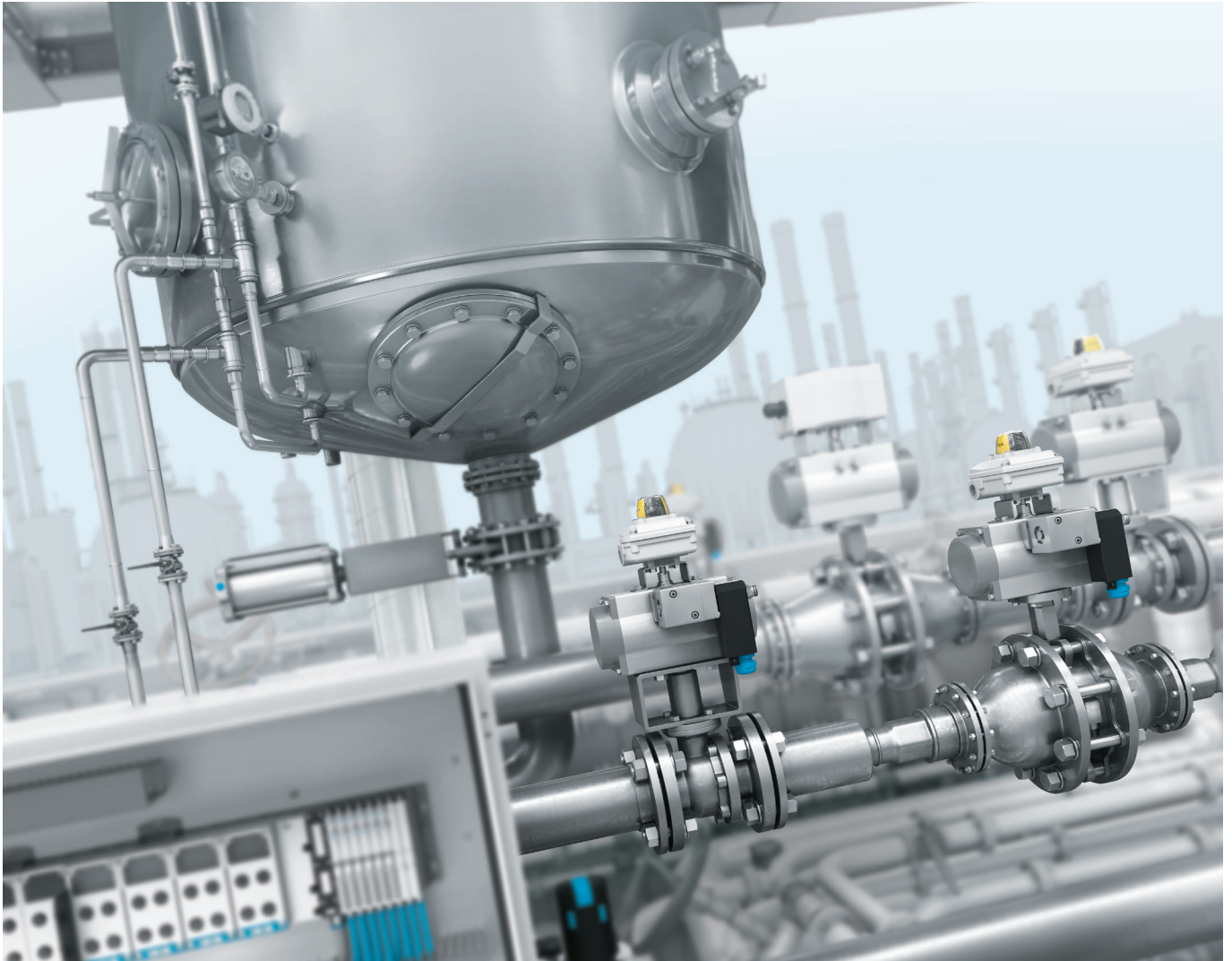


White Paper

Ansteuerung von Prozessarmaturen unter Berücksichtigung der funktionalen Sicherheit (SIL)



Seit dem Inkrafttreten der IEC 61508 ist das Thema "Funktionale Sicherheit" in der Prozessindustrie sehr stark in den Vordergrund getreten. Oftmals wird nur der Ausdruck SIL verwendet. Aber was genau ist eigentlich SIL und welche Lösungsansätze gibt es für die Ansteuerung von Prozessarmaturen?

In diesem White Paper finden Sie folgende Informationen:

- Was ist SIL (Safety Integrity Level)?
- Der normative Part
- Die Risikoanalyse
- Zertifikate und Herstellererklärungen
- Schutzeinrichtung am Beispiel eines Rührkesselreaktors
- Betriebsbewährung und Laufzeitverlängerung am Beispiel Magnetventil
- Redundante Ansteuerungen von Aktoren im Feld

1. Was ist SIL (Safety Integrity Level)?

Die Aufgabe von Sicherheitsfunktionen (Safety Functions) ist es, das Risiko von Prozessen zu minimieren, von denen Gefahren für Mensch, Umwelt und Sachwerte ausgehen. SIL (Safety Integrity Level) beschreibt das Maß der Risikoreduzierung auf ein vertretbares Niveau. Die IEC 61508 erklärt sowohl die Art der Risikobewertung (Risikograph) als auch die Maßnahmen zur Auslegung entsprechender Sicherheitsfunktionen von Sensoren, Logikverarbeitung bis hin zum Aktor bezüglich „Fehlervermeidung“ (systematische Fehler) und „Fehlerbeherrschung“ (zufällige Fehler). Dieser anwendungsunabhängige Basisstandard beschreibt die Anforderungen an Komponenten und Systeme für Sicherheitsfunktionen und hilft bei der Entwicklung sektorspezifischer Normen wie z. B. die IEC 61511-1 „Funktionale Sicherheit: Sicherheitstechnische Systeme für den Bereich der Prozessindustrie“. Unter anderem legt die IEC 61511-1 Auswahlkriterien für Komponenten der Sicherheitsfunktionen wie z. B. die Betriebsbewährung von Sensoren und Aktoren fest.

