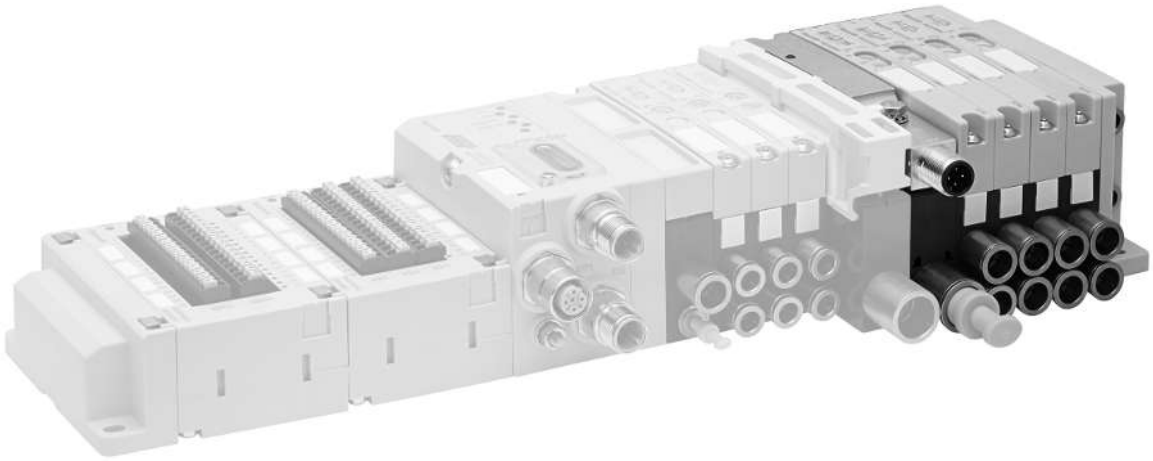
Betriebsanleitung | Operating instructions | Notice d'instruction
Istruzioni per l'uso | Instrucciones de servicio

R412018148-BAL-001-AC
2024-04; Replaces: 2023-03
DE/EN/FR/IT/ES

AVENTICS™ AV

Ventilsystem für Sicherheitsfunktionen
Valve system for safety functions
Îlot de distribution pour fonctions de sécurité
Sistema valvole per funzioni di sicurezza
Sistema de válvulas y funciones de seguridad



EMERSON™

Inhaltsverzeichnis

1 Zu dieser Dokumentation ... 3

1.1 Gültigkeit der Dokumentation ... 3

1.2 Erforderliche und ergänzende Dokumentationen ... 3

1.3 Darstellung von Informationen ... 3

1.3.1 Warnhinweise ... 3

1.3.2 Symbole ... 3

1.4 Bezeichnungen ... 3

1.5 Abkürzungen ... 3

2 Sicherheitshinweise ... 3

2.1 Zu diesem Kapitel ... 3

2.2 Qualifikation des Personals ... 3

2.3 Einsatz in sicherheitsrelevanten Steuerungsketten ... 3

3 Ventilsystem AV in einer sicherheitsgerichteten Steuerungskette ... 4

3.1 Allgemeine Präambel (Haftungsausschluss) ... 4

3.2 Der Prozess zur sicheren Maschine: die Risikobeurteilung ... 4

3.3 Informationen zu den Beispielen ... 4

3.3.1 Systematik der Beispiele ... 4

3.3.2 Technische Schutzmaßnahmen ... 4

3.4 Beispiel 1 mit PLr = e ... 4

3.4.1 Umsetzung von Beispiel 1 ... 5

3.4.2 Sicherheitsfunktionen ... 7

3.4.3 Berechnung des MTTF für den elektrischen und pneumatischen Teil des Ventilsystems ... 8

3.4.4 Diagnose ... 8

3.4.5 Verifikation des Diagnosebits ... 8

3.5 Beispiel 2 mit PLr = c ... 8

3.6 Beispiel 3 mit PLr = d ... 9

3.6.1 Fehlerausschluss ... 9

3.6.2 Kein Fehlerausschluss ... 10

3.7 Übersicht über verschiedene Möglichkeiten der Einspeisung ... 10

3.8 Zuordnung der Versorgungsspannungen im Ventilsystem ... 10

3.9 Verdrahtungskonzepte des Ventilsystems ... 10

3.10 Hinweise zur Verdrahtung ... 11

3.11 Beschreibung der UAoff- / UAon-Überwachung ... 11

4 Umbau und Reparatur ... 12

5 Technische Daten ... 12

6 Zuverlässigkeitskennwerte ... 12

1 Zu dieser Dokumentation

1.1 Gültigkeit der Dokumentation

Diese Dokumentation gilt für Komponenten der Serie AV, die in sicherheitsgerichteten Steuerungsketten eingesetzt werden. Diese Dokumentation richtet sich an Programmierer, Elektroplaner, Pneumatiker, Servicepersonal und Anlagenbetreiber.

Diese Dokumentation enthält wichtige Informationen, um für Ventilsysteme der Serie AV den Fehlerausschluss unter bestimmten Voraussetzungen zu bewerten.

1.2 Erforderliche und ergänzende Dokumentationen

- ▶ Nehmen Sie Ventilsysteme der Serie AV in sicherheitsgerichteten Steuerungsketten erst in Betrieb, wenn Ihnen die Dokumentationen zum Ventilsystem und den einzelnen Komponenten vorliegen und Sie diese beachtet und verstanden haben.

Alle Montageanleitungen und Systembeschreibungen der Serien AES und AV sowie die SPS-Konfigurationsdateien finden Sie auf der CD R412018133.

1.3 Darstellung von Informationen

1.3.1 Warnhinweise

In dieser Dokumentation stehen Warnhinweise vor einer Handlungsabfolge, bei der die Gefahr von Personen- oder Sachschäden besteht. Die beschriebenen Maßnahmen zur Gefahrenabwehr müssen eingehalten werden.

Aufbau von Warnhinweisen

⚠ SIGNALWORT

Art und Quelle der Gefahr

Folgen bei Nichtbeachtung

- ▶ Maßnahmen zur Gefahrenabwehr

Bedeutung der Signalwörter

⚠ GEFAHR

Unmittelbar drohende Gefahr für das Leben und die Gesundheit von Personen.

Das Nichtbeachten dieser Hinweise hat schwere gesundheitliche Auswirkungen zur Folge, bis hin zum Tod.

⚠ WARNUNG

Möglicherweise drohende Gefahr für das Leben und die Gesundheit von Personen.

Das Nichtbeachten dieser Hinweise kann schwere gesundheitliche Auswirkungen zur Folge haben, bis hin zum Tod.

⚠ VORSICHT

Möglicherweise gefährliche Situation.

Das Nichtbeachten dieser Hinweise kann leichte Verletzungen zur Folge haben oder zu Sachbeschädigungen führen.

ACHTUNG

Möglichkeit von Sachbeschädigungen oder Funktionsstörungen.

Das Nichtbeachten dieser Hinweise kann Sachbeschädigungen oder Funktionsstörungen zur Folge haben, jedoch keine Personenschäden.

1.3.2 Symbole

Empfehlung für den optimalen Einsatz unserer Produkte.

Beachten Sie diese Informationen, um einen möglichst reibungslosen Betriebsablauf zu gewährleisten.

1.4 Bezeichnungen

In dieser Dokumentation werden folgende Bezeichnungen verwendet:

Tab. 1: Bezeichnungen

Bezeichnung	Bedeutung
Backplane	interne elektrische Verbindung vom Buskoppler zu den Ventiltreibern und den E/A-Modulen
linke Seite	E/A-Bereich, links vom Buskoppler, wenn man auf dessen elektrische Anschlüsse schaut
rechte Seite	Ventilbereich, rechts vom Buskoppler, wenn man auf dessen elektrische Anschlüsse schaut
Ventiltreiber	elektrischer Teil der Ventilansteuerung, der das Signal aus der Backplane in den Strom für die Magnetspule umsetzt.

1.5 Abkürzungen

In dieser Dokumentation werden folgende Abkürzungen verwendet:

Tab. 2: Abkürzungen

Abkürzung	Bedeutung
AES	**A**dvanced **E**lectronic **S**ystem
AV	**A**dvanced **V**alve
E/A-Modul	**E**ingangs-/**A**usgangsmodul
IS12-PD	ISO-Ventil mit Schieberstellungsabfrage
PL	**P**erformance **L**evel
SPS	**S**peicher**p**rogrammierbare **S**teuerung oder PC, der Steuerungsfunktionen übernimmt
UA	Aktorspannung (Spannungsversorgung der Ventile und Ausgänge)
UAoff	Meldung, dass die Aktorspannung UA unter den Wert der Ausschaltspannung der Ventile gesunken ist. Die Ventile sind elektrisch ausgeschaltet.
UAon	Meldung, dass die Aktorspannung UA unter den Wert der Einschaltspannung der Ventile gesunken ist. Die Ventile können elektrisch nicht eingeschaltet werden.
UL	Logikspannung (Spannungsversorgung der Elektronik und Sensoren)

2 Sicherheitshinweise

2.1 Zu diesem Kapitel

Das Produkt wurde gemäß den allgemein anerkannten Regeln der Technik hergestellt. Trotzdem besteht die Gefahr von Personen- und Sachschäden, wenn Sie dieses Kapitel und die Sicherheitshinweise in dieser Dokumentation nicht beachten.

1. Lesen Sie diese Dokumentation gründlich und vollständig, bevor Sie mit dem Produkt arbeiten.
2. Bewahren Sie die Dokumentation so auf, dass sie jederzeit für alle Benutzer zugänglich ist.
3. Geben Sie das Produkt an Dritte stets zusammen mit den erforderlichen Dokumentationen weiter.
4. Beachten Sie die ISO 4414 zum sicheren Umgang mit Pneumatik.

2.2 Qualifikation des Personals

Die in dieser Dokumentation beschriebenen Tätigkeiten erfordern grundlegende Kenntnisse der Elektrik und Pneumatik sowie Kenntnisse der zugehörigen Fachbegriffe. Um die sichere Verwendung zu gewährleisten, dürfen diese Tätigkeiten daher nur von einer entsprechenden Fachkraft oder einer unterwiesenen Person unter Leitung einer Fachkraft durchgeführt werden.

Eine Fachkraft ist, wer aufgrund seiner fachlichen Ausbildung, seiner Kenntnisse und Erfahrungen sowie seiner Kenntnisse der einschlägigen Bestimmungen die ihm übertragenen Arbeiten beurteilen, mögliche Gefahren erkennen und geeignete Sicherheitsmaßnahmen treffen kann. Eine Fachkraft muss die einschlägigen fachspezifischen Regeln einhalten.

2.3 Einsatz in sicherheitsrelevanten Steuerungsketten

Buskoppler und Ventiltreiber dürfen in sicherheitsgerichteten Steuerungsketten für die Sicherheitsfunktion „**Sicherheitsbezogene Stoppfunktion und weitere Sicherheitsfunktionen, eingeleitet durch eine Schutzeinrichtung**“ verwendet werden, wenn die Gesamtanlage darauf ausgerichtet ist.

3 Ventilsystem AV in einer sicherheitsgerichteten Steuerungskette

3.1 Allgemeine Präambel (Haftungsausschluss)

Die in dieser Anleitung dargestellten Beispiele stellen einen Ausschnitt einer sicherheitsrelevanten Steuerung dar. Diese Beispiele zeigen die Prinzipien und nicht immer alle notwendigen Bauteile. Für Anwendungen in Maschinen können weitere Bauteile und Beurteilungen notwendig sein. Die Angaben entbinden den Verwender nicht von eigenen Beurteilungen und Prüfungen. Es ist zu beachten, dass unsere Produkte einem natürlichen Verschleiß- und Alterungsprozess unterliegen.

3.2 Der Prozess zur sicheren Maschine: die Risikobeurteilung

Die Risikobeurteilung

- muss vom Maschinenhersteller vorgenommen werden, ihre Ergebnisse verbleiben beim Hersteller
- muss die bestimmungsgemäße Verwendung und auch jede vorhersehbare Fehlanwendung der Maschine berücksichtigen
- bildet für den Maschinenhersteller eine wichtige Nachweisquelle, wenn es zu möglichen Haftungsansprüchen aufgrund eines Unfalls kommt

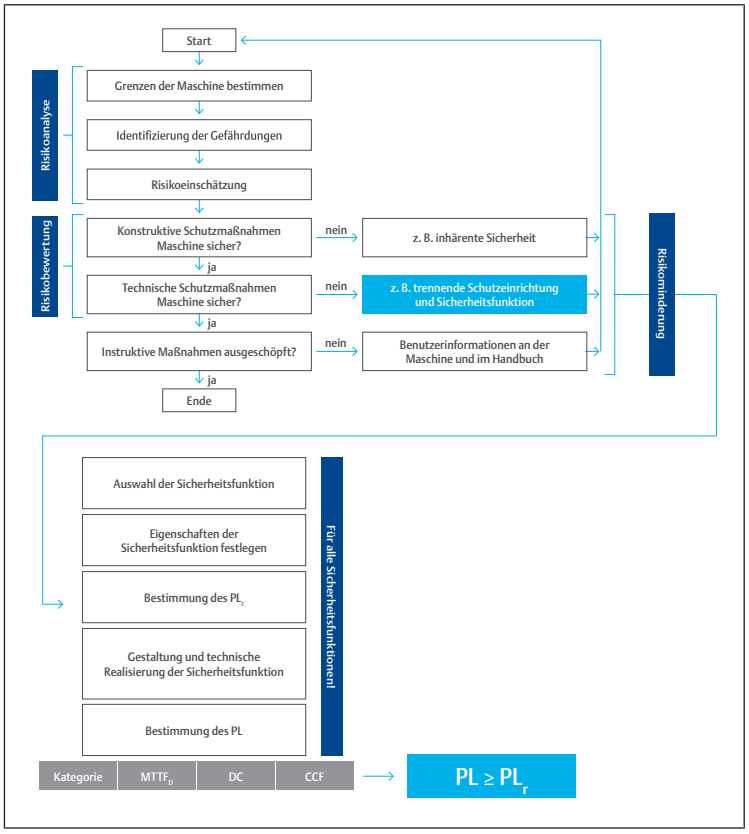


Abb. 1: Prozess zur Risikobeurteilung und Bestimmung des PL_r

In dieser Anleitung konzentrieren wir uns innerhalb des Prozesses der Risikobeurteilung auf die Umsetzung von technischen Schutzmaßnahmen zur Risikominderung, auf die Bewertung der Sicherheitsfunktion und das Bestimmen ihres Performance Levels. Die Abbildung zeigt Ihnen den notwendigen Prozess zur Risikobeurteilung. In Abhängigkeit von der Steuerungsarchitektur (Kategorie), der Mean Time To dangerous Failure ($MTTF_D$), dem Diagnosedeckungsgrad (DC) und den Fehlern gemeinsamer Ursache (CCF) muss der Performance Level (PL) mindestens dem erforderlichen Performance Level (PL_r) entsprechen.

3.3 Informationen zu den Beispielen

Die drei folgenden Beispiele zeigen:

- Beispiel 1: Gefährdung durch unerwarteten Anlauf, PL_r = e
- Beispiel 2: Gefährdung durch unerwarteten Anlauf, verbleibende kinetische Energie, PL_r = c
- Beispiel 3: Gefährdung durch unerwarteten Anlauf, PL_r = d mit Fehlerausschluss

3.3.1 Systematik der Beispiele

Die Systematik der Beispiele orientiert sich am Schlüssel für die Kennzeichnung von Teilen der Sicherheitsfunktionen aus dem Entwurf VDMA 66416:2016-01.

Die allgemeine Beschreibung ist wie folgt:

Vorbemerkung

Beschreibung der Randbedingungen:

- Maschinentyp, Betriebsart, ...
- Gefährdung durch ...
- Risikoparameter nach DIN EN ISO 13849-1:2016-06
- PL_r

Steuerungstechnische Maßnahmen (Sicherheitsfunktionen) und weitere Maßnahmen zur Risikoreduzierung:

- Name der Sicherheitsfunktion
- Name der Sicherheitsfunktion
- ...

Input

Auslösendes Ereignis:

- Abfrage von Zuständen von Sicherheitseinrichtungen und
- Überwachung von Ereignissen
  Beispiele: Zustimmungseinrichtung, Not-Halt, Sicherheitsschalter, Schlüsselschalter,
- Lichtgitter, Sicherheits-Druckschalter, ...

Logik

Evaluierung der Sicherheitsfunktion:

- Abschalten der Energiezufuhren, Sicherheitsrelais, Sicherheits-SPS

Output

Sicherheitsgerichtete Reaktion:

- Beispiele: Fluidventile, Schütze, Regler, Bremsen, ...

3.3.2 Technische Schutzmaßnahmen

Wenn die Sicherheit einer Maschine von einer korrekt funktionierenden Steuerung abhängt, spricht man von „funktionaler Sicherheit“. Die „aktiven“ Teile der Steuerung stehen im Vordergrund, d. h. Komponenten, die die gefährliche Situation erkennen (Signalerfassung, „I“ = Input), daraus geeignete Reaktionen ableiten (Auswertung, „L“ = Logik) und dann zuverlässig Maßnahmen umsetzen (Ausführung, „O“ = Output). Der Begriff „Steuerung“ beinhaltet also das gesamte Signalverarbeitungssystem.

