der Bremse nur geringfügig, wodurch die Bremse gelüftet bleibt. Der negative Spannungsgradient ergibt sich aus dem Strom durch die Bremse und der Kapazität des Entstörkondensators C aus Abbildung 22. Die an der Bremse anliegende gemessene Spannung u_brake sinkt während des Testimpulses entsprechend auf Werte kleiner als 12 V.

Abbildung 24 zeigt die Diagnose des 1. SBC-Funktionskanals. Das Signal nSBC_high wird zyklisch von der Sicherheits-SPS mit einem Testintervall von 1 s für 1 ms abgeschaltet, um einen Testimpuls zu generieren. Zum Zeitpunkt t_{k} wird der Stromfluss durch den MOSFET T_high unterbrochen und die Spannung u_brake sinkt nach einer gewissen Zeit unter 12 V. Das Signal diag_SBC wird bei der nächsten positiven Flanke des Signals Latch auf „Low“ gesetzt. Zum Zeitpunkt $t_{\mathrm{k+1}}$ wird der MOSFET T_high wieder eingeschaltet, wodurch die Spannung u_brake wieder ansteigt. In Abbildung 24 ist das Zurücklesen des Signals diag_SBC in einem Schaltbild als getakteter Komparator dargestellt. Das Rücklesen der Spannung u_brake wird aufgrund der Abtastung durch das im FPGA erzeugte Trägersignal nur über den 1. Funktionskanal im FPGA realisiert und als Signal diag_SBC an die übergeordnete Sicherheits-SPS gesendet. Auch hier ist bei ordnungsgemäßer Funktion das Signal diag_SBC nach einem Testimpuls, gestartet zum Zeitpunkt t_{k}, bei $t_{\mathrm{k+1}}$ „Low“, da die Spannung u_brake kurzzeitig unter 12 V gesunken ist und zum Zeitpunkt $t_{\mathrm{k+2}}$ wieder „High“. Die Tests der beiden Funktionskanäle finden zeitversetzt statt, da das Zurücklesen über den gleichen Optokoppler bzw. Diagnosepfad erfolgt.

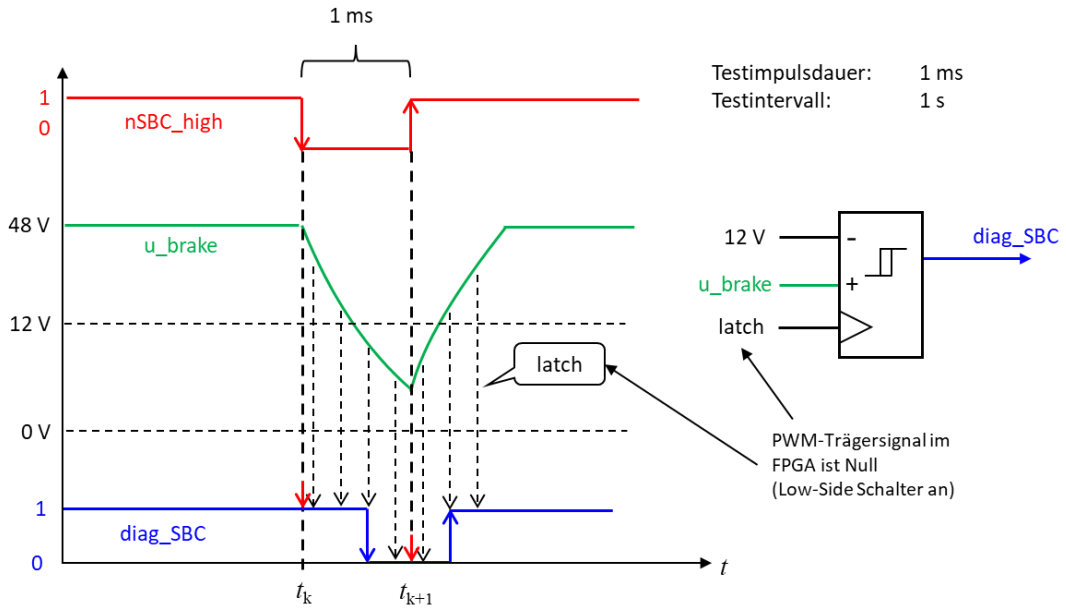


Abbildung 24: Diagnose des 1. SBC-Funktionskanals.

4.2.3 Sicherer Stopp

Bei der Stoppfunktion SS1 ist eine aktive Verzögerung der Motorgeschwindigkeit durch die Regelkreise vorgesehen. In der Norm DIN EN 61800-5-2 wird nochmal zwischen drei Optionen dieser Sicherheitsfunktion unterschieden:

1. Zeitgesteuert / engl.: time controlled (SS1-t)
2. Rampenüberwacht / engl.: ramp monitored (SS1-r)
3. Verzögerungsgesteuert / engl.: deceleration controlled (SS1-d)

Im IFA Report 4/2018 der Deutschen Gesetzlichen Unfallversicherung (DGUV) wird beschrieben, dass kein kommerzielles Produkt bekannt ist, welches die SS1-d Option bietet [51], bei der die sicherheitsbezogene Logik den Bremsvorgang übernimmt.

Statt sich beim Bremsen auf die nicht sicherheitsbezogene Antriebssteuerung mit ihren unbekannten oder hohen Ausfallraten zu verlassen (wie bei SS1-t und SS1-r), kann die kontrollierte Verzögerung eines PSMs auch zusammen mit der sicherheitsbezogenen Logik über ein zusätzliches Relais und Bremswiderstände R_b erreicht werden. Diese sicherheitsbezogene Logik kann, wie in Abbildung 25 gezeigt, die drei Bremswiderstände mit der Motorwicklung verbinden. Werden die Bremswiderstände entfernt, kann das Relais auch alle drei Motorphasen direkt kurzschließen. Um jedoch den Bremsstrom zu begrenzen und die Auswirkungen auf die Hardwarekomponenten des Servoreglers und die Motorwicklungen zu minimieren, werden üblicherweise Bremswiderstände verwendet [104]. Nach dem Abbremsen kann der Servoregler über STO abgeschaltet werden. Bei diesem bewährten Ansatz sind die Ausfallraten der beteiligten Komponenten (Relais und Bremswiderstände) zwar gering, aber die Kosten und der Platzbedarf steigen aufgrund der zusätzlichen Komponenten.

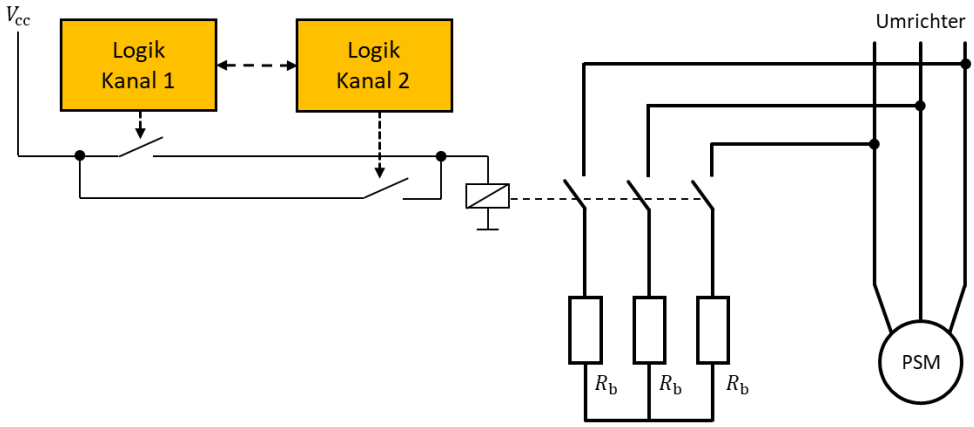


Abbildung 25: Bremsmethode für einen PSM über die sicherheitsbezogene Logik mit Relais und Bremswiderständen.

Statt der zusätzlichen Bremswiderstände kann auch der Wechselrichter zum Bremsen des Motors verwendet werden [104]. In Abbildung 26a) wird das einphasige Ersatzschaltbild eines PSMs mit der herkömmlichen Bremsmethode mit Relais und Bremswiderständen dargestellt. Abbildung 26b) zeigt die Bremsmethode mit dem Wechselrichter.

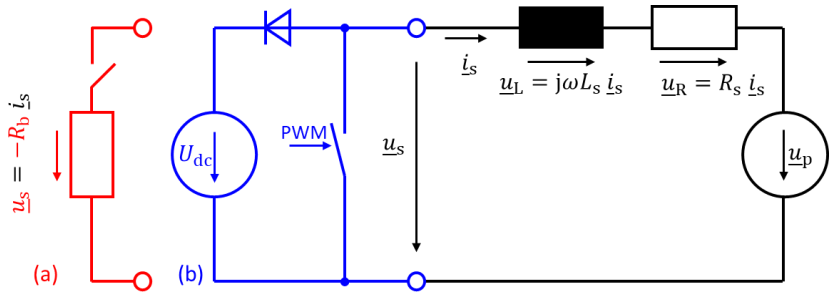


Abbildung 26: Einphasiges Ersatzschaltbild des PSMs mit a) Relais und Bremswiderstand und b) dem Wechselrichter zum Bremsen.

Zum Bremsen werden drei der sechs Leistungshalbleiter gemeinsam periodisch eingeschaltet, um alle drei Phasen des PSMs kurzzuschließen. Dieses Kurzschließen der drei Phasen entspricht der Vorgabe eines Nullzeigers bei der SVM [104]. In [105] werden die drei Leistungshalbleiter gleichzeitig mit einer einphasigen PWM angesteuert, um einen vorgegebenen Bremsstrom i_{s_cmd} zu erreichen. Bei der vorgestellten Antriebsstruktur übernimmt das FPGA die Ansteuerung der Leistungshalbleiter mit der PWM. Aus diesem Grund wird auch der Algorithmus für die SS1-d-Stoppfunktion im FPGA berechnet. Da es sich an dieser Stelle nicht um eine Kategorie-3-Architektur nach DIN EN ISO 13849 handelt, führt ein Ausfall dieses Kanals direkt zum Ausfall der Sicherheitsfunktion SS1-d. In diesem Fall können über den anderen Kanal im µC die Sicherheitsfunktionen STO und optional SBC aktiviert werden, um den Motor weiterhin stoppen zu können. Die in [105] vorgestellte Methode ermöglicht das sensorlose Bremsen eines PSMs ohne großen Aufwand und bleibt auch beim Ausfall eines einzelnen Leistungshalbleiters weiterhin funktionsfähig. Der Algorithmus eignet sich für die Implementierung im sicherheitsbezogenen

Teil des Antriebs. Bei dem Ansatz wird der Bremsstrom des Motors überwacht und vom sicherheitsbezogenen Teil des Antriebs auf einen vorgegebenen Sollwert geregelt. Die Struktur der Regelung ist in Abbildung 27 dargestellt.

Die Ströme der drei Motorphasen werden vom FPGA gemessen. Um den Bremsstrom für SS1 zu regeln, ist eine sicherheitsbezogene Strommessung erforderlich, wie in [106] beschrieben. In Kapitel 4.4 wird gezeigt, wie die gemessenen Motorströme in der überlagerten Sicherheits-SPS plausibilisiert und entsprechende Diagnosemaßnahmen durchgeführt werden, um sicherheitsbezogene Stromwerte für weitere Sicherheitsfunktionen zu erhalten. Da die gemessenen Ströme regelmäßig von der Sicherheits-SPS plausibilisiert und getestet werden, können diese auch für den verhältnismäßig kurzen Bremsvorgang (einige 100 ms) vom FPGA für SS1-d verwendet werden. Es können, wie bei der Antriebsregelung, ΣΔ-Modulatoren mit anschließender Sinc³-Filterung genutzt werden. Bei einer Modulationsfrequenz von 12 MHz und einer OSR von 256 ergibt sich eine Updatezykluszeit der Ausgangsdaten der Sinc³-Filter und damit eine Abtastzeit T_a von 21,33 µs. Die drei vollständig digitalen Phasenströme werden dann durch die Clarke-Transformation in i_α und i_β umgewandelt. Die beiden Stromkomponenten i_α und i_β werden quadriert und zu $|i_s|^2$ summiert. Der Bremsstrom-Sollwert bestimmt die Regelabweichung e eines einphasigen Zweipunkt-Reglers mit Hysterese:

$$e = {i_{\mathrm{s\_cmd}}}^2 - |i_s|^2 \tag{5}$$

Das Verhalten des Regler-Ausgangssignals kann wie folgt ausgedrückt werden:

$$\begin{aligned} e > \varepsilon &\rightarrow \text{Ausgang: Ein (High-Pegel)} \\ e < -\varepsilon &\rightarrow \text{Ausgang: Aus (Low-Pegel)} \end{aligned} \tag{6}$$

Wenn das Ausgangssignal „Low“ ist, werden die drei Low- oder alternativ die drei High-Side-Leistungshalbleiter ausgeschaltet. Wenn das Ausgangssignal des Reglers „High“ ist, werden die drei Transistoren eingeschaltet, um den dreiphasigen PSM kurzzuschließen. Aufgrund der genannten Abtastzeit T_a ist bei dieser Konfiguration die maximale Schaltfrequenz der Halbleiter auf $f_\mathrm{max} = 23{,}4\,\mathrm{kHz}$ begrenzt. Wegen dieser inhärenten Schaltfrequenzbegrenzung kann der Hysteresewert auch problemlos auf null konfiguriert werden. Mit dem Eingang zur Kanalauswahl wird festgelegt, ob die High- oder die Low-Side-Transistoren für die Motorbremsung verwendet werden. Bei Verwendung der Low-Side-Transistoren bleiben die High-Side-Transistoren immer ausgeschaltet und umgekehrt. Wenn also entweder ein High- oder ein Low-Side- Transistor ausfällt, kann der Motor weiterhin zuverlässig gebremst werden. Damit ist der Ansatz fehlertolerant und auch für den degradierten Betrieb nach [12] geeignet.

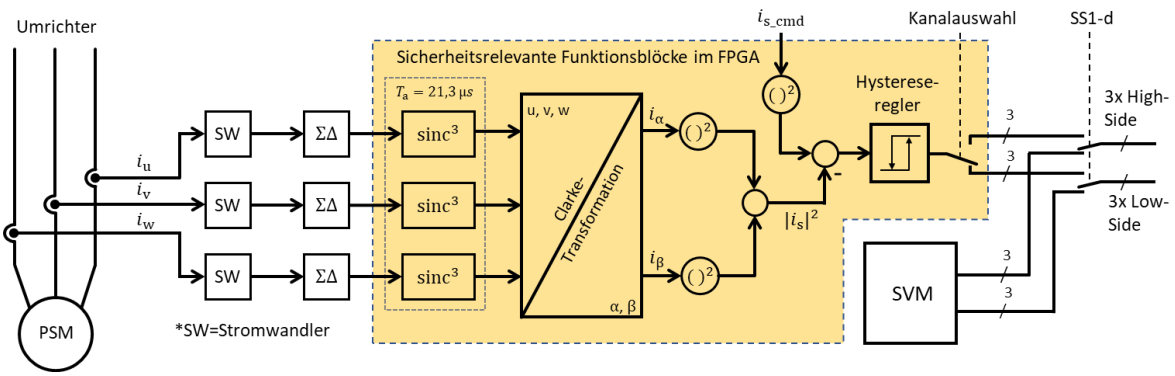


Abbildung 27: Regelstruktur für das sensorlose Bremsen eines PSMs über das FPGA im Antrieb.

Der maximale Bremsstrom hängt von der jeweiligen Anwendung ab. Je größer der Bremsstrom ist, desto schneller wird der Motor gestoppt. Um Schäden an Bauteilen zu vermeiden, sollte jedoch sichergestellt sein, dass die verwendete Hardware im Servoregler für den Bremsstrom ausgelegt ist. Das Signal SS1-d aktiviert oder deaktiviert die Sicherheitsfunktion. Wird die Sicherheitsfunktion ausgelöst, schaltet das Signal die Ausgänge für die Gate-Treiber von der SVM auf den Zweipunkt-Regler im FPGA um, damit der Motor gebremst werden kann.

Abbildung 28 veranschaulicht die Raumzeiger des PSMs während eines beispielhaften Bremsvorgangs mit einem vorgegebenen maximalen Bremsstrom. Da der Strom vom FPGA geregelt wird, ändert sich der Stromzeiger zunächst nicht. Der Bremsvorgang startet bei der Kreisfrequenz ω_3. Bei dieser Drehzahl beträgt der resultierende PWM-Tastgrad des Zweipunkt-Reglers $\alpha = 0{,}57$. Somit sind die drei Phasen im Durchschnitt etwas mehr als die Hälfte der Zeit kurzgeschlossen. Mit abnehmender Drehzahl nehmen die Polradspannung $\underline{u}_\mathrm{p}$ und die Spannung an der Induktivität $\underline{u}_\mathrm{L}$ proportional ab. Da der Stromzeiger konstant bleibt, ist auch die Spannung über den Wicklungswiderstand $\underline{u}_\mathrm{R}$ konstant. Während die Drehzahl beim Bremsvorgang sinkt, nimmt der Tastgrad α zu. Bei einer bestimmten Drehzahl wird ein Punkt erreicht, an dem der vorgegebene Bremsstrom nicht mehr erreicht werden kann, auch wenn der Motor permanent kurzgeschlossen ist. In Abbildung 28 wird dieser Punkt bei ω_min erreicht. Da der Tastgrad von eins erreicht ist und die drei Leistungshalbleiter ständig eingeschaltet sind, ist die Ausgangsspannung des Wechselrichters gleich null ($\underline{u}_\mathrm{s} = 0$). Wenn die Drehzahl weiter sinkt, kann der eingestellte Bremsstrom nicht mehr erreicht werden. Der Strom sinkt dann entsprechend dem in Abbildung 28 gezeigten violetten Verlauf, bis der Motor zum Stillstand kommt und damit der Strom auf null sinkt.

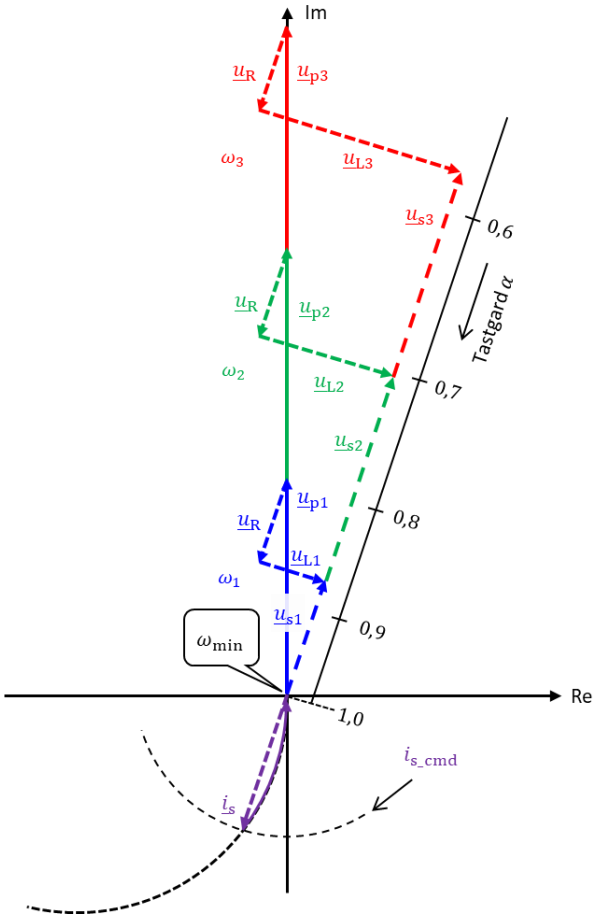


Abbildung 28: Polradspannung $\underline{u}_p$, Klemmenspannung $\underline{u}_s$ und PWM-Tastgrad α während eines Bremsvorgangs mit vorgegebenem maximalen Bremsstrom i_{s_cmd}.

Abbildung 29 zeigt die Struktur des Wechselrichters und den sicherheitsbezogenen Teil im Antrieb bei einem Bremsvorgang mit den drei unteren Leistungsschaltern. Sobald die Sicherheitsfunktion SS1-d von der Sicherheits-SPS ausgelöst wird, löst der 1. Kanal im µC die Sicherheitsfunktion STO aus. Dadurch werden die Gate-Treiber der oberen drei Transistoren gesperrt und sind somit unabhängig vom Pulsmuster dauerhaft ausgeschaltet und lediglich die drei Body-Dioden bleiben wirksam. Der 2. Kanal im FPGA hingegen erzeugt das Pulsmuster für die drei unteren Transistoren über die vorgestellte Regelstruktur, um den Motor abzubremsen.

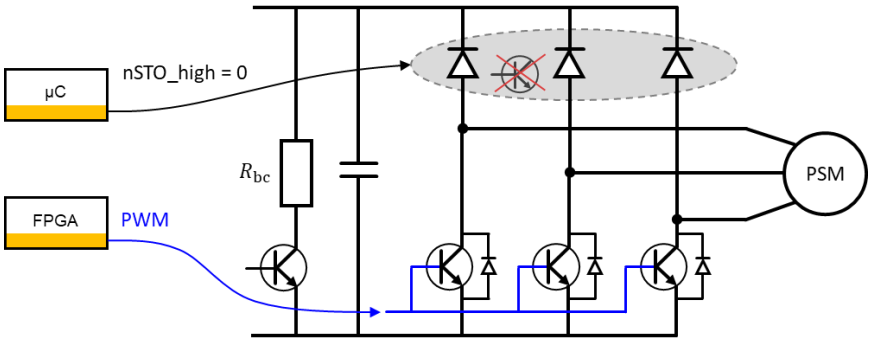


Abbildung 29: Blockschaltbild des Antriebs während eines Bremsvorgangs mit den drei unteren Transistoren.

Ein Bremschopper-Widerstand R_{bc} wie in Abbildung 29 wird zur Aufnahme der rückgespeisten Energie des Bremsvorgangs verwendet. In der Praxis ist es vorteilhaft, mehr als einen Bremschopper zu verwenden, wie es bei mehrachsigen Systemen üblich ist. Bei Ausfall eines Bremschoppers werden so Überspannungen durch Redundanz vermieden. Wird der Steuerteil des Antriebs durch eine unterbrechungsfreie Stromversorgung (USV) gespeist, ist ein kontrolliertes Bremsen auch ohne Netzversorgung möglich.

4.3 Sicherheitsbezogene Kommunikation

Wird eine sicherheitsbezogene Struktur verwendet, bei der eine übergeordnete Sicherheits-SPS als sicherheitsbezogene Logik dient und der Antrieb für sicherheitsbezogene Ein- und Ausgänge verwendet wird, sind die Sicherheitsfunktionen STO und SBC aus Sicht der übergeordneten Sicherheits-SPS digitale Ausgänge. Diese Sicherheitsfunktionen sind nach Kategorie 3 zweikanalig umzusetzen und somit sind pro Sicherheitsfunktion zwei Abschaltpfade notwendig [60]. Um diese digitalen Ausgänge von der Sicherheits-SPS aus im Antrieb schalten zu können, wird eine sicherheitsbezogene Kommunikation in Form eines sicherheitsbezogenen Feldbusses zwischen Steuerung und Antrieb eingesetzt. Zusätzlich sollen weitere sicherheitsrelevante Eingangsdaten für eine sichere Bewegungsüberwachung zur Sicherheits-SPS übertragen werden. Wie bei den sicherheitsbezogenen Drehgebern findet die Auswertung der im Antrieb gebildeten SPDUs erst in der übergeordneten sicherheitsbezogenen Logik statt. Aus diesem Grund werden die SPDUs aus dem Antrieb via Black-/Gray-Channel an die Sicherheits-SPS übertragen.