Sensor ≥ 35 %		Logik ≥ 15 %		Aktor ≥ 50 %	
					
PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
SIL _{erforderlich} (SIL _r)					
PFD _{gesamt} /PFH _{gesamt}					

	vom Hersteller bekannt gegeben
	vom Anlagenbetreiber zu ermitteln

Wichtig zu wissen

Die Anforderung an die Ausfallwahrscheinlichkeit nach IEC 61508 bezieht sich immer auf eine komplette Schutzeinrichtung und nicht auf einzelne Komponenten. Eine Komponente kann deshalb für sich genommen kein SIL-Level haben, sondern nur der gesamte Sicherheitskreis, genannt SIS - Safety Integrated System.

Üblicherweise besteht ein Sicherheitskreis aus folgenden Komponenten:

- Sensorik, z. B. Druck-, Temperatur-, Füllstandmesser
- Auswerte- und Ausgabereinheit, z.B. Sicherheits-SPS
- Automatisierte Armatur bestehend aus Magnetventil, Antrieb und Armatur

Übliche Verteilung des PFD/PFH auf die Teilsysteme einer Sicherheitsfunktion bei einkanaligen Systemen

2. Der normative Part

Die Normenwelt rund um die Thematik „Funktionale Sicherheit“ ist umfangreich und selbst für erfahrene Anwender nicht immer leicht zu durchschauen. In diesem White Paper konzentrieren wir uns auf die praktische Umsetzung sowie die Interpretation dieser Normen und werden daher nicht im Detail auf den normativen Part eingehen.

Grundsätzlich sind folgende Normen relevant:

- IEC 61508 „Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer Systeme“
→ Basisnorm für die Thematik funktionale Sicherheit
- IEC 61511 „Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie“
→ gilt für die Prozessautomation

3. Die Risikoanalyse

Zur Minimierung des Risikos schreiben sowohl IEC 61508 als auch IEC 61511 im Wesentlichen folgende Schritte vor:

- Risikodefinition und -bewertung nach detaillierten Versagenswahrscheinlichkeiten vom Sensor über die Steuerung bis zum Aktor über die gesamte Lebensdauer der Komponenten.
- Festlegung und Umsetzung der Maßnahmen zur Restrisikominimierung.
- Einsatz geeigneter Geräte (bewertet oder zertifiziert).
- Wiederkehrende Prüfung der korrekten Einhaltung der Sicherheitsfunktionen.

3.1. Die HAZOP-Analyse und weitere Verfahren

Als Hazards werden mögliche kritische Abweichungen von den Plänen zum Produktionsablauf bezeichnet. Hazards sind also Gefahren, die eine tatsächliche oder potenzielle Bedrohung darstellen. HAZOP („Hazard and Operability Study“) dient zur systematischen Identifizierung von Fehlern und produktivitätsmindernden Betriebsstörungen (Operability Problems). Diese Technik ist heute universell einsetzbar für Anlagen aller Art, die kontinuierlich oder diskontinuierlich produzieren. Die grundlegenden Schritte einer HAZOP-Analyse sind:

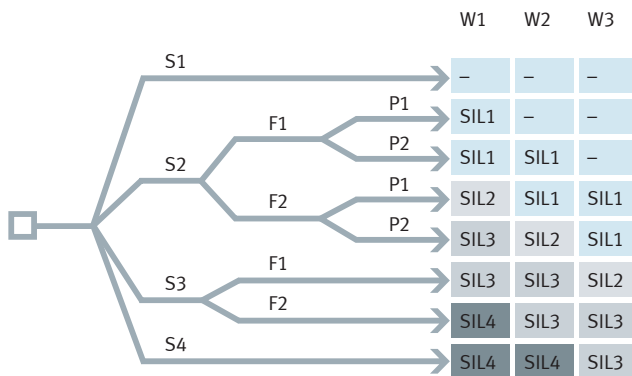
- 1) Prognose eines möglichen Ereignisses
- 2) Auffinden der Ursachen
- 3) Abschätzen der Auswirkungen
- 4) Gegenmaßnahmen

Als weitere Verfahren, die in der Gefahrenanalyse zum Einsatz kommen, sind z.B. die Ausfalleffekt- und Bedeutungs-Analyse (FMEA), die Ereignisbaumanalyse (ETA) oder die Fehlerbaumanalyse (FTA) zu nennen. Die Verfahren kann man in drei Gruppen einteilen: induktive

Verfahren wie FMEA, bei denen die Ursachen für das Versagen, aber nicht die resultierenden Konsequenzen bekannt sind, deduktive Verfahren wie FTA, bei denen die Konsequenzen, aber nicht die Ursachen bekannt sind und explorative Verfahren, bei denen weder Ursachen noch Folgen der Abweichungen bekannt sind, wie HAZOP. Die fehlenden Informationen sollen durch den Einsatz der Methoden ermittelt werden.

Weiterhin kann eine Unterscheidung in Vorwärts-Suche (Bottom-Up) und Rückwärts-Suche (Top-Down) vorgenommen werden. Vorwärts bedeutet, dass man von einem kritischen Fehler ausgeht und versucht, die Konsequenzen herauszufinden (FMEA). Bei der Rückwärts-Suche geht man von gefährlichen Konsequenzen aus und versucht die Ursachen zu bestimmen (FTA).

SIL (Safety Integrity Level)



Risikograph: Vier diskrete Stufen (SIL1 bis SIL4). Je höher der SIL eines sicherheitsbezogenen Systems, desto geringer die Wahrscheinlichkeit, dass das System die geforderten Sicherheitsfunktionen nicht ausführen kann.

S	Schadensausmaß
S1	leichte Verletzung einer Person
S2	schwere Verletzung mehrerer Personen bis hin zum Tod einer Person
S3	Tod mehrerer Personen
S4	katastrophale Auswirkungen mit vielen Toten
F	Aufenthaltswahrscheinlichkeit
F1	selten bis etwas öfter
F2	häufig bis andauernd
P	Gefahrenabwehr/Vermeidung
P1	möglich unter bestimmten Bedingungen
P2	kaum möglich
W	Eintrittswahrscheinlichkeit
W1	relativ hoch
W2	gering
W3	sehr gering

3.2. Relevante Begriffe und Kennwerte

HFT

Die Hardware Fehler Toleranz beschreibt die Fähigkeit die Sicherheitsfunktion auch bei (mehreren) Fehlern und Abweichungen auszuführen. Sollte aufgrund von diesen Werten der erforderliche SIL nicht erreicht werden, besteht die Möglichkeit über Redundanzen den SIL zu erreichen.