Die „sicherheitsbezogenen Teile einer Steuerung (SRP/CS)“ sind nicht zwangsläufig „Sicherheitsbauteile“ nach Maschinenrichtlinie. SRP/CS (Safety Related Part of a Control System) können aber derartige Sicherheitsbauteile sein, z. B. Zweihandsteuerungen oder Logik-Einheiten mit Sicherheitsfunktion. Antriebe (Zylinder), die Energieversorgung (wie die Druckversorgung oder Wartungseinheiten) und Verbindungen gehen nicht direkt in die Abschätzung der Gefahr bringenden Ausfallwahrscheinlichkeiten ein.

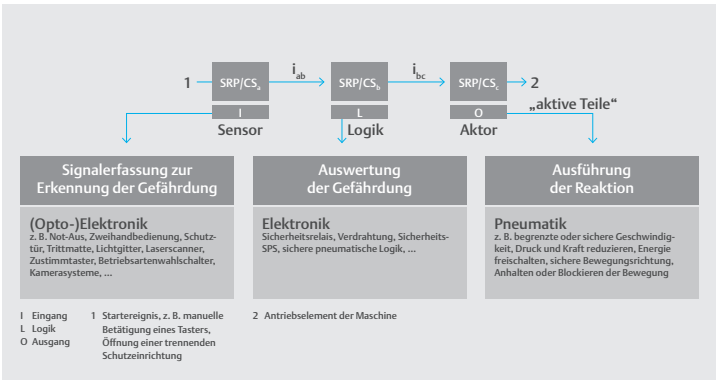


Abb. 2: Fokus auf sicherheitsbezogene Teile einer Steuerung (SRP/CS nach ISO 13849-1)

3.4 Beispiel 1 mit PLr = e

Beispiel 1, in Anlehnung an VDMA 66416:2016-01, Nummer 2.1.1.1 und 2.2.1.1

Vorbemerkung

Beschreibung der Randbedingungen:

- Betriebsart: Automatik (BA1)
- Maschinentaktzeit: 5 bis 15 Sekunden
- Gefährdung durch unerwarteten Anlauf
- PL_r = e

Steuerungstechnische Maßnahmen (Sicherheitsfunktionen):

- Sicheres Abschalten des Moments (STO) oder
- Sicheres Abschalten der Energiezufuhr (SEC)
- Vermeidung des unerwarteten Anlaufs (PUS)

Input

Auslösendes Ereignis:

- Lichtgitter unterbrochen oder verriegelte Schutztüren geöffnet oder nicht zugehalten

Logik

Evaluierung der Sicherheitsfunktion:

- Abschalten der Energiezufuhren

Output

Sicherheitsgerichtete Reaktion:

- Trennen von Fluid-Energiezufuhr: $PL_r \geq d$ => 2-kanalig
  und von elektrischer Energiezufuhr: $PL_r \geq d$ => 2-kanalig empfohlen

3.4.1 Umsetzung von Beispiel 1

Nach ISO 13849 kann PL = e mit Kategorie 3 erreicht werden, wenn folgende Sachverhalte zutreffen:

- DC_{avg} = mittel
- MTTF = hoch

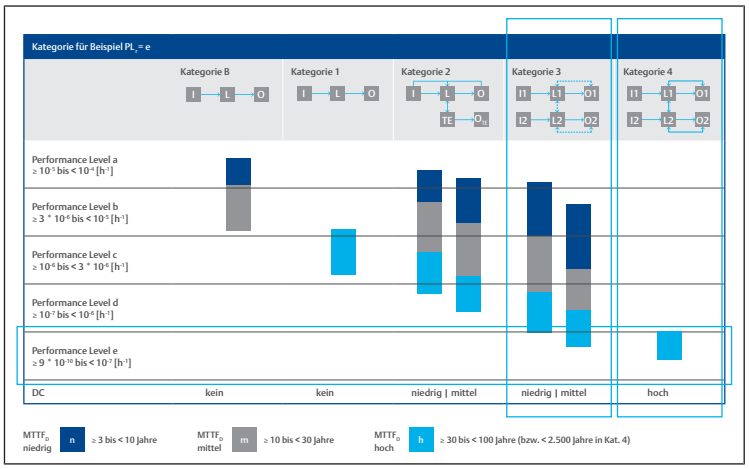


Abb. 3: Umsetzung von Beispiel 1: PL_e mit Kategorie 3, DC = mittel, $MTTF_D$ = hoch

Dabei sind nach dem vereinfachten Ansatz der ISO 13849-1 die vier Klassen für den Diagnosedeckungsgrad DC wie folgt definiert:

- kein: DC < 60%
- niedrig: 60% < DC < 90%
- mittel: 90% < DC < 99%
- hoch: 99% < DC

Gestaltung und technische Realisierung der Sicherheitsfunktion

Handarbeitsplatz
TM=20Jahre
d/a=320Tage
h/d=24h / min. 10sek Zykluszeit = 55.296.000 Schaltzyklen für Arbeits- und Hauptluftventil

Im Einrichtbetrieb müssen bewegliche, trennende Schutzeinrichtungen überbrückt und geöffnet sowie feste trennende Schutzeinrichtungen montiert sein.

INFO: Ein einzelner Fehler führt nicht zum Verlust der Sicherheitsfunktion. Einige aber nicht alle Fehler werden erkannt. Eine Anhäufung von unbekannten Fehlern kann aber zum Verlust der Sicherheitsfunktion führen.

Ventilauswahl

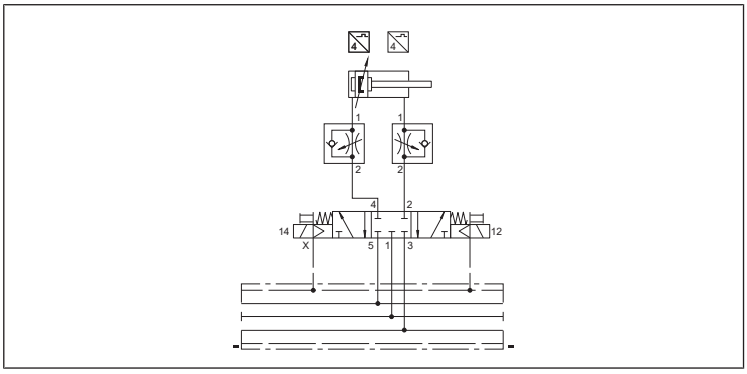


Abb. 4: Schaltbild: Ventilauswahl

- Definierte, sichere Schaltstellung im stromlosen Zustand durch mechanische Feder
- Druckleitungen sind im stromlosen Zustand gesperrt
- Abluftleitungen sind nicht offen
- Zylinder nach NOT-HALT ist nicht verschiebbar, d.h. Personenbefreiung ist erforderlich
- Abbremsen auslaufender Massen möglich
- Sicheres Stillsetzen bei Vertikalbewegungen mit Massen (ab PL_d nur mit Zusatzmaßnahmen -> 2-kanalig)
- JOG-Betrieb ist möglich (Zylinderhub tippend)
- Querbeeinflussung durch Abluft großer Nachbarzylinder nicht möglich
- Geeignet bis Performance Level PL_e (Zusatzmaßnahmen siehe → Abb. 5.)
- Zulässige gefahrbringende Bewegungsrichtung des Zylinders aus- und einfahren
- Lebensdauer der Ventile ist nach ISO 19973-1 und -2 getestet worden

Pneumatische Sicherheitsschaltung Kategorie 3 PL_e

Bezeichnung:
Vermeidung von unerwartetem Anlauf (Prevention of unexpected start-up, PUS) nach VDMA Einheitsblatt 24584.

Blockieren der Volumenströme in und aus beiden Kolbenräumen.

INFO: Bei Wiederanlauf beachten:
Zylinderkammern können sich aufgrund von Leckagen einzelner Bauteile entlüften.

INFO: Prüfimpulse können zum Schalten der Ventile führen.

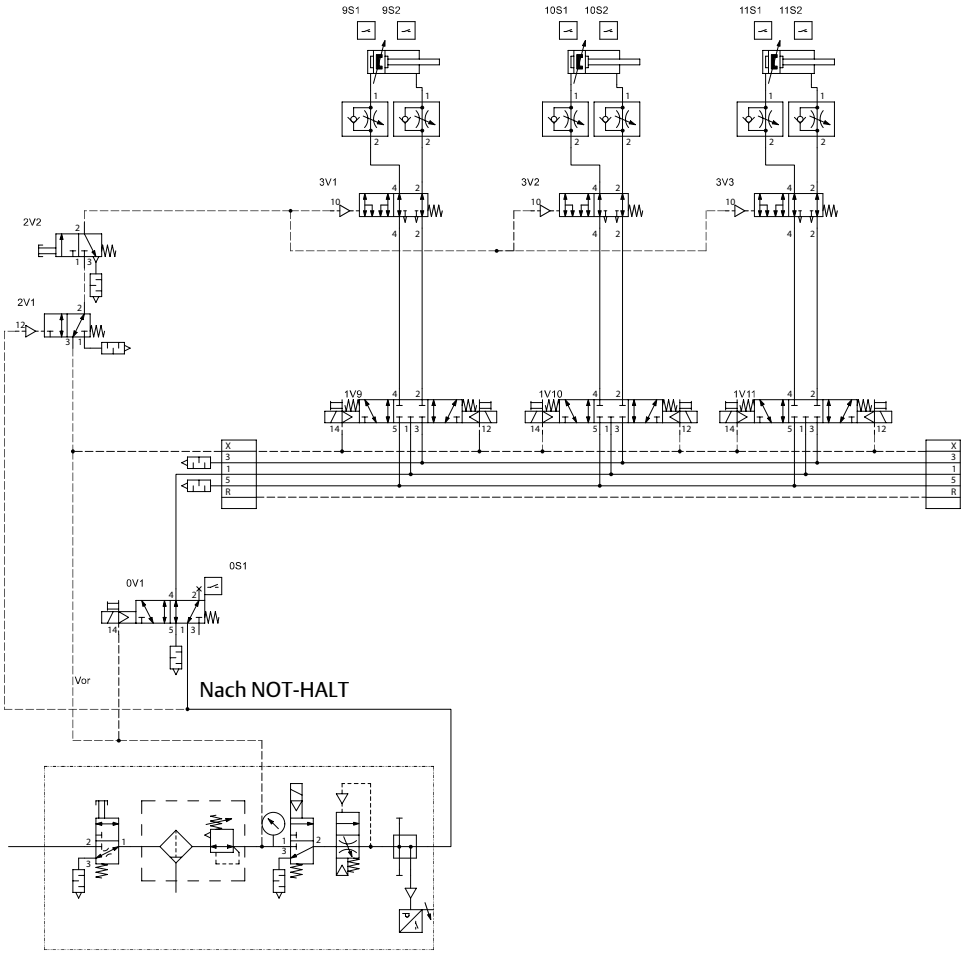


Abb. 5: Prinzipschaltbild: Funktions- und Testkanäle

INFO: Wenn Sie mehr als 8 Ventile gleichzeitig belüften/entlüften, achten Sie auf zusätzliche Belüftung/Entlüftung über Einspeiseplatten.

Personenbefreiung durch Entlüften (für Schaltungen mit Lageerhaltung)

Für vertikale und horizontale Bewegungen:

- Schwere der Verletzung = S2 (überweise irreversible Verletzung, einschließlich Tod)
- Gefahrenstelle liegt im zugänglichen Bereich
- der Bediener kann sich nicht selbst befreien
- durch das Entlüften darf keine zusätzliche Gefährdung entstehen

Die Personenbefreiung kann nur durch folgende Sachverhalte realisiert werden:

- Nur im drucklosen Zustand
- Nach aktivem Not-Halt durch 2V1 (ein 2V1 kann mehrere 2V2 versorgen), dieser muss in Nähe der Gefahrenstelle montiert sein
- Für Zylinder-Gruppen eine gemeinsame Personenbefreiung vorsehen (ein 2V2 kann mehrere Zylinder entlüften)

Blockschaltbild

In folgender Abbildung ist das sicherheitstechnische Blockdiagramm für Beispiel 1 dargestellt.

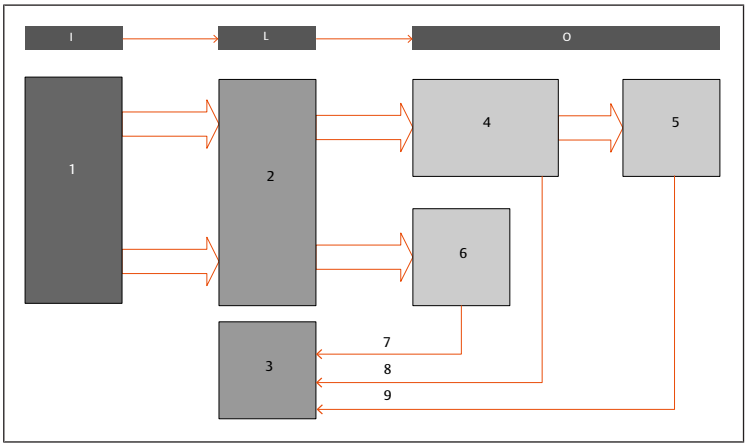


Abb. 6: Sicherheitstechnisches Blockdiagramm, Beispiel 1

1 Schutztürschalter (z. B. PILZ PSEN cs3.1 oder PSEN sl-0.5p 1.1)

2 Sicherheitsbaustein (z. B. PILZ PNOZ)

3 SPS (speicherprogrammierbare Steuerung)

4 elektrischer Teil des AV-Ventilsystems UA-Einspeisung über elektrische Einspeiseplatte

5 pneumatischer Teil des AV-Ventilsystems

6 Hauptluftventil mit Schieberstellungsabfrage (z. B. IS12-PD)

7 Diagnose „Abfrage der Schieberstellung des Hauptluftventils"

8 Diagnosemeldung „Ventilspannung UA ist kleiner als Abschaltspannung (UA < UAoff)"

9 Diagnose "indirekte Abfrage des Arbeitsventils"

Pneumatisches Schaltbild

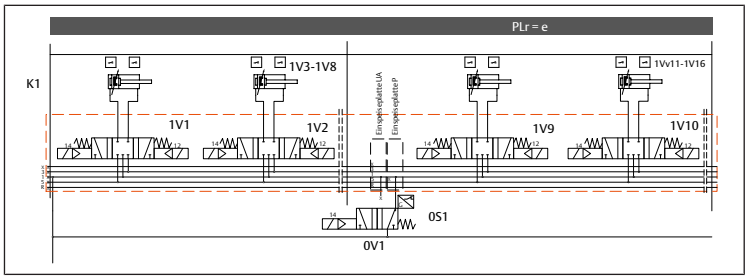


Abb. 7: Pneumatisches Schaltbild, Beispiel 1

K1	Ventilträgersystem	1V1 – 1V8	Ventile außerhalb der sicherheitsgerichteten Steuerungskette
1V3 – 1V8	Nicht gezeichnet	1V9 – 1V16	Ventile für Antriebe mit PL_r = e
1V1 – 1V16	Nicht gezeichnet	0S1	Positionserkennung von 0V1
0V1	Hauptluftventil		

Komplettes Ventilsystem mit externen Komponenten

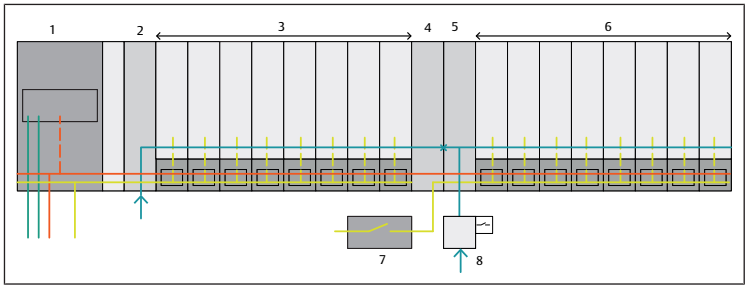


Abb. 8: Ventilsystem und externe Komponenten

1	Buskoppler	2	Pneumatische Einspeiseplatte
3	Ventile (nicht im Sicherheitskreis)	4	Elektrische Einspeiseplatte - entspricht Block 4 im sicherheitstechnischen Blockdiagramm
5	Pneumatische Einspeiseplatte, - keine Überwachung (UAoff) notwendig, keine aktive Elektronik eingebaut	6	Ventile (Sicherheitskreis) - entspricht Block 5 im sicherheitstechnischen Blockdiagramm - der elektrische Teil der Ventile (Ventiltreiber) entspricht Block 4 im sicherheitstechnischen Blockdiagramm
7	Sicherheitsbaustein, entspricht Block 2 im sicherheitstechnischen Blockdiagramm	8	Hauptluftventil entspricht Block 6 und 7 im sicherheitstechnischen Blockdiagramm

3.4.2 Sicherheitsfunktionen

Sicherheitsbezogene Vermeidung des unerwarteten Anlaufs aus der Ruhelage, mit Option der Personenbefreiung.

In dieser Dokumentation, ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

- Schwere der Verletzung = S2
- Gefahrenstelle liegt im zugänglichen Bereich und der Bediener kann sich nicht selbst befreien
- durch das Entlüften darf keine zusätzliche Gefährdung entstehen
- da die Personenbefreiung 2V1, 2V2, 3V1 und 3Vn nach Not-Halt also nach dem Entlüften des 3/2 Wegeventils in der Wartungseinheit voll funktionsfähig ist und keinen Einfluss auf die Sicherheitsfunktion hat, werden diese nicht bei der Berechnung berücksichtigt.