Welcher sicherheitsbezogene Feldbus eingesetzt wird, ist für das vorgestellte Konzept nicht relevant. Allerdings ist zu beachten, dass neben den wenigen Daten (< 1 Byte) für die Ansteuerung und Diagnose der antriebsinternen Sicherheitsfunktionen mehrere Bytes für die SPDUs für die sichere Bewegungsüberwachung zu übertragen sind. Allein die EnDat-3-Drehgeber-SPDU besteht aus 18 Byte [107]. Hinzu kommen Stromdaten und ggf. weitere sicherheitsrelevante Eingangsdaten, die zur Sicherheits-SPS übertragen werden. Bei einem an der Sicherheits-SPS angeschlossenen mehrachsigen Roboter für MRK entsteht schnell ein großer Feldbus-Frame, der zu einer hohen Auslastung des Feldbusses führt. Dies hat unter Umständen zur Folge, dass eine höhere sicherheitsbezogene Zykluszeit erforderlich ist und somit die für eine sichere Bewegungsüberwachung notwendigen schnellen Reaktionszeiten nicht mehr eingehalten werden können. In [60] wird ein Konzept vorgestellt, wie eine große Datenmenge effizient mit dem sicherheitsbezogenen Protokoll FSoE über EtherCAT übertragen werden kann. Statt die SPDUs innerhalb des FSoE-Protokolls zu übertragen, wodurch zusätzlich Daten für den CRC anfallen, werden die SPDUs an den FSoE-Frame angehangen. Die Übertragung aller SPDUs erfolgt unverändert via Black-/Gray-Channel über EtherCAT. PROFIsafe hingegen ist besser geeignet für die Übertragung großer Datenmengen, da bei diesem Protokoll bis zu 123 Byte si-

cherheitsbezogene Daten mit einem gemeinsamen 3- oder 4-Byte-CRC versendet werden können [60]. Daher besteht bei diesem Protokoll die Möglichkeit, die SPDUs aus dem Antrieb innerhalb des Protokolls zu übertragen.

Typischerweise wird nur eine Verbindung über einen sicherheitsbezogenen Feldbus zwischen Sicherheits-SPS und Antrieb verwendet. Dies erfordert allerdings eine vollwertige zertifizierte sicherheitsbezogene Logik im Antrieb für den Feldbus-Slave [60]. Die beiden Kanäle im Slave prüfen die empfangene Master-SPDU in der Regel unabhängig voneinander und können beide in den sicheren Zustand schalten. Abbildung 30 zeigt die zweikanalige Verarbeitung der Feldbus-SPDUs im Antrieb. Der µC ist über eine erste und das FPGA über eine zweite Verbindung über ein sicherheitsbezogenes Feldbusprotokoll angeschlossen. Es gibt also zwei Verbindungen über ein sicherheitsbezogenes Feldbusprotokoll, anstatt typischerweise nur eine Verbindung zwischen der Sicherheits-SPS und dem Antrieb. Der Master des sicherheitsbezogenen Feldbusses kann in der SRASW doppelt instanziiert werden. Somit entstehen zwei einzelne Kanäle mit jeweils einer Punkt-zu-Punkt-Verbindung zwischen Master und Slave. Aufgrund dieser zweikanaligen diversitären Struktur in der Verarbeitung der SPDUs und der beiden Verbindungen ist keine vollständig zertifizierte sicherheitsbezogene Logik im Antrieb für die sicherheitsbezogene Kommunikation erforderlich. Die zyklisch zu berechnenden Slave-SPDUs für die Übertragung zur Sicherheits-SPS werden jeweils unabhängig voneinander vom µC (1. Kanal) und vom FPGA (2. Kanal) diversitär berechnet. [108]

Wie Abbildung 30 zeigt, werden in den Master-SPDUs die digitalen Ausgänge für den Antrieb übertragen, während in den Slave-SPDUs die Daten zur Diagnose zurückgelesen werden. Die digitalen Ausgänge werden auch zur Übertragung der Testsignale für die Sicherheitsfunktionen STO und SBC genutzt. Bei einem Kommunikationsausfall über den Feldbus kann ein Watchdog im Antrieb den sicheren Zustand herbeiführen.

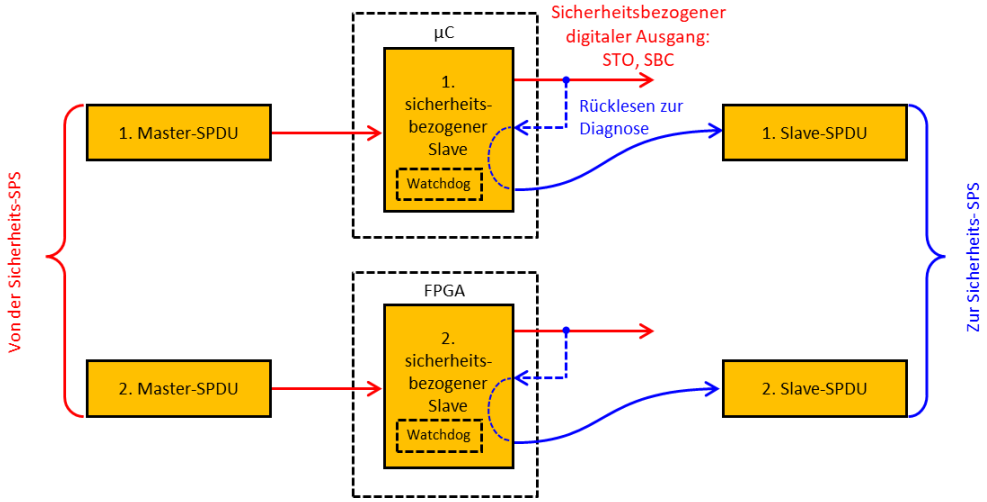


Abbildung 30: Diversitäre Verarbeitung der beiden SPDUs im Antrieb mit dem µC und dem FPGA über jeweils eine Verbindung über ein sicherheitsbezogenes Feldbusprotokoll.

4.4 Sicherheitsbezogene Strommessung

Um die Kraft einer Maschine oder das Drehmoment einzelner Achsen in einer zentralen Steuerung für eine sichere Bewegungsüberwachung zu nutzen, kann eine sicherheitsbezogene Messung des Stroms im Antrieb verwendet werden, da das Drehmoment M eines PSMs in etwa proportional zum Storm i_q ist. Betrachtet man die Drehmomente aller Achsen, kann unter Berücksichtigung der Geometrie des Roboters der Druck an den Kontaktflächen von der Sicherheits-SPS berechnet und überwacht werden [9]. Zur Überwachung des Drehmoments der einzelnen Achsen kann die Sicherheitsfunktion sicher begrenztes Drehmoment (engl.: safely-limited torque, SLT) verwendet werden.

In [106] wird ein Konzept für eine sicherheitsbezogene Strommessung mit anschließender Auswertung in einer zweikanaligen Logik nach Kategorie 3 vorgestellt. Dort werden alle drei Motorströme gemessen, um eine Redundanz zu erreichen und die Ströme unter Verwendung der Kirchhoffschen Knotenregel zu plausibilisieren, da die Summe der drei Phasenströme im Motor unter Berücksichtigung von Messungenauigkeiten null ergibt. Dadurch können Fehler in den Stromsensoren erkannt bzw. diagnostiziert werden, um den entsprechenden DC zu erreichen. Die verwendeten ΣΔ-Modulatoren bilden einen 1-Bit Bitstrom, bei dem der Kurzzeitmittelwert der Pulsdichte proportional zum gemessenen Phasenstrom verläuft. Der so generierte ΣΔ-Bitstrom ist daher prinzipbedingt ein dynamisches Signal. Der spezifizierte Eingangsspannungsbereich eines ΣΔ-basierten ADCs entspricht typischerweise einem Ausgangssignal mit einer Pulsdichte von 8 % bis 92 % [109]. Ein Fehler, bei dem der Ausgang des Modulators bei 0 % oder 100 % hängen bleibt, kann dadurch sicher aufgedeckt werden [106]. Typischerweise liegt die ΣΔ-Modulationsfrequenz $f_{\Sigma\Delta}$ zwischen 10 und 25 MHz. Dieser ΣΔ-Takt wird ebenfalls überwacht und an die Sicherheits-SPS übertragen, um eine fehlerfreie Funktion der Modulatoren zu gewährleisten [106]. Der Bitstrom wird durch Sinc^3-Dezimierungsfilter tiefpassgefiltert und in ein digitales Wort umgewandelt. Jede Millisekunde ergibt sich ein abgetastetes vorzeichenbehaftetes (signed) 12-Bit Datenwort in Zweierkomplementdarstellung mit dem Wertebereich von -2048 bis 2047. Bei der zulässigen Pulsdichte von 8 % bis 92 % ergibt sich ein nutzbarer Messbereich von -1719 bis 1719. Bei der Verwendung von ΣΔ-Modulatoren mit anschließendem Sinc^3-Dezimierungsfilter kann eine maximale effektive Anzahl an Bits (engl.: effective number of bits, ENOB) von 16 erreicht werden [35]. Für die Berechnung und Überwachung des Drehmoments und um die Auslastung des Feldbusses durch die Übertragung der Daten zur überlagerten Sicherheits-SPS zu minimieren, ist ein 12-Bit Stromsignal ausreichend.

Abbildung 31 zeigt den im Messbereich linearen Zusammenhang zwischen dem Strom einer Motorphase und dem zugehörigen 12-Bit Datenwort nach dem Sinc^3-Filter (blauer Verlauf). Liegt der Strom außerhalb des maximalen Messbereichs, also oberhalb von i_max bzw. unterhalb von i_min, wird ein Maximalwert von 2047 bzw. Minimalwert von -2048

erzeugt. Falls die Sinc³-Filter nicht innerhalb einer sicherheitsbezogenen Logik implementiert werden, ist das Testen der Filter erforderlich, um eine ordnungsgemäße Funktion sicherzustellen [106]. Daher wird in regelmäßigen Zeitabständen der Eingang des Sinc³-Dezimierungsfilters zum Testen für eine sicherheitsbezogene Zykluszeit auf „Low“ geschaltet. Als Ausgangsgröße des Sinc³-Filters bildet sich der Wert -2048, welcher außerhalb des sicherheitsbezogenen Messbereichs liegt (rote Linie in Abbildung 31).

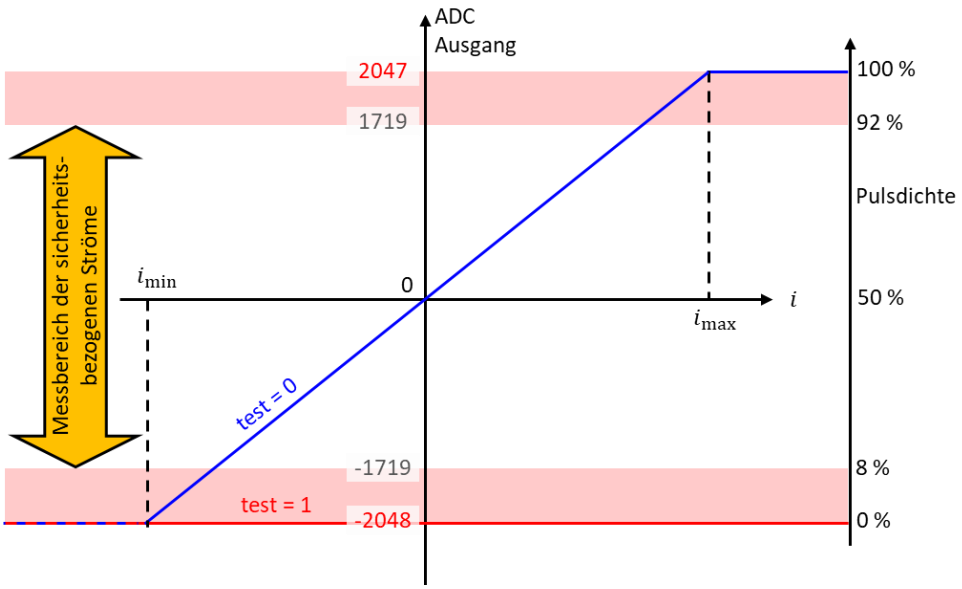


Abbildung 31: Digitales 12-Bit Datenwort nach dem Sinc³-Dezimierungsfilter in Abhängigkeit des Phasenstroms.

Abbildung 32 zeigt das Blockschaltbild der sicherheitsbezogenen Strommessung für die vorgestellte Architektur. Mit drei Stromwandlern mit anschließenden ΣΔ-Modulatoren zur Digitalisierung werden alle drei Motorphasenströme gemessen. Die beiden Kanäle im Antrieb wandeln jeweils zwei Bitströme in ein digitales 12-Bit Datenwort um. Somit werden vom ersten Kanal im µC die Ströme i_u und i_v und vom zweiten Kanal im FPGA die Ströme i_v und i_w verarbeitet. In jedem Kanal kann über die Kirchhoffsche Knotenregel der dritte Phasenstrom bestimmt werden. Daher ist es nicht notwendig, in beiden Kanälen alle drei Phasenströme zu messen [106].

Üblicherweise findet, wie auch bei den sicherheitsbezogenen Drehgebern, die Plausibilisierung der gemessenen Stromwerte mittels Kreuzvergleich im Antrieb in einer zweikanaligen sicherheitsbezogenen Logik statt. Dort können die sicherheitsbezogenen Stromwerte für die Sicherheitsfunktion SLT für eine Einzelachs-Überwachung genutzt werden. Optional können die plausibilisierten Stromwerte zur weiteren Verarbeitung über einen sicherheitsbezogenen Feldbus zur Sicherheits-SPS übertragen werden. Um auf eine sicherheitsbezogene Logik im Antrieb zu verzichten, werden die Stromwerte zur Plausibilisierung via Black-/Gray-Channel direkt zur Sicherheits-SPS übertragen (vgl. Abbildung 32). Eine Möglichkeit ist die Übertragung der vier Stromwerte innerhalb eines sicher-

heitsbezogenen Feldbusprotokolls. Wenn das Konzept aus [60] genutzt wird, können die Stromwerte antriebsintern zweikanalig zu einer ersten Strom-SPDU im µC und zu einer zweiten Strom-SPDU im FPGA verarbeitet werden. Dabei werden die Stromwerte mit zusätzlichen CRCs versehen, mit dem FSoE-CRC verknüpft und dann zusammen mit dem FSoE-Frame über EtherCAT übertragen. Ebenso werden die Diagnosemaßnahmen wie das Testen der Sinc³-Filter von der Sicherheits-SPS übernommen. Das Testsignal zum Testen der beiden Sinc³-Filter im ersten Funktionskanal wird über die erste Verbindung gesendet, während das Testsignal zum Testen der beiden Sinc³-Filter im zweiten Funktionskanal über die zweite Verbindung des sicherheitsbezogenen Feldbusprotokolls übertragen wird.

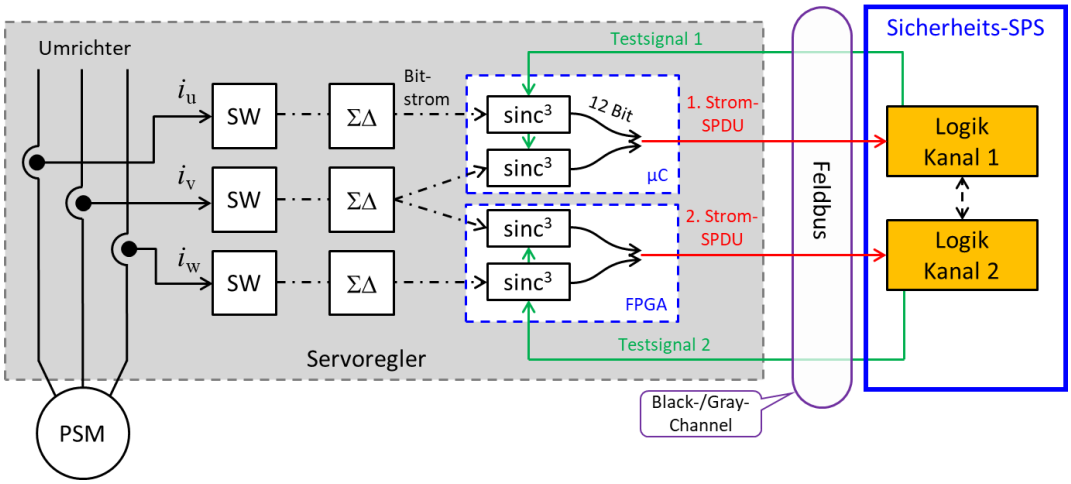


Abbildung 32: Blockschaltbild der sicherheitsbezogenen Strommessung und Übertragung zur überlagerten Sicherheits-SPS via Black-/Gray-Channel.

Abbildung 33 zeigt, dass der in Rot eingezeichnete Strom i_u immer synchron zur sicherheitsbezogenen Zykluszeit abgetastet wird. Wenn das Testsignal 1 „High“ ist und somit kein Test der Sinc³-Filter durchgeführt wird, gelangt der ΣΔ-Bitstrom des gemessenen Stroms über das „UND“-Gatter zum Sinc³-Filter und es ergibt sich ein entsprechender 12-Bit-Filterwert in Blau. Während des Tests wird das Testsignal und somit auch der Ausgang des „UND“-Gatters für eine sicherheitsbezogene Zykluszeit, z. B. 1 ms, auf „Low“ gesetzt. Bei einem erfolgreichen Test, der zum Zeitpunkt t_k gestartet wird, entspricht der Filterwert des Sinc³-Filters im Antrieb zum Zeitpunkt t_{k+1} dem Wert -2048 (maximaler negativer Wert). Zum Zeitpunkt t_{k+2} kann dieser Wert von der Sicherheits-SPS verarbeitet und ausgewertet werden.

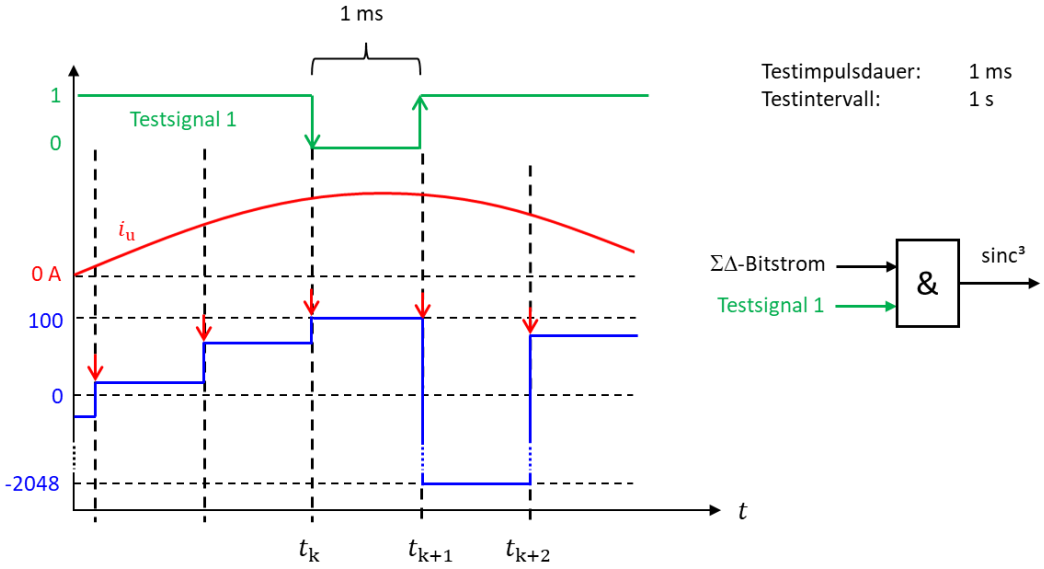


Abbildung 33: Zeitlicher Verlauf des Sinc³-Filtertests im 1. Kanal mit einem Testsignal über den sicherheitsbezogenen Feldbus.

Mit dem hier vorgestellten Konzept zur sicherheitsbezogenen Strommessung im Antrieb können in der übergeordneten Sicherheits-SPS folgende Tests zur Diagnose durchgeführt werden:

1. $|i_u| \leq 1719$ → Pulsdichte i_u
2. $|i_{v1}| \leq 1719$ → Pulsdichte i_{v1}
3. $|i_{v1} - i_{v2}| \leq$ Messfehler → $i_{v1} = i_{v2} \pm$ Messfehler
4. $|i_u + 1/2\,(i_{v1} + i_{v2}) + i_w| \leq 16$ → $i_u + i_v + i_w = 0 \pm$ Messfehler (Kirchhoff)
5. Sinc³-Filter Test Kanal 1: → i_u = -2048 i_{v1} = -2048
6. Sinc³-Filter Test Kanal 2: → i_{v2} = -2048 i_w = -2048

Die Überprüfung der Pulsdichte der Ströme i_u und i_{v1} ist ausreichend, da die Pulsdichte von i_{v2} über den dritten Test implizit getestet wird. Zusätzlich wird über den vierten Test die Pulsdichte des Stroms i_w überprüft. Arbeitet ein Stromsensor im Antrieb nicht korrekt, wird dies ebenfalls über die Kirchhoffsche Knotenregel aufgedeckt. Die Sicherheits-SPS kann aus den vier 12-Bit-Strommesswerten und einer antriebsabhängigen Skalierungskonstante C_{i_scale} die Phasenströme als Fließkomma-Variablen in die SI-Einheit Ampere umrechnen. Dabei sind auch bei der Strommessung auftretende Verstärkungsfehler und Offsetfehler zu korrigieren bzw. zu berücksichtigen.

Während der Sinc³-Filtertests des 1. Kanals im µC werden die skalierten Phasenströme in der Sicherheits-SPS mit Hilfe der Kirchhoffschen Knotenregel nur mit den Stromdaten des 2. Kanals berechnet. Umgekehrtes gilt für die Berechnung während des Filtertests des 2. Kanals. Mit der Clarke-Transformation können die drei Phasenströme in die zwei Ströme i_α und i_β umgerechnet werden. Für die nachfolgende Park-Transformation wird der elektrische Winkel φ_e des PSMs benötigt. Dadurch werden der drehmomentbildende

Strom i_q und der feldbildende Strom i_d berechnet. Für die Berechnung des Drehmoments für die Sicherheitsfunktion SLT ist neben den Strömen auch der Rotorwinkel sicherheitsbezogen zu messen. Beide motorabhängigen Konstanten (P und φ_com) zur Berechnung von φ_e können sicherheitsbezogen im remanenten Speicher des im Motor verbauten Drehgebers hinterlegt und beim Hochfahren des Antriebs ausgelesen werden. Der Strom i_q ist proportional zum Drehmoment M des PSMs und kann daher für die sichere Überwachung des Drehmoments für die Sicherheitsfunktion SLT in der Sicherheits-SPS genutzt werden. Dies gilt nur, wenn die feldbildende Stromkomponente i_d durch die FOC auf null geregelt wird und somit keinen Einfluss auf das Drehmoment hat [106]. Da ein Feldschwächbetrieb zum Erreichen höherer Drehzahlen in Kombination mit der sicherheitsbezogenen Drehmomentüberwachung nicht sinnvoll ist, kann diese Annahme getroffen werden. Weiterhin ist zu beachten, dass bei der Drehmomentkonstanten Fertigungstoleranzen und Temperaturabhängigkeiten zu berücksichtigen sind [110] und dass sich K_T mit der mechanischen Last und der magnetischen Sättigung bei hohen Strömen ändert [111].