SFF

Die Safe Failure Fraction bestimmt den Anteil der sicheren Fehler an der Gesamtfehleranzahl. Als sichere Fehler werden Fehler bezeichnet, die nicht zu einem gefährlichen Zustand der Anlage führen oder, die zwar zu einem gefährlichen Zustand der Anlage führen könnten, jedoch detektierbar sind.

Die Produkteignung für einen geforderten SIL lassen sich anhand mehrerer Parameter feststellen:

Low Demand

Betriebsart mit niedriger Anforderungsrate an das Sicherheitssystem. Das Sicherheitssystem darf nicht häufiger als einmal pro Jahr angefordert werden.

→ PFD (probability of failure on demand) = Ausfallwahrscheinlichkeit bei Anforderung ist ereignisbezogen.

High Demand

Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung an das Sicherheitssystem. Das Sicherheitssystem arbeitet kontinuierlich oder wird häufiger als einmal pro Jahr angefordert.
→ PFH (probability of failure per hour) = Ausfallwahrscheinlichkeit pro Stunde ist zeitbezogen

Gerätetyp A/B

Typ A: Ausfallverhalten aller Bauteile ist ausreichend beschrieben. Somit gehören einfache (neue) Geräte sowie betriebsbewährte Geräte zu diesem Typ.

Typ B: Ausfallverhalten min. eines Bauteils ist nicht vollständig bekannt. Somit gehören komplexe Geräte sowie Neuentwicklungen zu diesem Typ.

Ziel: $SIL \geq SIL_r$

SIL-Level			Gerätetyp A				Gerätetyp B					
			Safe Failure Fraction (SFF)									
	High Demand Mode	Max. akzeptabler Ausfall des Sicherheitssystems	< 60%	60...90%	90...99%	> 99%	< 60%	60...90%	90...99%	> 99%	Low Demand Mode	Max. akzeptabler Ausfall des Sicherheitssystems
	$10^{-5} \leq PFH < 10^{-4}$	ein Risikoausfall alle 10.000 Stunden										
1	$3 \times 10^{-6} \leq PFH < 10^{-5}$	ein Risikoausfall alle 1.250 Tage	HFT 0				HFT 1	HFT 0			$10^{-2} \leq PFD < 10^{-1}$	einmal in 10 Jahren
	$10^{-6} \leq PFH < 3 \times 10^{-6}$	ein Risikoausfall alle 115,74 Jahre										
2	$10^{-7} \leq PFH < 10^{-6}$	ein Risikoausfall alle 115,74 Jahre	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \leq PFD < 10^{-2}$	einmal in 100 Jahren
3	$10^{-8} \leq PFH < 10^{-7}$	ein Risikoausfall alle 1.157,41 Jahre	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \leq PFD < 10^{-3}$	einmal in 1.000 Jahren
4	$10^{-9} \leq PFH < 10^{-8}$	ein Risikoausfall alle 11.574,1 Jahre		HFT 2	HFT 1	HFT 1			HFT 2	HFT 1	$10^{-5} \leq PFD < 10^{-4}$	einmal in 10.000 Jahren
					HFT 2	HFT 2			HFT 2	HFT 2		
(pro Stunde)												

(pro Stunde)

Übersicht Ausfallwahrscheinlichkeit und Hardware Failure Tolerance

4. Zertifikate und Herstellererklärungen

Die Anlagenbetreiber benötigen einen Nachweis über die SIL Klassifizierung der vom SIS (Safety Instrumented Systems) eingesetzten Komponenten. Nach IEC 61511 sind hierfür Herstellererklärungen völlig ausreichend. Zertifikate sind weder gesetzlich vorgeschrieben noch von der Norm gefordert. Um eine Herstellererklärung oder ein Zertifikat ausstellen zu können, bedarf es einer technischen Beurteilung der einzusetzenden Sicherheitskomponente. Häufig erfolgt diese Beurteilung durch eine unabhängige Organisation wie z. B. TÜV oder Exida. Der Hersteller kann nach einer erfolgreichen Beurteilung eine Herstellererklärung ausstellen und sich gegebenenfalls auf den Prüfbericht der Beurteilung beziehen.

Im Gegensatz zu Herstellererklärungen dürfen Zertifikate nur von einer akkreditierten Organisation (z. B. TÜV) ausgestellt werden.

Je höher die geforderte Sicherheit einer Anlage ist, desto höher sind die Anforderungen an die Unabhängigkeit der Stelle, die die funktionale Sicherheit beurteilt und die Beurteilung ausstellt:

Safety Integrity Level	Beurteilende Stelle
SIL 1	unabhängige Person
SIL 2	unabhängige Abteilung
SIL 3	unabhängige Organisation
SIL 4	unabhängige Organisation