Dies kann nur durch folgenden Sachverhalt realisiert werden:

- Nur im drucklosen Zustand
- Nach aktivem Not-Halt durch 2V1 (ein 2V1 kann mehrere 2V2 versorgen), dieser muss in Nähe der Gefahrenstelle montiert sein
- Für Zylinder-Gruppen eine gemeinsame Personenbefreiung vorsehen (ein 2V2 kann mehrere Zylinder entlüften)

Funktionsbeschreibung der Schaltung PL c, d, e_Kat-3_02 bei Verwendung in einem Handarbeitsplatz

- Bewegungen werden redundant durch Hauptluftventil 0V1 und Arbeitsventil 1Vn gesteuert
- Ventil 0V1 muss ständig angesteuert werden, damit 1Vn angesteuert werden kann
- der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion
- alle Ventile werden zyklisch im Prozess angesteuert
- die Funktion des Hauptluftventils 0V1 wird durch eine Ventilstellungsabfrage 0S1 überwacht
- die Funktion des Arbeitsventils 1Vn wird während des Prozesses indirekt durch die Schalter nS1 und nS2 erkannt
- die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen
- bei Gefährdung durch gespeicherte Energie (Druck, Masse, Feder) sind zusätzliche Maßnahmen erforderlich

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderung der Kategorie B sind eingehalten
- Hauptluftventil 0V1 wird durch eine Feder in die sichere Schaltstellung gebracht
- Arbeitsventil nV1 hat eine gesperrte Mittelstellung (Überschneidungsfrei) mit Federzentrierung
- die sichere Schaltstellung wird bei beiden Ventilen nach Wegnahme der Steuerspannung erreicht
- die Signalverarbeitung der Ventilabfragen und Überwachungen erfolgt in einer einkanaligen SPS Ansteuerung
- Steuerung EIN und Beladetür geschlossen:
  - Hauptluftventil 0V1 ist geschaltet und an dem Ventilsystem liegt Spannung an
- Automatikbetrieb EIN und Beladetür offen:
  - an Hauptluftventil 0V1 und an dem Ventilsystem liegt keine Spannung an
- Einrichtbetrieb und Schutztür mit Schlüsselschalter überbrückt:
  - an Hauptluftventil 0V1 und an dem Ventilsystem liegt keine Spannung an
  - die Pneumatikleitung zwischen Hauptluftventil 0V1 und Arbeitsventil nV1 ist entlüftet
  - Bewegungen sind nur mit zusätzlichem Zustimmschalter möglich
  - der Zustimmschalter schaltet das Hauptluftventil 0V1 und an dem Ventilsystem liegt Spannung an
  - Gefährliche Bewegungen ohne Zusatzmaßnahmen mit Begründung sind nur bei geschlossener Schutztür zulässig

Berechnung der Ausfallwahrscheinlichkeit und Lebensdauer

Geforderte Lebensdauer:
20 Jahre / 320 Tage / 24 h / 10 sek. Taktzeit (nop = 2764800 Zyklen/Jahr)

- Ventil 0V1 B_{10D} = 79,2 Mio (IS12-PD)
- Ventil nV1 B_{10D} = 39,6 Mio (AV05) bzw. Ventil nV1 B_{10D} = 105,8 Mio (AV03)

3.4.3 Berechnung des MTTF für den elektrischen und pneumatischen Teil des Ventilsystems

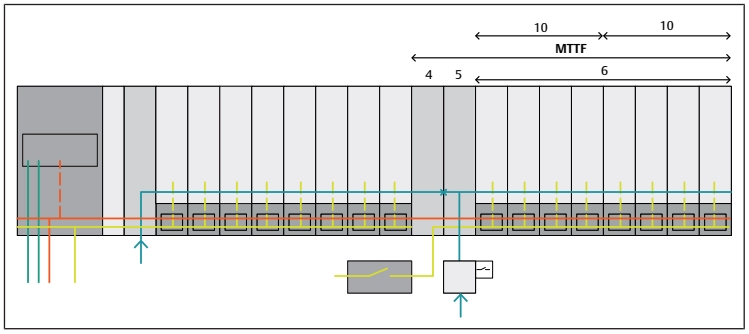


Abb. 9: Relevante Komponenten zur Berechnung des $MTTF_D$ für den elektrischen Teil

4 Elektrische Einspeiseplatte mit UAon-Überwachung, entspricht Block 4 im Sicherheitstechnisches Blockdiagramm

5 Pneumatische Einspeiseplatte mit UAoff-Überwachung, die elektrische Funktion = UAoff-Überwachung entspricht Block 4 und 8 im sicherheitstechnischen Blockdiagramm

6 Ventile (Sicherheitskreis) entspricht Block 5 im sicherheitstechnischen Blockdiagramm der elektrische Teil der Ventile (Ventiltreiber) entspricht Block 4 im sicherheitstechnischen Blockdiagramm

10 4-fach-Ventiltreiberplatine

Siehe → 6. Zuverlässigkeitskennwerte und siehe → Abb. 9

Daraus folgt:

- Elektrische Einspeiseplatte (**4**) MTTF = 854 Jahre
- UAoff-Überwachung (**5**) MTTF = 1094 Jahre
- 4-fach-Ventiltreiberplatine (**10**) MTTF = 630 Jahre
- Ventile AV03 5/3 Federrückgestellt (**6**) MTTF = 382,7 Jahre

$$MTTF_{ges} = \frac{1}{\frac{1}{854\,[a]} + \frac{1}{1094\,[a]} + \frac{1}{630\,[a]} + \frac{1}{630\,[a]} + \frac{1}{382{,}7\,[a]}} = 127\,[a]$$

Die MTTF-Werte der AES-Module wurden mit Hilfe der Ausfallraten aus einer Datenbank berechnet.

Nach DIN EN 13849-1, Anhang C ist nicht jeder Ausfall ein gefährlicher Ausfall. In diesem Fall kann für die Berechnung des gesamten Systems $MTTF_D = 2 \times MTTF_{ges}$ gesetzt werden.

$MTTF_D = 2x\ MTTF_{ges} = 2 \times 127\,[a] = 254\,[a]$

3.4.4 Diagnose

Die pneumatische Einspeiseplatte überwacht die Aktorspannung UA und sendet das Diagnosebit UAoff, wenn UA die Abschaltspannung unterschreitet.

Die elektrische Einspeiseplatte überwacht die Aktorspannung UA und sendet das Diagnosebit UAon, wenn UA die Einschaltspannung unterschreitet.

Das Diagnosebit (UAoff) muss überwacht werden. Dazu ist ein Wechsel des Signals notwendig. Dies kann z. B. beim Einschalten der Maschine oder mit speziellen Testzyklen durchgeführt werden.

Direkte Funktionsabfrage der Schieberstellung am Hauptventil 99 %.

Indirekte Funktionsabfrage des Arbeitsventils 90 %.

DC = 94,4% $MTTF_D$ = hoch (100J) CCF = 95

CCF in unserem Beispiel				
Maßnahme gegen CCF	Fluidtechnik	Elektronik	Punkte	
Trennung zwischen den Signalpfaden	Trennung der Verrohrung	Luft- und Kriechstrecken auf gedruckten Schaltungen	15	☑
Diversität	z. B. unterschiedliche Ventile	z. B. unterschiedliche Prozessoren	20	☑
Schutz gegen Überspannung, Überdruck ...	Aufbau nach EN ISO 4413 bzw. EN ISO 4414 (Druckbegrenzungsventil)	Schutz gegen Überspannung (z. B. Schütze, Netzteil)	15	☑
Verwendung bewährter Bauteile	Anwender		5	☑
FMEA in der Entwicklung	FMEA bei der Konzeption des Systems		5	☑
Kompetenz/Ausbildung	Qualifizierungsmaßnahme		5	☑
Schutz vor Verunreinigung und EMV	Fluidqualität	EMV-Prüfung	25	☑
Andere Einflüsse (u.a. Temperatur, Schock)	Einhalten EN ISO 4413 und EN ISO 4414 und Produktspezifikation	Einhalten der Umweltbedingungen gemäß Produktspezifikation	10	☑
CCF-Gesamt	Summe der Punktezahl (65 ≤ CCF ≤ 100):			95

Abb. 10: Beispiel: CCF - Fehler gemeinsamer Ursache

Performance Level = PL_e / Kategorie = 3

Austausch des Hauptluftventils 0V1 (IS12-PD) nicht erforderlich.

Austausch des Ventils nV1 (AV03) nicht erforderlich.

Austausch des Ventils nV1 (AV05) nach 14,3J - bei Taktzeit ≥ 14 sek. nicht erforderlich bzw. Gebrauchsdauer 20 Jahre.

3.4.5 Verifikation des Diagnosebits

Eine detaillierte Beschreibung der Überwachung finden Sie im Kapitel → 3.11 Beschreibung der UAoff- / UAon-Überwachung.

Wenn die Spannung UA abgeschaltet wird, muss sowohl die Diagnosemeldung UAon und UAoff gesendet werden.

Tab. 3: Verifikation des Diagnosebits

UA = 0, abgeschaltet	UAon-Einschaltdiagnose	UAoff-Ausschaltdiagnose
gültig	1	1
nicht gültig	1	0
nicht gültig	0	1

Wenn die vorgenannten Bedingungen berücksichtigt werden, kann mit den Angaben der folgenden Normen die Überwachung der abgeschalteten Ventilspannung mit einem DC = 90% bis <99% (mittel) abgeschätzt werden:

- DIN EN ISO 13849-1 Anhang E: „Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module“
- DIN EN 61508-2: „Tabelle A.14 – Stellglieder (Aktoren)“
- DIN EN 61508-2: „Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation)“

3.5 Beispiel 2 mit PLr = c

Beispiel 2, in Anlehnung an 66416:2016-01, Nummer 1.1.2.1 und 2.1.2.3

Vorbemerkung

Beschreibung der Randbedingungen:

- Betriebsart BA2 Einricht- oder Servicebetrieb
- Gefährdung durch unerwarteten Anlauf, verbleibende kinetische Energie
- PL_r = c

Steuerungstechnische Maßnahmen (Sicherheitsfunktionen) (siehe Anmerkung):

- Sicheres Abschalten des Moments (STO)
- Sicheres Abschalten der Energiezufuhr (SEC)
- Vermeidung des unerwarteten Anlaufs (PUS)

Input

Auslösendes Ereignis:

- Betriebsartenschalter, Zustimmungseinrichtung

Logik

Evaluierung der Sicherheitsfunktion:

- Abschalten der Energiezufuhren

Output

Sicherheitsgerichtete Reaktion:

- 1-kanaliges Einsperren von Fluid-Medium. Folgende Umsetzungen sind möglich:
  - Wegeventil in Sperrstellung
  - Ansteuerung von Sperrventile(n)
  - S1 möglich, weil Restenergie nur reversible Verletzungen erzeugt

- Trennen der elektrischen Energiezufuhr: $PL_r \geq d$ => 2-kanalig empfohlen

Anmerkung

Das Thema Restenergie wird in folgenden Dokumenten näher beschrieben:

- Entwurf VDMA 66416: Kapitel 5.1.3 Einrichtbetrieb / Servicebetrieb (BA2) „Reduzierte Geschwindigkeiten sind wie folgt vorzusehen ...“
- Entwurf VDMA 66416: Tabelle A2 - Schlüssel für die Kennzeichnung der Parametereinschätzungen des Risikographen in Tabelle A7

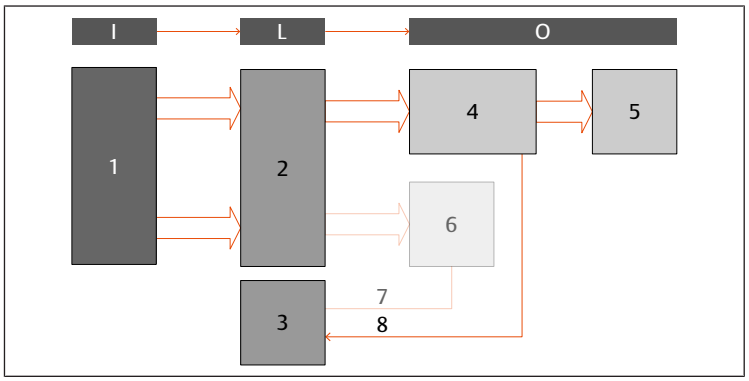


Abb. 11: Sicherheitstechnisches Blockdiagramm, Beispiel 2

1 Zustimmungseinrichtung
2 Sicherheitsbaustein (z. B. PILZ PNOZ)
3 SPS (speicherprogrammierbare Steuerung)
4 elektrischer Teil des AV-Ventilsystems, UA-Einspeisung über elektrische Einspeiseplatte
5 Wegeventile des AV-Ventilsystems
6 Hauptluftventil mit Schieberstellungsabfrage (z. B. IS12-PD, ...) nicht aktiv für diese Sicherheitsfunktion
7 Diagnose „Abfrage der Schieberstellung des Hauptluftventils“ nicht aktiv für diese Sicherheitsfunktion
8 Diagnose „Ventilspannung UA ist kleiner als Abschaltspannung (UA < UAoff)“

3.6 Beispiel 3 mit PLr = d

Beispiel 3, in Anlehnung an VDMA 66416, Nummer 2.1.1.1 und 2.2.1.1

Dieses Beispiel ist ähnlich Beispiel 1, der geforderte PL_r ist jedoch d.

Vorbemerkung

Beschreibung der Randbedingungen:

- Betriebsart Automatik (BA1)
- Gefährdung durch unerwarteten Anlauf
- $PL_r = d$

Steuerungstechnische Maßnahmen (Sicherheitsfunktionen):

- Sicheres Abschalten des Moments (STO)
- Sicheres Abschalten der Energiezufuhr (SEC)
- Vermeidung des unerwarteten Anlaufs (PUS)

Input

Auslösendes Ereignis:

- Lichtgitter unterbrochen oder verriegelte Schutztüren geöffnet oder nicht zugehalten

Logik

Evaluierung der Sicherheitsfunktion:

- Abschalten der Energiezufuhren

Output

Sicherheitsgerichtete Reaktion:

- Trennen von Fluid-Energiezufuhr: $PL_r \geq d$ => 2-kanalig und von elektrischer Energiezufuhr: $PL_r \geq d$ => 2-kanalig empfohlen

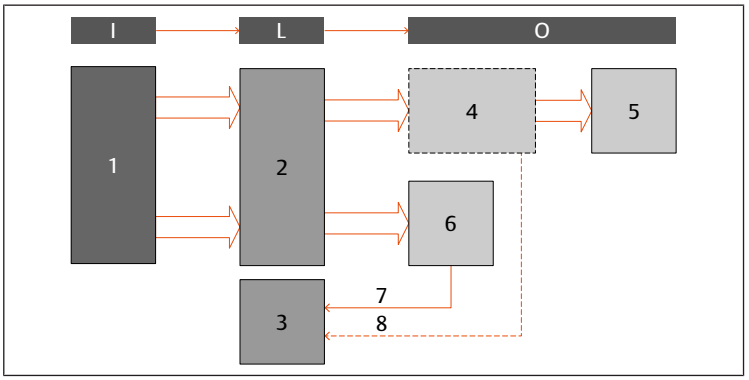


Abb. 12: Sicherheitstechnisches Blockdiagramm, Beispiel 3

1 Schutztürschalter (z.B. PILZ PSEN cs3.1 oder PSEN sl-0.5p 1.1)
2 Sicherheitsbaustein (z.B. PILZ PNOZ)
3 SPS (speicherprogrammierbare Steuerung)
4 Elektrischer Teil des AV-Ventilsystems

Entweder UA-Einspeisung über elektrische Einspeiseplatte. Für diesen Block ist ein Fehlerausschluss möglich (siehe → 3.6.1 Fehlerausschluss).

Oder UA-Einspeisung über Buskoppler. Kein Fehlerausschluss möglich (siehe → 3.6.2 Kein Fehlerausschluss).

5 Wegeventile des AV-Ventilsystems
6 Hauptluftventil mit Schieberstellungsabfrage (z. B. IS12-PD, ...)
7 Diagnose „Abfrage der Schieberstell des Hauptluftventils“
8 Diagnose „Ventilspannung UA ist kleiner als Abschaltspannung (UA < UAoff)“

Wenn für (**4**) ein Fehlerausschluss angewendet wird, ist diese Diagnose nicht notwendig.

3.6.1 Fehlerausschluss

Wenn das Ventilsystem wie in den folgenden Kapiteln beschrieben aufgebaut und angewendet wird, muss die Ventilelektronik nicht in die Berechnung der MTTF-Werte einer sicherheitsgerichteten Steuerungskette einbezogen werden.

Voraussetzung für die Anwendung des Fehlerausschlusses ist,

- dass maximal PL d anwendbar ist (PL e muss, wie im Beispiel 1 berechnet werden),
- dass das Ventilsystems mit einer oder mehreren elektrischen Einspeiseplatten aufgebaut wird,
- dass die Ventile, die abgeschaltet werden sollen, über diese elektrische Einspeiseplatten versorgt werden,
- dass die elektrischen Einspeiseplatten gemäß den Verdrahtungskonzepten 1–3 verdrahtet werden,
- dass das Kabel für den Anschluss der Einspeiseplatte nur die 24-V-Versorgungsspannung UA beinhaltet,
- dass das Kabel nach DIN EN 60204 verlegt wird.