4.5 Sicherheitsbezogene Positionsmessung

Bei einer sicheren Bewegungsüberwachung einer Maschine werden sicherheitsbezogene Positionssignale für die Überwachung von Position, Geschwindigkeit und Beschleunigung benötigt. Betrachtet man die Geschwindigkeiten aller Achsen, kann durch eine geeignete kinematische Transformation nicht nur die Geschwindigkeit einer einzelnen Achse, sondern auch die Geschwindigkeit jedes beliebigen Punktes der Maschine (z. B. Tool Center Point eines Delta-Roboters) von der Sicherheits-SPS berechnet werden [112]. Üblicherweise werden die gemessenen Positionssignale im Antrieb in einer sicherheitsbezogenen Logik plausibilisiert, verarbeitet und ggf. zur Sicherheits-SPS weitergesendet. In diesem Kapitel soll gezeigt werden, dass die Plausibilisierung und die Diagnose für die sicherheitsbezogene Positionsmessung auch von der Sicherheits-SPS übernommen werden kann und der Zwischenschritt im Antrieb nicht erforderlich ist. Dazu werden im Folgenden digitale Positionsgeber und eine sicherheitsbezogene Positionsmessung mit einem einzelnen Resolver betrachtet.

4.5.1 Digitale Drehgeber

Zur Messung der sicherheitsbezogenen Position kann ein digitales sicherheitsbezogenes Drehgeber-Protokoll verwendet werden. Die von dem Drehgeber zur Verfügung gestellte Drehgeber-SPDU ist herstellerspezifisch und zwischen 16 und 22 Byte groß [60]. Für die Auswertung der Drehgeber-SPDU in der übergeordneten Sicherheits-SPS wird diese unverändert über den Feldbus weitergeleitet. Der Antrieb und der Feldbus werden somit Teil des Black-/Gray-Channels. Für eine eindeutige Zuordnung der sicherheitsbezogenen

Position zu einer Achse ist, wie auch bei sicherheitsbezogenen Feldbusprotokollen üblich, im Drehgeberprotokoll eine sicherheitsbezogene Achsadresse notwendig, welche in einem Maschinenmodul, bestehend aus einer Sicherheits-SPS und mehreren Achsen, einmalig ist.

Abbildung 34 zeigt schematisch die Anbindung eines sicherheitsbezogenen Drehgebers über den Antrieb an die übergeordnete Sicherheits-SPS. Die sicherheitsbezogenen Positionsdaten werden im Drehgeber erzeugt und in der Sicherheits-SPS verarbeitet. Die zyklische Abtastung der sicherheitsbezogenen Positionswerte erfolgt jede Millisekunde und wird mit der sicherheitsbezogenen Zykluszeit des Feldbusses synchronisiert. Die SPDU (Rot) wird vom Antrieb unverändert über den Feldbus an die übergeordnete Sicherheits-SPS übermittelt. Der Antrieb und der Feldbus sind somit Teil eines Black-/Gray-Channels für das Drehgeber-Protokoll. Die nicht sicherheitsbezogenen Positionsdaten (Grün) werden mit der Zykluszeit der Antriebsregelung im µC des Antriebs verarbeitet. Diese Verarbeitung hat keinen Einfluss auf die Drehgeber-SPDU. Die Auswertung der Drehgeber-SPDU wird nicht mehr im Antrieb, sondern zweikanalig in der übergeordneten Sicherheits-SPS durchgeführt. Somit ist auch für die sicherheitsbezogene Positionsmessung keine vollständige sicherheitsbezogene Logik im Antrieb mehr nötig.

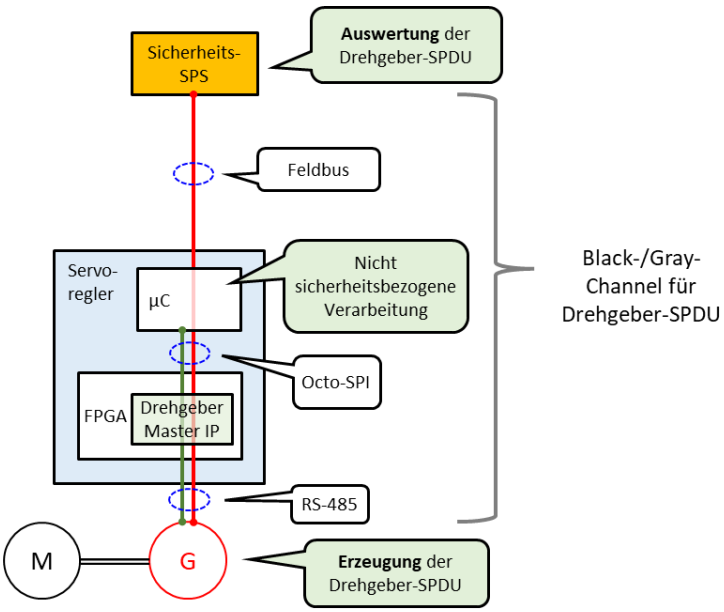


Abbildung 34: Schematische Darstellung der Anbindung eines sicherheitsbezogenen Drehgebers über den Antrieb (FPGA und µC) an die übergeordnete Sicherheits-SPS.

Alternativ zur Verwendung eines zertifizierten sicherheitsbezogenen Drehgebers unterstützt die diversitäre Architektur auch zwei konventionelle Drehgeber. Für eine diversitäre Positionsmessung werden zwei digitale Drehgeber von verschiedenen Herstellern oder mit unterschiedlichen Messprinzipien eingesetzt. Die Position des ersten Drehgebers wird zum 1. Kanal im µC und die Position des zweiten Drehgebers zum 2. Kanal im FPGA übertragen. Die Positionssignale können dann entweder über ein sicherheitsbezogenes

Feldbusprotokoll oder verarbeitet als SPDUs nach dem Konzept aus [60] zur Sicherheits-SPS übertragen werden. In der Sicherheits-SPS können die beiden Positionen miteinander verglichen werden, um ein sicherheitsbezogenes Positionssignal zu erhalten. Da es sich hierbei um nicht sicherheitszertifizierte Drehgeber handelt, können diese mit geringem Aufwand ausgetauscht werden, ohne dabei die funktionale Sicherheit des Systems zu beeinträchtigen. Um Ausfälle in einem Kanal zu erkennen ist neben dem Kreuzvergleich eine entsprechende externe Diagnose in der Sicherheits-SPS durchzuführen.

Unabhängig von der Erzeugung der sicherheitsbezogenen Position kann diese in der übergeordneten Sicherheits-SPS direkt für die Sicherheitsfunktion SLP, durch einfache numerische Differentiation als Geschwindigkeit für SLS und durch zweifache Differentiation als Beschleunigung für SLA genutzt werden.

4.5.2 Gemischt kritische Resolver-Digital-Wandlung

Der gemischt kritische RDC erzeugt sowohl ein sicherheitsbezogenes Positionssignal für die übergeordnete Sicherheits-SPS als auch ein nicht sicherheitsbezogenes Positionssignal für die Antriebsregelung. Aufgrund ihrer geringen Ausfallrate werden Resolver als bewährte Komponenten betrachtet und in der Regel nicht, wie bei digitalen Drehgebern üblich, als sicherheitszertifizierte und somit teurere Version für sicherheitsbezogene Anwendungen angeboten. Für eine Kategorie-3-Architektur nach DIN EN ISO 13849-1 werden zur Erzeugung eines sicherheitsbezogenen Positionssignals zwei solcher RDCs und zwei Resolver benötigt. Durch den Sin- und Cos-Kanal allein liegt keine Zweikanaligkeit vor, da für die Sicherheitsfunktion SLP auch die Messung der Drehrichtung notwendig ist. Für diese Messung ist die Phasenverschiebung zwischen den beiden Resolversignalen ausschlaggebend, weshalb für diese Sicherheitsfunktion sowohl das Sin-Signal als auch das Cos-Signal benötigt werden [84].

Nach DIN EN ISO 13849-1 ist der zweikanalige Aufbau jedoch für Kategorie 3 nicht zwingend erforderlich. Es können auch einkanalige Teile ohne gefährliches Fehlerpotential verwendet werden. Für die mechanische Verbindung zwischen Motor und Resolver ist z. B. der Nachweis eines Fehlerausschlusses durch den Hersteller erforderlich. Darüber hinaus ist durch die Überwachung eine ausreichend schnelle Fehlererkennung in Bezug auf die Prozesssicherheitszeit zu gewährleisten, um das System in einen sicheren Zustand zu schalten und gefährliche Zustände zu verhindern. Die Prozesssicherheitszeit ist dabei die Zeit, die ein Fehler braucht, um einen gefährlichen Zustand auszulösen bzw. einen Schaden zu verursachen. Bei der Verwendung eines Resolvers sind auch die Sin- und Cos-Leitungen nur noch einkanalig, sodass bei den Resolver-Leitungen ein Drahtbruch oder Spannungsausfall über die Diagnose aufzudecken ist. Durch die kurze sicherheitsbezogene Zykluszeit zwischen dem Antrieb und der Sicherheits-SPS ist eine schnelle Fehleraufdeckung über die Diagnose möglich. Werden diese Anforderungen eingehalten,

kann die zweikanalige Struktur so angepasst werden, dass nur ein Resolver mit seinen zwei analogen Ausgangssignalen als sicherheitsrelevanter Sensor verwendet wird, der die Anforderungen an Kategorie 3 erfüllt. [52], [84]

Für den gemischt-kritischen RDC sollen die bereits bewährten Methoden für digitale sicherheitsbezogene Drehgeber verwendet werden. Abbildung 35a) zeigt die traditionelle Konfiguration, bei der die sicherheitsbezogene Logik des Antriebs aus den analogen Resolversignalen ein digitales sicherheitsbezogenes Positionssignal bildet. Diese Position kann über einen sicherheitsbezogenen Feldbus an eine übergeordnete Sicherheits-SPS übertragen werden. In Abbildung 35b) wird ein sicherheitsbezogenes digitales Drehgeber-Protokoll vom Antrieb direkt via Black-/Gray-Channel an die Sicherheits-SPS weitergeleitet. Abbildung 35c) zeigt eine Konfiguration, bei der die Analog-Digital-Wandlung ähnlich wie in Abbildung 35a) im Antrieb realisiert ist. Jedoch erfolgt die Übertragung an die Sicherheits-SPS wie bei den sicherheitsbezogenen Drehgebern als redundante Positionssignale mit CRC. Die Plausibilisierung der redundanten Positionen und die Diagnose werden von der Sicherheits-SPS durchgeführt.

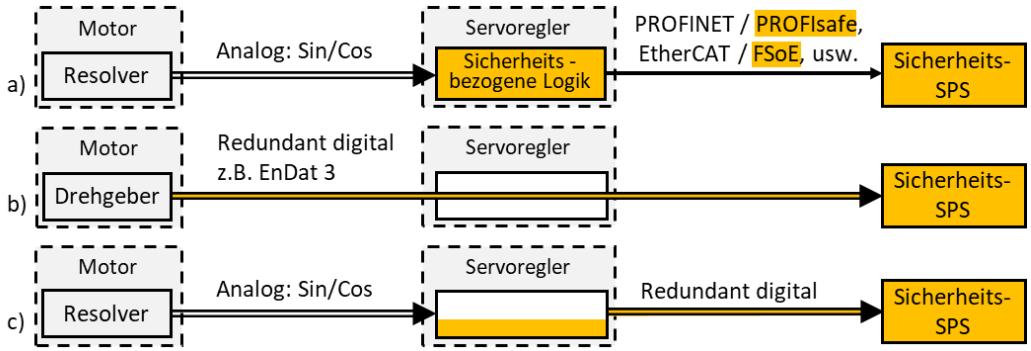


Abbildung 35: Bereitstellung eines sicherheitsbezogenen Positionssignals über den Antrieb an eine übergeordnete Sicherheits-SPS.

Abbildung 36 zeigt das Blockschaltbild des sicherheitsbezogenen, kostengünstigen und volldigitalen RDCs. Die RDCs können dabei nach dem in [46] vorgestellten Konzept umgesetzt werden. Die 8-kHz-Sinusspannung U_{ref}, die den Resolver anregt, wird digital als ΣΔ-Bitstrom erzeugt. Dies ähnelt der gängigen Class-D-Audioverstärkertechnik und bietet einen hohen Wirkungsgrad bei maximaler Flexibilität hinsichtlich der Signalform mit nur wenigen nicht-integrierten Komponenten. Zur Signalverstärkung wird ein herkömmlicher Treiber-IC verwendet und zur Signalglättung genügt ein LC-Tiefpassfilter. Die beiden winkelabhängigen Ausgangssignale des Resolvers werden quasi-kontinuierlich (z. B. $f_{\Sigma\Delta} = 10$ MHz) durch zwei ΣΔ-Modulatoren 2. Ordnung digitalisiert. Die digitalen Sinc³-Filter in beiden Kanälen (FPGA und µC) verarbeiten unabhängig voneinander beide Bitströme und wandeln diese in ein digitales Wort um. Für eine synchrone Abtastung werden alle Sinc³-Dezimierungsfilter vom FPGA gestartet. Wie in Abbildung 36 dargestellt, kann der erste Kanal im µC und der zweite Kanal im FPGA der

vorgestellten Antriebsstruktur implementiert werden. Der ΣΔ-Modulator erzeugt im Hinblick auf die funktionale Sicherheit prinzipbedingt ein dynamisches Signal und Stuck-at-Fehler werden aufgedeckt. Außerdem sind die beiden Resolver-Ausgangsspannungen $U_{\sin}$ und $U_{\cos}$ zur Bildung des sicherheitsbezogenen Positionssignals prinzipbedingt dynamisch, was eine Diagnose ohne Zwangsdynamisierung liefert.

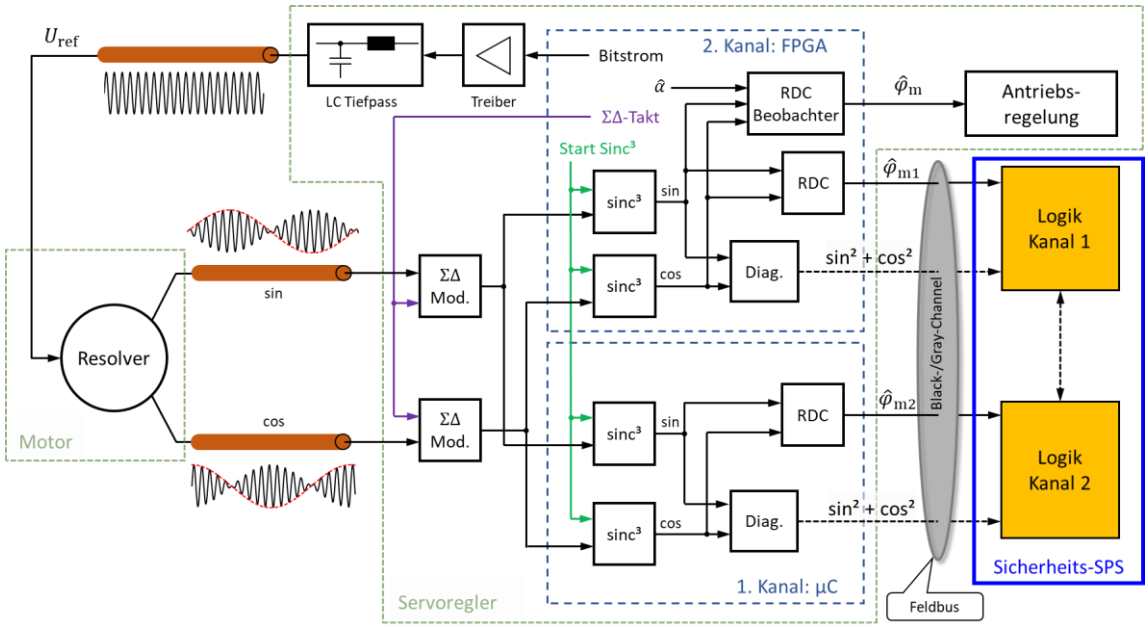


Abbildung 36: Blockschaltbild des sicherheitsbezogenen volldigitalen RDCs mit einer diversitären redundanten Verarbeitung der Resolversignale im µC und FPGA.

Die beiden sicherheitsrelevanten RDC-Tracking-Loops sind unabhängig voneinander in beiden Kanälen mit konstanter Bandbreite implementiert. Die folgende Gleichung wird verwendet, um den Betrag der Resolversignale für die Diagnose zu überprüfen:

$$U_{\sin}^2 + U_{\cos}^2 = C \pm \varepsilon \tag{7}$$

Die beiden Kanäle führen die Berechnung nach Gleichung (7) durch und die Sicherheits-SPS überwacht, ob das Ergebnis innerhalb der vorgegebenen Abweichung ε liegt [84]. Über diese Diagnose kann ein Fehler wie Drahtbruch oder Spannungsausfall in der Resolver-Leitung erkannt und über die Sicherheits-SPS in den sicheren Zustand geschaltet werden. Die beiden Positionssignale $\hat{\varphi}_{\mathrm{m1}}$ und $\hat{\varphi}_{\mathrm{m2}}$ sowie deren Diagnosedaten können für die Black-/Gray-Channel-Kommunikation nach [60] mit Zusatzinformationen versehen und an die übergeordnete Sicherheits-SPS als Resolver-SPDUs übertragen werden. Alternativ können $\hat{\varphi}_{\mathrm{m1}}$ und $\hat{\varphi}_{\mathrm{m2}}$ über ein sicherheitsbezogenes Feldbusprotokoll übertragen werden. Obwohl die sicherheitsrelevanten Positionssignale mit einer Aktualisierungsrate von 16 kHz von den Tracking-Loops erzeugt werden, erfolgt die Übertragung der beiden Positionen an die Sicherheits-SPS nur mit 1 kHz. Für die sicherheitsrelevanten Positionssignale ist eine Auflösung von 12 Bit ausreichend und auch die Diagnosedaten bestehen aus 12 Bit.

Prinzipbedingt liefern Resolver nur Singleturn-Informationen, sodass nach der Inbetriebnahme eine sicherheitsbezogene Referenzfahrt erforderlich sein kann. Neben der sicherheitsbezogenen Position kann ein weiterer RDC im FPGA für ein nicht sicherheitsbezogenes Positionssignal implementiert werden. Um die Regelkreise im Antrieb zu schließen und eine durch die Tracking-Loop verursachte Phasenverschiebung zu kompensieren, kann die nicht sicherheitsbezogene Tracking-Loop zu einem konfigurierbaren quasi-zeitkontinuierlichen modellbasierten Luenberger-Beobachter erweitert werden, wie in [43] beschrieben. Dazu wird ein geschätztes Beschleunigungssignal $\hat{\alpha}$ hinzugefügt, um ein hochauflösendes nicht sicherheitsbezogenes Positionssignals $\hat{\varphi}_\mathrm{m}$ mit hoher Bandbreite bereitzustellen. Für die Sicherheits-SPS sind die Signalverzögerungen nicht kritisch, da die Abtastrate der sicherheitsbezogenen Position viel niedriger ist als die der Regelkreise. Ein Vorteil der nicht sicherheitsbezogenen Tracking-Loop für die Antriebsregelung ist, dass neben dem Positionssignal $\hat{\varphi}_\mathrm{m}$ auch das Geschwindigkeitssignal $\hat{\omega}_\mathrm{m}$ implizit berechnet wird. Dadurch ist es möglich, sowohl den Lageregelkreis als auch direkt den Drehzahlregelkreis zu schließen.

4.6 Sicherheitsbezogene Ein- und Ausgänge mit IO-Link

In der IEC 61131-9 [113] ist die digitale Kommunikationsschnittstelle IO-Link spezifiziert. Diese Punkt-zu-Punkt-Schnittstelle ist für kleine und günstige Sensoren und Aktoren mit integrierten Mikrocontrollern vorgesehen. Diese Technologie dient der Übertragung von Parametern und Diagnosedaten von Geräten zu Automatisierungssystemen. Bei Automatisierungssystemen mit Feldbus-Struktur kann IO-Link als Standardschnittstelle für die Verbindung von Sensoren und Aktoren via Gateway an eine zentrale SPS genutzt werden. IO-Link-Treiber können auch für klassische digitale 24-V-Ein- und Ausgänge nach DIN EN 61131-2 sowie für einfach schaltende Sensoren und Aktoren wie induktive Näherungsschalter verwendet werden. Somit werden mit einem Baustein sowohl klassische Ein- und Ausgänge als auch IO-Link-Geräte unterstützt. [114]

In diesem Kapitel wird gezeigt, wie mit der IO-Link-Schnittstelle kostengünstig sicherheitsbezogene digitale Ein- und Ausgänge für den Antrieb realisiert und IO-Link-Sensoren an die übergeordnete Sicherheits-SPS angeschlossen werden können. Der IO-Link-Master ist im Antrieb integriert und es kann jedes IO-Link kompatible Gerät angeschlossen werden. Der Antrieb ist somit einerseits ein IO-Link-Master und hat direkten Zugriff auf die Daten des IO-Link-Geräts. Andrerseits dient er als eine Art Gateway, um die Daten der übergeordneten Steuerung zur Weiterverarbeitung bereitzustellen [115]. Im Antrieb kommuniziert der IO-Link-Master-Transceiver mit der Steuerelektronik (FPGA bzw. µC). Je nach Konfiguration des IO-Link-Master-Transceivers können die drei Leitungen L+, C/Q und DI/DO für verschiedene Zwecke verwendet werden. Falls ein IO-Link-Gerät angeschlossen wird, werden nur die Leitungen L+, C/Q und L- benötigt [114].

L+ ist die Spannungsversorgung und L- das Massepotential des IO-Link-Geräts. Über die Leitung C/Q werden die Daten vom Gerät zum Master übertragen bzw. umgekehrt. Diese Leitung kann für eine serielle Halb-Duplex-Datenübertragung verwendet werden. Um die IO-Link-Technologie nutzen zu können, ist die Implementierung eines IO-Link-Master-Software-Stacks in der Steuerelektronik des Antriebs notwendig. Dieser kann im µC oder optional in einem Softcore-Prozessor im FPGA implementiert werden. Wenn kein IO-Link-Gerät angeschlossen ist, kann ein einziger IO-Link-Master-Transceiver für mehrere digitale Ein- und Ausgänge zur gleichen Zeit verwendet werden. Die Leitung L+ ist abschaltbar und kann als digitaler Ausgang mit Kurzschlusserkennung dienen. Die C/Q-Leitung kann sowohl als digitaler Eingang als auch als digitaler Ausgang verwendet werden. Zusätzlich kann diese Leitung als Testsignalausgang für sicherheitsbezogene digitale Eingänge genutzt werden. Die DI/DO-Leitung, welche bei einem IO-Link-Gerät nicht angeschlossen wird, kann für digitale Ein- und Ausgänge genutzt werden. Bei den meisten Transceivern kann dieser zusätzliche Anschluss lediglich als digitaler Eingang DI konfiguriert werden [116]. Die Konfiguration des IO-Link-Master-Transceivers kann über eine SPI erfolgen. Die Datenübertragung über die C/Q-Leitung kann ebenfalls über die SPI oder über eine universelle asynchrone Empfänger/Sender-Schnittstelle (engl.: universal asynchronous receiver/transmitter, UART) vom Prozessor gesteuert werden.