5. Schutzeinrichtung am Beispiel eines Rührkesselreaktors

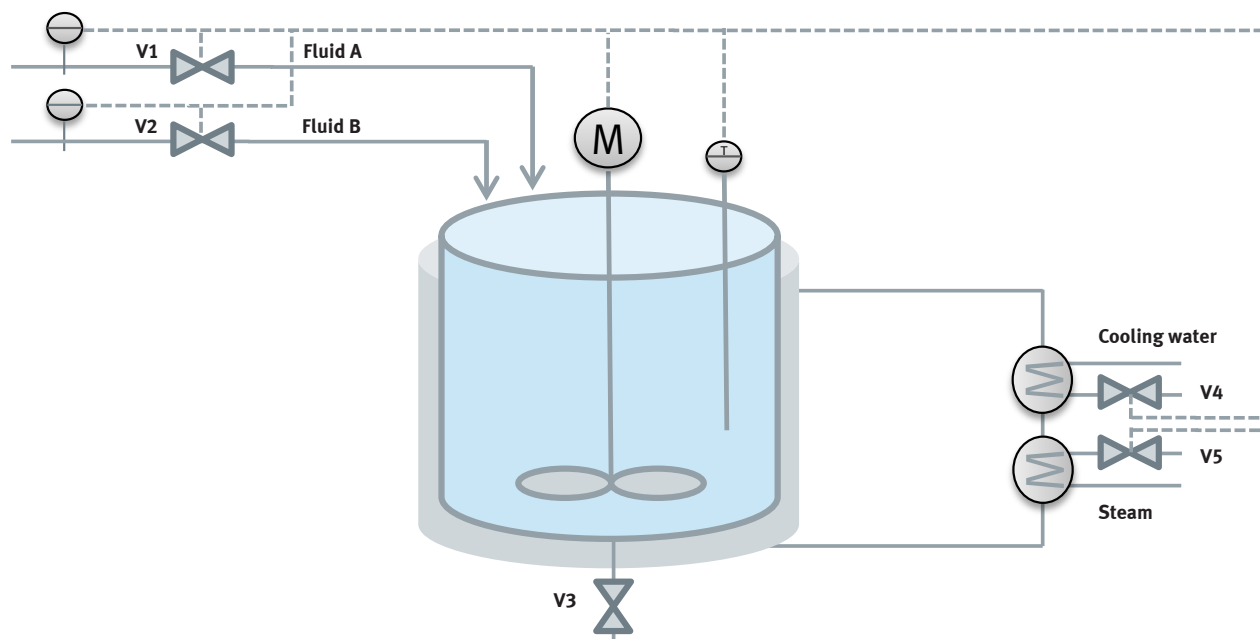
In einem Rührkesselreaktor werden unterschiedliche Komponenten (im untenstehenden Beispiel über die Ventile V1 und V2) zusammengeführt und reagieren entweder durch Wärmezufuhr (endotherm) oder unter Wärmeentwicklung (exotherm) miteinander. Durch Rühren wird dafür gesorgt, dass eine intensive Durchmischung stattfindet. Bei exothermen Reaktionen müssen Überhitzungen vermieden werden.

Ein Beispiel aus unten gezeigtem Schema, für welches eine Schutz-einrichtung notwendig ist, ist die Druckregelung für den Reaktionsver-lauf. Wird der Druck im Reaktor zu hoch, ist eine Fehlermöglichkeit,

dass die Wärmeabfuhr nicht richtig arbeitet. Die Konsequenz daraus wäre, dass das Mischungsverhältnis nicht in Ordnung ist.

Aus diesem Szenario ergibt sich folgende Anforderung an die Schutz-einrichtung: Schließen der Zulaufventile V1, V2 und des Dampfventils V5, sowie gleichzeitiges Öffnen des Kühlwasserventils V4 um den Reaktor abzukühlen.

Um die oben genannte Problemstellung zu lösen gibt es je nach Risi-koeinstufung unterschiedliche Möglichkeiten:



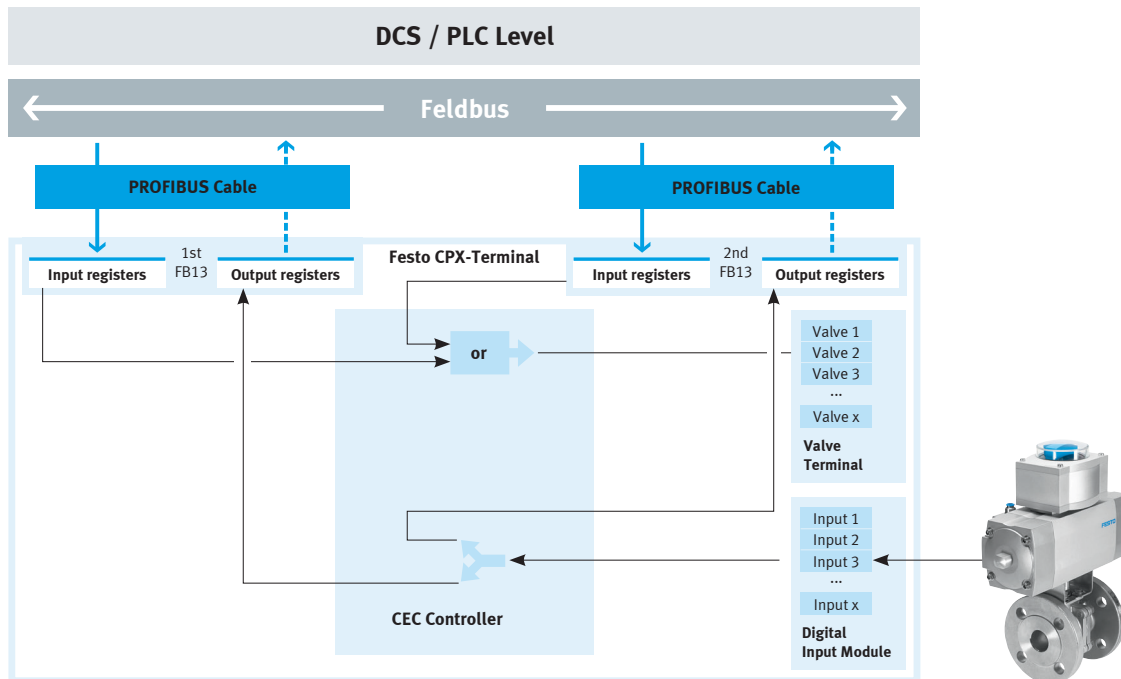
Schematische Darstellung eines Rührkesselreaktors

5.1. Über eine redundante PROFIBUS-Lösung zwischen Leitsystem (DCS) und Remote I/O kann die Sicherheit erhöht werden.

Sollte eine PROFIBUS-Leitung entfernt werden oder der PROFIBUS-Knoten defekt sein, übernimmt hier die zweite PROFIBUS-Leitung/der zweite PROFIBUS-Knoten die Aufgaben. Diese senden und empfangen weiterhin zuverlässig die Protokolle aus dem Leitsystem.