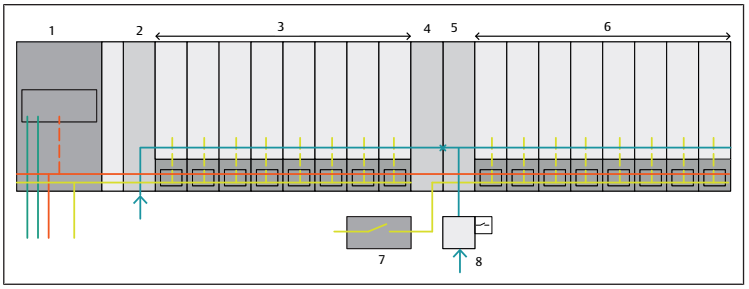


Abb. 13: Ventilsystem und externe Komponenten

1 Buskoppler
2 Pneumatische Einspeiseplatte
3 Ventile (nicht im Sicherheitskreis)
4 Elektrische Einspeiseplatte - entspricht Block 4 im sicherheitstechnischen Blockdiagramm
5 Pneumatische Einspeiseplatte, - keine Überwachung (UAoff) notwendig, keine aktive Elektronik eingebaut
6 Ventile (Sicherheitskreis) - entspricht Block 5 im sicherheitstechnischen Blockdiagramm - der elektrische Teil der Ventile (Ventiltreiber) entspricht Block 4 im sicherheitstechnischen Blockdiagramm
7 Sicherheitsbaustein, entspricht Block 2 im sicherheitstechnischen Blockdiagramm
8 Hauptluftventil entspricht Block 6 und 7 im sicherheitstechnischen Blockdiagramm

3.6.2 Kein Fehlerausschluss

Wird die UA-Einspeisung über den Buskoppler vorgenommen, ist kein Fehlerausschluss möglich. Die Ausfallwahrscheinlichkeit muss berechnet werden.

Weitere Maßnahmen sind:

- Die UA-Einspeisung über den Buskoppler muss sicher abgeschaltet werden, um ein unerwartetes Schalten der Ventile zu vermeiden.
- Die Kabel müssen nach DIN EN 60204 verlegt werden.
- Die Diagnose des Buskoppler (UAon und UAoff) muss ausgewertet werden.

Je nach gefordertem Performancelevel müssen weitere Maßnahmen getroffen werden.

3.7 Übersicht über verschiedene Möglichkeiten der Einspeisung

Tab. 4: Verschiedene Möglichkeiten der Einspeisung

	UA-Einspeisung über Buskoppler	UA-Einspeisung über elektrische Einspeiseplatte
Maximal erreichbarer PL_r	d (e nicht empfohlen)	e
Ist Fehlerausschluss möglich	nein siehe → 3.6.2 Kein Fehlerausschluss	$PL_r \leq$ d: ja PL_r = e: nein
Auswertung der Diagnose	ja (UAon und UAoff des Buskopplers)	$PL_r \leq$ d: nein (nicht notwendig wegen Fehlerausschluss) PL_r = e: ja (UAon und UAoff) Pneumatische Einspeiseplatte muss mit UAoff-Überwachung ausgerüstet sein.
DC	90 % ... <99 %	90 % ... <99 %
Einschaltstrombegrenzung	ja	ja
Testung möglich (Querschluss)	nein	ja

Einschaltstrombegrenzung

Der sehr hohe Einschaltstrom der Einheit, wie er bei kapazitiven Lasten normalerweise vorhanden ist, wird auf einen Wert von maximal 5 A begrenzt.

Definition Testimpuls

Ein Testimpuls ist eine zeitlich begrenzte Änderung eines Signalspannungspegels zur Überprüfung der Funktionstüchtigkeit des Ausgangs oder Gerätes oder zur Überprüfung der Übertragungsstrecke.
[Quelle: ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V., Positionspapier „Klassifizierung binärer 24 -V-Schnittstellen mit Testung im Bereich der Funktionalen Sicherheit“]

Testung möglich

Sichere Ausgänge und/oder Sicherheitsbausteine erzeugen Taktsignale oder Testimpulse auf ihren Ausgängen. Wenn ein solcher Ausgang mit der elektrischen Einspeiseplatte verbunden wird, gibt es keine Fehlinterpretation der Querschlussprüfung. Wenn ein solcher Ausgang für die UA-Einspeisung am Buskoppler verwendet wird, führt dies zu einer Fehlinterpretation der Querschlussprüfung.

Anmerkung

Es kann nur die Übertragungsstrecke bis zur elektrischen Einspeiseplatte geprüft werden.

3.8 Zuordnung der Versorgungsspannungen im Ventilsystem

Folgende Abbildung zeigt die Zuordnung der Versorgungsspannungen zu den Funktionen innerhalb des Ventilsystems.

- Die am Buskoppler (**1**) eingespeiste Versorgungsspannung **UL** versorgt die komplette Elektronik des Ventilsystems.
- Die am Buskoppler eingespeiste Versorgungsspannung **UA** versorgt die Ausgänge des DO-Moduls (**6**) (digitaler Ausgang, digital output) und alle Ventile zwischen Buskoppler und UA-Einspeisung.

Der Baustein „Elektrische Einspeiseplatte“ (**5**) unterbricht die ankommende Versorgungsspannung **UA**. Für alle rechts von der elektrischen Einspeiseplatte liegende Ventile wird die Versorgungsspannung dieses Bausteins verwendet. Der Baustein „Elektrische Einspeiseplatte“ kann im Ventilbereich mehrfach verwendet werden.

Die Spannung **UL** ist in der Ventileinheit grundsätzlich von der Spannung **UA** galvanisch getrennt.

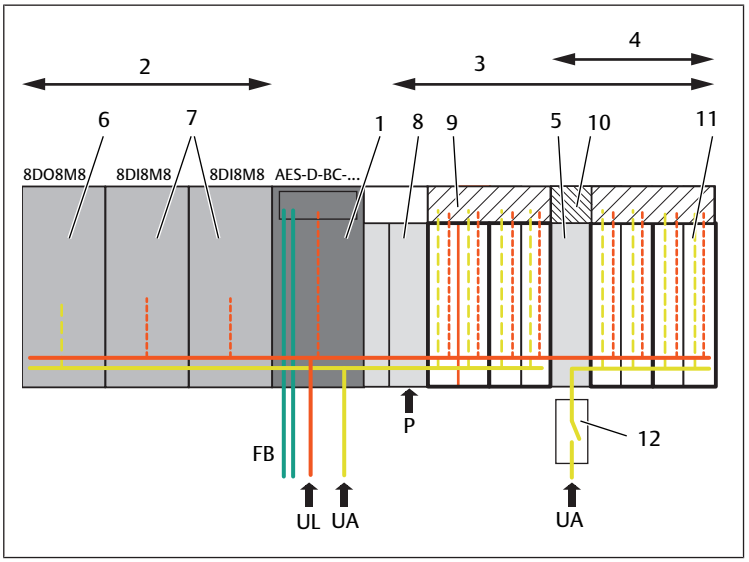


Abb. 14: Zuordnung der Versorgungsspannungen UL und UA

1	Buskoppler	2	E/A-Module
3	Ventilbereich	4	Teil der sicherheitsgerichteten Steuerungskette
5	elektrische Einspeiseplatte	6	Ausgangsmodul
7	Eingangsmodul	8	pneumatische Einspeiseplatte
9	4-fach-Ventiltreiberplatine	10	Einspeiseplatine
11	Ventil	12	Sicherheitsbaustein
UL	24-V-Versorgungsspannung für die Elektronik und Logik	UA	24-V-Versorgungsspannung für die Aktorik
FB	Feldbus		

3.9 Verdrahtungskonzepte des Ventilsystems

Die drei nachfolgenden Abbildungen zeigen die unterschiedlichen Verdrahtungskonzepte des Ventilsystems.

Für alle drei Darstellungen gilt:

- Die Spannungseinspeisung am Buskoppler (K1) für **UL** und **UA** erfolgt über Stecker **X1S1**.
- Die Einspeisung der sicheren Versorgungsspannung für die Ventile erfolgt grundsätzlich über den Anschluss der zusätzlichen elektrischen Einspeiseplatte (**X1S2**) der Ventile.

Für die nachfolgenden Verdrahtungskonzepte werden die Betriebsmittel mit den Referenzkennzeichen in Anlehnung an EN 81346 verwendet. Die Beispiele zeigen nur den relevanten Ausschnitt der Spannungsversorgung und sind nicht vollständig. Für die Anwendung innerhalb einer Maschine sind zusätzliche Betriebsmittel notwendig.

Siehe → Abb. 14. Im Schaltbild wird ein gemeinsames Netzteil (**L01**) für die beiden Spannungen **UL** und **UA** verwendet. Die Spannung für die Ventile am Anschluss **X1S2** wird zweipolig (d. h. **UA+** und **UA-**) über den Sicherheitsbaustein abgeschaltet.

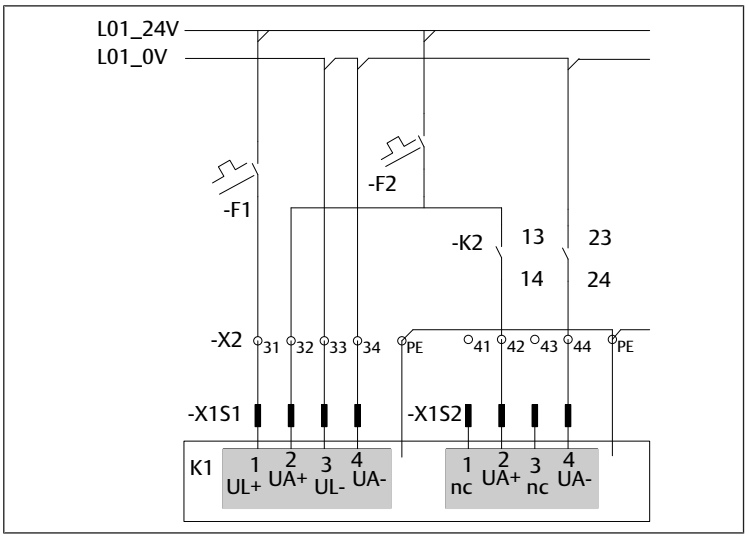


Abb. 15: Verdrahtungskonzept 1

-K1	Ventilsystem mit zwei Steckern für die Spannungsversorgung	**-K2**	Sicherheitsbaustein
-X1S1	Anschluss für die Spannungsversorgung des Buskopplers	**-X1S2**	Anschluss für die Spannungsversorgung der elektrischen Einspeiseplatte
-F1	Absicherung der Spannung **UL**	**-F2**	Absicherung der Spannung **UA**
-X2	Klemmleiste	**L0x**	Spannungsversorgung

Im folgenden Beispiel werden zwei getrennte Netzteile für die beiden Spannungen **UL** (**L01**) und **UA** (**L02**) verwendet. Die Spannung für die Ventile am Anschluss **X1S2** wird zweipolig (d. h. **UA+** und **UA-**) über den Sicherheitsbaustein abgeschaltet.

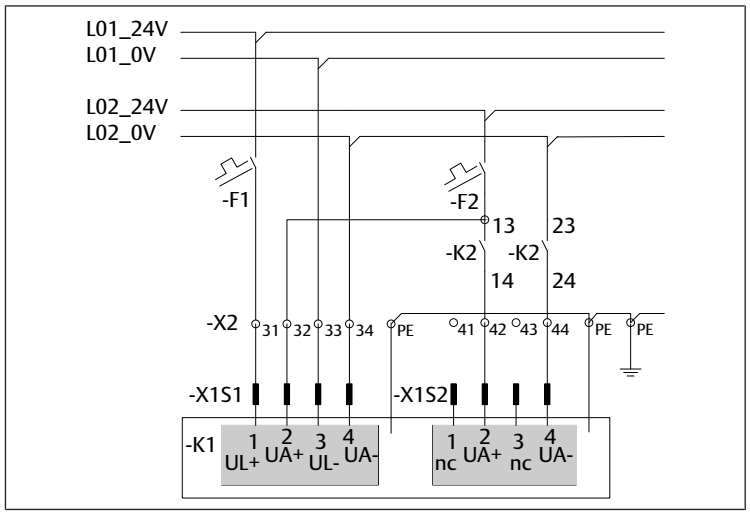


Abb. 16: Verdrahtungskonzept 2

-K1	Ventilsystem mit zwei Steckern für die Spannungsversorgung	**-K2**	Sicherheitsbaustein
-X1S1	Anschluss für die Spannungsversorgung des Buskopplers	**-X1S2**	Anschluss für die Spannungsversorgung der elektrischen Einspeiseplatte
-F1	Absicherung der Spannung **UL**	**-F2**	Absicherung der Spannung **UA**
-X2	Klemmleiste	**L0x**	Spannungsversorgung

Im folgenden Beispiel wird ein gemeinsames Netzteil (**L01**) für die beiden Spannungen **UL** und **UA** verwendet. Die Spannung für die Ventile am Anschluss **X1S2** wird einpolig **UA+** über den Sicherheitsbaustein abgeschaltet.

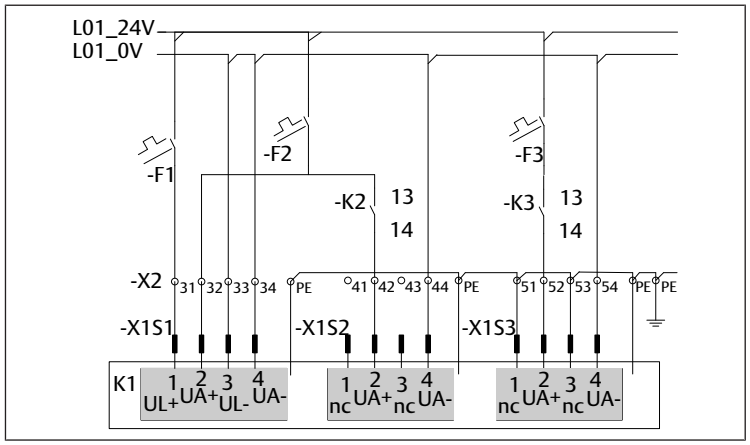


Abb. 17: Verdrahtungskonzept 3

-K1	Ventilsystem mit drei Steckern für die Spannungsversorgung	**-K2**	Sicherheitsbaustein
-X1S1	Anschluss für die Spannungsversorgung des Buskopplers	**-X1S2**	Anschluss für die Spannungsversorgung der elektrischen Einspeiseplatte
-X1S3	Anschluss für die Spannungsversorgung der elektrischen Einspeiseplatte	**-F1**	Absicherung der Spannung **UL**
-F3	Absicherung der Spannung **UA**	**-F2**	Absicherung der Spannung **UA**
-K3	Sicherheitsbaustein	**-X2**	Klemmleiste
L0x	Spannungsversorgung		

3.10 Hinweise zur Verdrahtung

Bei der Verwendung der vorgenannten Verdrahtungskonzepte sind folgende Hinweise zu beachten:

1. Schließen Sie das Ventilsystem wie in den drei Verdrahtungskonzepten dargestellt an.
2. Stellen Sie sicher, dass sich die Ventile, die sicher abgeschaltet werden sollen, hinter der elektrischen Einspeiseplatte befinden.
3. Schließen Sie **X1S2** über eine 2-adrige Leitung an.

Bei Verwendung einer Leitung mit mehr als 2 Adern sollten folgende Sachverhalte zutreffen. Siehe → Abb. 17:

- ungenutzte Adern sind aus EMV Gründen mit PE verbunden
- keine weitere Spannung im Kabel vorhanden.

Bei einpoliger Abschaltung der Spannung UA muss die entsprechende Leitung querschlusssicher verlegt werden.

3.11 Beschreibung der UAoff- / UAon-Überwachung

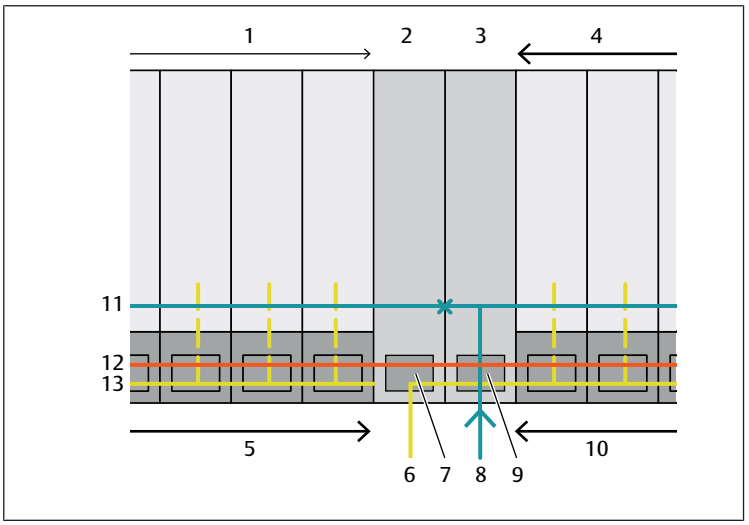


Abb. 18: Detailbild UAoff / UAon

1	vorangegangene Ventile
2	elektrische Einspeiseplatte
3	pneumatische Einspeiseplatte
4	nachfolgende Ventile
5	Ventiltreiber
6	Aktorspannung UA der elektrischen Einspeiseplatte
7	UAon-Überwachung in elektrischer Einspeiseplatte
8	Drucklufteinspeisung der pneumatischen Einspeiseplatte
9	UAoff-Überwachung in pneumatischer Einspeiseplatte
10	Ventiltreiber
11	vorhandene P-Versorgung
12	durchgehende UL-Spannung
13	vorhandene Spannung UA

Die elektrische Einspeiseplatte (**2**) unterbricht die UA-Versorgung der Ventile. Die vorangegangenen Ventile (**1**) werden mit der vorhandenen Ventilspannung versorgt. Die nachfolgenden Ventile (**4**) werden mit der neuen Ventilspannung (**6**) versorgt.