Abbildung 37 zeigt, wie mit zwei Standard-IO-Link-Master-Transceivern eine zweikanalige Struktur für sicherheitsbezogene Ein- und Ausgänge nach Kategorie 3 mit dem µC und FPGA im Antrieb realisiert werden kann. Abbildung 37a) zeigt den zweikanaligen Anschluss eines Not-Halt-Schalters an zwei IO-Link-Master. Die beiden C/Q-Leitungen dienen als Ausgänge für die Testsignale, während die beiden DI-Leitungen zum Zurücklesen des Signals genutzt werden. Dabei wird das von dem einen IO-Link-Master erzeugte Testsignal von dem anderen IO-Link-Master zurückgelesen und umgekehrt. Abbildung 37b) zeigt eine zweikanalige Abschaltung der Motorversorgung über zwei Relais mit zwangsgeführten Kontakten, ähnlich wie sie auch für die Sicherheitsfunktion STO verwendet wird. Die drei Schließerkontakte werden für die drei Phasen des Motors verwendet, wohingegen der Öffnerkontakt für die Diagnose eingesetzt wird. Die C/Q-Leitungen werden als Ausgänge für die Ansteuerung der Relais verwendet. Über L+ kann der Öffner mit 24 V versorgt werden und der Status zur Diagnose kann über die DI-Leitung zurückgelesen werden. Abbildung 37c) zeigt den Anschluss einer Lichtschranke an zwei IO-Link-Master. Das obere Gerät stellt den Sender dar und das untere den Empfänger. Über die Leitungen L+ und L- werden sowohl Sender als auch Empfänger mit Spannung versorgt. Bei dieser Lichtschranke besitzt der Sender einen Testeingang, welcher von dem C/Q-Ausgang des ersten IO-Link-Masters angesteuert wird. Während dieses Tests wird der Sender periodisch abgeschaltet (0 V), sodass auch die Ausgänge des Empfängers abschalten sollen [117]. Der Empfänger verfügt über zwei Schaltausgänge, die als Output Signal Switching Device (OSSD) Ausgang bekannt sind. Der Empfänger sendet Testim-

pulse auf den Ausgang, um die Funktion des Ausgangs selbst zu überprüfen, was dem Interface Typ C nach [118] entspricht. Die Testimpulse dürfen dabei keine Auswirkung auf die Auswertung der OSSD-Ausgangssignale haben. Die beiden OSSD-Ausgangssignale werden in Abbildung 37c) über die beiden DI-Leitungen zurückgelesen.

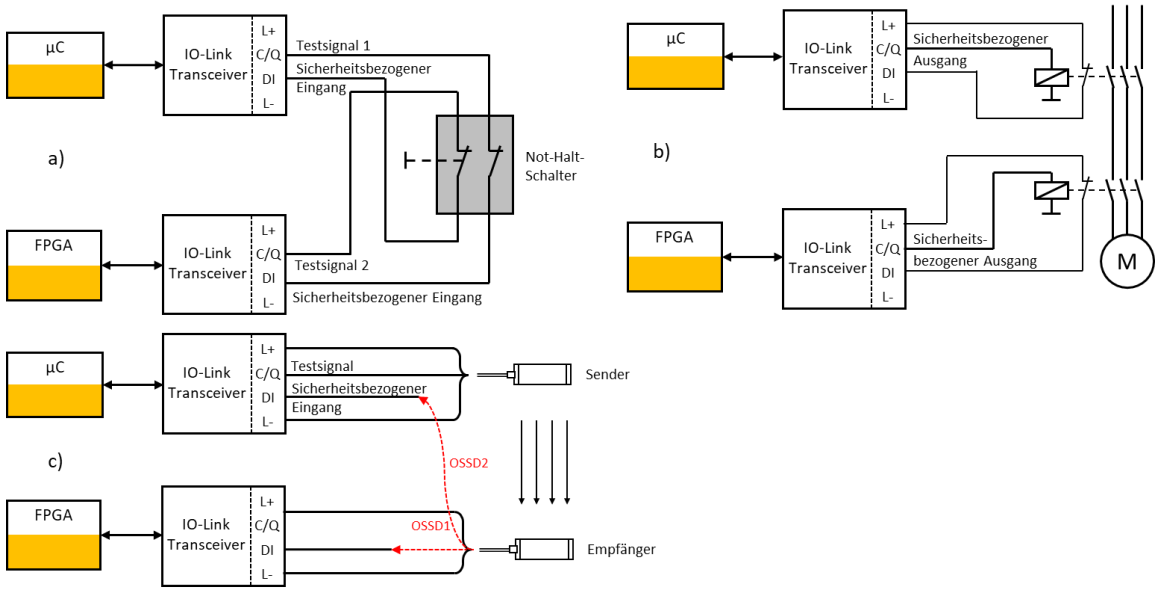


Abbildung 37: Konfigurationen der IO-Link-Master für verschiedene Anwendungen zur Verwendung als sicherheitsbezogene digitale Ein- und Ausgänge am Antrieb.

Die Auswertung der sicherheitsrelevanten Eingangssignale und die Erzeugung der Testsignale wird in allen drei Fällen von der übergeordneten Sicherheits-SPS übernommen und nicht vom IO-Link-Master im FPGA oder µC des Antriebs. Diese dienen lediglich als Schnittstelle zur Sicherheits-SPS. Für die Weiterleitung der Signale zwischen Antrieb und Sicherheits-SPS kann ein sicherheitsbezogenes Feldbusprotokoll verwendet werden. Obwohl der IO-Link-Master-Software-Stack nur in einem Prozessor implementiert werden kann, wird das FPGA, wie in Abbildung 37 gezeigt, als zweiter Kanal zum Rücklesen und Ansteuern der C/Q- und DI-Leitungen über die UART-Schnittstelle genutzt.

Der zusätzliche Aufwand im Antrieb für die sicherheitsbezogenen Ein- und Ausgänge ist gering und beschränkt sich lediglich auf die Hardwarekomponenten durch die Transceiver und den IO-Link-Software-Stack im Prozessor, wodurch dieser Ansatz ideal für einen kompakten und kostengünstigen Antrieb geeignet ist.

4.7 Degradierter Betrieb

In [12] werden verschiedene Varianten des degradierten Betriebs vorgestellt. Eine Variante ist der zeitlich begrenzte Betrieb. Bezogen auf die vorgestellte Antriebsstruktur kann sich folgendes Verhalten der Sicherheitsfunktion STO ergeben. Falls der Abschalttest im ersten Kanal nicht erwartungsgemäß funktioniert, ist der Funktionskanal im µC als fehlerhaft anzusehen. Über den zweiten Funktionskanal im FPGA kann weiterhin abgeschal-

tet werden, wodurch die Sicherheitsfunktion STO immer noch einkanalig ausgeführt werden kann. Diese strukturelle Veränderung hat Einfluss auf die Kategorie und somit auf die PFH_D und das PL nach DIN EN ISO 13849-1. Dadurch erhöht sich das Risiko zur Entstehung eines gefahrbringenden Ausfalls, weshalb der degradierte Betrieb zeitlich begrenzt wird. Wird diese spezifizierte Zeit vom degradierten Betrieb überschritten oder entsteht ein weiterer Fehler, hat der Entscheider sofort sicher abzuschalten. Folgende Bedingungen sind nach [12] zu erfüllen, damit der zeitlich begrenzte sichere Betriebszustand ausgeführt werden darf:

- Redundante Systemarchitektur: Die diversitäre Redundanz des Antriebssystems bestehend aus µC und FPGA erfüllt dieses Kriterium.
- Widerstandsfähigkeit gegen CCF: Es sind die Anforderungen nach der DIN EN ISO 13849-1 zu erfüllen (vgl. Tabelle 2) und es sind mehr als 65 Punkte erforderlich.

Eine weitere Variante ist der Betriebszustand ohne Zeitbegrenzung. Diese Variante könnte bei dem vorgestellten Antriebssystem beim Ausfall eines Kanals bei der sicherheitsbezogenen Strommessung zur Überwachung des Drehmoments eingesetzt werden. Wenn der $Sinc^3$-Filtertest im FPGA nicht erfolgreich ist, ist dieser Kanal als fehlerhaft anzusehen. Das Drehmoment kann dann nicht mehr sicherheitsbezogen überwacht werden. Das dadurch entstehende Risiko kann durch die Verringerung der Geschwindigkeit und Aktivierung der Sicherheitsfunktion SLS zur Überwachung dieser Geschwindigkeit reduziert werden. Das Risiko einer gefahrbringenden Bewegung, die zur Verletzung von Personen führen kann, wird reduziert, da die kinetische Energie der Maschine abnimmt.

Da es sich bei der vorgestellten Antriebsarchitektur nach [95] um ein Teilsystem aus Standardkomponenten handelt und nicht um ein qualifiziertes Teilsystem, das die Diagnose selbst ausführt und den Entscheider beinhaltet, kann die Diagnose nur extern durchgeführt werden und auch der Entscheider befindet sich in einer externen sicherheitsbezogenen Logik. Dieser Ansatz wird in Abbildung 38 dargestellt. Der Antrieb besitzt, wie für den degradierten Betrieb zwingend erforderlich, eine zweikanalige Struktur für die Sicherheitsfunktion. Dadurch ist die Fehlertoleranz gegeben und bei einem Fehler in einem Kanal kann die Sicherheitsfunktion weiterhin über den anderen Kanal ausgeführt werden. Die Diagnose der Ausgänge und der Kreuzvergleich werden nicht mehr im Antrieb durchgeführt, sondern in der überlagerten Sicherheits-SPS. Wie in Abbildung 38 gezeigt, werden die Diagnosesignale durch die Logik im Antrieb und den sicherheitsbezogenen Feldbus bis hin zur zentralen qualifizierten Diagnose in der Sicherheits-SPS weitergeleitet. Auch hier bewertet der Entscheider anhand der $Diagnose^+$, ob ein degradierter Betrieb des Antriebs möglich ist oder ob eine Abschaltung der Ausgänge des Antriebs in den sicheren Zustand erforderlich ist. Über ein Statussignal, das ebenfalls über den sicherheits-

bezogenen Feldbus übertragen wird, kann dem Antrieb mitgeteilt werden, ob der degradierte Zustand aktiv ist (Z_{in} und Z_{out}).

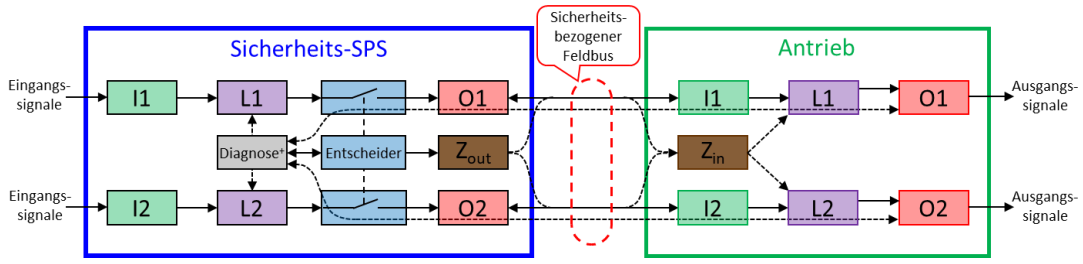


Abbildung 38: Sicherheitsbezogene Antriebsstruktur mit externer qualifizierter Diagnose und Entscheider in der überlagerten Sicherheits-SPS.

Der Vorteil bei einer zentralen Diagnose$^+$ ist, dass die Sensoren und Aktoren bzw. der Antrieb keine sicherheitsbezogene Logik für die qualifizierte Diagnose benötigen und somit auch Standardkomponenten eingesetzt werden können. Außerdem wird nur eine einzige Diagnose$^+$ und ein zentraler Entscheider benötigt, der für mehrere Antriebe und Sensoren bzw. Aktoren die Bewertung für den degradierten Betrieb übernehmen kann. Dieser Ansatz ist auch mit der gezeigten sicherheitsbezogenen Antriebsstruktur kompatibel, bei der ebenfalls diversitäre redundante Standardkomponenten verwendet werden. Durch die geringe sicherheitsbezogene Buszykluszeit ist eine schnelle Diagnose und demnach auch eine schnelle Reaktion des Entscheiders bei einem Fehlerfall in einem Kanal möglich.

4.8 Antriebsinterne Diagnose

Obwohl der Großteil der Diagnose in der übergelagerten Sicherheits-SPS durchgeführt wird, sind gewisse Tests weiterhin im Antrieb zu realisieren. Bei den Maßnahmen gegen CCF wird in dem Punkteschema nach der DIN EN ISO 13849-1 der Schutz gegen Überspannung und Übertemperatur aufgelistet (vgl. Tabelle 2). Diese Maßnahmen können nicht direkt von der Sicherheits-SPS übernommen werden und sind weiterhin im Antrieb durchzuführen.

4.8.1 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache

Abbildung 39 zeigt die Konfiguration einer möglichen Spannungsversorgung der Steuerelektronik im Antrieb. Je nach verwendeten Komponenten sind die benötigten Spannungen unterschiedlich, dennoch kann das Konzept zur Spannungsüberwachung mit geringen Anpassungen verwendet werden. Die Steuerelektronik erhält die Versorgungsspannung durch ein separates 24-V-Netz in Form einer Sicherheitskleinspannung (engl.: safety extra low voltage, SELV) oder Schutzkleinspannung (engl.: protective extra low voltage, PELV). Falls keine USV vorhanden ist, steht der Steuerelektronik bei Netzausfall auch

keine Versorgungsspannung mehr zur Verfügung und die Abschaltung der Maschine in den sicheren Zustand ist erforderlich. Durch den Wegfall der Versorgungsspannung wird der Motor automatisch drehmomentfrei geschaltet, da keine Pulsmuster mehr erzeugt werden können. Außerdem fällt auch, falls vorhanden, die Motorhaltebremse ein, da kein Strom mehr fließen kann, wodurch eine Gefährdung durch hängende Lasten verhindert wird. Das kontrollierte Abbremsen mit der Sicherheitsfunktion SS1 ist in diesem Fall nicht mehr möglich. Wird zusätzlich noch ein Filter für eine verbesserte elektromagnetische Verträglichkeit (EMV) im 24-V-Netz im Einklang mit der für die Anwendung passenden Norm vorgesehen, können nach Tabelle 2 noch weitere Punkte für Maßnahmen gegen CCF angerechnet werden [52].

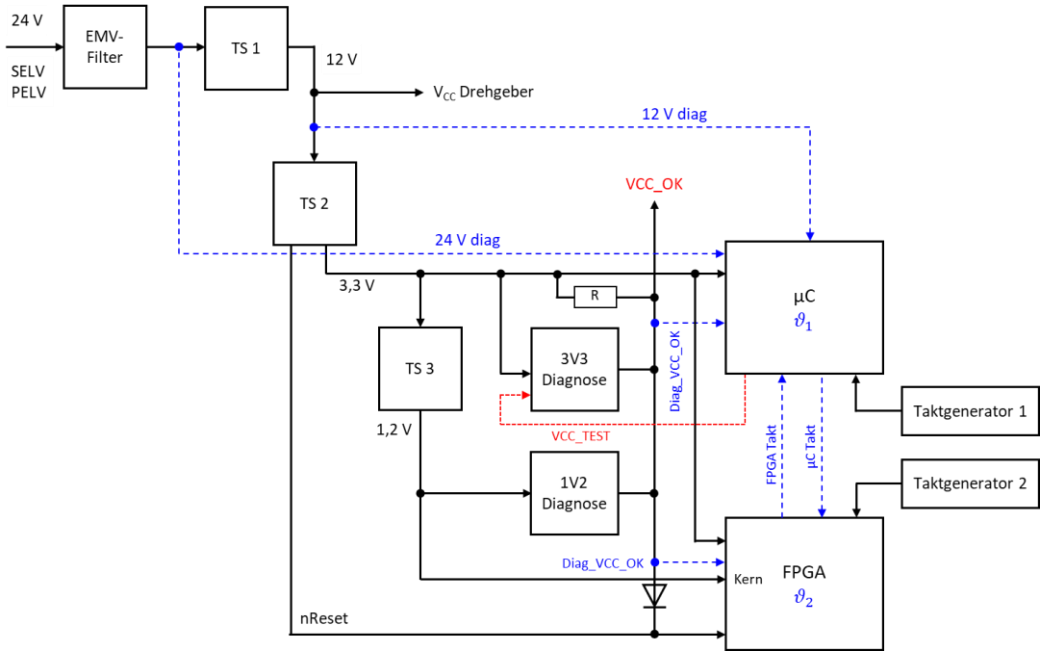


Abbildung 39: Blockschaltbild der Spannungsversorgung für die Steuerelektronik im Antrieb.

Der erste Tiefsetzsteller TS 1 erzeugt aus der 24-V-Eingangsspannung eine 12-V-Gleichspannung, die auch optional angeschlossene Drehgeber versorgt. Der benutzte Tiefsetzsteller sollte mit einer höheren Eingangsspannung spezifiziert sein, um auch bei auftretenden Spannungsschwankungen aus dem Versorgungsnetz weiterhin funktionsfähig zu bleiben. Diese 12-V-Spannung kann ebenso wie die 24-V-Eingangsspannung von dem µC mit On-Chip-ADCs auf Über- und Unterspannung überwacht werden.

Der Tiefsetzsteller TS 2 erzeugt aus den 12 V von TS 1 eine 3,3-V-Gleichspannung zur Versorgung von µC und FPGA. Diese Spannung wird von einem speziellen Baustein (3V3 Diagnose) auf Über- und Unterspannung überwacht. Dieser Baustein kann das Signal VCC_OK mit Open-Drain-Ausgängen inaktiv schalten, um ohne µC und FPGA den sicheren Zustand (STO und SBC ausgelöst) herbeizuführen. Die Parallelschaltung mehrerer Open-Drain-Ausgänge bewirkt eine „UND“-Verknüpfung. Nur wenn alle Open-Drain-Ausgänge hochohmig sind, kann der Pull-up-Widerstand das Signal VCC_OK auf

„High“ (3,3 V) schalten. Das low-aktive Signal nReset wird erst dann auf „High“ geschaltet, wenn TS 2 ordnungsgemäß arbeitet. Wenn nReset „Low“ ist, wird VCC_OK über die Diode ebenfalls auf „Low“ geschaltet. Das Signal VCC_OK wird vom µC und FPGA ausgewertet (diag_VCC_OK) und zur Diagnose an die Sicherheits-SPS gesendet. Über das Signal VCC_TEST kann die Funktion und der Abschaltpfad des 3,3-V-Überwachungsbausteins getestet werden und das Ergebnis kann über diag_VCC_OK zurückgelesen werden. Dies kann beim Hochfahren des Antriebs oder in Ruhephasen durchgeführt werden, wenn der Antrieb nicht aktiv ist.

Der Tiefsetzsteller TS 3 erzeugt aus den 3,3 V eine 1,2-V-Versorgungsspannung nur für den FPGA-Kern. Auch diese Spannung wird von einem speziellen Baustein (1V2 Diagnose) auf Über- und Unterspannung überwacht, der das Signal VCC_OK ebenfalls mit Open-Drain-Ausgängen inaktiv schalten kann, um den sicheren Zustand herbeizuführen.

Fällt der Tiefsetzsteller TS 1 aus, sodass die Eingangsspannung von 24 V am Tiefsetzsteller TS 2 anliegt, sollte dieser trotzdem die Versorgungsspannung von 3,3 V stabil halten, um einen Weiterbetrieb der Steuerelektronik zu gewährleisten. Durch die Messung der 12-V-Spannung durch den µC wird der Fehler aufgedeckt und es kann der sichere Zustand, optional auch mit SS1, kontrolliert über die Steuerelektronik herbeigeführt werden. Bei der Sicherheitsfunktion SS1 ist jedoch zu beachten, dass nur die zeitüberwachte Option SS1-t ausgeführt werden kann, da ggf. der Drehgeber durch eine Überspannung nicht mehr funktionsfähig ist. Falls der Tiefsetzsteller TS 2 ausfällt und die Ausgangsspannung 12 V beträgt, zieht der Überwachungsbaustein für die 3,3 V das Signal VCC_OK auf „Low“ und schaltet den Antrieb mit STO und SBC direkt über die Hardware in den sicheren Zustand. Bei der Konfiguration der Überwachungsbausteine (3V3 Diagnose und 1V2 Diagnose) ist zu beachten, dass die von den Herstellern angegebenen Spannungstoleranzen für das FPGA und den µC nicht überschritten werden.

Zur Temperaturüberwachung der Steuerelektronik ($\vartheta_1$und ϑ_2 in Abbildung 39) besitzen sowohl µC als auch FPGA üblicherweise On-Chip-Temperatursensoren [119], [120]. Bevor die spezifizierte maximale bzw. minimale Betriebstemperatur über- bzw. unterschritten wird, kann die Steuerelektronik den Antrieb über den nicht sicherheitsrelevanten Teil rechtzeitig abschalten.

Den Takt erhalten µC und FPGA, wie in Abbildung 39 gezeigt, durch externe Taktgeneratoren. Idealerweise stammen diese von verschiedenen Herstellern und haben unterschiedliche Taktraten, um CCF auszuschließen. Beide Logikeinheiten erzeugen auf Basis dieses Taktsignals über die integrierten PLLs ein 1 kHz Signal. Dieses Signal wird von der jeweils komplementären Logik mit dem anderen Takt überprüft. Wenn die so ermittelten Periodendauern nicht innerhalb des Erwartungswerts mit einer spezifizierten Toleranz liegen, schalten beide Kanäle unabhängig voneinander in den sicheren Zustand. Da

bei einer solchen Abweichung nicht mehr von einem normalen Betrieb des µCs oder FPGAs auszugehen ist, wird der sichere Zustand sofort über STO und SBC herbeigeführt.

4.8.2 Zusammenfassung sicherheitsrelevanter Logik und Diagnose im Antrieb

Bisher wurde sowohl das Konzept der Sicherheitsfunktionen im Antrieb (STO, SBC und SS1) als auch das Konzept für die sicherheitsbezogene Positions- und Strommessung im Einzelnen betrachtet. Ebenso wurden verschiedene Diagnosetests vorgestellt, um den notwendigen DC zu erreichen. In diesem Kapitel soll die gesamte sicherheitsrelevante Logik im µC und FPGA des Antriebs noch einmal zusammenfassend dargestellt werden. Außerdem werden alle externen und internen Diagnosemaßnahmen und ihre Auswirkungen auf die Fehlererkennung zusammengefasst.

Heute werden in der Regel für den geforderten DC und zur Erkennung von systematischen Fehlern die SRESW-Anforderungen und die Diagnose der komplexen elektronischen Komponenten wie PLÜ, CPU- und Speicher-Test innerhalb des Antriebs durchgeführt. Diese Maßnahmen werden im Vorfeld implementiert und im Zertifizierungsprozess des Gerätes berücksichtigt. Der Austausch von Komponenten ist daher zeitaufwändig und teuer. Durch den diversitären redundanten Aufbau mit externer Diagnose kann mit einem Standard-µC und einem Standard-FPGA im Antrieb bis zu PL d erreicht werden, sodass keine oder nur eine begrenzte Zertifizierung der Komponenten im Antrieb notwendig ist. Im Folgenden wird gezeigt, dass eine Diagnosekette entsteht, wobei Ausfälle im µC und im FPGA von der übergeordneten Sicherheits-SPS ohne zyklischen Aufruf einer gängigen antriebsinternen Software-Testbibliothek zur Diagnose erkannt werden.