Zusätzlicher Vorteil:

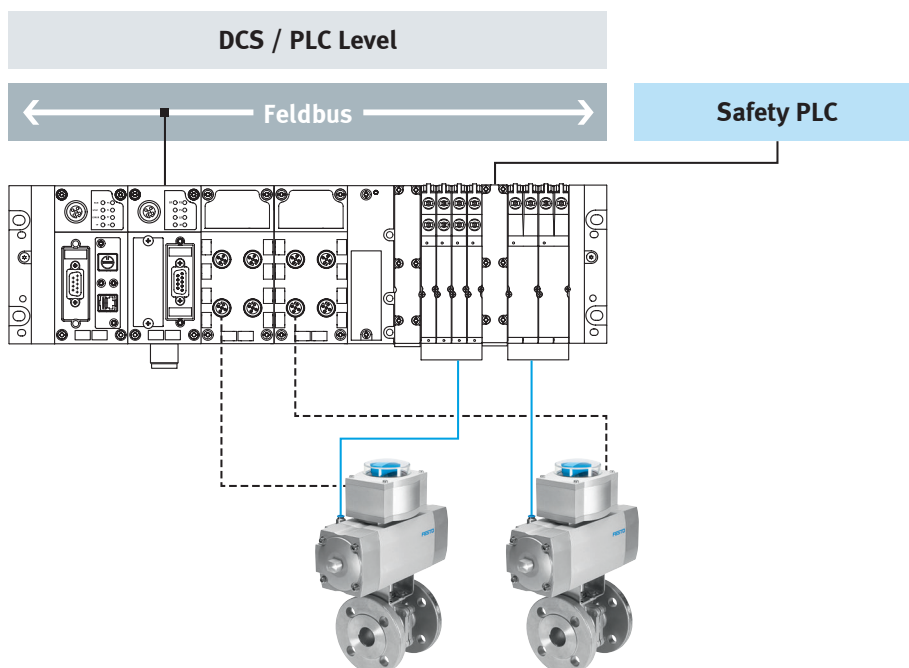
Über einen zusätzlichen Controller mit Ethernet-Schnittstelle kann vor Ort direkt auf die Remote I/O aufgeschaltet und die Parametrierung vorgenommen oder zusätzliche Abläufe implementiert werden. Die bewährte Technologie der Remote I/O übernimmt mit ihren Eingangsmodulen zum Anschließen von NAMUR-Sensoren die Aufgaben der Steuerungsebene zuverlässig. Die modular aufgebauten Terminals sind zusammen mit der nach SIL2 erhältlichen und bewerteten Ventilinsel eine kompakte Alternative.



5.2. Ventilinsel mit integrierter Sicherheitsabschaltung

Der Betriebsmodus wird über Feldbusmodule und Ventilinsel mit in Reihe angeordneten Aktoren realisiert. Die Ventilinsel verfügt über eine separate Einspeisung der SSPS, die separate Ventile schaltet.

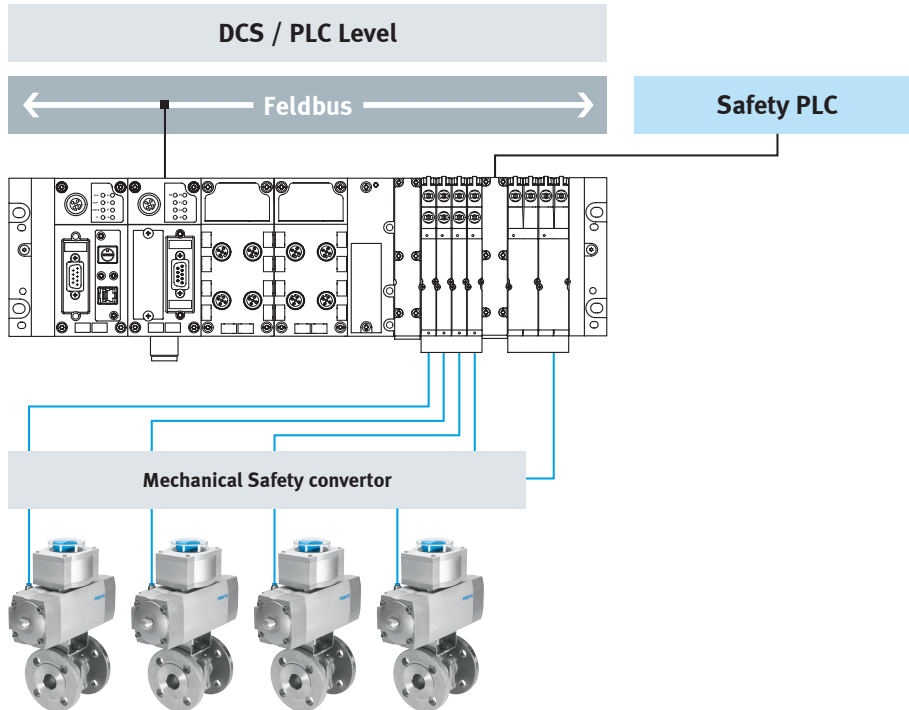
Hierüber werden Aktoren geschaltet, die den Prozess sicher abschalten. Diese Lösung ist für SIL 2 Kreise geeignet. Um den Sicherheitslevel zu erhöhen, gibt es zudem die Möglichkeit die Ventile redundant zu verschalten.



5.3. Ventilinsel mit integrierter Sicherheitsabschaltung

Im Betriebsmodus wird die Ventilinsel über einen Feldbus angesteuert und schaltet Aktoren im Prozess. Zusätzlich verfügt die Ventilinsel über eine separate Einspeisung der SSPS, die die Ventile auf der Ventilinsel für die Sicherheitsabschaltung ansteuert. Die Entlüftung erfolgt über ein zusätzliches 3/2-Wegeventil, welches im Normalbetrieb geschaltet ist und damit das Öffnen der in Stichleitungen mon-