In der elektrischen Einspeiseplatte wird die neue Spannung aus (**6**) auf die Grenze UAon überwacht.

Wenn die Spannung UA die Einschaltspannung UAon unterschreitet, dann sendet die elektrische Einspeiseplatte das Diagnosebit UAon.

Die pneumatische Einspeiseplatte (**3**) unterbricht die P-Versorgung (**11**) der Ventile. Die vorangegangenen Ventile (**1**) werden mit der vorhandenen Druckluft versorgt. Die nachfolgenden Ventile (**4**) werden mit der neuen Druckluft aus (**8**) versorgt.

In der pneumatischen Einspeiseplatte wird die vorhandene Spannung UA auf die Grenze UAoff überwacht.

Wenn die Spannung UA die Ausschaltspannung UAoff unterschreitet, dann sendet die pneumatische Einspeiseplatte das Diagnosebit UAoff.

Die Überwachung der Spannung UA in der pneumatischen Einspeiseplatte steht nur zur Verfügung, wenn das Ventilträgersystem entsprechend konfiguriert wurde. Die Position der Diagnosebits im Datenbereich für die Steuerungen finden Sie in den entsprechenden Beschreibungen zu den Buskopplern aus der Serie AES.

4 Umbau und Reparatur

Sie dürfen das Ventilsystem umbauen und reparieren, wie in den Systembeschreibungen der Buskoppler AES und Ventiltreiber AV beschrieben.

▶ Siehe auch Kapitel → 2. Sicherheitshinweise und → 2.2 Qualifikation des Personals

5 Technische Daten

Die Technischen Daten für das Ventilsystem finden Sie in den jeweiligen Systembeschreibungen.

▶ Wenden Sie sich für die notwendigen Daten für die Sicherheitsfunktion an die AVENTICS GmbH, Adresse siehe Rückseite.

6 Zuverlässigkeitskennwerte

Gern erhalten Sie die Erklärungen (Zuverlässigkeitskennwerte und weitere Angaben zur Anwendung der ISO 13849-1) zum Download auf unserer Website: www.emerson.com/de-de/expertise/automation/improving-safety-security/machine-safety.

Die Werte in der Tabelle entsprechen dem Stand bei Redaktionsschluss. Die Daten werden regelmäßig aktualisiert und können ebenfalls auf unserer Website heruntergeladen werden.

Contents

1 About this documentation 14
1.1 Documentation validity 14
1.2 Required and supplementary documentation 14
1.3 Presentation of information 14
1.3.1 Warnings 14
1.3.2 Symbols 14
1.4 Designations 14
1.5 Abbreviations 14

2 Safety instructions 14
2.1 About this chapter 14
2.2 Personnel qualifications 14
2.3 Use in safety-related control chains 14

3 AV valve system in a safety-related control chain 14
3.1 General preamble (disclaimer) 14
3.2 Towards safe machinery: Risk assessment 15
3.3 Information about the examples 15
3.3.1 Systematics of the examples 15
3.3.2 Technical safety measures 15
3.4 Example 1 with PLr = e 15
3.4.1 Implementation of example 1 16
3.4.2 Safety functions 18
3.4.3 Calculation of the MTTF for the electrical and pneumatic part of the valve system 18
3.4.4 Diagnosis 19
3.4.5 Verification of the diagnostic bit 19
3.5 Example 2 with PLr = c 19
3.6 Example 3 with PLr = d 19
3.6.1 Fault exclusion 20
3.6.2 No fault exclusion 20
3.7 Overview of various options for supply 20
3.8 Assignment of the supply voltages in the valve system 21
3.9 Wiring concepts of the valve system 21
3.10 Instructions for wiring 22
3.11 Description of UAoff / UAon monitoring 22

4 Conversion and repair 22

5 Technical data 22

6 Reliability values 22

1 About this documentation

1.1 Documentation validity

This documentation applies to components of the AV series that are used in safety-related control chains. This documentation is intended for programmers, electrical planners, pneumatic engineers, service personnel and plant operators.

This documentation contains important information for evaluating fault exclusion under certain conditions for valve systems of the AV series.

1.2 Required and supplementary documentation

- ▶ Do not start up valve systems of the AV series in safety-related control chains until you have received the documentation on the valve system and the individual components and have read and understood it.

All assembly instructions and system descriptions for the AES and AV series, as well as the PLC configuration files, can be found on the CD R412018133.

1.3 Presentation of information

1.3.1 Warnings

In this documentation, there are warning notes before the steps whenever there is a risk of personal injury or damage to equipment. The measures described to avoid these hazards must be followed.

Structure of warnings

⚠ SIGNAL WORD

Hazard type and source

Consequences of non-observance

- ▶ Precautions

Meaning of the signal words

⚠ DANGER

Immediate danger to the life and health of persons.

Failure to observe these notices will result in serious health consequences, including death.

⚠ WARNING

Possible danger to the life and health of persons.

Failure to observe these notices can result in serious health consequences, including death.

⚠ CAUTION

Possible dangerous situation.

Failure to observe these notices may result in minor injuries or damage to property.

NOTICE

Possibility of damage to property or malfunction.

Failure to observe these notices may result in damage to property or malfunctions, but not in personal injury.

1.3.2 Symbols

Recommendation for the optimum use of our products.

Observe this information to ensure the smoothest possible operation.

1.4 Designations

The following designations are used in this documentation:

Table 1: Designations

Designation	Meaning
Backplane	Internal electrical connection from the bus coupler to the valve drivers and the I/O modules
Left side	I/O zone, located to the left of the bus coupler when facing its electrical connectors
Right side	Valve zone, located to the right of the bus coupler when facing its electrical connectors
Valve Driver	Electrical valve actuation component that converts the signal from the backplane into current for the solenoid coil

1.5 Abbreviations

This documentation uses the following abbreviations:

Table 2: Abbreviations

Abbreviation	Meaning
AES	**A**dvanced **E**lectronic **S**ystem
AV	**A**dvanced **V**alve
I/O module	**I**nput/**O**utput module
IS12-PD	ISO valve with slider position detection
PL	**P**erformance **L**evel
PLC	**P**rogrammable **L**ogic **C**ontroller or PC assuming control functions
UA	Actuator voltage (power supply for valves and outputs)
UAoff	Message that the actuator voltage UA has fallen below the value of the switch-off voltage of the valves. The valves are switched off electrically.
UAon	Message that the actuator voltage UA has fallen below the value of the switch-on voltage of the valves. The valves cannot be switched on electrically.
UL	Logic voltage (power supply for electronic components and sensors)

2 Safety instructions

2.1 About this chapter

The product has been manufactured according to the accepted rules of current technology. Even so, there is danger of injury and damage to equipment if the following chapter and safety instructions of this documentation are not followed.

1. Read these instructions completely before working with the product.
2. Keep this documentation in a location where it is accessible to all users at all times.
3. Always include the operating instructions when you pass the product onto third parties.
4. Observe ISO 4414 for the safe handling of pneumatics.

2.2 Personnel qualifications

The work described in this documentation requires basic electrical and pneumatic knowledge, as well as knowledge of the appropriate technical terms. In order to ensure safe use, these activities may therefore only be carried out by qualified technical personnel or an instructed person under the direction and supervision of qualified personnel.

Qualified personnel are those who can recognize possible dangers and institute the appropriate safety measures, due to their professional training, knowledge, and experience, as well as their understanding of the relevant regulations pertaining to the work to be done. Qualified personnel must observe the rules relevant to the subject area.

2.3 Use in safety-related control chains

Bus couplers and valve drivers may be used in safety-related control chains for the safety function **"Safety-related stop function and other safety functions initiated by a protective device"** if the entire system is geared toward this purpose.

3 AV valve system in a safety-related control chain

3.1 General preamble (disclaimer)

The examples shown in these instructions represent a cut-out of a safety-related control. These examples show the principles and not always all required components. Further components and assessments may be necessary for applications in machines. The information given does not release the user from the obligation of

own judgment and verification. It must be remembered that our products are subject to a natural process of wear and aging.

3.2 Towards safe machinery: Risk assessment

Risk assessment

- Must be performed by machine manufacturer; results remain with the manufacturer
- Must account for both proper use and any foreseeable misuse of the machine
- Provides an important body of proof for the manufacturer for liability claims in accident cases

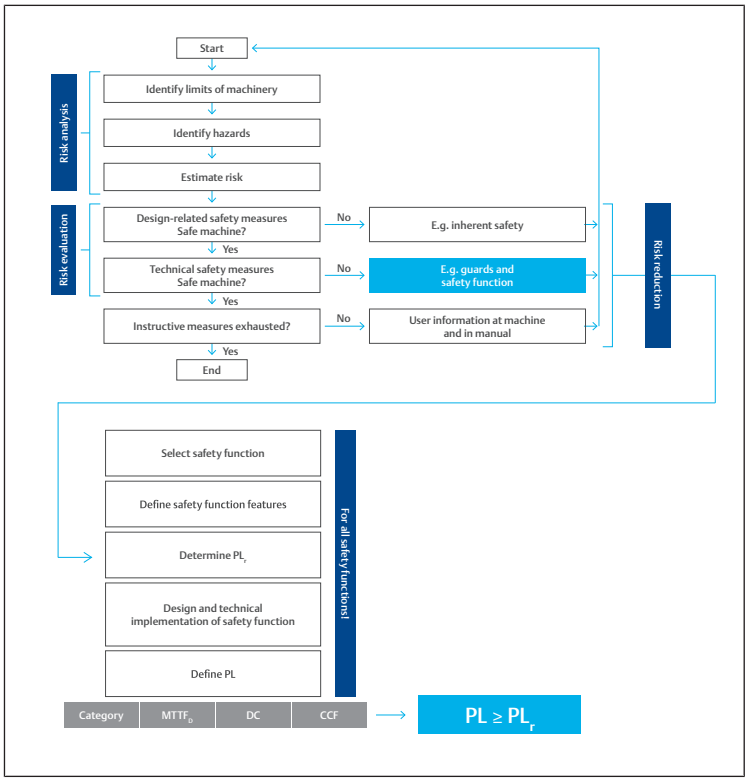


Fig. 1: Process for risk assessment and determination of PL_r

In these instructions, we focus on the implementation of technical safeguards to mitigate risk, assessing the safety function, and determining its performance level within the risk assessment process. The figure shows you the process required for risk assessment. Depending on the control architecture (category), Mean Time To dangerous Failure ($MTTF_D$), Diagnostic Coverage (DC) and Common Cause Failures (CCF), the Performance Level (PL) must be at least equal to the required Performance Level (PL_r).

3.3 Information about the examples

The following 3 examples show:

- Example 1: Hazard due to unexpected start-up, PL_r = e
- Example 2: Hazard due to unexpected start-up, remaining kinetic energy, PL_r = c
- Example 3: Hazard due to unexpected start-up, PL_r = d with fault exclusion

3.3.1 Systematics of the examples

The systematics of the examples is based on the key for the identification of parts of the safety functions from the draft VDMA 66416:2016-01.

The general description is as follows:

Preliminary note

Description of the framework conditions:

- Machine type, operating mode, ...
- Hazard due to ...
- Risk parameters according to DIN EN ISO 13849-1:2016-06
- PL_r

Control measures (safety functions) and other risk reduction measures:

- Name of the safety function
- Name of the safety function
- ...

Input

Triggering event:

- Query of states of safety equipment and
- Monitoring of events
  Examples: Enabling device, emergency stop, safety switch, key switch,
- Light grid, safety pressure switch, ...

Logic

Evaluation of the safety function:

- Switching off the energy supplies, safety relay, safety PLC

Output

Safety-directed response:

- Examples: Fluid valves, contactors, regulators, brakes, ...

3.3.2 Technical safety measures

If the safety of a machine depends on a correctly functioning control, this is referred to as “functional safety”. The “active” parts of the control are the main focus, i.e. components that detect a dangerous situation (signal recording, “I” = input), derive suitable reactions (evaluation, “L” = logic), and implement reliable measures (execution, “O” = output). The term “control” thus refers to the entire signal processing system.

“Safety-related parts of a control (SRP/CS)” are not necessarily “safety components” as defined by the Machinery Directive. SRP/CS (Safety Related Parts of a Control System) can, however, be such safety components, e.g. 2-hand controls or logic units with safety function. Actuators (cylinders), energy supply (e.g. pressure supply or maintenance units) and connections are not directly factored into dangerous failure rates.

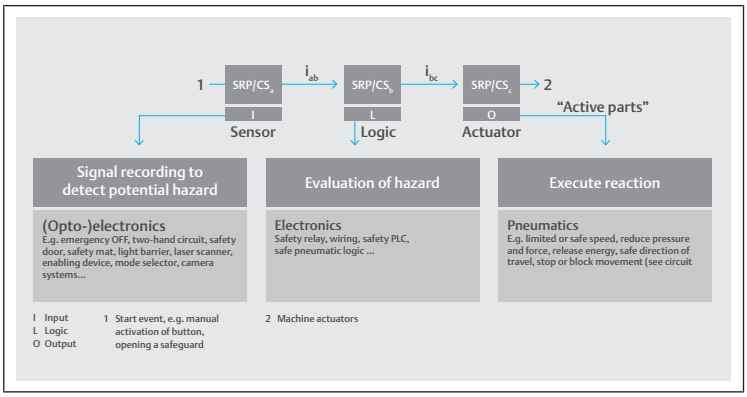


Fig. 2: Focus on safety-related parts of a control (SRP/CS acc. to ISO 13849-1)

3.4 Example 1 with PLr = e

Example 1, based on VDMA 66416:2016-01, number 2.1.1.1 and 2.2.1.1

Preliminary note

Description of the framework conditions:

- Operating mode: Automatic (BA1)
- Machine cycle time: 5 to 15 seconds
- Hazard due to unexpected start-up
- PL_r = e

Control measures (safety functions):

- Safe torque off (STO) or
- Safe disconnection of the energy supply (SEC)
- Prevention of unexpected start-up (PUS)

Input

Triggering event:

- Light grid interrupted or interlocked safety doors open or not kept closed

Logic

Evaluation of the safety function:

- Switching off the energy supplies

Output

Safety-directed response:

- Disconnection of fluid power supply: $PL_r \geq d$ => 2-channel
  and of electrical energy supply: $PL_r \geq d$ => 2-channel recommended

3.4.1 Implementation of example 1

According to ISO 13849, PL = e can be achieved with category 3 if the following circumstances apply:

- DC_{avg} = average
- MTTF = high

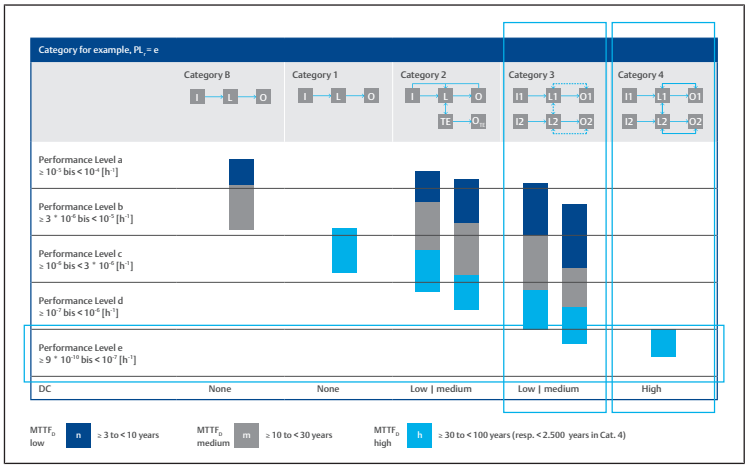


Fig. 3: Implementation of example 1: PL_e with category 3, DC = average, $MTTF_D$ = high

According to the simplified approach of ISO 13849-1, the 4 classes for the diagnostic coverage DC are defined as follows:

- none: DC < 60 %
- low: 60 % < DC < 90 %
- average: 90 % < DC < 99 %
- high: 99 % < DC

Design and technical implementation of safety function

Manual workplace
TM=20 years
d/a=320 days
h/d=24 h / min. 10 sec cycle time = 55,296,000 switching cycles for working and main air valve

During setup operation, movable, separating guards must be bridged and open, and fixed separating guards must be mounted.

INFO: A single error does not lead to loss of the safety function. Some, but not all, faults are detected. However, an accumulation of undetected faults can lead to a loss of the safety function.