In Abbildung 40 sind alle sicherheitsrelevanten Funktionsblöcke des 1. Kanals, implementiert im µC, dargestellt. Folgende Funktionsblöcke sind in diesem Konzept für den µC vorgesehen:

- Abtastung der Motorphasenströme i_u und i_v mit anschließender Sinc³-Dezimierungsfilterung.
- Abschaltung der drei High-Side-Gate-Treiber für die Sicherheitsfunktion STO mit dem Signal nSTO_high über das sicherheitsbezogene Feldbusprotokoll.
- Abschaltung des High-Side-MOSFET für die Sicherheitsfunktion SBC mit dem Signal nSBC_high über das sicherheitsbezogene Feldbusprotokoll.
- 1. Verbindung über das sicherheitsbezogene Feldbusprotokoll (1. Slave mit Zustandsautomat) für die sicherheitsbezogene Kommunikation des ersten Kanals mit der übergeordneten Sicherheits-SPS. Das Signal SS1 löst je nach Konfiguration des sicheren Zustands die Sicherheitsfunktion SS1 aus. Der Watchdog kann im µC mit einem Zähler in Hardware umgesetzt werden.

- Die Drehgeber-SPDU wird vom FPGA unverändert über die Octo-SPI, den µC und den Feldbus an die Sicherheits-SPS via Black-/Gray-Channel versendet.
- Optional kann statt einem sicherheitsbezogenen Drehgeber ein Resolver oder ein konventioneller digitaler Drehgeber angeschlossen werden. Diese Positionssignale stellen nur einen von zwei notwendigen Kanälen für die Auswertung dar.

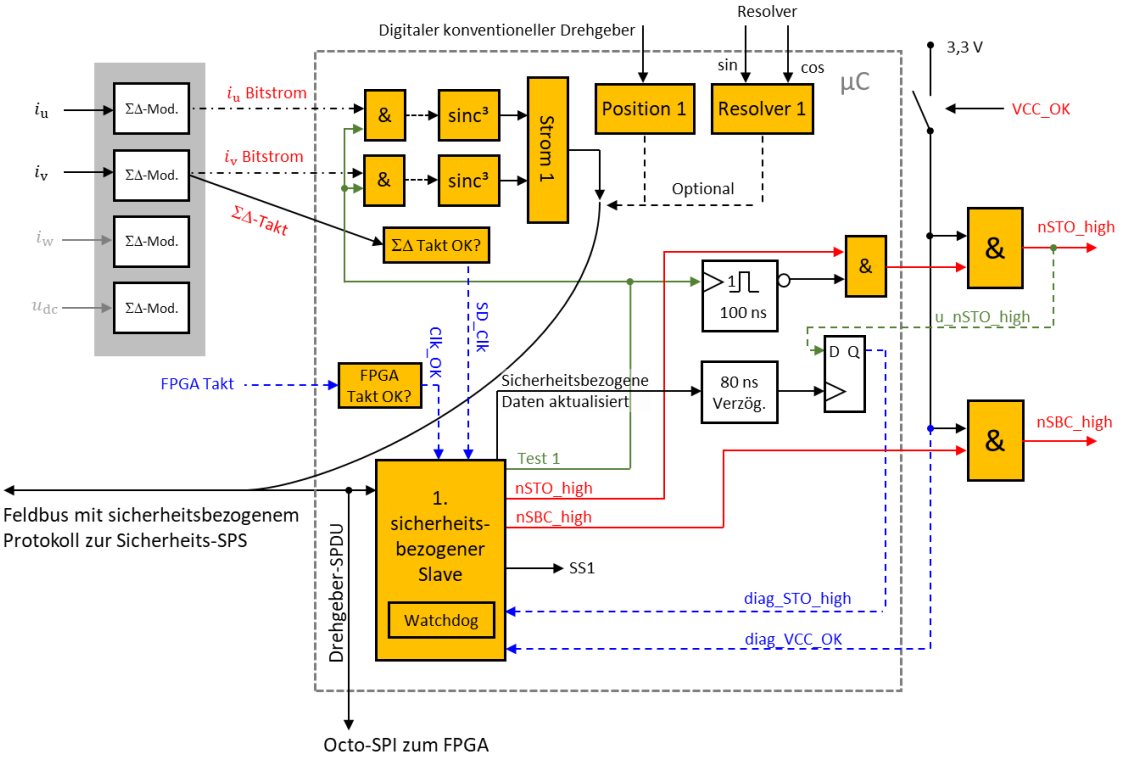


Abbildung 40: Sicherheitsrelevante Funktionsblöcke des 1. Kanals implementiert im µC.

Die folgenden Maßnahmen zur Diagnose und Fehleraufdeckung ergeben sich aus den in Abbildung 40 dargestellten Funktionsblöcken:

- Taktüberwachung des FPGA-Takts und Weiterleitung des Status mit Clk_Ok an die Sicherheits-SPS: Bei Ausfall des Takts oder zu hoher Abweichung der Taktfrequenz wird dies durch den µC erkannt und dieser kann in den sicheren Zustand schalten.
- Spannungsversorgung der Steuerelektronik und Weiterleitung des Status mit Diag_VCC_OK an die Sicherheits-SPS: Wenn die Spannungsversorgung nicht im erlaubten Bereich liegt und FPGA und µC nicht mehr ordnungsgemäß arbeiten, wird das über die in Hardware realisierte Spannungsüberwachung aufgedeckt. Das Signal VCC_OK wird „Low“ und schaltet den Antrieb direkt in den sicheren Zustand.
- Kommunikationsausfall des sicherheitsbezogenen Feldbusses: Der Watchdog schlägt an sobald keine neuen SPDUs innerhalb einer anwendungsspezifischen

Zeit empfangen werden und setzt den Zustandsautomaten zurück, wodurch auch der Antrieb in den sicheren Zustand schaltet.

- Interne Funktionen des µCs: Durch das zyklische Rücklesen der dynamischen Feldbus-SPDU wird von der Sicherheits-SPS aufgedeckt, falls das Programm vom µC nicht mehr ordnungsgemäß ausgeführt wird (logische PLÜ). Die Sicherheits-SPS kann über den anderen Kanal im FPGA den sicheren Zustand herbeiführen. Dies deckt ebenfalls einen Kommunikationsausfall der Octo-SPI auf. Zusätzlich wird mit dem zyklischen Auslösen des Watchdogs in der Sicherheits-SPS eine zeitliche PLÜ realisiert.
- Digitale Ausgänge für STO/SBC mit den Diagnosesignalen diag_STO_high und diag_SBC zur Übermittlung an die Sicherheits-SPS: Wenn die Peripherie (I/Os) des µCs nicht mehr ordnungsgemäß schaltet, wird dies spätestens mit dem nächsten dynamischen Test und Rücklesen der Ausgänge von der übergeordneten Sicherheits-SPS erkannt. Das FPGA kann (spätestens durch den Watchdog, falls die I/Os der Octo-SPI auch betroffen sind) in den sicheren Zustand schalten. Durch das Testen der sicherheitsbezogenen Ausgänge wird ebenfalls ein falscher Programmablauf aufgedeckt.
- Schnelle sicherheitsbezogene Kommunikation über den Feldbus mit sicherheitsbezogenem Protokoll: Eine geringe Zykluszeit von einer Millisekunde sorgt für eine schnelle Fehlererkennung und Abschaltung in einen sicheren Zustand.
- Hinzu kommen die vorgestellten Diagnosemaßnahmen für die sicherheitsbezogene Strom- und Positionsmessung.

Abbildung 41 zeigt alle sicherheitsrelevanten Funktionsblöcke des im FPGA implementierten 2. Kanals. Da dieser Kanal ähnlich aufgebaut ist wie der 1. Kanal, werden hier nur die Unterschiede zum µC aufgezeigt. Im FPGA werden die Ströme i_{v} und i_{w} gemessen und die Low-Side-Gate-Treiber für STO und der Low-Side-MOSFET für SBC angesteuert. Zusätzlich zur Abschaltung der Bremse über die Sicherheitsfunktion SBC ist im FPGA die nicht sicherheitsbezogene Bremsansteuerung sowie die PWM zum Herabsetzen der Bremsspannung implementiert. Die Maßnahmen zur Diagnose sind komplementär zu den aufgelisteten Maßnahmen aus dem ersten Kanal.

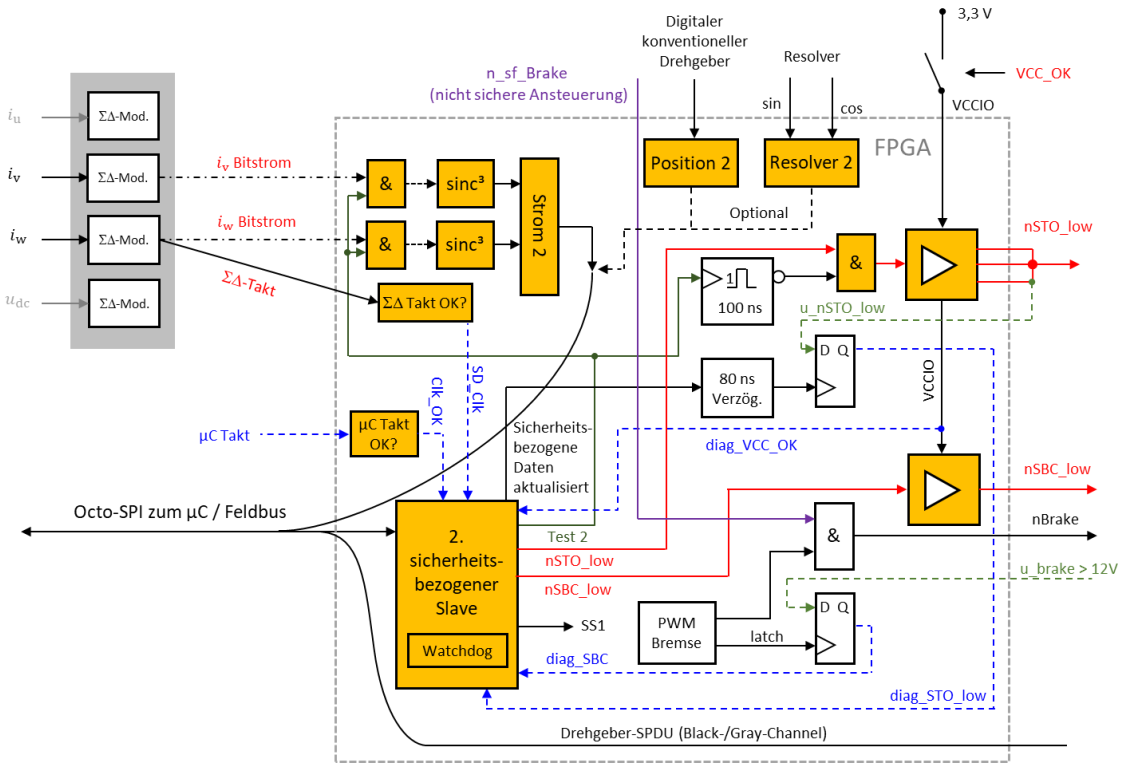


Abbildung 41: Sicherheitsrelevante Funktionsblöcke des 2. Kanals implementiert im FPGA.

Durch die diversitäre redundante Struktur, den DC und die bekannte Ausfallrate der Komponenten kann PL d mit einem Standard-µC und einem Standard-FPGA erreicht werden, die den Anforderungen des Qualitätsmanagements entsprechen. Da es sich um nicht sicherheitszertifizierte Komponenten handelt, erlaubt dieser Ansatz eine größere Freiheit beim Austausch vom FPGA oder µC, ohne die funktionale Sicherheit des Systems zu beeinflussen, wie bei der Sicherheitslösung mit Sicherheitsschaltgerät, Not-Halt-Schalter und Schütz.

Mit zusätzlichem Aufwand kann auch PL e mit dem gezeigten Konzept erreicht werden. Es können zwar keine Standardkomponenten mehr verwendet werden, aber die Diagnose über die Sicherheits-SPS kann weiterhin genutzt werden. Aufgrund der diversitären redundanten Architektur sind keine weiteren Maßnahmen nach DIN EN 61508 erforderlich, sondern nur die genannten SRESW-Anforderungen nach DIN EN ISO 13849-1 sind einzuhalten. Für PL e ist außerdem eine Isolierung zwischen nicht sicherheitsbezogener und sicherheitsbezogener Software erforderlich. Für das FPGA kann ein Entwurfsverfahren zur Trennung zwischen dem nicht sicherheitsbezogenen und sicherheitsbezogenen Teil verwendet werden. Für den µC kann beispielsweise die Arm TrustZone genutzt werden. Beide Maßnahmen werden in [21] genauer beschrieben.

Abschließend wird die vorgestellte Antriebsarchitektur mit bisherigen sicherheitsbezogenen Architekturen in Tabelle 1 verglichen. Außerdem werden die Maßnahmen gegen CCF zusammenfassend in Tabelle 3 im Anhang untersucht. Dafür wird das bereits vorgestellte Punkteschema aus der DIN EN ISO 13849-1 verwendet. Wie Tabelle 3 im Anhang

zeigt, wird die geforderte Punktzahl von mindestens 65 Punkten für die Maßnahmen gegen CCF von der vorgestellten Antriebsstruktur erfüllt.

Merkmal	Gängiger Ansatz	Vorgestellter Ansatz
Programmierbare Elektronik für die Antriebsregelung	µC, FPGA oder Kombination aus beiden	Standard-µC und Standard-FPGA
Programmierbare Elektronik für die sicherheitsbezogene Logik	Typischerweise zwei zusätzliche µCs	
Zertifizierungsaufwand	Zertifizierung der sicherheitsbezogenen Logik in der Steuerung und dem Antrieb	Zertifizierung der sicherheitsbezogenen Logik nur in der Steuerung
Diagnose für systematische Ausfälle	Antriebsinterne Software-Testbibliothek für PLÜ, Peripherie- und Speicher-Tests	Großteil der Diagnose extern über Sicherheits-SPS, keine Zertifizierung der sicherheitsbezogenen Logik im Antrieb
CCF	Zertifizierte Software-Testbibliothek	Diversitäre redundante Architektur (vgl. Tabelle 3)
Sicherheitsbezogene Zykluszeit	≥10 ms	≥1 ms
Sicherheitsfunktionen	STO ist typischerweise im Antrieb integriert, Optionskarte für komplexere Einzelachs-Sicherheitsfunktionen	STO, SBC und SS1 sind im Antrieb integriert, übergeordnete Sicherheits-SPS für komplexere Mehrachs-Sicherheitsfunktionen

Tabelle 1: Vergleich von gängigen sicherheitsbezogenen Antriebsarchitekturen und dem vorgestellten Ansatz.

5 Validierung des Konzepts

Für die Validierung des Konzepts wurde im Rahmen dieser Arbeit die in Abbildung 42 dargestellte Leiterplatte für die Steuerelektronik des Antriebs realisiert. Für die Kommunikation mit einer übergeordneten Steuerung wird EtherCAT mit dem sicherheitsbezogenen Protokoll FSoE verwendet. Das vorgestellte Konzept für die sicherheitsbezogene Architektur ist in Absprache mit dem TÜV Rheinland entwickelt. Im Folgenden sollen die wichtigsten Bestandteile beschrieben werden:

- MAX® 10 FPGA von Intel® mit 25 000 Logikelementen und der entsprechenden Programmierschnittstelle. Clarke-Transformation, Park-Transformation, Inverse Park-Transformation und SVM benötigen insgesamt etwa 2 500 MAX® 10 Logikelemente.
- RZ/N2L µC von Renesas mit einem 400 MHz Arm Cortex-R52 mit der entsprechenden Programmierschnittstelle. Dieser unterstützt die gängigen Industrial-Ethernet-Protokolle wie EtherCAT. Der RZ/N2L beinhaltet die Funktionalität des EtherCAT-Slave-Controllers (ESC) und stellt eine ausreichende Performanz für die Realisierung eines Doppelachsantriebs bereit. Zu Beginn des Projekts wurde ein µC von STMicroelectronics mit einem 110 MHz Arm Cortex-M33 mit 256 kByte On-Chip-RAM und 512 kByte On-Chip-Flash genutzt. Durch den On-Chip-Speicher wurde annähernd eine Zwei-Chip-Lösung für den Steuerteil des Antriebs erreicht. Aufgrund der geänderten Anforderungen wurde zu einem späteren Zeitpunkt ein leistungsfähigerer µC benötigt, welcher einen externen Flash-Speicher erfordert.
- RJ45-Buchsen und Ethernet Physical Layer Transceiver für die Anbindung über EtherCAT an die übergeordnete Steuerung.
- Stecker für die Spannungsversorgung, mehrere DC/DC-Wandler und die Spannungsüberwachungsbausteine entsprechend dem Konzept aus Abbildung 39.
- Dual-Channel IO-Link-Transceiver MAX14819 von Analog Devices mit zwei MOSFETs zum Ein- und Ausschalten der Leitung L+ für die Realisierung der digitalen (sicherheitsbezogenen) Ein- und Ausgänge.
- Jeweils zwei MOSFETs für den 1. Abschaltpfad im µC für STO und SBC nach dem Konzept aus Abbildung 17. Die zwei MOSFETs für den 2. Abschaltpfad im FPGA über die IO-Bank nach Abbildung 19 sind auf der Rückseite der Leiterplatte platziert.
- RS-485-Transceiver für die Kommunikation mit einem digitalen Drehgeber-Protokoll.

- Stecker für die Verbindung zum Leistungsteil des Antriebs. Hierzu zählen beispielsweise die sechs PWM-Signale, die ΣΔ-Signale sowie die STO- und SBC-Signale mit den entsprechenden Rücklesesignalen zur Diagnose.

Der EMV-Filter für die Maßnahmen gegen CCF ist nicht auf der Leiterplatte integriert.

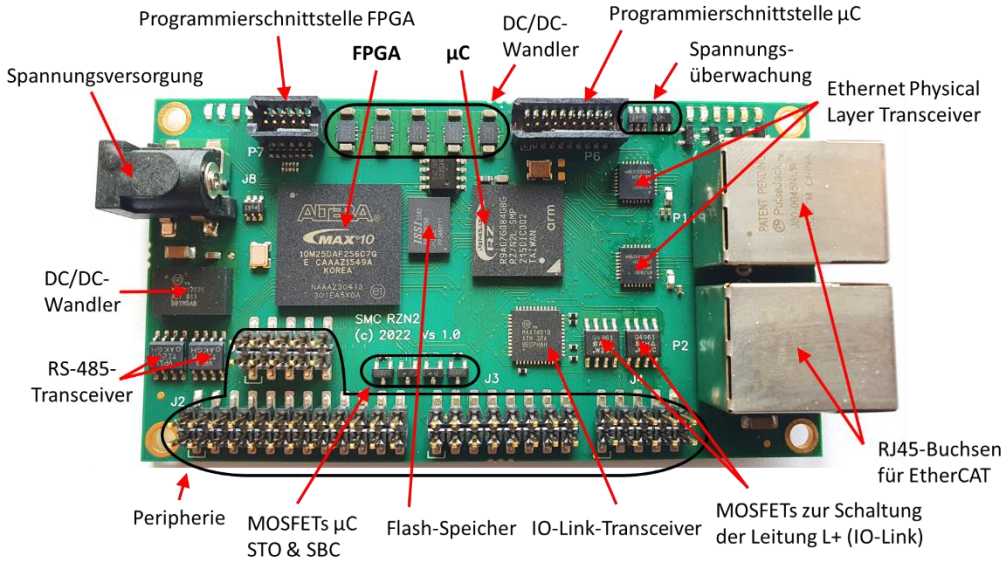


Abbildung 42: Leiterplatte mit der Steuerelektronik des Antriebs.

Für die weitere Validierung des Konzepts wurde die Leiterplatte aus Abbildung 42 in einen MOVIDRIVE® Servoregler vom Typ MDA90A der Firma SEW-EURODRIVE eingebaut, um die ursprüngliche Steuerkarte vom Hersteller zu ersetzen. Für die Validierung der beschriebenen Konzepte wurde eine entsprechende Software im µC und FPGA realisiert, die zum einen die Antriebsregelung aus Kapitel 3 und zum anderen die funktional sicheren Aspekte aus Kapitel 4 beinhaltet. Dazu zählen beispielsweise die Implementierung der Regelkreise mit Interpolation, der SVM, der Kommunikation über die Octo-SPI, der Diagnosetests und der FSoE-Slaves im µC und FPGA. Drei dieser Servoregler wurden zusammen mit drei CMP50S Synchronmotoren der Firma SEW-EURODRIVE mit eingebauten EnDat-3-Drehgebern als Motor-Feedback-System in einem Delta-Roboter der Firma autonox Robotics eingebaut. Durch die 8-Bit sicherheitsbezogene Achsadresse in der Endat-3-SPDU können bis zu 256 sicherheitsrelevante EnDat-3-Drehgeber eindeutig unterschieden und somit an eine Sicherheits-SPS angeschlossen werden. Zusammen mit einer übergeordneten Intel® Atom® x6427FE-basierten gemischtkritischen SPS nach dem Konzept aus [77] dient der Delta-Roboter als Technologiedemonstrator und wurde wie in Abbildung 43 dargestellt auf der SPS – Smart Production Solutions – Messe 2022 in Nürnberg ausgestellt. Die Compound-SPS kann mit der Entwicklungsumgebung CODESYS Development System programmiert werden, um die Positionssollwerte für die drei Achsen des Delta-Roboters vorzugeben. Die Sicherheitsfunktionen für eine Überwachung im dreidimensionalen Raum können in der Compound-

SPS mit der zertifizierten IEC 61131-3-Software für funktionale Sicherheit CODESYS Safety SIL2 umgesetzt werden.

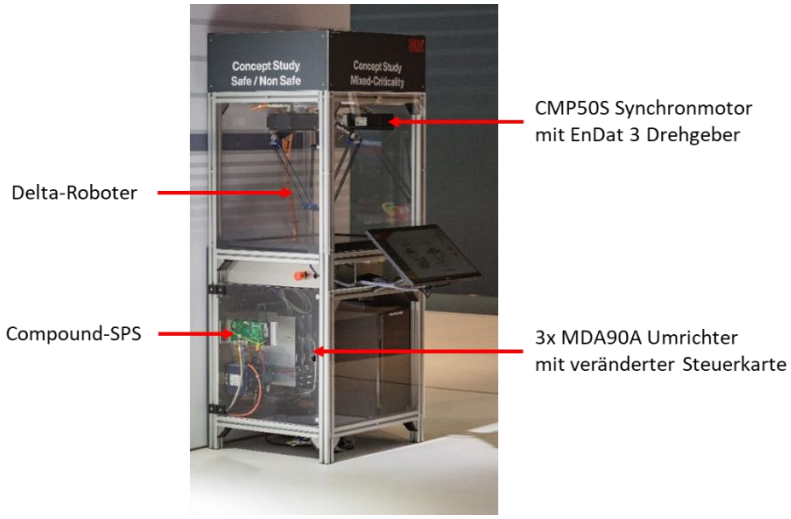


Abbildung 43: Delta-Roboter als Technologiedemonstrator mit der verbauten Steuerelektronik auf der SPS-Messe 2022 in Nürnberg.

Im Rahmen einer Masterarbeit wurde ein Servoregler für einen 48-V-Doppelachsantrieb entwickelt, der die hier gestellten Anforderungen an die Leistungsfähigkeit eines Antriebs sowie an die sicherheitsbezogene Architektur erfüllt. In Abbildung 50 im Anhang ist der Testaufbau dieses Servoreglers zusammen mit der oben gezeigten Steuerelektronik dargestellt. Die folgenden Betrachtungen bezüglich der Leistungsfähigkeit des Antriebs und die Validierung der sicherheitsbezogenen Antriebsstruktur wurden mit diesem Testaufbau durchgeführt, da die oben gezeigten MOVIDRIVE® Servoregler nicht die technischen Voraussetzungen für alle vorgestellten Konzepte erfüllen.