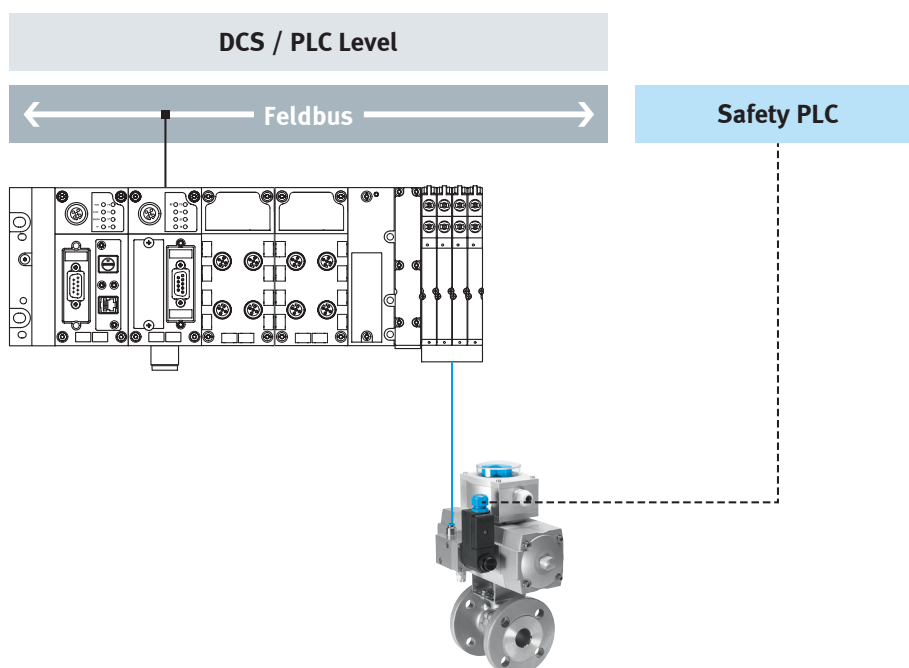
tierten Rückschlagventile verhindert. Zusätzlich wird die Schaltstellung des Ventils durch Überwachung des Drucks gewährleistet. Hierüber werden dieselben Aktoren angesteuert, um den Prozess sicher abzuschalten. Diese Lösung ist für SIL 2 Kreise geeignet. Um den Sicherheitslevel zu erhöhen, gibt es die Möglichkeit die Ventile redundant zu verschalten.



5.4. Ventilinsel plus Einzelventil zur Sicherheitsabschaltung

Der Betriebsmodus wird über den Feldbus und die Ventilinsel gesteuert und hierüber Aktoren im Feld geschaltet. Das auf demselben Aktor

montierte, zertifizierte Einzelventil wird direkt über die SSPS angesteuert und schaltet im Bedarfsfall sicher ab. Diese Ventile sind in sicherheitsgerichteten Kreisen bis zu einem SIL3-Level einsetzbar.



6. Betriebsbewährung und Laufzeitverlängerung am Beispiel Magnetventil

Die Globalisierung, speziell auch in der Chemieindustrie, zwingt die Unternehmen, immer mehr aus den Anlagen herauszuholen. Dies vor allem, um den Preisverfall am Markt zu kompensieren und wettbewerbsfähig zu bleiben. Da moderne Anlagen verfahrenstechnisch oft weitgehend optimiert sind, kann das nur mit einer zuverlässig funktionierenden und hochproduktiven Anlage ohne Ausfallzeiten erreicht werden. Das bedeutet, Reduktion der Revisionszyklen und Revisionszeiten sowie Vermeidung von Ausfallzeiten durch Reparaturen außerhalb der geplanten Revisionen oder Stillstandzeiten.

Eine Möglichkeit, das sicher zu stellen, bietet der Einsatz von betriebsbewährten Komponenten der elektrischen Mess-, Steuer- und Regelungstechnik (EMSR), wie z.B. Magnetventilen, die nach IEC 61508 zertifiziert sind.

Aber auch bei zertifizierten Magnetventilen gibt es große Unterschiede, was dann an ihrer Performance und den Sicherheitskennzahlen ersichtlich ist. Speziell für den Low-Demand Mode, das heißt für Sicherheitseinrichtungen, sind viele Lösungen von Magnetventilen auf dem Markt verfügbar. Hiervon weisen viele eine beschränkte Lebensdauer auf oder aber haben Vorgaben bezüglich der Stillstandzeit oder der Anzahl der Schaltungen, die jährlich durchgeführt werden müssen, um die sicherheitstechnischen Kennzahlen erfüllen zu können.

Eine Steigerung der Zuverlässigkeit ist die Voraussetzung für die Verlängerung der Prüfintervalle. Damit können sehr große Beträge eingespart werden. Erdölraffinerien sind es schon lange gewohnt, Abstellungen nur alle fünf Jahre vorzunehmen. Dort wurde die hohe Zuverlässigkeit vor allem durch die „zwei von drei-Philosophie“ (2003)

erreicht und durch redundante Anlagen und Geräte unterstützt. Dieser teurere Weg rechnet sich dank der hohen Kapazitäten dieser Anlagen. Dies gilt nicht immer für Chemieanlagen. Dort wird heute versucht, mittels zertifizierter, hochzuverlässiger Geräte (Elektromotoren, Transmitter, Steuerungen, Magnetventilen oder sogar Prozessventilen) eine ähnlich hohe Zuverlässigkeit zu erreichen, wie mit redundanten Komponenten.

Vorgesteuerte Magnetventile in Sitzventiltechnik mit TÜV-Gutachten gemäß IEC 61508 sind auf dem Markt bis einschließlich SIL 3 erhältlich. Diese Ventile garantieren gemäß SIL-Klassifizierung eine Ausfallwahrscheinlichkeitsrate von $2,41 \cdot 10^{-4}$, mit anderen Worten, bei 2.410 Schaltungen kann es bei fachgerechtem Einsatz zu maximal einer Fehlschaltung führen.

Erste SIL-zertifizierte Magnetventile stehen mittlerweile seit etwa dem Jahre 2002 in Anlagen im Dienst. Die anfänglich über Labor-Tests erreichten Sicherheitswerte sind mittlerweile von aus dieser Zeit stammenden und seither im Einsatz stehenden Magnetventilen bestätigt worden. Was bedeutet, dass es in der Zwischenzeit SIL-zertifizierte Magnetventile gibt, die im Zertifikat ohne zeitliche Begrenzung auskommen. Im Labor durchgeführte Nachprüfungen solcher Magnetventile haben aufgezeigt, dass Magnetventile in Sitzventiltechnik auch nach über 12 Jahren und im Vergleich zu neuen Ventilen, nahezu unveränderte kurze Schaltzeiten aufweisen und die Dichtheit nach außen, sowie über den Dichtsitz voll gewährleistet ist.