Valve selection

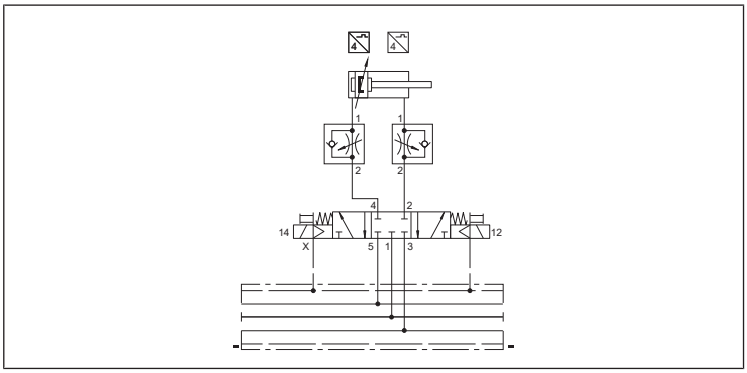


Fig. 4: Wiring diagram: valve selection

- Defined, safe switching position in state without current by mechanical spring
- Pressure lines are blocked in the state without current
- Exhaust lines are not open
- Cylinder after EMERGENCY STOP cannot be moved, i.e. personal rescue is required
- Braking of decelerated masses possible
- Safe stopping during vertical movements with masses (from PL_d only with additional measures -> 2-channel)
- JOG operation is possible (cylinder stroke jogging)
- Transverse influence by exhaust air from large neighboring cylinders not possible
- Suitable up to Performance Level PL_e (additional measures see → Fig. 5.)
- Extend and retract the permissible hazardous direction of movement of the cylinder
- Service life of the valves has been tested according to ISO 19973-1 and -2

Pneumatic safety switch category 3 PL_e

Designation:
Prevention of unexpected start-up (PUS) acc. to VDMA standard sheet 24584.

Blocking the volume flows into and out of both piston chambers.

INFO: Observe during restart:
Cylinder chambers can exhaust due to leakage of individual components.

INFO: Test pulses can cause the valves to switch.

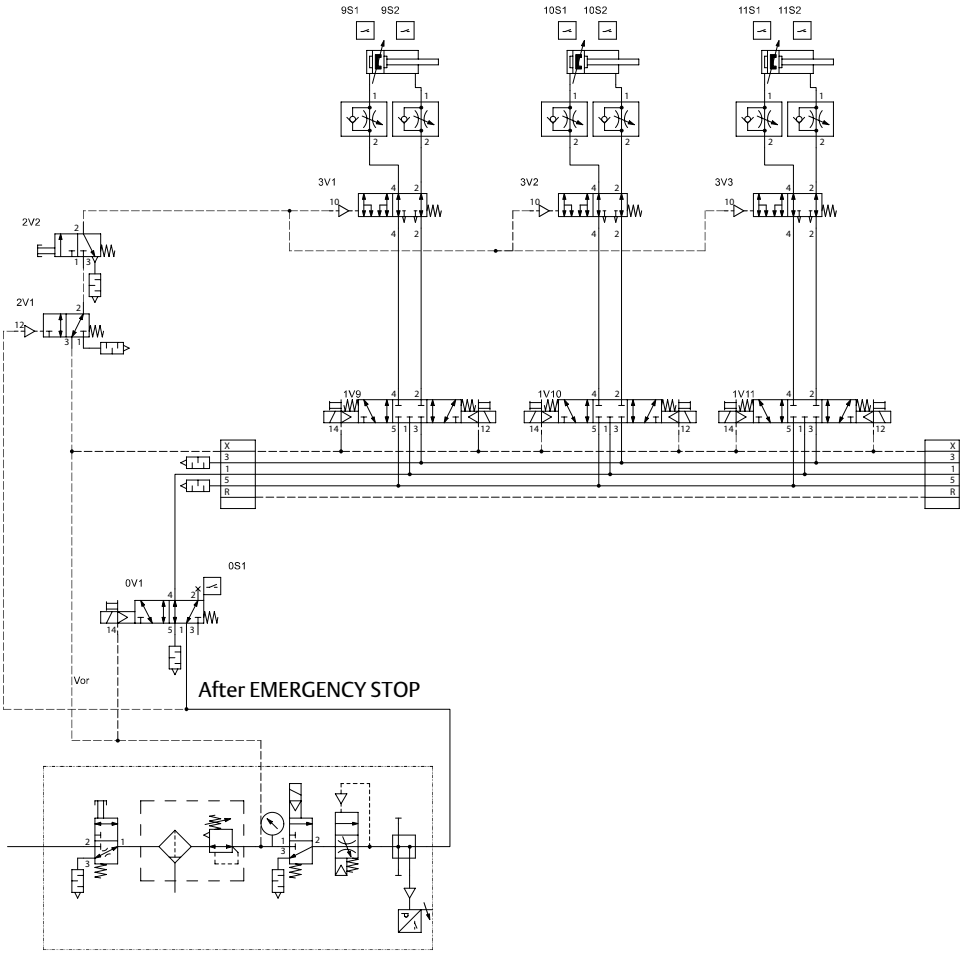


Fig. 5: Schematic diagram: Function and test channels

INFO: If you pressurize/exhaust more than 8 valves at the same time, make sure that additional supply air/exhaust is available via the supply plates.

Personal rescue by exhausting (for circuits with position retention)

For vertical and horizontal movements:

- Severity of injury = S2 (usually irreversible injury, including death)
- Hazardous point is within the accessible area
- the operator cannot free himself
- exhausting must not cause any additional hazard

Personal rescue can be achieved only by the following circumstances:

- Only in a state without pressure
- After active emergency stop by 2V1 (a 2V1 can supply several 2V2), this must be mounted close to the hazardous point
- Provide a joint personal rescue for cylinder groups (a 2V2 can exhaust several cylinders)

Block diagram

The following figure shows the safety-related block diagram for example 1.

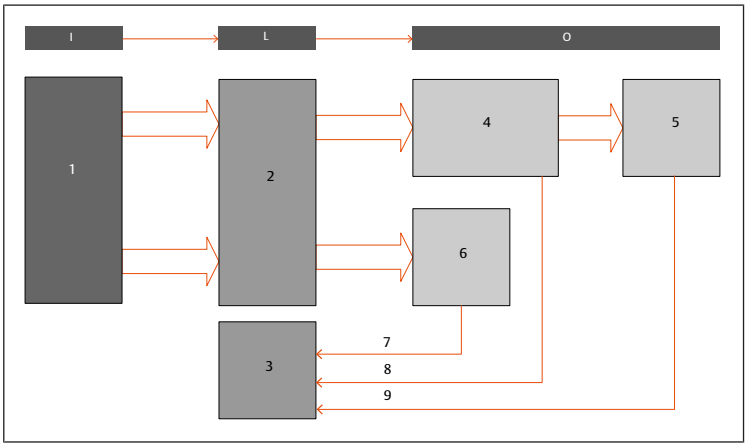


Fig. 6: Safety-related block diagram, example 1

1 Safety door switch (e.g. PILZ PSEN cs3.1 or PSEN sl-0.5p 1.1)

2 Safety module (e.g. PILZ PNOZ)

3 PLC (programmable logic controller)

4 electrical part of the AV valve system UA supply via electrical supply plate

5 pneumatic part of the AV valve system

6 Main air valve with position detection (e.g. IS12-PD)

7 Diagnosis “Query of the position of the main air valve”

8 Diagnostic message “Valve voltage UA is lower than switch-off voltage (UA < UAoff)”

9 Diagnosis “indirect query of the working valve”

Pneumatics wiring diagram

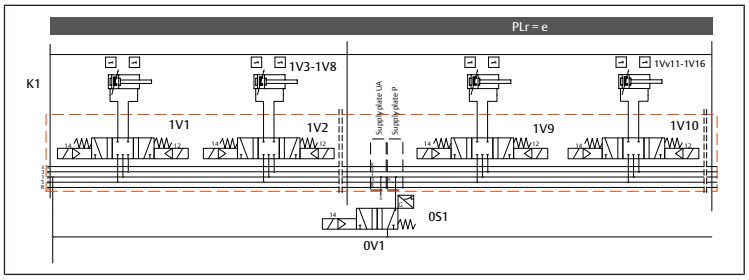


Fig. 7: Pneumatics wiring diagram, example 1

K1	Valve terminal system	1V1 – 1V8	Valves outside the safety-related control chain
1V3 – 1V8	Not drawn	1V9 – 1V16	Valves for actuators with PL_r = e
1V1 – 1V16	Not drawn	0S1	Position detection of 0V1
0V1	Main air valve		

Complete valve system with external components

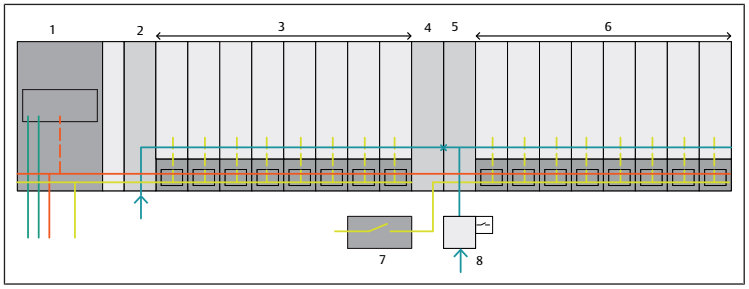


Fig. 8: Valve system and external components

1	Bus coupler	2	Pneumatic supply plate
3	Valves (not in the safety circuit)	4	Electrical supply plate - corresponds to block 4 in the safety-related block diagram
5	Pneumatic supply plate, - no monitoring (UAoff) required, no active electronics installed	6	Valves (safety circuit) - corresponds to block 5 in the safety-related block diagram - the electrical part of the valves (valve driver) corresponds to block 4 in the safety-related block diagram
7	Safety module, corresponds to block 2 in the safety-related block diagram	8	Main air valve corresponds to block 6 and 7 in the safety-related block diagram

3.4.2 Safety functions

Safety-related prevention of unexpected start-up from the rest position, with the option of personal rescue.

In this documentation, only the pneumatic control component is shown as a subsystem. For the complete safety function, additional safety-related control components (e.g. guards and electrical logic) must be added as subsystems.

- Severity of injury = S2
- Hazardous point is within the accessible area and the operator cannot free himself
- exhausting must not cause any additional hazard
- as the personal rescue 2V1, 2V2, 3V1 and 3Vn are fully functional after emergency stop, i.e. after exhausting the 3/2 directional control valve in the air preparation unit, and have no influence on the safety function, they are not taken into account in the calculation.

This can only be implemented by the following circumstance:

- Only in a state without pressure
- After active emergency stop by 2V1 (a 2V1 can supply several 2V2), this must be mounted close to the hazardous point
- Provide a joint personal rescue for cylinder groups (a 2V2 can exhaust several cylinders)

Functional description of switching PL c, d, e_Kat-3_02 when used in a manual workplace

- Movements are redundantly controlled by main air valve 0V1 and working valve 1Vn
- Valve 0V1 must be actuated constantly, so that 1Vn can be actuated
- the sole failure of 1 of the mentioned valves does not jeopardize the safety function
- all valves are actuated cyclically in the process
- the function of the main air valve 0V1 is monitored by a valve position query 0S1
- the function of the working valve 1Vn is indirectly detected during the process by the switches nS1 and nS2
- the accumulation of undetected faults can lead to a loss of the safety function
- in case of danger due to stored energy (pressure, mass, spring), additional measures are required

Design features

- Basic and proven safety principles as well as the category B requirement are met
- Main air valve 0V1 is moved to the safe switching position by a spring
- Working valve nV1 has a locked center (zero overlap) with spring centering
- the safe switching position is reached for both valves after the control voltage is removed
- signal processing of the valve queries and monitoring is carried out in a single-channel PLC control
- Control ON and loading door closed:
  - Main air valve 0V1 is switched and voltage is applied to the valve system
- Automatic mode ON and loading door open:
  - there is no voltage applied at main air valve 0V1 and at the valve system
- Setup operation and safety door bridged with key switch:
  - there is no voltage applied at main air valve 0V1 and at the valve system
  - the pneumatic line between main air valve 0V1 and working valve nV1 is exhausted
  - Movements are only possible with additional consent switch
  - the consent switch switches the main air valve 0V1 and voltage is applied at the valve system
  - Dangerous movements without additional measures with justification are only permitted with the safety door closed

Calculation of the probability of failure and service life

Required service life:
20 years / 320 days / 24 h / 10 sec. cycle time (nop = 2764800 cycles/year)

- Valve 0V1 B_{10D} = 79.2 million (IS12-PD)
- Valve nV1 B_{10D} = 39.6 million (AV05) or valve nV1 B_{10D} = 105.8 million (AV03)

3.4.3 Calculation of the MTTF for the electrical and pneumatic part of the valve system

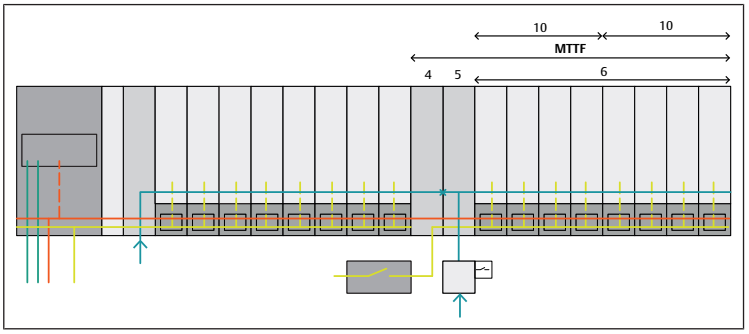


Fig. 9: Relevant components for calculating the $MTTF_D$ for the electrical part

4	Electrical supply plate with UAon monitoring, corresponds to block 4 in the safety-related block diagram	5	Pneumatic supply plate with UAoff monitoring, the electrical function = UAoff monitoring corresponds to blocks 4 and 8 in the safety-related block diagram
6	Valves (safety circuit) corresponds to block 5 in the safety-related block diagram the electrical part of the valves (valve driver) corresponds to block 4 in the safety-related block diagram	10	Valve driver board, 4x

See → 6. Reliability values and see → Fig. 9

It follows:

- Electrical supply plate (**4**) MTTF = 854 years
- UAoff monitoring (**5**) MTTF = 1094 years

- Valve driver board, 4x (**10**) MTTF = 630 years
- Valves AV03 5/3 spring return (**6**) MTTF = 382.7 years

$$MTTF_{ges} = \frac{1}{\frac{1}{854\ [a]} + \frac{1}{1094\ [a]} + \frac{1}{630\ [a]} + \frac{1}{630\ [a]} + \frac{1}{382{,}7\ [a]}} = 127\ [a]$$

The MTTF values of the AES modules were calculated using the failure rates from a database.

According to DIN EN 13849-1, Annex C, not every failure is a dangerous failure. In this case, $MTTF_D = 2 \times MTTF_{ges}$ can be set for the calculation of the entire system.

$MTTF_D = 2x\ MTTF_{ges} = 2 \times 127\ [a] = 254\ [a]$

3.4.4 Diagnosis

The pneumatic supply plate monitors the actuator voltage UA and sends the diagnostic bit UAoff when UA falls below the switch-off voltage.

The electrical supply plate monitors the actuator voltage UA and sends the diagnostic bit UAon when UA falls below the switch-on voltage.

The diagnostic bit (UAoff) must be monitored. This requires a change of the signal. This can be done, for example, during switching on the machine or with special test cycles.

Direct function query of the position at the main valve 99 %.

Indirect function query of the working valve 90 %.

DC = 94.4 % $MTTF_D$ = high (100 J) CCF = 95

CCF in our example			
Countermeasure for CCF	Fluid technology	Electronics	Points
Separation of signal paths	Separation of tubing	Air and creepage distance on activated circuits	15
Diversity	E.g. different valves	E.g. different processors	20
Protection against overvoltage, overpressure ...	Setup acc. to EN ISO 4413 to EN ISO 4414 (pressure relief valve)	Overvoltage protection (e.g. contactors, power pack)	15
Use of well-tried components	User		5
FMEA in development	FMEA during initial system conception		5
Competence/training	Qualification measure		5
Protection against contamination and EMC	Fluid quality	EMC test	25
Other effects (e.g. temperature, shock)	Compliance with EN ISO 4413 and EN ISO 4414 and product spec	Observe ambient conditions as described in product spec	10
Total CCF	Total points(65 ≤ CCF ≤ 100):		95

Fig. 10: Example: CCF – Common cause failure

Performance level = PL_e / category = 3

Replacement of main air valve 0V1 (IS12-PD) not required.

Replacement of valve nV1 (AV03) not required.

Replacement of valve nV1 (AV05) after 14.3 years – not required for cycle time ≥ 14 sec., or operational life 20 years.

3.4.5 Verification of the diagnostic bit

A detailed description of the monitoring can be found in chapter → 3.11 Description of UAoff / UAon monitoring.

When the voltage UA is switched off, both the diagnostic message UAon and UAoff must be sent.