5.1 Leistungsfähigkeit des Antriebssystems

Im Folgenden werden auf Grundlage der vorgestellten Antriebsarchitektur experimentell ermittelte Bode-Diagramme dargestellt, eines für jeden Regelkreis. Der dafür verwendete PSM hat einen Widerstand von $R_s = 0{,}4\ \Omega$ und eine Induktivität von $L_s = 0{,}7$ mH. Der verwendete Leistungsteil besitzt Silizium-MOSFETs von Infineon mit einem $R_{DSon} = 1{,}2\ \text{m}\Omega$ und nutzt die ΣΔ-Modulatoren 2. Ordnung ADS1204 von Texas Instruments für die Analog-Digital-Wandlung der Motorströme.

Abbildung 44 zeigt das Bode-Diagramm des Stromregelkreises. Es zeigt eine Bandbreite des Stromreglers von etwa 3 kHz. Die schwarzen gestrichelten Linien markieren die -3 dB bzw. die -90°-Grenze.

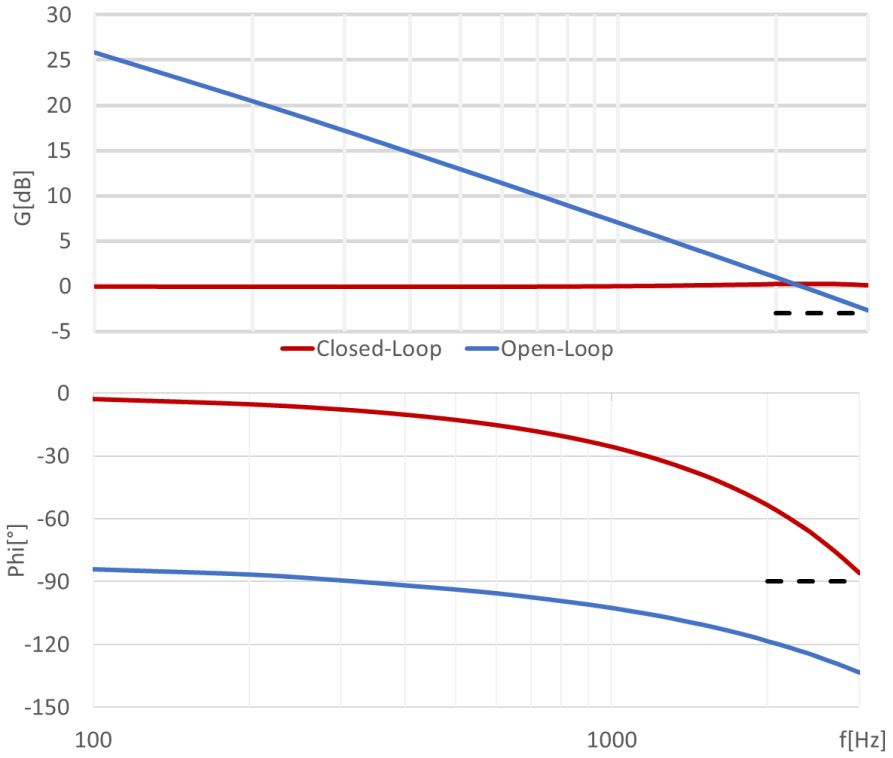


Abbildung 44: Gemessenes Bode-Diagramm des Stromregelkreises mit Smith-Prädiktor bei 8 kHz Schaltfrequenz.

Bei der Aufnahme des Bode-Diagramms für den Drehzahlregelkreis wird der digitale Absolutwertgeber EQN 1337 von Heidenhain mit dem Kommunikationsprotokoll EnDat 3 verwendet. Dieser verfügt über eine Singleturn-Auflösung von 25 Bit und zusätzlich 12 Bit für Multiturn. Die rote Kurve in Abbildung 45 zeigt das Bode-Diagramm mit dem Beobachter und FFA, während die grüne Kurve das Bode-Diagramm ohne Vorsteuerung darstellt. Mit der Vorsteuerung ist eine deutliche Verbesserung zu erkennen. Bei einer Frequenz von etwa 1,3 kHz ist eine kleine Spitze im Amplituden- und Phasengang zu erkennen, die auf den elastisch gekoppelten Drehgeber zurückzuführen ist.

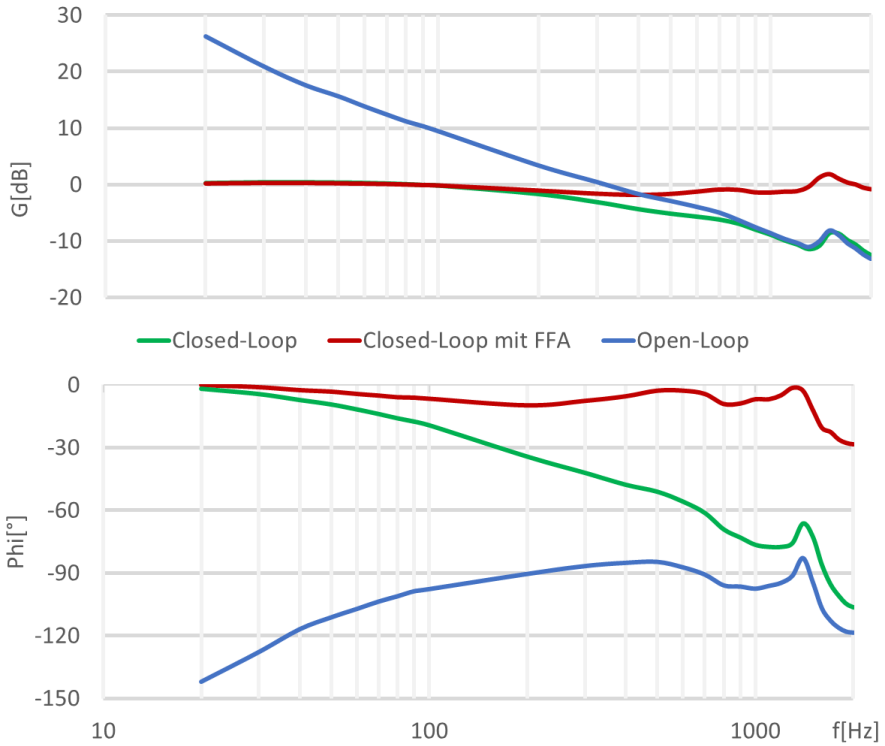


Abbildung 45: Gemessenes Bode-Diagramm des Drehzahlregelkreises mit Drehzahl-Beobachter mit 400 Hz Bandbreite bei 8 kHz Schaltfrequenz.

Das Bode-Diagramm des Lageregelkreises für das gesamte Antriebssystem ist in Abbildung 46 dargestellt. Die Feininterpolation führt zu einer zusätzlichen Verzögerung des Sollwerts von $T_\mathrm{t} = T_\mathrm{a} = 250\ \mu s$. Als Referenz ist die Phasenverschiebung durch die Feininterpolation im Phasengang als gestrichelte Kurve in grau dargestellt. Zur Kompensation der Verzögerungszeit wird das Vorsteuersignal der Drehzahl um $T_\mathrm{cv} = 62{,}5\ \mu s$ und das Beschleunigungssignal um $T_\mathrm{ca} = 125\ \mu s$ voreilend eingestellt. Die schwarzen gestrichelten Linien in Abbildung 46 zeigen die -3 dB bzw. die -90°-Grenze. Die berechneten Vorsteuersignale werden an die entsprechenden Stellen der kaskadierten Regelkreisstruktur übergeben. Um das Stromvorsteuersignal zu erhalten, wird die Beschleunigung mit der Drehmomentkonstante K_T und dem Trägheitsmoment J des Systems multipliziert bzw. dividiert. Die Bandbreite des Lageregelkreises ist in Abbildung 46 zu sehen und beträgt für das Antriebssystem mit FFV und FFA etwa 550 Hz. Zum Vergleich sind auch die Bode-Diagramme ohne Vorsteuerung und nur mit FFV dargestellt. Mit FFV wird eine Bandbreite von 300 Hz und ohne Vorsteuerung eine Bandbreite von 60 Hz erreicht.

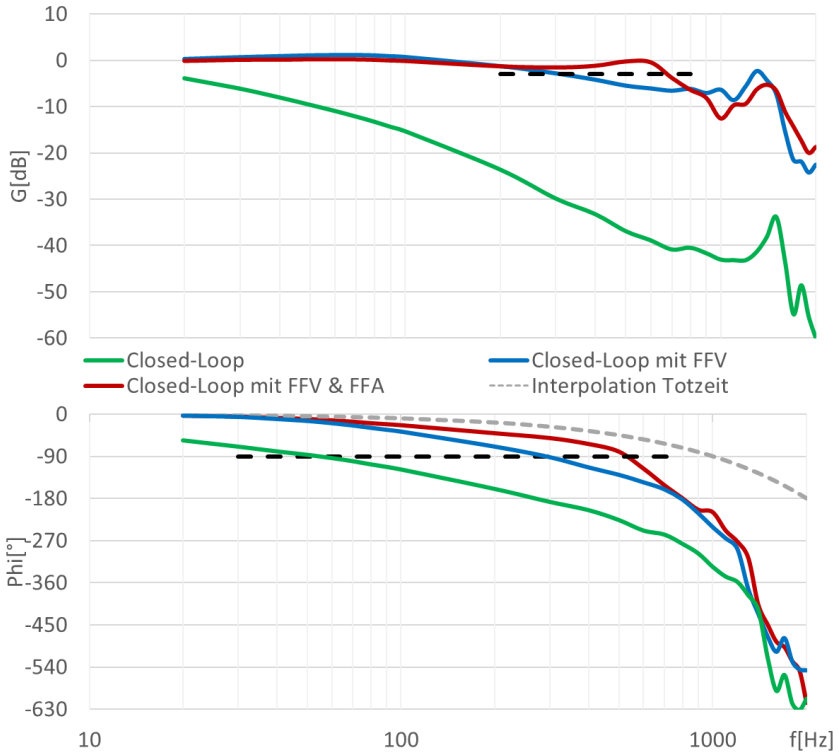


Abbildung 46: Gemessenes Bode-Diagramm des Lageregelkreises mit Feininterpolation für das Antriebssystem.

5.2 Validierung der Diagnosetests

Zur Validierung der Diagnosetests für die sicherheitsbezogene Antriebsarchitektur werden in der übergeordneten Compound-SPS mit Hilfe der Entwicklungsumgebung CODESYS Development System Funktionsbausteine programmiert, sodass die Compound-SPS über FSoE/EtherCAT die in dieser Arbeit beschriebenen Sicherheitsfunktionen auslösen und die Diagnoseinformationen zurücklesen kann. Der EtherCAT-Feldbus arbeitet mit einer Zykluszeit von 1 ms. Da FSoE auf einer bidirektionalen Kommunikation basiert, dauert ein FSoE-Kommunikationszyklus doppelt so lange wie der Zyklus des sicherheitsbezogenen Feldbusprotokolls, welches ebenfalls mit der Zykluszeit von EtherCAT arbeitet. Um Zeitverläufe aufzunehmen, wurde die Trace-Funktionalität im CODESYS Development System verwendet.

5.2.1 Validierung der Abschaltpfade

Abbildung 47 zeigt den Test der Abschaltpfade für die Sicherheitsfunktionen STO und SBC. Der obere Verlauf zeigt die sicherheitsbezogenen Daten der FSoE-Master-SPDU des 1. Kanals im µC und des 2. Kanals im FPGA. Nach dem Hochfahren des FSoE-Zustandsautomaten, bei ordnungsgemäßer Funktion der Kommunikation und bei Freigabe der Sicherheitsfunktionen sind das nSTO-Signal, das nSBC-Signal und das Testsignal „High“ (0b111 = 0d7). Jede Sekunde wird das Testsignal für einen FSoE-

Kommunikationszyklus (2 ms) abgeschaltet (0b011 = 0d3). Ebenso wird jede Sekunde das nSBC-Signal für 2 ms abgeschaltet (0b101 = 0d5). Wie in Abbildung 47 dargestellt, finden alle Tests zeitversetzt um 250 ms statt.

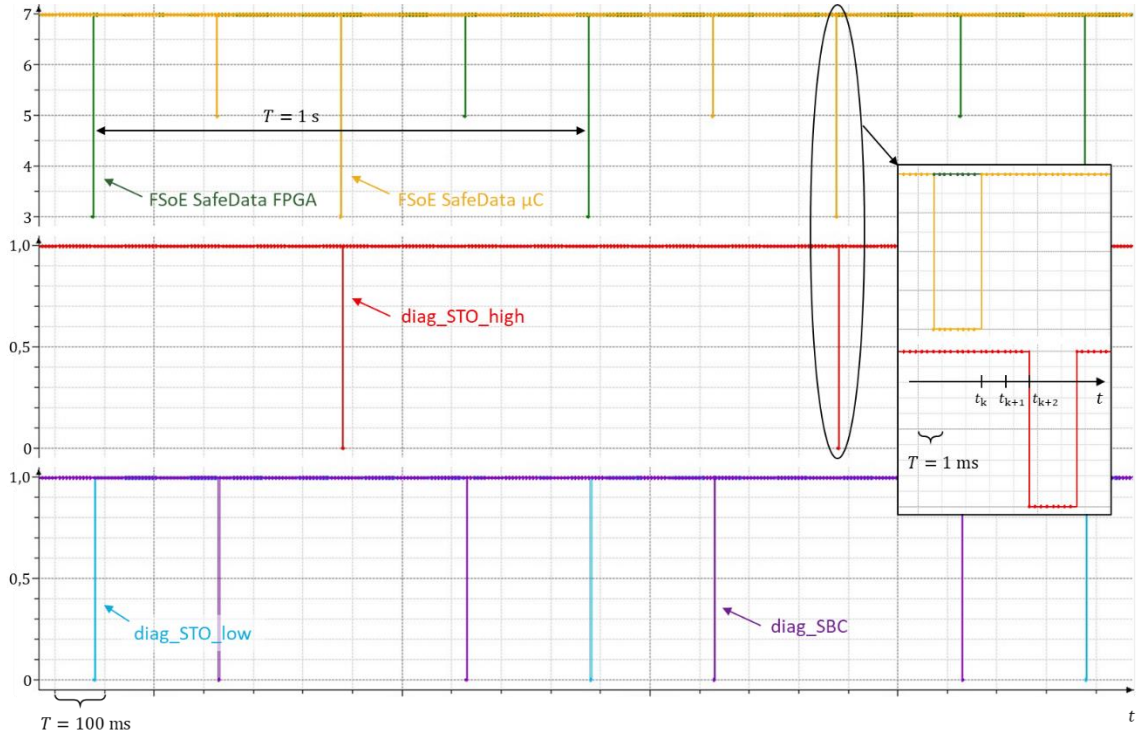


Abbildung 47: Testung der Abschaltpfade für die Sicherheitsfunktionen STO und SBC.

Der mittlere Zeitverlauf zeigt das über FSoE zurückgelesene Signal diag_STO_high aus dem µC. Bei ordnungsgemäßer Funktion wird zwei EtherCAT-Feldbuszyklen nach der Auslösung des Testsignals in der übergeordneten Steuerung der Pegel des zurückgelesenen Signals diag_STO_high für 2 ms „Low“. Der Test der Abschaltpfade im Antrieb wird durch eine steigende Flanke des Testsignals ausgelöst. Zum Zeitpunkt t_k wird das Testsignal in der Steuerung von „Low“ auf „High“ gesetzt. Mit dem nächsten EtherCAT-Feldbuszyklus (1 ms später) zum Zeitpunkt t_{k+1} wird diese steigende Flanke an den Antrieb übertragen, wodurch die beschriebenen Testroutinen im µC und FPGA ausgeführt werden. Mit dem nächsten Feldbuszyklus zum Zeitpunkt t_{k+2} wird das Ergebnis zurück zur Steuerung übertragen. Da das Signal diag_STO_high mit der FSoE-Zykluszeit aktualisiert wird, ist die steigende Flanke im Diagnosesignal erst 2 ms später zu erkennen. In der Sicherheits-SPS ist die Abschaltung und die Zeit zwischen der Auslösung des Tests und der Abschaltung des zurückgelesenen Diagnosesignals zu überprüfen. Der untere Zeitverlauf zeigt die über FSoE zurückgelesenen Signale diag_STO_low und diag_SBC aus dem FPGA. Hier gelten die gleichen Annahmen wie für das Signal diag_STO_high. Das Signal diag_STO_low wird zwei EtherCAT-Feldbuszyklen nach der Auslösung des Testsignals in der übergeordneten Steuerung für 2 ms „Low“. Das Signal diag_SBC wird bei ordnungsgemäßer Funktion jede 500 ms für einen FSoE-Kommunikationszyklus

„Low“, da dieser Test sowohl vom µC als auch vom FPGA ausgelöst wird und über dasselbe Signal zurückgelesen wird.

5.2.2 Validierung der Sinc-Filtertests

Abbildung 48 zeigt den Test der Sinc³-Dezimierungsfilter für die sicherheitsbezogene Strommessung. Der obere Verlauf zeigt wieder die sicherheitsbezogenen Daten der FSoE-Master-SPDU des 1. Kanals im µC und des 2. Kanals im FPGA. Für eine bessere Darstellung wird hier nur das Abschalten der Testsignale gezeigt. Jede Sekunde wird das Testsignal in der Steuerung für einen FSoE-Kommunikationszyklus abgeschaltet.

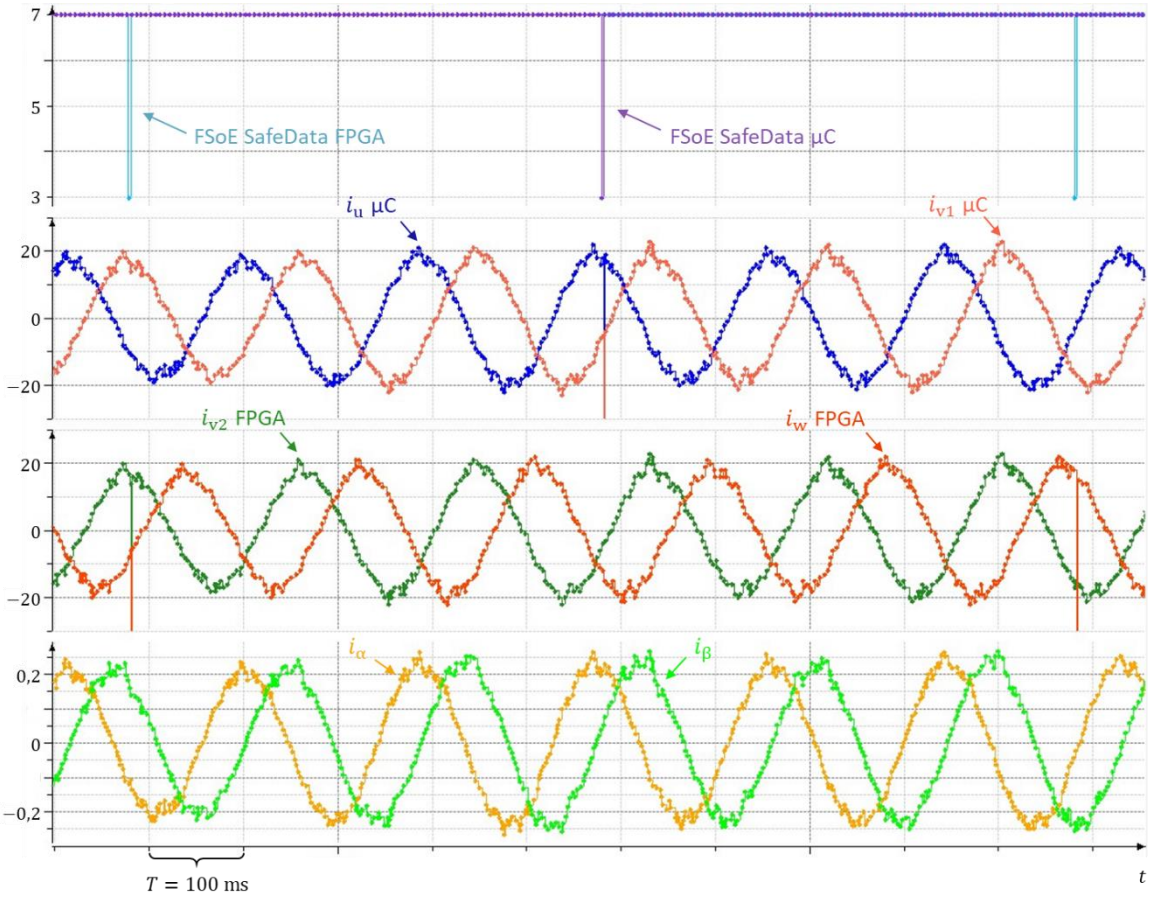


Abbildung 48: Test der Sinc³-Dezimierungsfilter für die sicherheitsbezogene Strommessung.

Die beiden mittleren Verläufe zeigen die über die ΣΔ-Modulatoren gemessenen und anschließend von den Sinc³-Filtern ausgewerteten Motorphasenströme als digitales 12-Bit Datenwort. Der obere Verlauf zeigt die vom µC ausgewerteten Ströme i_u und i_{v1} und der untere Verlauf die vom FPGA ausgewerteten Ströme i_{v2} und i_w. In den Verläufen ist zu erkennen, dass beide Stromwerte eines Kanals zwei EtherCAT-Feldbuszyklen nach der Initialisierung des Tests im jeweiligen Kanal auf einen negativen Wert fallen. Für eine bessere Darstellung der sinusförmigen Stromverläufe ist der Wertebereich der Ordinate begrenzt. Die Stromwerte fallen während der Tests auf einen Wert von -2048. Außerdem ist zu erkennen, dass der Verlauf des Phasenstroms i_v beider Kanäle ähnlich ist.

Der untere Verlauf in Abbildung 48 zeigt den aus den Phasenströmen berechneten Strom i_α und i_β in der SI-Einheit Ampere. Während die Sinc³-Filtertests in den Verläufen der Phasenströme noch erkennbar sind, sind sie in den statorfesten Stromkomponenten nicht mehr sichtbar. Zum Zeitpunkt des Filtertests in einem Kanal werden i_α und i_β nur aus den Strömen des jeweils anderen Kanals berechnet. Für die Auswertung der Phasenströme und die Durchführung der im Kapitel 4.4 vorgestellten Diagnosemaßnahmen für die sicherheitsbezogene Strommessung wurde ein entsprechender Funktionsbaustein implementiert.

Da für die Validierung des Konzepts EtherCAT mit dem sicherheitsbezogenen Protokoll FSoE verwendet wird, werden die Stromdaten nach [60] im Antrieb im µC zu einem ersten Strom-SPDU und im FPGA zu einem zweiten Strom-SPDU verarbeitet und an den FSoE-Frame angehangen. Die SPDUs bestehen jeweils aus zwei Stromwerten und einem CRC, welcher mit dem FSoE-CRC verkettet ist, um eine eindeutige Zuordnung der Ströme zum Antrieb zu erreichen. Die Umsetzung dieser Verkettung für den zweiten Kanal im FPGA ist in Abbildung 51 im Anhang dargestellt.

6 Fazit

In dieser Arbeit wurde eine Antriebsarchitektur für autonome Fahrzeuge wie FTFs und AMRs für eine kollaborierende Automatisierung vorgestellt. Durch die Verwendung von kostengünstigen Standardkomponenten, insbesondere bei der Steuerelektronik des Antriebs, bestehend aus einem FPGA und einem µC, kann den in der Vergangenheit aufgetretenen Lieferengpässen und Bauteilknappheiten entgegengewirkt werden. Diese Komponenten sind nicht nur kostengünstiger und haben eine bessere Verfügbarkeit als spezielle Bauteile, sondern werden auch oftmals von verschiedenen Herstellern angeboten.