3/2-Wege-Kolbensitzventil mit erweitertem NAMUR-Anschluss und TÜV-Zertifikat gemäß IEC 61508

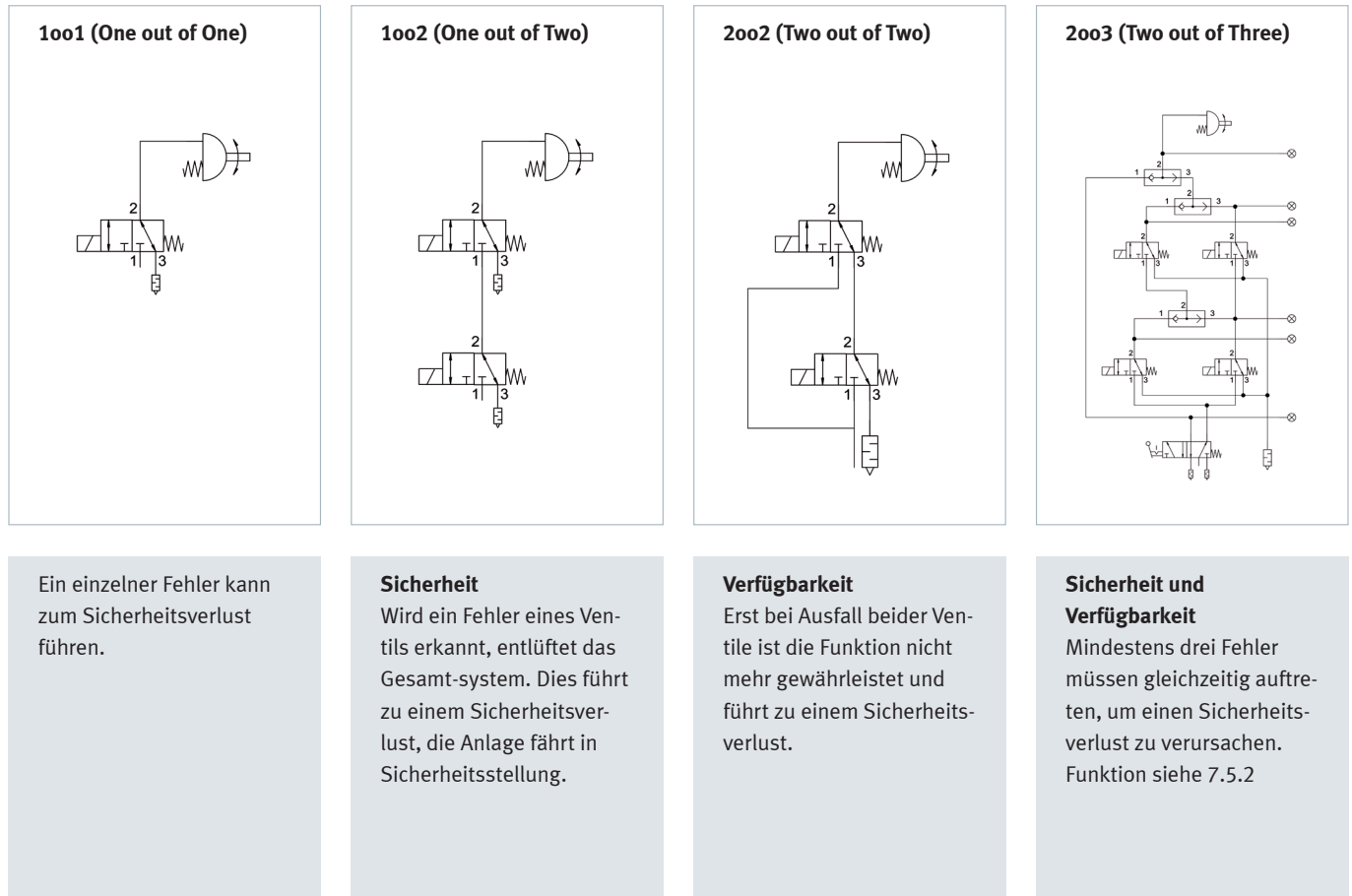
7. Redundante Ansteuerungen von Aktoren im Feld

Falls die unter „6 Betriebsbewährung und Laufzeitverlängerung am Beispiel Magnetventil“ genannten Maßnahmen nicht ausreichen, gibt es wie bereits oben erwähnt noch die Möglichkeit, einer redundanten Verschaltung der Magnetventile (HFT1 bzw. HFT2).

Prozesssicherheit und Zuverlässigkeit stehen bei der Verwendung von Redundanzen immer im Vordergrund. Gängige Sicherheitsverschaltungen in der Verfahrenstechnik sind 1oo2 (One out of Two), 2oo2 (Two out of Two) und 2oo3 (Two out of Three). Diese finden Anwendung in der Förderung und Verarbeitung von hochwertigen und gefährlichen Stoffen wie Erdöl, Erdgas, Chemikalien...

7.1. Die Funktionen im Schaltbild

Um bei Ausfall eines Ventils die Redundanz zur Verfügung zu stellen, sind die Systeme in sicherheits- oder prozesskritischen Anlagen installiert. Durch die kompakte Bauweise reduzieren sie den Aufwand für die Verrohrung und verringern zugleich mögliche Leckagen im System. Dies spart Kosten bei Montage und Betrieb der Anlage.



Übersicht der gängigsten redundanten Ansteuerungen von Aktoren im Feld

7.2. Erhöhte Sicherheit (1oo2)

Bei der erhöhten Sicherheit (1oo2) werden zwei Ventile in Reihe geschaltet. Diese befinden sich während des Betriebs im bestromten Zustand. Sollte ein Ventil oder eines der beiden Ansteuersignale im Betrieb ausfallen, wird das Gesamtsystem entlüftet, um die Anlage vor Folgeschäden zu schützen. Förderleitungen von Medien erfordern häufig diese erhöhte Sicherheit.