Table 3: Verification of the diagnostic bit

UA = 0, switched off	UAon switch-on diagnosis	UAoff switch-off diagnosis
valid	1	1
not valid	1	0
not valid	0	1

If the above conditions are taken into account, the following standards can be used to estimate the monitoring of the switched-off valve voltage with a DC = 90 % to < 99 % (medium):

- DIN EN ISO 13849-1 Annex E: “Estimates of diagnostic coverage (DC) for functions and modules”
- DIN EN 61508-2: “Table A.14 – Actuators”
- DIN EN 61508-2: “Table A.7 – I/O units and interfaces (external communication)”

3.5 Example 2 with PLr = c

Example 2, based on 66416:2016-01, number 1.1.2.1 and 2.1.2.3

Preliminary note

Description of the framework conditions:

- Operating mode BA2 Setup or service mode
- Hazard due to unexpected start-up, remaining kinetic energy
- PL_r = c

Control measures (safety functions) (see comment):

- Safe torque off (STO)
- Safe disconnection of the energy supply (SEC)
- Prevention of unexpected start-up (PUS)

Input

Triggering event:

- Operating mode switch, enabling device

Logic

Evaluation of the safety function:

- Switching off the energy supplies

Output

Safety-directed response:

- 1-channel confinement of fluid medium. The following implementations are possible:
  - Directional valve in locked position
  - Control of blocking valve(s)
  - S1 possible because residual energy causes only reversible injuries
- Disconnection of electrical power supply: $PL_r \geq d$ => 2-channel recommended

Comment

The topic of residual energy is described in more detail in the following documents:

- Draft VDMA 66416: Chapter 5.1.3 Setup operation / service operation (BA2) “Reduced speeds are to be provided as follows ...”
- Draft VDMA 66416: Table A2 – Key for identification of the parameter estimates of the risk graph in table A7

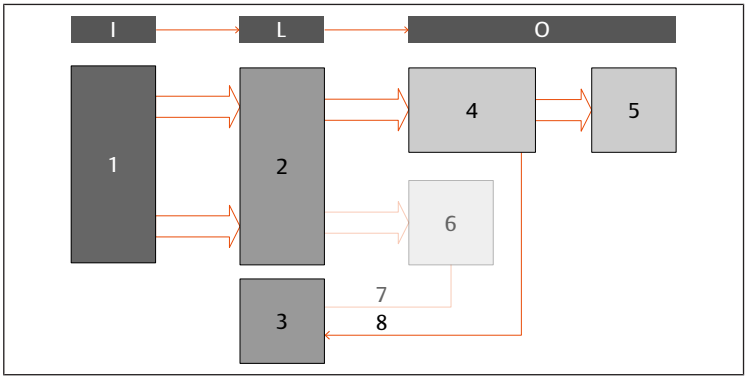


Fig. 11: Safety-related block diagram, example 2

1	Enabling device
2	Safety module (e.g. PILZ PNOZ)
3	PLC (programmable logic controller)
4	electrical part of the AV valve system, UA supply via electrical supply plate
5	Directional valves of the AV valve system
6	Main air valve with position detection (e.g. IS12-PD, ...) not active for this safety function
7	Diagnosis “Query of the position of the main air valve” not active for this safety function
8	Diagnosis “Valve voltage UA is lower than switch-off voltage (UA < UAoff)”

3.6 Example 3 with PLr = d

Example 3, based on VDMA 66416, number 2.1.1.1 and 2.2.1.1

This example is similar to Example 1, but the required PL_r is d.

Preliminary note

Description of the framework conditions:

- Automatic operating mode (BA1)
- Hazard due to unexpected start-up
- PL_r = d

Control measures (safety functions):

- Safe torque off (STO)
- Safe disconnection of the energy supply (SEC)
- Prevention of unexpected start-up (PUS)

Input

Triggering event:

- Light grid interrupted or interlocked safety doors open or not kept closed

Logic

Evaluation of the safety function:

- Switching off the energy supplies

Output

Safety-directed response:

- Disconnection of fluid power supply: $PL_r \geq d$ => 2-channel and of electrical energy supply: $PL_r \geq d$ => 2-channel recommended

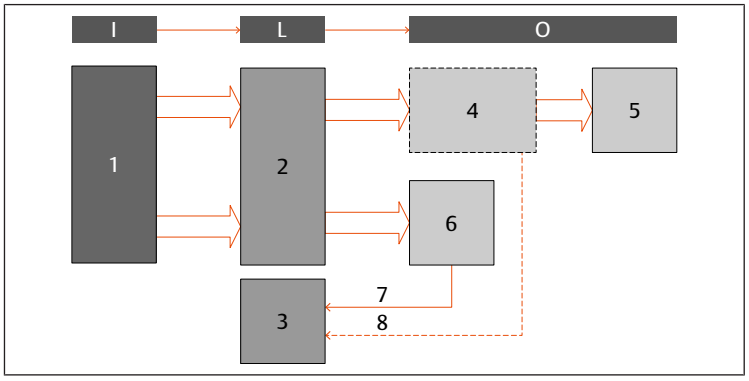


Fig. 12: Safety-related block diagram, example 3

1 Safety door switch (e.g. PILZ PSEN cs3.1 or PSEN sl-0.5p 1.1)
2 Safety module (e.g. PILZ PNOZ)
3 PLC (programmable logic controller)
4 Electrical part of the AV valve system
Either UA supply via electrical supply plate. For this block, fault exclusion is possible (see → 3.6.1 Fault exclusion).
Or UA supply via bus coupler. Fault exclusion is not possible (see → 3.6.2 No fault exclusion).
5 Directional valves of the AV valve system
6 Main air valve with position detection (e.g. IS12-PD, ...)
7 Diagnosis “Query of the position of the main air valve”
8 Diagnosis “Valve voltage UA is lower than switch-off voltage (UA < UAoff)”
If fault exclusion is applied for (**4**), this diagnosis is not required.

3.6.1 Fault exclusion

If the valve system is set up and used as described in the following chapters, the valve electronics do not have to be included in the calculation of the MTTF values of a safety-related control chain.

Prerequisite for the application of the fault exclusion is,

- that PL d is applicable as a maximum (PL e must be calculated as in example 1),
- that the valve system is built with 1 or more electrical supply plates,
- that the valves which are to be switched off are supplied via these electrical supply plates,
- that the electrical supply plates are wired according to the wiring concepts 1–3,
- that the cable for connecting the supply plate contains only the 24 V supply voltage UA,
- that the cable is laid in accordance with DIN EN 60204.

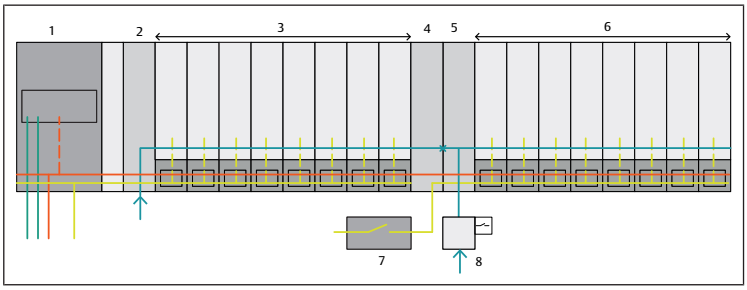


Fig. 13: Valve system and external components

1 Bus coupler
2 Pneumatic supply plate
3 Valves (not in the safety circuit)
4 Electrical supply plate - corresponds to block 4 in the safety-related block diagram
5 Pneumatic supply plate, - no monitoring (UAoff) required, no active electronics installed
6 Valves (safety circuit) - corresponds to block 5 in the safety-related block diagram - the electrical part of the valves (valve driver) corresponds to block 4 in the safety-related block diagram
7 Safety module, corresponds to block 2 in the safety-related block diagram
8 Main air valve corresponds to block 6 and 7 in the safety-related block diagram

3.6.2 No fault exclusion

If the UA supply is carried out via the bus coupler, fault exclusion is not possible. The probability of failure must be calculated.

Additional measures include:

- The UA supply via the bus coupler must be safely switched off to prevent the valves switching unexpectedly.
- The cable must be laid in accordance with DIN EN 60204.
- The diagnosis of the bus coupler (UAon and UAoff) must be evaluated.

Depending on the required performance level, further measures must be taken.

3.7 Overview of various options for supply

Table 4: Various options for supply

	UA supply via bus coupler	UA supply via electrical supply plate
Maximum achievable PL_r	d (e not recommended)	e
Is fault exclusion possible	no See → 3.6.2 No fault exclusion	$PL_r \leq$ d: yes PL_r = e: no
Evaluation of diagnosis	yes (UAon and UAoff of bus coupler)	$PL_r \leq$ d: no (not necessary due to fault exclusion) PL_r = e: yes (UAon and UAoff) Pneumatic supply plate must be equipped with UAoff monitoring.
DC	90 % ... <99 %	90 % ... <99 %
Inrush current limitation	yes	yes
Testing possible (cross-circuit)	no	yes

Inrush current limitation

The very high inrush current of the unit, as normally present with capacitive loads, is limited to a value of 5 A maximum.

Definition of test pulse

A test pulse is a time-limited change of a signal voltage level to check the functionality of the output or device or to check the transmission path.
[Source: ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V., Position paper “Classification of binary 24 V interfaces with testing in the field of functional safety”]

Testing possible

Safe outputs and/or safety modules generate clock signals or test pulses on their outputs. If such an output is connected to the electrical supply plate, there is no misinterpretation of the cross-circuit test. If such an output is used for the UA supply at the bus coupler, this leads to a misinterpretation of the cross-circuit test.

Comment

Only the transmission path up to the electrical supply plate can be checked.

3.8 Assignment of the supply voltages in the valve system

The following figure shows the assignment of the supply voltages to the functions within the valve system.

- The **UL** supply voltage fed to the bus coupler (**1**) supplies the complete electronics of the valve system.
- The supply voltage **UA** fed to the bus coupler supplies the outputs of the DO module (**6**) (digital output) and all valves between the bus coupler and UA supply.

The “Electrical supply plate” module (**5**) interrupts the incoming supply voltage **UA**. The supply voltage of this module is used for all valves located to the right of the electrical supply plate. The “Electrical supply plate” module can be used several times in the valve area.

The voltage **UL** is galvanically isolated from the voltage **UA** in the valve system.

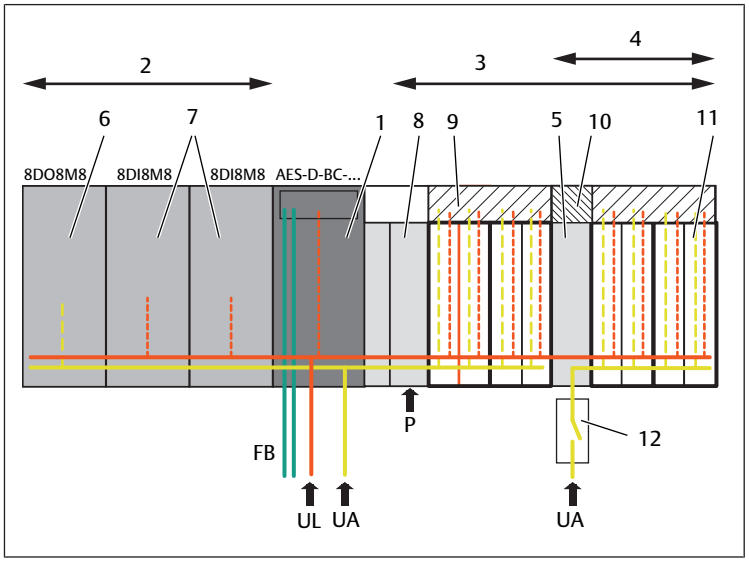


Fig. 14: Assignment of the supply voltages UL and UA

1	Bus coupler	2	I/O modules
3	Valve Zone	4	Part of the safety-related control chain
5	electrical supply plate	6	Output module
7	Input module	8	pneumatic supply plate
9	Valve driver board, 4x	10	Supply board
11	Valve	12	Safety module
UL	24 V supply voltage for the electronics and logic	UA	24 V supply voltage for the actuators
FB	Fieldbus		

3.9 Wiring concepts of the valve system

The 3 figures below show the various wiring concepts of the valve system.

The following applies to all 3 representations:

- The power supply at the bus coupler (K1) for **UL** and **UA** is provided via plug **X1S1**.
- The supply of the safe supply voltage for the valves is always made via the connection of the additional electrical supply plate (**X1S2**) of the valves.

For the following wiring concepts, the equipment with the reference designations based on EN 81346 is used. The examples only show the relevant section of the power supply and are not complete. For the application within a machine, additional equipment is necessary.

See → Fig. 14. In the wiring diagram, a common power pack (**L01**) is used for both voltages **UL** and **UA**. The voltage for the valves at connection **X1S2** is switched off in 2 poles (i.e. **UA+** and **UA-**) via the safety module.

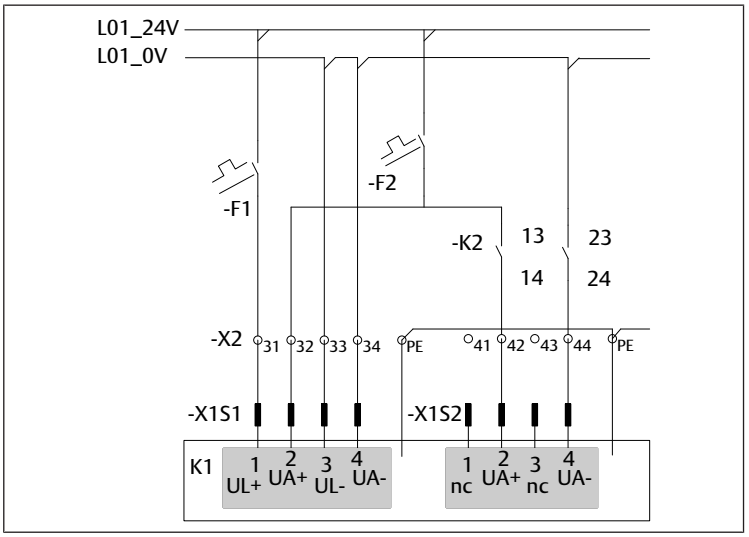


Fig. 15: Wiring concept 1

-K1	Valve system with 2 plugs for power supply	**-K2**	Safety module
-X1S1	Connection for the power supply of the bus coupler	**-X1S2**	Connection for the power supply of the electrical supply plate
-F1	Fuse for voltage **UL**	**-F2**	Fuse for voltage **UA**
-X2	Terminal strip	**L0x**	Power supply

In the following example, 2 separate power packs are used for both voltages **UL** (**L01**) and **UA** (**L02**). The voltage for the valves at connection **X1S2** is switched off in 2 poles (i.e. **UA+** and **UA-**) via the safety module.

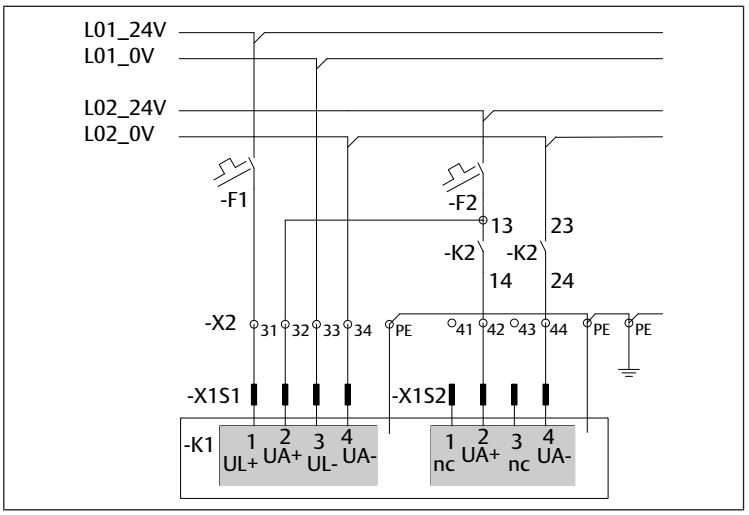


Fig. 16: Wiring concept 2

-K1	Valve system with 2 plugs for power supply	**-K2**	Safety module
-X1S1	Connection for the power supply of the bus coupler	**-X1S2**	Connection for the power supply of the electrical supply plate
-F1	Fuse for voltage **UL**	**-F2**	Fuse for voltage **UA**
-X2	Terminal strip	**L0x**	Power supply

In the following example, a shared power pack (**L01**) is used for both voltages **UL** and **UA**. The voltage for the valves at connection **X1S2** is switched off single-pole **UA+** via the safety module.

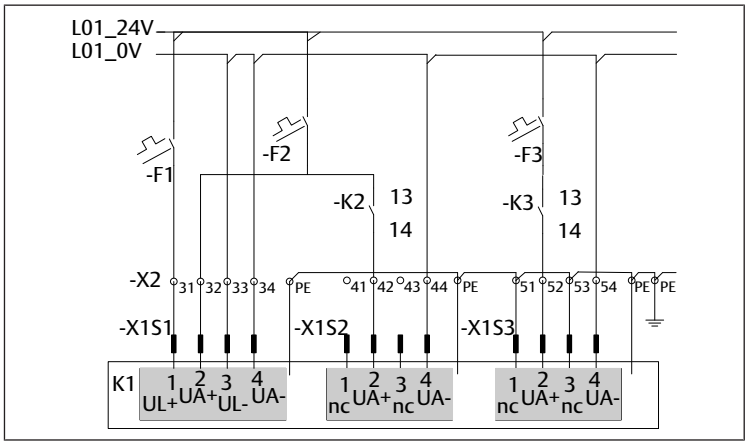


Fig. 17: Wiring concept 3

-K1	Valve system with 3 plugs for power supply	**-K2**	Safety module
-X1S1	Connection for the power supply of the bus coupler	**-X1S2**	Connection for the power supply of the electrical supply plate
-X1S3	Connection for the power supply of the electrical supply plate	**-F1**	Fuse for voltage **UL**
-F3	Fuse for voltage **UA**	**-F2**	Fuse for voltage **UA**
-K3	Safety module	**-X2**	Terminal strip
L0x	Power supply		

3.10 Instructions for wiring

When using the aforementioned wiring concepts, the following instructions must be observed:

1. Connect the valve system as shown in the 3 wiring concepts.
2. Make sure that the valves that are to be safely switched off are located downstream of the electrical supply plate.
3. Connect **X1S2** via a 2-wire cable.