Um die Anforderungen an eine hohe Leistungsfähigkeit und Dynamik des Antriebs für eine MRK zu erreichen, wird die gängige Kaskaden-Regelkreisstruktur um bereits bekannte Mechanismen wie Smith-Prädiktor, Drehzahl-Beobachter und Vorsteuerung erweitert. In Kombination mit der FOC, der angepassten Aufteilung der Verarbeitung der Algorithmen im FPGA und µC und dem effizienten Datenaustausch über die Octo-SPI können hohe Aktualisierungsraten von bis zu 50 kHz für den Stromregelkreis erreicht werden. Für die Erfassung der Motorströme wird die weit verbreitete ΣΔ-ADC-Technologie mit nachfolgender $Sinc^3$-Dezimierungsfilterung verwendet. Im FPGA können durch die schnelle parallele Verarbeitung besonders die SVM sowie Park- und Clarke-Transformationen durchgeführt werden. Im µC hingegen können die Regelalgorithmen in SI-Einheiten ausgeführt, die SDO-Verarbeitung strukturierter durchgeführt und eine Kommunikationsschnittstelle für einen Feldbus implementiert werden. Damit die Performanz des realen Antriebs bestimmt werden kann, wurde neben dem Strom- und Drehzahlregelkreis ein Bode-Diagramm des Lageregelkreises unter der Berücksichtigung der zusätzlichen Totzeit durch die Interpolation vorgestellt. Außerdem können aus der Interpolation direkt die Vorsteuersignale für den Strom- und Drehzahlregelkreis berechnet werden. Für das vorgestellte Antriebssystem wird so, experimentell gemessen, eine Bandbreite des Lageregelkreises von etwa 550 Hz erreicht.

Auch bei der Feldbuskommunikation zum Motion-Controller wird auf Standardtechnologien gesetzt. Aus diesem Grund wurde bei der Validierung der vorgestellten Antriebsstruktur der EtherCAT-Feldbus verwendet. Für eine synchrone Datenübertragung und Abtastung der Prozessdaten in Mehrachs-Anwendungen wird die PWM des Antriebs mit einer PLL auf den Feldbus synchronisiert. Neben der Datenübertragung für PDOs und SDOs wird der Feldbus aber auch für die Inbetriebnahme des Antriebs genutzt. Über den Feldbus können entsprechende Oszilloskopfunktionen oder Bode-Diagramme gestartet und die Messdaten zur Darstellung in der übergeordneten Steuerung übertragen werden. Dadurch werden im Antrieb integrierte Schnittstellen zum Anschluss von externen Geräten überflüssig. Ebenso wird der Feldbus für eine zentrale Fehlerdiagnose genutzt, damit ein zusätzlicher Fehlerspeicher im Antrieb eingespart werden kann. Ein weiterer Vorteil

ergibt sich durch die Parameterverwaltung in der zentralen Steuerung, wodurch keine zusätzlichen Parameterspeicher mehr im Antrieb benötigt werden. Sowohl beim Neustart als auch beim Austausch defekter Geräte können die in der Steuerung gespeicherten und optimal eingestellten Parameter über den Feldbus übertragen werden. Aufgrund der genannten Eigenschaften entsteht eine kompakte und kostengünstige Antriebsarchitektur für hochdynamische Anwendungen.

Die Kombination aus µC und FPGA bietet aber nicht nur Vorteile in der Verarbeitung der Regelalgorithmen, sondern auch hinsichtlich des funktional sicheren Aspekts des Antriebs. So wird anstelle von zwei zusätzlichen Logikeinheiten für Kategorie 3 für die sicherheitsbezogene Logik im Antrieb oder in einer zusätzlichen Sicherheitsoptionskarte die diversitäre redundante Architektur für die sicherheitsrelevanten Funktionen im Antrieb verwendet.

Die antriebsinternen Sicherheitsfunktionen beschränken sich auf die wesentlichen Funktionen STO, SBC und SS1 für ein zuverlässiges Anhalten des Motors. Für die Sicherheits-SPS sind diese Sicherheitsfunktionen digitale Ausgänge, die über einen Feldbus mit sicherheitsbezogenem Protokoll im Antrieb angesteuert werden können. Es wurden Konzepte vorgestellt, wie die Abschaltpfade der Sicherheitsfunktionen im Antrieb durch die übergeordnete Sicherheits-SPS getestet werden können. Neben der Sicherheitsfunktion SS1-t und SS1-r wurde auch ein Konzept für SS1-d gezeigt, bei dem der sicherheitsrelevante Teil im FPGA den geregelten Bremsvorgang übernimmt. Da das Antriebskonzept eine sicherheitsbezogene Strommessung für die Überwachung des Drehmoments beinhaltet, ist der zusätzliche Aufwand für SS1-d gering. Zusätzliche Komponenten, wie Relais und Bremswiderstände, werden bei dem Konzept eingespart, wodurch sich der Ansatz auch für räumlich begrenzte Anwendungen wie FTFs eignet. Die beschriebenen Sicherheitsfunktionen sind standardmäßig im Antrieb integriert und es kann auf eine zusätzliche Sicherheitsoptionskarte verzichtet werden. Komplexere Sicherheitsfunktionen zur Überwachung von Mehrachs-Kinematiken werden von der zentralen Sicherheits-SPS ausgeführt.

Die im Antrieb gemessenen sicherheitsrelevanten Strom- und Positionswerte werden via Black-/Gray-Channel über den Feldbus direkt an die Sicherheits-SPS übertragen. Der Kreuzvergleich und die Plausibilisierung der Strom- und Positionswerte finden nicht wie heute üblich im Antrieb statt. Dadurch entfällt der Rechenschritt im Antrieb sowie die damit verbundene Verzögerungszeit und die Daten können in der zentralen Sicherheits-SPS für eine mehrachsige Bewegungsüberwachung verwendet werden. Um die beim FSoE-Protokoll anfallenden zusätzlichen CRC-Daten bei der Übertragung der sicherheitsbezogenen Daten zu vermeiden, können diese als SPDUs an den FSoE-Frame angehangen und zusammen über EtherCAT übertragen werden. Durch die Einsparung der zu übertragenden Daten kann insbesondere auch bei Mehrachs-Anwendungen die kurze

Zykluszeit von einer Millisekunde für die sicherheitsbezogenen Daten erreicht werden. Alternative geeignete Feldbusse mit sicherheitsbezogenem Protokoll können ebenfalls für den gezeigten Ansatz verwendet werden.

Für die Positionsmessung können ein sicherheitsbezogener Drehgeber oder zwei diversitäre Standard-Drehgeber benutzt werden. Zusätzlich wurde ein Ansatz gezeigt, der die Verwendung eines einzelnen Resolvers erlaubt. Hierzu werden die Sin/Cos-Signale in zwei diversitären RDCs im FPGA und µC des Antriebs ausgewertet und als redundante digitale Positionssignale via Black-/Gray-Channel übertragen. Neben dem Positionswert wird auch der Betrag der Resolversignale $\sin^2 + \cos^2$ übertragen und von der Sicherheits-SPS ausgewertet, um den benötigten DC zu erreichen. Zusätzlich kann ein nicht sicherheitsbezogenes Positionssignal für die Regelkreise erzeugt werden. Die fast vollständig digitale Verarbeitung der Signale verringert die Anfälligkeit gegenüber EMI und macht den Ansatz kostengünstig.

Wie in dieser Arbeit gezeigt wurde, können für ein sicherheitsbezogenes Positionssignal zwei diversitäre Standard-Drehgeber verwendet werden, die nach entsprechender geltender Norm qualitätsgeprüft sind. Dieser Ansatz kann auch auf andere Sensoren, wie beispielsweise LiDAR- oder Radarsensoren angewendet werden. Diese werden heute üblicherweise noch als sicherheitsbezogene Variante bei FTFs oder AMRs für eine Abstands- oder Gegenstandserkennung im dreidimensionalen Raum eingesetzt. Die Verwendung nicht sicherheitszertifizierter Komponenten hingegen ist kostengünstiger und erleichtert den Austausch von Geräten.

Der IO-Link-Standard ist eine kostengünstige Möglichkeit für die Realisierung der klassischen digitalen 24-V-Ein- und Ausgänge sowohl für den Anschluss von nicht sicherheitsbezogenen als auch von sicherheitsbezogenen Geräten in der Antriebsarchitektur. Durch die Standardisierung in der IEC-Norm bieten verschiedene Hersteller entsprechende kostengünstige Transceiver an. Es wurde ein Ansatz gezeigt, wie zwei Standard-Transceiver für sicherheitsbezogene Ein- und Ausgänge verwendet werden können. Der Antrieb dient dabei lediglich als Schnittstelle zu den Sensoren und Aktoren, die Auswertung und Diagnose wird von der Sicherheits-SPS durchgeführt. Der zusätzliche Aufwand im Antrieb ist gering und beschränkt sich lediglich auf die Hardwarekomponenten durch die Transceiver und den Software-Stack im Prozessor.

Um auf eine vollständige zertifizierte Logik und die Erfüllung der SRESW-Anforderungen im Antrieb zu verzichten, basiert das vorgestellte Konzept auf einer diversitären redundanten Antriebsarchitektur mit übergeordneter externer Diagnose durch eine Sicherheits-SPS. Wie bei den sicherheitsbezogenen Drehgebern wird der größte Teil der Diagnose in einer antriebsexternen sicherheitsbezogenen Logik durchgeführt. Aufgrund der diversitären redundanten Architektur, den DC und der bekannten Ausfallrate der Komponenten kann PL d mit einem Standard-µC und einem Standard-FPGA reali-

siert werden. Die daraus resultierende Diagnosekette über die Sicherheits-SPS macht antriebsinterne Diagnosetests wie PLÜ, Peripherie- und Speichertests in einer Software-Testbibliothek überflüssig. Lediglich wenige Maßnahmen wie die Überwachung der Spannungsversorgung werden im Antrieb integriert, um die Maßnahmen gegen CCF zu erfüllen. Mit mehr Aufwand kann auch PL e mit dem gezeigten Konzept erreicht werden.

Da die beschriebene Antriebsarchitektur auf einer externen Diagnose und einer kurzen sicherheitsbezogenen Zykluszeit basiert, ist eine übergeordnete Sicherheits-SPS mit hoher Rechenleistung erforderlich. Eine solche Sicherheits-SPS in Kombination mit dem vorgestellten Antrieb ermöglicht eine Umsetzung des degradierten Betriebs nach ZVEI, bei dem ein zentraler Entscheider eine Fehlereinschätzung durchführt und einen sicheren Betriebs- oder Abschaltzustand herbeiführt. Diese Möglichkeit führt zu einer hohen Verfügbarkeit der Maschine und somit zu einer höheren Produktivität, wie es in Zukunft von intelligenten Fabriken gefordert wird.

Das Konzept führt zu einer kompakten sicherheitsbezogenen Antriebsstruktur, bei der der funktional sichere Aspekt zu Beginn des Entwurfs berücksichtigt wurde, wodurch die heute noch häufig parallelen Architekturen für Standard- und Sicherheitsanwendung vermieden werden. Durch die Platzersparnis ist der Ansatz ideal für FTFs und AMRs in einer intelligenten Fabrik geeignet und führt gleichzeitig zu einer Kostenreduzierung des Systems, da für den Antrieb eine vollständige Zertifizierung entfällt und Standardkomponenten verwendet werden können. Somit wird eine größere Freiheit beim Austausch vom FPGA und µC ermöglicht, ohne die funktionale Sicherheit des Systems zu beeinträchtigen. Der Ansatz eignet sich insbesondere für MRK aufgrund der kurzen sicherheitsbezogenen Zykluszeit und der Möglichkeit zur sicheren Bewegungsüberwachung im dreidimensionalen Raum.

Für die Validierung des beschriebenen Konzepts wurde als Technologiedemonstrator ein Delta-Roboter bestehend aus einer Compound-SPS und drei Servoreglern mit veränderter Steuerkarte realisiert. Für den Delta-Roboter konnte somit eine Auswertung der sicherheitsbezogenen Strom- und Positionsdaten in der Sicherheits-SPS durchgeführt werden, um eine sichere Bewegungsüberwachung des Tool Center Points im dreidimensionalen Raum zu ermöglichen. Anhand eines entwickelten 48-V-Servoreglers wurden Funktions- und Leistungsfähigkeit der beschriebenen Antriebsarchitektur aufgezeigt. Es wurde gezeigt, dass sowohl die kaskadenförmigen Regelkreise mit Interpolation und Vorsteuerung als auch die Funktion der sicherheitsbezogenen Kommunikation sowie die Ausführung und Diagnose der Sicherheitsfunktionen durch die übergeordnete Sicherheits-SPS erfolgreich umgesetzt wurden.

Anhang

Anhang 1: Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache

Maßnahme	Beispiele	Punkte
Trennung: Physische Trennung zwischen den Signalpfaden	• Getrennte Verdrahtung • Erkennung von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Testung • Separate Schirmung der Signalpfade beider Kanäle • Ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen	15
Diversität: In beiden Steuerungskanälen werden unterschiedliche Technologien verwendet	• Ein Kanal programmierbare Elektronik, der andere fest verdrahtet • Bauteile von unterschiedlichen Herstellern	20
Entwurf/Anwendung/Erfahrung	• Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur usw. (15 Punkte) • Verwendung bewährter Bauteile (5 Punkte)	20
Beurteilung/Analyse	• Für jedes Teil des SRP/CS wurde eine FMEA durchgeführt und bei der Entwicklung berücksichtigt	5
Kompetenz/Ausbildung	• Schulung des Konstruktionspersonals, Ursachen und Auswirkung von Ausfällen zu verstehen	5
Umgebungsbedingungen: Hinsichtlich Schutz vor schädlichen Einflüssen auf elektrische/elektronische Systeme	• Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMV) im Einklang mit den zutreffenden Normen	25
Umgebungsbedingungen: Hinsichtlich anderer Einflüsse	• Berücksichtigung der Anforderungen hinsichtlich der Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte	10

Tabelle 2: Punkteschema zur Bewertung der Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache [52].

Anhang 2: Systemarchitektur für eine mehrachsige Bewegungsüberwachung

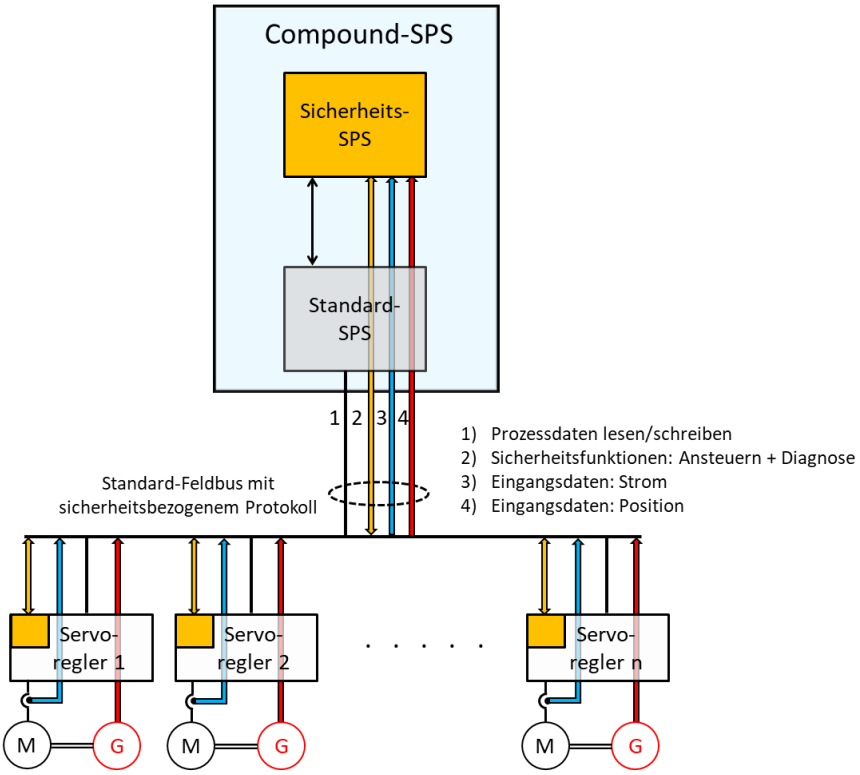


Abbildung 49: Gemischt-kritische Systemarchitektur für Mehrachs-Anwendungen.

Anhang 3: Erreichte Punktzahl gegen Ausfälle infolge gemeinsamer Ursache

Maßnahme	Umsetzung im Antrieb	Punkte
Trennung	• Erkennung von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Testung bei der Anbindung von Geräten über IO-Link an den Antrieb. • Ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen kann beim Layout berücksichtigt werden.	15
Diversität	• Diversität durch den ersten Kanal im µC in „C“ und den zweiten Kanal im FPGA in „VHDL“. • Anschluss von diversitären Standard-Sensoren an die beiden Kanäle, wie z. B. Drehgeber, Laserscanner und Radarsensoren.	20
Entwurf/Anwendung/Erfahrung	• Schutz gegen Überspannung, Überstrom, Übertemperatur durch die antriebsinterne Diagnose.	15
Umgebungsbedingungen	• EMV-Filter für die Spannungsversorgung im Antrieb im Einklang mit den zutreffenden Normen.	25
Gesamt		**75**

Tabelle 3: Erreichte Punktzahl für die Maßnahmen gegen CCF des vorgestellten Antriebssystems.

Anhang 4: Testaufbau zur Validierung der Antriebsarchitektur

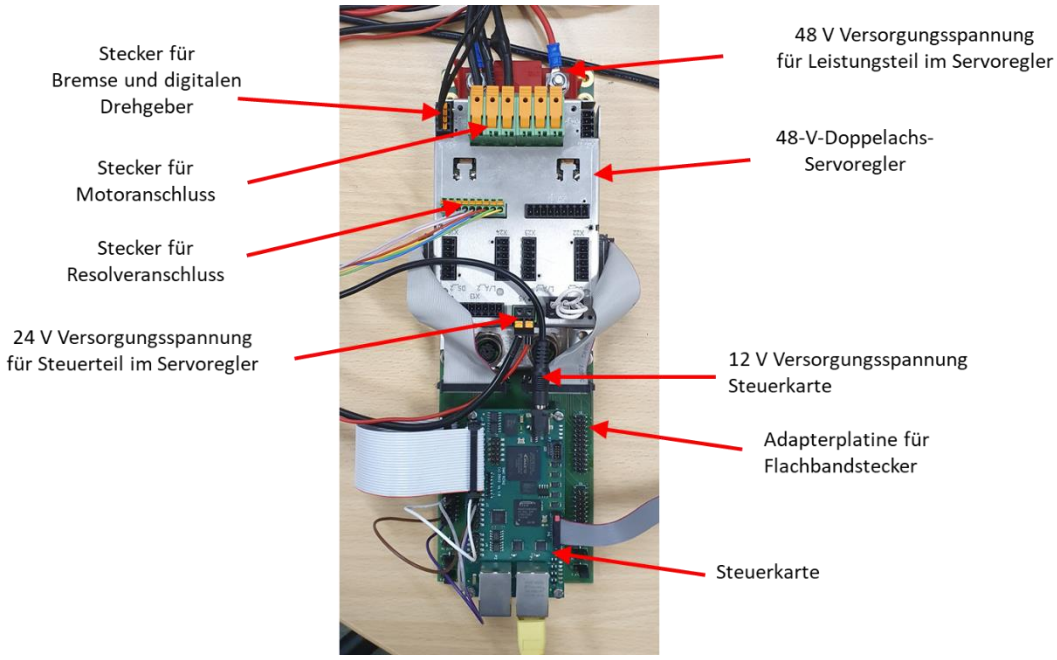


Abbildung 50: Entwickelter 48-V-Doppelachs-Antrieb mit der externen Steuerelektronik verbunden über Flachbandkabel.

Anhang 5: Übertragung der sicherheitsbezogenen Stromdaten über EtherCAT

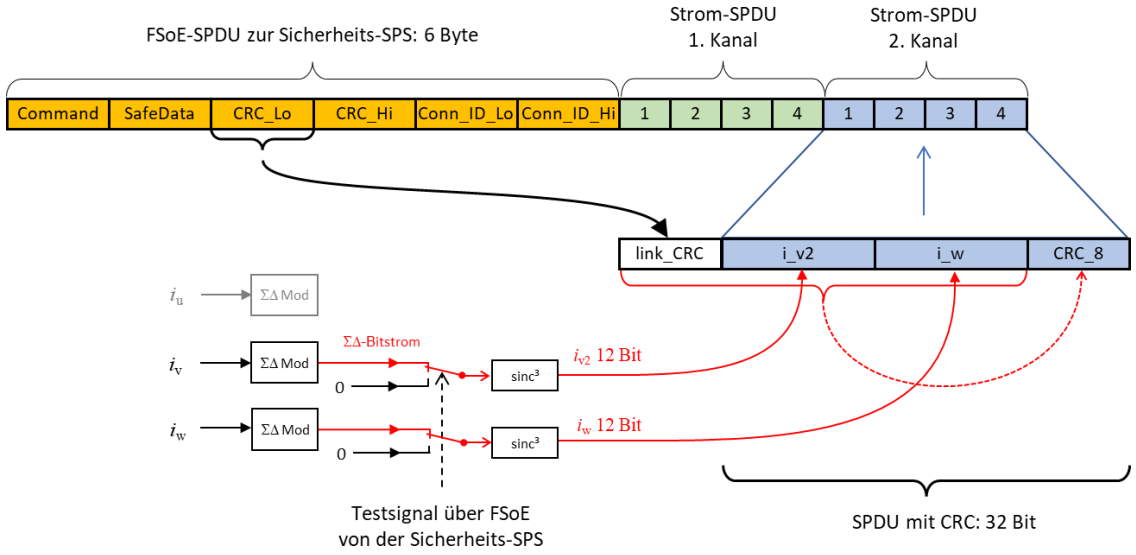


Abbildung 51: Verkettung der 2. Strom-SPDU mit dem FSoE-CRC und Anhängen an die FSoE-Slave-SPDU.

Literaturverzeichnis

[1] J. Dispan und L. Mendler, „Branchenanalyse Elektroautomation," Hans Böckler Stiftung, Düsseldorf, Juli, 2022.

[2] B. Wacker et al., „Antrieb 2030 – Zwölf Thesen," ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie e. V., Frankfurt am Main, September, 2020.

[3] U. Nuß, Hochdynamische Regelung elektrischer Antriebe, Berlin: VDE Verlag GmbH, 2. Auflage, 2017.

[4] R. Dumitrescu, T. Westermann und T. Falkowski, „Autonome Systeme in der Produktion," *Industrie 4.0 Management,* Juni 2018.

[5] M. Breque, L. D. Nul und A. Petridis, „Industry 5.0 - Towards a sustainable, human-centric and resilient European industry," European Commission, Luxembourg, Januar, 2021.

[6] D. P. F. Möller, H. Vakilzadian und R. E. Haas, „From Industry 4.0 towards Industry 5.0," in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022.

[7] M. Happacher, „Ist Industrie 4.0 passé?," *computer & automation,* 23 04 2024.

[8] T. Wilkening, J. Holtz und J. O. Krah, „Mixed-Critical Control Architecture for Industry 5.0," in *2024 4th International Conference on Smart Grid and Renewable Energy (SGRE)*, 2024.

[9] „Kollaborierende Robotersysteme," Fachbereich Holz und Metall der DGUV, Mainz, 2017.

[10] U. Schnell, „Funktionale Sicherheit als integraler Bestandteil," *Konstruktion,* 22 November 2022.