7.3. Erhöhte Verfügbarkeit (2oo2)

Bei der erhöhten Verfügbarkeit (2oo2) werden zwei Ventile parallel geschaltet. Diese befinden sich während des Betriebs im bestromten Zustand. Sollte ein Ventil oder eines der beiden Ansteuersignale im

Betrieb ausfallen, bleibt die Anlage weiterhin aktiv und das Gesamtsystem arbeitet weiter. Kühlkreisläufe z.B. benötigen diese erhöhte Verfügbarkeit.

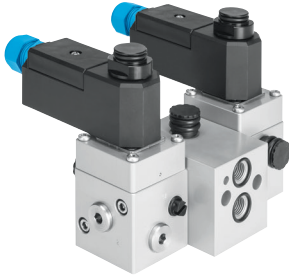
7.4. Erhöhte Sicherheit und Verfügbarkeit (2oo3)

Bei einer 2oo3 Verschaltung ist die erhöhte Sicherheit und die erhöhte Verfügbarkeit kombiniert. Dies hat den Vorteil, dass die einzelnen Ventile im Betrieb auf Funktionsfähigkeit getestet werden können ohne den Antrieb zu schalten. Diese Ventilkombination kommt in sehr kritischen Applikationen in der Öl und Gas Industrie wie auch in Raffinerien vor.

7.5. Verfügbare Lösungen

7.5.1. Erhöhte Sicherheit NAMUR-Block (1oo2) und erhöhte Verfügbarkeit (2oo2)

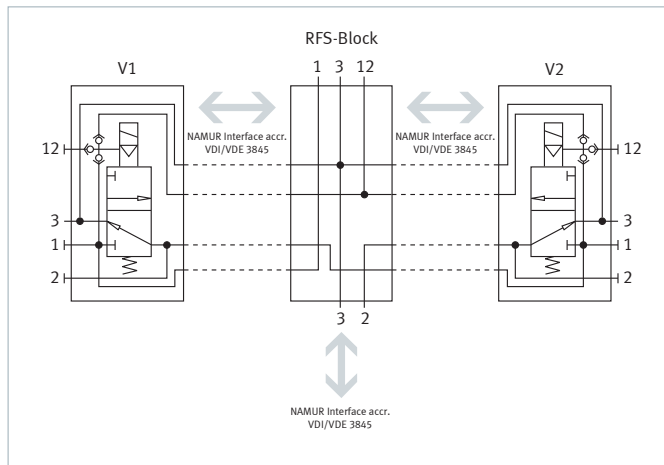
Der NAMUR Block ermöglicht die Installation von zwei Magnetventilen mit NAMUR- Anschlussbild. Durch die NAMUR-Schnittstellen wird eine einfach zu realisierende Redundanz möglich. Die Vorteile: geringe Lagerhaltungskosten und einfacher Austausch der Magnetventile.



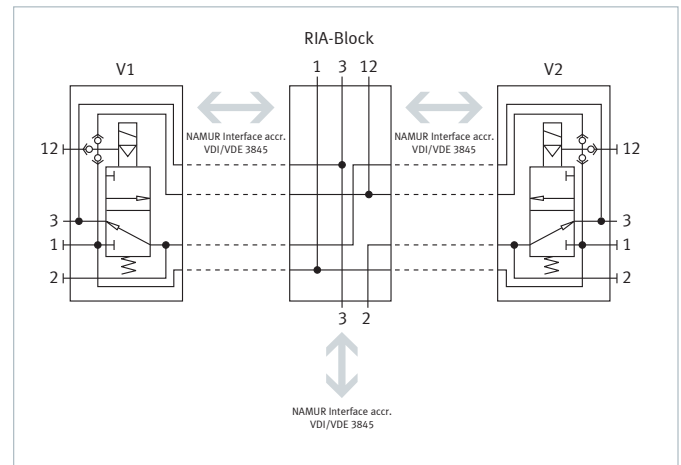
Redundanter NAMUR-Block

Der NAMUR Block kann über die NAMUR-Schnittstelle direkt auf Schwenkantriebe montiert werden. Auch eine separate Installation mit zugehöriger Verrohrung ist möglich.

Mit dem zusätzlichen Hilfsenergieanschluss kann der NAMUR Block auch mit vorgesteuerten Magnetventilen an Antrieben mit Stellungsreglern für Fail-Safe-Funktionen eingesetzt werden.



Redundant Fail Safe – 1oo2



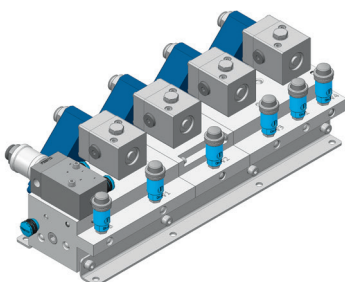
Redundant Increased Availability – 2oo2

7.5.2. Sicherheit und Verfügbarkeit Inline/Namur (2oo3)

Für maximale Sicherheit und Verfügbarkeit zugleich gibt es eine Kombination. Dieses sogenannte 2oo3-System vereint beide Technologien und wird höchsten Ansprüchen an eine Anlage gerecht.

Der Ventilblock ist eine Inline-Variante und wird in der Anlage verrohrt. Die auf dem Block verbauten Standardventile sind über die NAMUR-Schnittstelle nach VDI/VDE 3845 definiert und montiert. Durch diese Kombination wird der Block einmalig montiert und nur

die Ventile über die NAMUR-Schnittstelle bei Bedarf nach einem Service-Life/Safety-Lifecycle-Plan getauscht. Zusätzlich kann man beim 2oo3-System die Funktionen der vier Ventile durch einen Bypass umgehen. Dieser ist mit einem Schlüssel entriegelbar, so dass die Wartung im laufenden Betrieb erledigt werden kann. Die direkt am Block montierten Druckanzeigen signalisieren immer zuverlässig auf einen Blick, ob an einem Ventil Druck ansteht.



Beispiel für einen Funktionsblock - 2oo3

Autor:

Reiner Laun
Industriesegment Management

Festo AG & Co. KG
Rechbergstr. 19
73770 Denkendorf
Tel.: +49 711 347 76585
reiner.laun@festo.com