[11] J. Croyle, „Holistic Functional Safety in Robotics," in *14th Int. TÜV Rheinland Symposium – Functional Safety and Cybersecurity in Industrial Applications*, Köln, 2022.

[12] M. Winzenick, „Whitepaper: Fehlertoleranz in der Maschinensicherheit, Teil 1 - Grundlagen," Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI), Version 1.0, Frankfurt, 2019.

[13] U. Probst, Servoantriebe in der Automatisierungstechnik, Wiesbaden: Springer Vieweg, 2022.

[14] U. Riefenstahl, Elektrische Antriebssysteme, Wiesbaden: Springer Vieweg, 2021.

[15] A. Binder, Elektrische Maschinen und Antriebe, Heidelberg: Springer-Verlag, 2012.

[16] J. O. Krah, C. Klarenbach und J. Achterberg, „Modulare Antriebsregelung für Servoantriebe in der Automatisie-rungstechnik," in *SPS / IPC / Drives*, 2010.

[17] C. Buccella, C. Cecati und H. Latafat, „Digital Control of Power Converters—A Survey," *IEEE Transactions on Industrial Informatics,* Bd. 8, pp. 437-447, 2012.

[18] J. O. Krah und K. Neumayer, „System-on-a-Programmable-Chip-Enhanced Solutions for High Performance Servo Drives," in *PCIM Europe 2003; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2003.

[19] E. Monmasson, L. Idkhajine, M. N. Cirstea, I. Bahri, A. Tisan und M. W. Naouar, „FPGAs in Industrial Control Applications," *IEEE Transactions on Industrial Informatics,* Bd. 7, pp. 224-243, 2011.

[20] B. Fortman, „Industrial drive control architectures," Texas Instruments, 16 02 2016. [Online]. Available: https://e2e.ti.com/blogs_/b/industrial_strength/posts/industrial-drive-control-architectures-part-1. [Zugriff am 31 05 2023].

[21] T. Schmidt, J. O. Krah und J. Holtz, „High-Performance Control Architecture for Automation Drives based on a Low-Cost Microcontroller in Combination with a Low- Cost FPGA," in *PCIM Europe digital days 2021; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2021.

[22] „Aplication Report - Designing With the C2000™ Configurable Logic Block (CLB)," Texas Instruments, 2019. [Online]. Available: https://www.ti.com/lit/an/spracl3/spracl3.pdf?ts=1685607262219&ref_url=https%253A%252F%252Fwww.google.com%252F. [Zugriff am 01 06 2023].

[23] D. Casadei, F. Profumo, G. Serra und A. Tani, „FOC and DTC: two viable schemes for induction motors torque control," *IEEE Transactions on Power Electronics,* Bd. 17, pp. 779-787, 2002.

[24] V. M. Bida, D. V. Samokhvalov und F. S. Al-Mahturi, „PMSM vector control

techniques — A survey,“ in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2018.

[25] C. Klarenbach, H. Schmirgel und J. O. Krah, „Design of Fast and Robust Current Controllers for Servo Drives based on Space Vector Modulation,“ in *PCIM Europe digital days 2011; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2011.

[26] R. H. Park, „Two-reaction theory of synchronous machines generalized method of analysis-part I,“ *Transactions of the American Institute of Electrical Engineers,* Bd. 48, pp. 716-727, 1929.

[27] X. Zhang, X. Xie und R. Yao, „Field oriented control for permanent magnet synchronous motor based on DSP experimental platform,“ in *The 27th Chinese Control and Decision Conference (2015 CCDC)*, 2015.

[28] F. Jenni und D. Wüest, Steuerverfahren für selbstgeführte Stromrichter, vdf Hochschulverlag AG an der ETH Zürich und B.G. Teubner Stuttgart, 1995.

[29] J. Holtz, „Pulsewidth modulation for electronic power conversion,“ *Proceedings of the IEEE,* Bd. 82, pp. 1194-1214, 1994.

[30] J. O. Krah und J. Holtz, „High-performance current regulation and efficient PWM implementation for low-inductance servo motors,“ *IEEE Transactions on Industry Applications,* Bd. 35, pp. 1039-1049, 1999.

[31] J. O. Krah, T. Schmidt und J. Holtz, „Predictive Current Control with Synchronous Optimal Pulse Patterns,“ in *2019 2nd International Conference on Smart Grid and Renewable Energy (SGRE)*, 2019.

[32] H. Schmirgel und J. O. Krah, „Optimization of Servo Drive Parameters Utilizing New Built in Frequency Analysis Functionality,“ in *SPS IPC Drives*, Nürnberg, 2007.

[33] J. Hilverkus, R. Hagl und R. Kennel, „Structural Mechanical Limitations of Dynamics of Servo Drives,“ in *2020 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, 2020.

[34] Y. Olca, M. N. Ekım und A. F. Boz, „Investigation of the Effects of Current Measurement Methods on Servo Motor Dynamics,“ in *2019 20th International Symposium on Power Electronics (Ee)*, 2019.

[35] A. Rath, C. Klarenbach, O. D. Djouosseu und J. O. Krah, „Fast Current

Measurement based on Enhanced ΣΔ Technology," in *PCIM Europe digital days 2012; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2012.

[36] J. O. Krah, E. Fitz und P. Maeder, „Very Efficient Current Observer for Sigma Delta Modulation based Current Transducers for High Bandwidth Current Control," in *PCIM Europe 2019; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2019.

[37] C. Li, B. T. Vankayalapati, B. Akin und Z. Yu, „Analysis and Compensation of Sigma-Delta ADC Latency for High Performance Motor Control and Diagnosis," *IEEE Transactions on Industry Applications,* Bd. 59, pp. 873-885, 2023.

[38] S. Basler, Encoder und Motor-Feedback-Systeme, Wiesbaden: Springer Vieweg, 2016.

[39] T. Wilkening, J. O. Krah und H. Goergen, „Safety-Related Interfaces for Position Encoders - a Survey," in *PCIM Europe 2019; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2019.

[40] T. Wilkening, T. Cetin, H. Reiter und J. O. Krah, „EnDat 3 – Safety-Related Fully Digital Encoder Interface from the Application Point of View," in *PCIM Europe digital days 2020; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management,* 2020.

[41] J. O. Krah, T. Schmidt und R. Richter, „Multi-Protocol Position Encoder Interface IP for Safety-Related Automation Drives," 2021.

[42] „Elektronisches Typenschild erleichtert Inbetriebnahme," *SPS Magazin,* pp. 96-97, 03 2020.

[43] J. O. Krah, H. Schmirgel und M. Albers, „FPGA Based Resolver to Digital Converter Using Sigma-Delta Analog to Digital Technology," in *PCIM Europe 2006; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management,* 2006, pp. 931-936.

[44] „Variable Resolution, Resolver-to-Digital Converter AD2S83," Analog Devices, 2000. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/ad2s83.pdf. [Zugriff am 08 03 2023].

[45] J. O. Krah, „Software Resolver to Digital Converter for High Performance Servo Drives," in *PCIM Europe 1999; International Exhibition and Conference for*

Power Electronics, Intelligent Motion, Renewable Energy and Energy Management, June 1999, pp. 301-308.

[46] T. Schmidt, J. Holtz und J. O. Krah, „Mixed Critical Resolver to Digital Conversion for Safety-Related Servo Drive Applications," in *PCIM Europe 2023; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2023.

[47] D. Janssen, „EtherCAT als Antriebsbus: Synchronität ist nicht genug," 11 2004. [Online]. Available: https://www.ethercat.org/download/documents/iee_1104.pdf. [Zugriff am 08 04 2024].

[48] J. Hibbard, „5 Real-Time, Ethernet-Based Fieldbuses Compared," Whitepaper, KingStar, 2016.

[49] „Systemhandbuch AX5000 Servoverstärker," Beckhoff, 2023. [Online]. Available: https://www.beckhoff.com/de-de/produkte/motion/servoverstaerker/ax5000-digital-kompakt-servoverstaerker/. [Zugriff am 20 09 2023].

[50] „Bedienungsanleitung VLT AQUA Drive FC 202," Danfoss, 2016. [Online]. Available: https://www.danfoss.com/de-de/products/dds/low-voltage-drives/vlt-drives/vlt-aqua-drive-fc-202/. [Zugriff am 10 06 2023].

[51] C. Werner, H. Zilligen, B. Köhler und R. Apfeld, „Sichere Antriebssteuerungen mit Frequenzumrichtern," IFA Report 4 / 2018, Deutsche Gesetzliche Unfallversicherung (DGUV), 2018.

[52] M. Hauke et al., „Funktionale Sicherheit von Machinensteuerungen - Anwendung der DIN EN ISO 13849," IFA Report 2 / 2017, Deutsche Gesetzliche Unfallversicherung (DGUV), 2021.

[53] „Europäische Normen, Your Europe (offizielle Website der Europäischen Union)," 10 10 2022. [Online]. Available: https://europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_de.htm. [Zugriff am 14 06 2023].

[54] DIN EN ISO 12100:2011-03, „Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung," Berlin, 2011, www.beuth.de.

[55] IEC 62061:2021, „Safety of machinery - Functional safety of safety-related control systems," Berlin, 2021, www.vde-verlag.de.

[56] DIN EN 61800-5-2:2017-10, „Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl - Teil 5-2: Anforderungen an die Sicherheit - Funktionale Sicherheit," Berlin, 2017, www.beuth.de.

[57] DIN EN ISO 13849-1:2016-05, „Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze," Berlin, 2016, www.beuth.de.

[58] T. Huckle, „Kleine BUGs, große GAUs. Vortrag über Softwarefehler und ihre Folgen.," 27 03 2003. [Online]. Available: https://www5.in.tum.de/~huckle/bugsn.pdf. [Zugriff am 21 06 2023].

[59] „Kann mit einer Standard-SPS PL c erreicht werden?," Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, 2022.

[60] J. O. Krah, M. Katz, T. Schmidt und B. Jeppesen, „Lean Safe Drive Architecture with Fully Integrated Multi-Axis Safety Functions due to an Extremely Fast Safety-related Fieldbus Interface," in *PCIM Europe digital days 2021; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2021.

[61] T. Bömer, K.-H. Büllesbach, M. Hauke, S. Otto und C. Werner, „Praxisgerechte Umsetzung der Anforderungen für sicherheitsbezogene Embedded-Software nach DIN EN ISO 13849-1," IFA Report 1 / 2020, Deutsche Gesetzliche Unfallversicherung (DGUV), 2020.

[62] M. Mai und G. Reuß, „Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben," BGIA Report 7 / 2006, Hauptverband der gewerblichen Berufgenossenschaften (HVBG), Sankt Augustin, 2006.

[63] I. Krischke, „Die Jubiläums-Steuerung," computer & automation, 14 11 2022. [Online]. Available: https://www.computer-automation.de/steuerungsebene/safety-security/die-jubilaeums-steuerung.200439.html. [Zugriff am 22 06 2023].

[64] „Sicherheitsrelais Funktion," Pilz, [Online]. Available: https://www.pilz.com/de-DE/support/knowhow/lexicon/articles/072106. [Zugriff am 22 06 2023].

[65] DIN EN ISO 13849-2:2013-02, „Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung," Berlin, 2013, www.beuth.de.

[66] DIN EN ISO 9001:2015-11, „Qualitätsmanagementsysteme - Anforderungen," Berlin, 2015, www.beuth.de.

[67] W. Möller, „Feldbusse krempeln an Maschinen und Anlagen die Sicherheitstechnik um,“ Industrieanzeiger, 21 09 2009. [Online]. Available: https://www.computer-automation.de/steuerungsebene/safety-security/die-jubilaeums-steuerung.200439.html. [Zugriff am 23 06 2023].

[68] G. Herkommer, „Nur ein Controller für SPS, Motion und Safety,“ computer & automation, 08 07 2010. [Online]. Available: https://www.computer-automation.de/steuerungsebene/steuern-regeln/nur-ein-controller-fuer-sps-motion-und-safety.72809.html. [Zugriff am 26 06 2023].

[69] „Option Sicherheitsmodul MOVISAFE DCS21B/22B/31B/32B,“ SEW Eurodrive, 2013. [Online]. Available: https://download.sew-eurodrive.com/download/pdf/20084137.pdf. [Zugriff am 23 06 2023].

[70] „ctrlX SAFETY - Sicherheitsoption "Safe Torque Off" in ctrlX DRIVE,“ Bosch Rexroth, 2020.

[71] „PMCprotego - Safe Motion,“ Pilz, 2021. [Online]. Available: https://www.pilz.com/de-DE/eshop/Antriebstechnik/Servoverst%C3%A4rker/PMCprotego-Safe-Motion/PMCprotego-S-Sicherheitskarte/c/0010700229707380N3#components. [Zugriff am 26 06 2023].

[72] „AX5805 und AX5806 - TwinSAFE-Drive-Optionskarten für den Servoverstärker AX5000,“ Beckhoff, 2023. [Online]. Available: https://www.beckhoff.com/de-de/produkte/automation/twinsafe/twinsafe-hardware/ax5805.html. [Zugriff am 26 06 2023].

[73] „SINAMICS S210 - Servo Drive System,“ Siemens, 2023. [Online]. Available: https://support.industry.siemens.com/cs/document/109754381/catalog-d-32-sinamics-s210-servo-drive-system?dti=0&lc=en-DE. [Zugriff am 27 06 2023].

[74] „AX8911 - TwinSAFE-Drive-Option für Servoverstärker AX8xxx-xxxx,“ Beckhoff, 2020. [Online]. Available: https://download.beckhoff.com/download/Document/automation/twinsafe/ax8911de.pdf. [Zugriff am 27 06 2023].

[75] „ctrlX SAFETY "Safe Motion" - ctrlX DRIVEplus,“ Bosch Rexroth, 2023. [Online]. Available: https://www.boschrexroth.com/de/de/search.html?q=R911404904&lang=DE&origin=header&num=10&s=download. [Zugriff am 27 06 2023].

[76] M. Kempf und U. Klaus, „Sicherheit individuell skalierbar,“ wirautomatisierer.de,

14 10 2014. [Online]. Available: https://wirautomatisierer.industrie.de/safety/sicherheit-individuell-skalierbar/. [Zugriff am 27 06 2023].

[77] T. Wilkening, J. O. Krah, M. Salardi und F. Heinzelmann, „Safety-Related High-Performance Motion Control based on a Quad-Core SoC," in *PCIM Europe digital days 2021; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2021.

[78] G. Creech, „Black Channel Communication: What is it and how does it work?," *Measurement + Control Vol 40*, pp. 304-309, 2007.

[79] DIN EN 61508-2:2010, „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme," Berlin, 2010, www.vde-verlag.de.

[80] D. Reinert und M. Schaefer, Sichere Bussysteme für die Automation, Heidelberg: Hüthig GmbH & Co. KG, 2001.

[81] F. Schiller, D. Judd, P. Supavatanakul, T. Hardt und F. Wieczorek, „Enhancement of safety communication model," *at - Automatisierungstechnik,* 2022.

[82] DIN EN IEC 61784-3:2021, „Industrielle Kommunikationsnetze – Profile, Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile," Berlin, 2022, www.vde-verlag.de.

[83] S. Ditting, „The Oxymoron of Modern Automation," in *14th Int. TÜV Rheinland Symposium – Functional Safety and Cybersecurity in Industrial Applications*, Köln, 2022.

[84] R. Apfeld, „Brauchen sichere Antriebssteuerungen auch sichere Positionsgeber?," Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), 12.2017.

[85] DIN EN 61800-5-3:2019-07, „Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl - Teil 5-3: Anforderungen an die Sicherheit von Encodern (Gebern) – Funktional, elektrisch und umwelttechnisch," Berlin, 2019, www.vde-verlag.de.

[86] Posital, „Divers-Redundante Absolutgeber von Posital," [Online]. Available: http://test.posital.com/de/unternehmen/neuigkeiten/redundant-safety-encoder.php. [Zugriff am 01 08 2023].

[87] „Safety Integrated,“ Siemens, 2022. [Online]. Available: https://mall.industry.siemens.com/mall/de/WW/Catalog/Products/10290371. [Zugriff am 27 06 2023].

[88] A. Markis et al., „Sicherheit in der Mensch-Roboter-Kollaboration, Whitepaper, TÜV Austria und Frauenhofer Austria,“ 2016.

[89] H.-J. Buxbaum, Mensch-Roboter-Kollaboration, Wiesbaden: Springer Gabler, 2020.

[90] DIN ISO/TS 15066:2017-04, „Roboter und Robotikgeräte - Kollaborierende Roboter,“ Berlin, 2017, www.beuth.de.

[91] G. Lefranc, I. Lopez-Juarez, R. Osorio-Comparán und M. Peña-Cabrera, „Impact of Cobots on automation,“ in *Procedia Computer Science; 9th International Conference on Information Technology and Quantitative Management*, 2022.

[92] A. Barnitzke, „Fahrerlose Transportsysteme und autonome mobile Roboter: Was ist der Unterschied zwischen FTS und AMR?,“ automationspraxis, 22 07 2021. [Online]. Available: https://automationspraxis.industrie.de/servicerobotik/fahrerlose-transportsysteme-und-autonome-mobile-roboter-im-ueberblick-vom-fts-zum-amr/. [Zugriff am 05 07 2023].

[93] A. Trenkle, „Entwurfsmuster für Fahrerlose Transportsysteme,“ Dissertation Karlsruher Institut für Technologie, Fakultät für Maschinenbau, Karlsruhe, 2018.

[94] M. B. Alatise und G. P. Hancke, „A Review on Challenges of Autonomous Mobile Robot and Sensor Fusion Methods,“ *IEEE Access*, Bd. 8, pp. 39830-39846, 2020.

[95] M. Winzenick, „Whitepaper: Fehlertoleranz in der Maschinensicherheit, Teil 2 - Anforderungen,“ Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI), Version 1.0, Frankfurt, 2021.

[96] „AN5050 Application note - Octo-SPI interface on STM32 microcontrollers,“ STMicroelectronics, 2021. [Online]. Available: https://www.st.com/resource/en/application_note/dm00407776-octospi-interface-on-stm32-microcontrollers-stmicroelectronics.pdf. [Zugriff am 08 03 2023].

[97] „Avalon® Interface Specifications,“ Intel, 2022. [Online]. Available: https://www.intel.com/content/www/us/en/docs/programmable/683091/20-1/introduction-to-the-interface-specifications.html. [Zugriff am 06 09 2023].

[98] H. Schmirgel, J. O. Krah und R. Berger, „Delay Time Compensation in the Current Control Loop of Servo Drives–Higher Bandwidth at no Trade-off," in *PCIM Europe 2006; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2006, pp. 541-546.

[99] G. Ellis und J. O. Krah, „Observer-based Resolver Conversion in Industrial Servo Systems," in *PCIM Europe 2001; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2001.

[100] T. Grohmann, S. Künzel, W. Papiernik, B. Quaschner, G. Seeger und J. Welker, „Steuerungsverfahren sowie Regelungsstruktur zur Bewegungsführung, Vorsteuerung und Feininterpolation von Objekten in einem Drehzahlreglertakt, der schneller als der Lagereglertakt ist," in *EP 1 229 411 A3, Europäisches Patentamt*, 07.08.2002.

[101] EtherCAT Technology Group, „EtherCAT – Der Ethernet-Feldbus," 12 2022. [Online]. Available: https://www.ethercat.org/de/technology.html. [Zugriff am 09 09 2023].

[102] DIN EN 60204-1:2019-05, „Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen - Teil 1: Allgemeine Anforderungen," Berlin, 2019, www.beuth.de.

[103] „Intel® MAX® 10 General Purpose I/O User Guide," Intel, 2022. [Online]. Available: https://www.intel.com/content/www/us/en/docs/programmable/683751/21-1/i-o-overview.html. [Zugriff am 27 03 2023].

[104] Z. Haitao, Z. Zhengming, Y. Liqiang und B. Hua, „Simulation, Test and Analysis of Three-phase Short-Circuit Braking in IGCT-based MV Adjustable Speed Drive Systems," in *2005 International Conference on Electrical Machines and Systems*, 2005.

[105] T. Schmidt, F. Heinzelmann, J. Holtz und J. O. Krah, „Fault-Tolerant Regenerative Sensorless Braking of PMAC Motors Enables Degraded Mode of Operation for Functional Safety," in *PCIM Europe 2022; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2022.

[106] J. O. Krah, B. Koehler und J. Koss, „Safety Related Current Monitoring for Multiphase Motors built with Digital Current Transducers," in *PCIM Europe*

2019; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management, 2019.

[107] „EnDat3 - Anwendungsbedingungen Funktionale Sicherheit," DR. JOHANNES HEIDENHAIN GmbH, 10.2021.

[108] T. Schmidt, J. O. Krah und J. Holtz, „Diverse Redundant Drive Architecture with External Diagnostics Enables Safety-Related Motor Control based on Proven Standard Components at Low Cost," in *2024 4th International Conference on Smart Grid and Renewable Energy (SGRE)*, 2024.

[109] „ADS1209," Texas Instruments, 2010. [Online]. Available: https://www.ti.com/product/ADS1209. [Zugriff am 11 04 2023].

[110] Z. Zhang, G. Li, Z. Qian, Q. Ye und Y. Xia, „Research on effect of temperature on performance and temperature compensation of interior permanent magnet motor," in *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, 2016.

[111] D. Lin, P. Zhou und Z. J. Cendes, „In-Depth Study of the Torque Constant for Permanent-Magnet Machines," *IEEE Transactions on Magnetics*, Bd. 45, pp. 5383-5387, 2009.

[112] Z. Shareef, Path Planning and Trajectory Optimization of Delta Parallel Robot, 2015.

[113] DIN EN 61131-9:2013, „Speicherprogrammierbare Steuerungen – Teil 9: Schnittstelle für die Kommunikation mit kleinen Sensoren und Aktoren über eine Punkt-zu-Punkt-Verbindung," Berlin, 2015, www.vde-verlag.de.

[114] „IO-Link Interface and System - Specification," IO-Link Community, Version 1.1.3, 2019.

[115] T. Wilkening, J. Randerath, M. Avendano, J. Holtz und J. O. Krah, „Modular System Architecture for Large Multi-Axis Motion Control Systems in Automation," in *PCIM Europe 2022; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management*, 2022.

[116] „MAX14819 / MAX14819A Dual IO-Link Master Transceiver," Analog Devices, 2020. [Online]. Available: https://www.analog.com/en/products/max14819.html. [Zugriff am 16 05 2023].

[117] „SLB240 - Betriebsanleitung Sicherheits-Lichtschranken," Schmersal, 2020.

[Online]. Available: https://products.schmersal.com/de_DE/slb240-er-1-lst-5271.html?type=product. [Zugriff am 17 05 2023].

[118] F. Bauder et al., „Positionspapier CB 24 I - Klassifizierung binärer 24-V-Schnittstellen mit Testung im Bereich der Funktionalen Sicherheit," ZVEI – Zentralverband der Elektrotechnik und Elektronikindustrie e.V., 05.2021.

[119] „Intel® MAX® 10 FPGA Device Datasheet," Intel, 2022. [Online]. Available: https://www.intel.com/content/www/us/en/docs/programmable/683794/current/fpga-device-datasheet.html. [Zugriff am 03 05 2023].

[120] „STM32L552xx," STMicroelectronics, 2020. [Online]. Available: https://www.st.com/en/microcontrollers-microprocessors/stm32l5x2.html. [Zugriff am 03 05 2023].

[121] A. Kumar und D. Chatterjee, „A survey on space vector pulse width modulation technique for a two-level inverter," in *2017 National Power Electronics Conference (NPEC)*, 2017.