When using a cable with more than 2 cores, the following circumstances should apply. See → Fig. 17:

- unused cores are connected to PE for EMC reasons
- no further voltage is present in the cable.

In case of single-pole disconnection of the voltage UA, the corresponding cable must be laid cross-circuit proof.

3.11 Description of UAoff / UAon monitoring

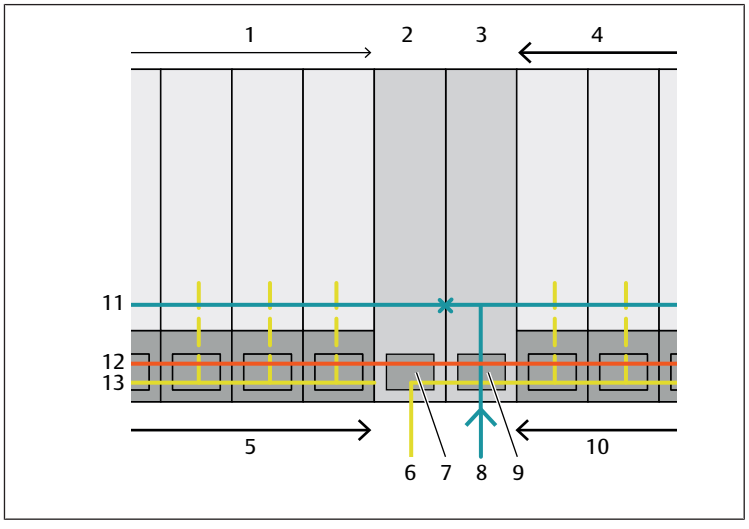


Fig. 18: Detail image UAoff / UAon

1	preceding valves
2	electrical supply plate
3	pneumatic supply plate
4	downstream valves
5	Valve Driver
6	Actuator voltage UA of the electrical supply plate
7	UAon monitoring in electrical supply plate
8	Compressed air supply of the pneumatic supply plate
9	UAoff monitoring in pneumatic supply plate
10	Valve Driver
11	existing P-supply
12	through UL voltage
13	existing voltage UA

The electrical supply plate (**2**) interrupts the UA supply to the valves. The preceding valves (**1**) are supplied with the existing valve voltage. The downstream valves (**4**) are supplied with the new valve voltage (**6**).

In the electrical supply plate, the new voltage from (**6**) is monitored for the limit UAon.

When the voltage UA falls below the switch-on voltage UAon, the electrical supply plate sends the diagnostic bit UAon.

The pneumatic supply plate (**3**) interrupts the P supply (**11**) to the valves. The preceding valves (**1**) are supplied with the existing compressed air. The downstream valves (**4**) are supplied with the new compressed air from (**8**).

In the pneumatic supply plate, the existing voltage UA is monitored for the limit UAoff.

If the voltage UA falls below the switch-off voltage UAoff, the pneumatic supply plate sends the diagnostic bit UAoff.

Monitoring of the voltage UA in the pneumatic supply plate is only available if the valve terminal system has been configured accordingly. The position of the diagnostic bits in the data area for the controllers can be found in the corresponding descriptions for the AES series bus couplers.

4 Conversion and repair

You may convert and repair the valve system as described in the system descriptions of the bus coupler AES and valve driver AV.

▶ See also chapter → 2. Safety instructions and → 2.2 Personnel qualifications

5 Technical data

You can find the technical data for the valve system in the respective system descriptions.

▶ Contact AVENTICS GmbH for the data required for the safety function, see back side for address.

6 Reliability values

We provide explanations (reliability values and further information for the application of ISO 13849-1) as downloads online: www.emerson.com/de-de/expertise/automation/improving-safety-security/machine-safety.

The values in the table reflect the current status as of the editorial deadline. This data is updated on a regular basis and can also be downloaded from our website.

Sommaire

1 À propos de cette documentation 24

1.1 Validité de la documentation 24

1.2 Documentations nécessaires et complémentaires 24

1.3 Présentation des informations 24

1.3.1 Avertissements 24

1.3.2 Symboles 24

1.4 Désignations 24

1.5 Abréviations 24

2 Consignes de sécurité 24

2.1 À propos de ce chapitre 24

2.2 Qualification du personnel 24

2.3 Utilisation dans des chaînes de commande importantes pour la sécurité 24

3 Îlot de distribution AV dans une chaîne de commande de sécurité 25

3.1 Introduction générale (exclusion de la responsabilité) 25

3.2 Processus pour une machine fiable : l'appréciation du risque 25

3.3 Informations relatives aux exemples 25

3.3.1 Systématique des exemples 25

3.3.2 Mesures de protection techniques 25

3.4 Exemple 1 avec PLr = e 25

3.4.1 Mise en œuvre de l'exemple 1 26

3.4.2 Fonctions de sécurité 28

3.4.3 Calcul du MTTF pour les parties électrique et pneumatique de l'îlot de distribution 29

3.4.4 Diagnostic 29

3.4.5 Vérification du bit de diagnostic 29

3.5 Exemple 2 avec PLr = c 29

3.6 Exemple 3 avec PLr = d 30

3.6.1 Exclusion des défauts 30

3.6.2 Aucune exclusion des défauts 31

3.7 Vue d'ensemble des différentes possibilités d'alimentation 31

3.8 Affectation des tensions d'alimentation dans l'îlot de distribution 31

3.9 Concept de câblage de l'îlot de distribution 31

3.10 Remarques sur le câblage 32

3.11 Description de la surveillance UAoff / UAon 32

4 Transformation et réparation 33

5 Données techniques 33

6 Indicateurs de fiabilité 33

1 À propos de cette documentation

1.1 Validité de la documentation

Cette documentation s'applique aux composants de la série AV, utilisés dans des chaînes de commande de sécurité. Cette documentation s'adresse aux programmateurs, aux planificateurs-électriciens, aux techniciens en circuit pneumatique, au personnel de maintenance et aux exploitants d'installation.

Cette documentation contient des informations importantes permettant d'évaluer l'exclusion des défauts dans certaines conditions pour les îlots de distribution de la série AV.

1.2 Documentations nécessaires et complémentaires

- ▶ Ne mettez en service les îlots de distribution de la série AV utilisés dans des chaînes de commande de sécurité qu'en présence des documentations sur l'îlot de distribution et des différents composants et une fois avoir consulté et compris ces documentations.

Toutes les instructions de montage et descriptions du système des séries AES et AV ainsi que les fichiers de configuration API figurent sur le CD R412018133.

1.3 Présentation des informations

1.3.1 Avertissements

Cette documentation contient des remarques d'avertissement préalables aux séquences de travail lorsqu'un risque de dommage corporel ou matériel subsiste. Les mesures décrites pour éviter ces risques doivent être suivies.

Structure des avertissements

⚠ MOT-CLE

Type et source de risque

Conséquences du non-respect

- ▶ Précautions

Signification des mots-clés

⚠ DANGER

Danger immédiat pour la vie et la santé des personnes.

Le non-respect de ces consignes entraînera de graves conséquences pour la santé, voire la mort.

⚠ AVERTISSEMENT

Danger potentiel pour la vie et la santé des personnes.

Le non-respect de ces consignes peut entraîner de graves conséquences pour la santé, voire la mort.

⚠ ATTENTION

Situation dangereuse potentielle.

Le non-respect de ces consignes risque d'entraîner de légères blessures ou des dommages matériels.

AVIS

Possibilité de dommages matériels ou de dysfonctionnement.

Le non-respect de ces consignes risque d'entraîner des dommages matériels ou des dysfonctionnements, mais pas de blessures.

1.3.2 Symboles

Recommandation pour une utilisation optimale de nos produits.

Respecter ces informations pour garantir un fonctionnement optimal.

1.4 Désignations

Cette documentation emploie les désignations suivantes :

Tab. 1: Désignations

Désignation	Signification
Backplane (platine bus)	Liaison électrique interne entre le coupleur de bus et les pilotes de distributeurs et les modules E/S
Côté gauche	Plage E/S, à gauche du coupleur de bus, lorsque l'on regarde ses raccords électriques
Côté droit	Plage de distributeurs, à droite du coupleur de bus, lorsque l'on regarde ses raccords électriques
Pilote de distributeurs	Partie électrique de la commande de distributeur qui convertit le signal venant de la platine bus en courant pour la bobine électromagnétique.

1.5 Abréviations

Les abréviations suivantes sont utilisées dans cette documentation :

Tab. 2: Abréviations

Abréviation	Signification
AES	**A**dvanced **E**lectronic **S**ystem
AV	**A**dvanced **V**alve
Module E/S	Module d'**E**entrée/de **S**ortie
IS12-PD	Distributeur ISO avec interrogation de position de tiroir
PL	**P**erformance **L**evel (niveau de performance)
API	**A**utomate **P**rogrammable **I**ndustriel ou ordinateur qui réalise des fonctions de commande
UA	Tension de l'actionneur (alimentation électrique des distributeurs et sorties)
UAoff	Message signalant que la tension de l'actionneur UA est tombée en dessous de la valeur de la tension de coupure des distributeurs. Les distributeurs sont coupés de l'alimentation électrique.
UAon	Message signalant que la tension de l'actionneur UA est tombée en dessous de la valeur de la tension de mise en marche des distributeurs. Les distributeurs ne peuvent pas être mis sous tension.
UL	Tension logique (alimentation électrique du système électronique et des capteurs)

2 Consignes de sécurité

2.1 À propos de ce chapitre

Le produit a été fabriqué selon les règles techniques généralement reconnues. Des dommages matériels et corporels peuvent néanmoins survenir si ce chapitre de même que les consignes de sécurité de la présente documentation ne sont pas respectés.

1. Lire la présente documentation attentivement et dans son intégralité avant d'utiliser le produit.
2. Conserver cette documentation de sorte que tous les utilisateurs puissent y accéder à tout moment.
3. Toujours transmettre le produit à des tiers, accompagné de la documentation nécessaire.
4. Respecter la norme ISO 4414 sur la manipulation sûre des composants de transmission pneumatique.

2.2 Qualification du personnel

Les opérations décrites dans cette documentation exigent des connaissances électriques et pneumatiques de base, ainsi que la connaissance des termes techniques qui y sont liés. Afin d'assurer une utilisation en toute sécurité, ces travaux ne doivent par conséquent être effectués que par des techniciens dans ces domaines ou par une personne initiée mais restant sous la direction d'un technicien.

Un technicien est une personne qui, en raison de sa formation, de ses connaissances et de son expérience ainsi que de sa connaissance des dispositions en vigueur, est capable d'évaluer les travaux qui lui sont confiés, de détecter les risques potentiels et de prendre les mesures de sécurité qui s'imposent. Une personne qualifiée doit se conformer aux règles techniques pertinentes.

2.3 Utilisation dans des chaînes de commande importantes pour la sécurité

Les coupleurs de bus et pilotes de distributeurs ne doivent être utilisés pour la fonction de sécurité « **fonction d'arrêt de sécurité et autres fonctions de sécurité, introduites par un dispositif de protection** » dans des chaînes de commande de sécurité que si l'installation complète est conçue à cet effet.

3 Îlot de distribution AV dans une chaîne de commande de sécurité

3.1 Introduction générale (exclusion de la responsabilité)

Les exemples cités dans ces instructions représentent un extrait d'une commande importante pour la sécurité. Ces exemples montrent les principes et non tous les composants nécessaires. D'autres composants et évaluations peuvent être requis en cas d'utilisations dans des machines. Les indications ne dispensent pas l'utilisateur d'une évaluation et d'une vérification personnelles. Il convient de tenir compte du fait que nos produits sont soumis à un processus naturel d'usure et de vieillissement.

3.2 Processus pour une machine fiable : l'appréciation du risque

L'appréciation du risque

- doit être réalisée par le constructeur de la machine qui conserve les résultats
- doit prendre en compte l'utilisation conforme, mais aussi un mauvais usage raisonnablement prévisible de la machine
- constitue pour les constructeurs de machines une preuve importante en cas d'éventuelles revendications suite à un accident

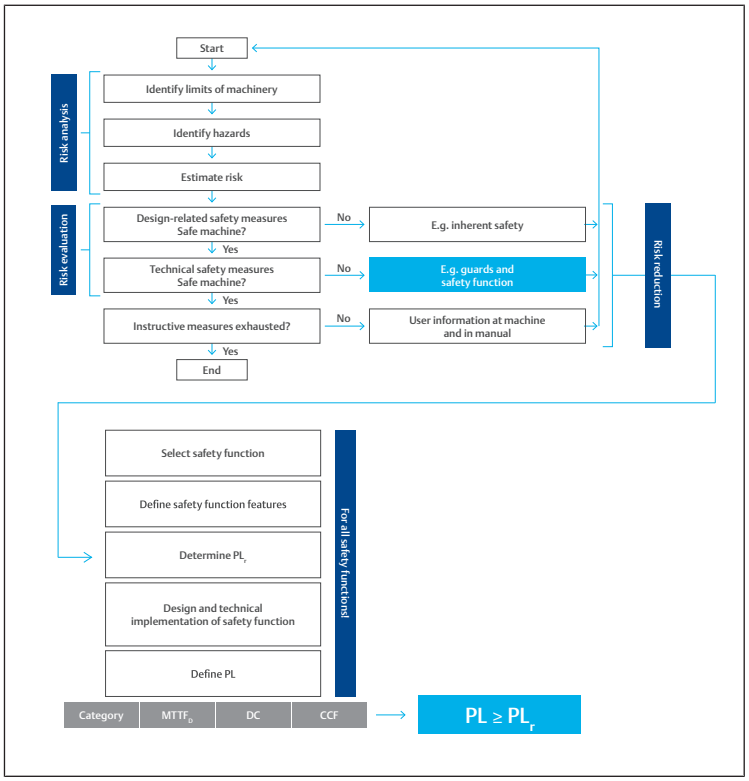


Fig. 1: Processus d'appréciation du risque et définition du PL_r

Concernant le processus d'appréciation du risque, nous nous concentrerons dans ces instructions sur la mise en place de mesures de protection techniques assurant une diminution du risque, sur l'analyse de la fonction de sécurité ainsi que sur la détermination de son niveau de performance. La figure vous montre le processus requis pour l'évaluation du risque. Déterminé en fonction de l'architecture de la commande (catégorie), du temps moyen avant défaillance dangereuse ($MTTF_D$), du taux de couverture de diagnostic (DC) et des défaillances de cause commune (CCF), le niveau de performance (PL) doit au moins équivaloir au niveau de performance requis (PL_r).

3.3 Informations relatives aux exemples

Les trois exemples suivants montrent :

- Exemple 1 : risque dû à un démarrage inattendu, PL_r = e
- Exemple 2 : risque dû à un démarrage inattendu, à une énergie cinétique résiduelle PL_r = c
- Exemple 3 : risque dû à un démarrage inattendu, PL_r = d avec exclusion des défauts

3.3.1 Systématique des exemples

La systématique des exemples s'appuie sur le code d'identification de parties des fonctions de sécurité mentionnées dans le projet VDMA 66416:2016-01.

La description générale est la suivante :

Remarque préliminaire

Description des conditions périphériques :

- type de machine, mode de fonctionnement, ...
- Risque dû à ...
- Paramètres de risque selon DIN EN ISO 13849-1:2016-06
- PL_r

Mesures techniques de commande (fonctions de sécurité) et autres mesures en vue de la réduction du risque :

- Nom de la fonction de sécurité
- Nom de la fonction de sécurité
- ...

Entrée

Événement déclencheur :

- interrogation sur les états et les dispositifs de sécurité et
- surveillance des événements
  Exemples : dispositif de validation, arrêt d'urgence, interrupteur de sécurité, contacteur à clé,
- barrière lumineuse, manostat de sécurité, ...

Logique

Évaluation de la fonction de sécurité :

- coupure des apports en énergie, relais de sécurité, API de sécurité

Sortie

Réaction de sécurité :

- Exemples : distributeurs de fluide, protections, régulateurs, freins, ...

3.3.2 Mesures de protection techniques

Lorsque la sécurité d'une machine dépend du fonctionnement correct d'une commande, on parle de « sécurité fonctionnelle ». La priorité est donnée aux parties « actives » de la commande, c'est-à-dire aux composants capables d'identifier les situations dangereuses (détection de signaux, « I »= Input), d'y réagir de manière adaptée (analyse, « L » = Logique) et de mettre en œuvre des mesures fiables (exécution, « O »= Output). La notion de « commande » englobe donc l'ensemble du système de traitement des signaux.

Les « parties du système de commande relatives à la sécurité » (SRP/CS) ne sont pas obligatoirement des « modules de sécurité » au sens de la directive Machines. Les SRP/CS (Safety Related Part of a Control System) peuvent cependant inclure des modules de sécurité tels que commandes bimanuelles ou unités logiques avec fonction de sécurité. Les entraînements (vérins), l'alimentation en énergie (telle qu'alimentation en pression ou unité de traitement de l'air) et les connexions n'entrent pas directement en ligne de compte dans l'estimation des probabilités de défaillances dangereuses.

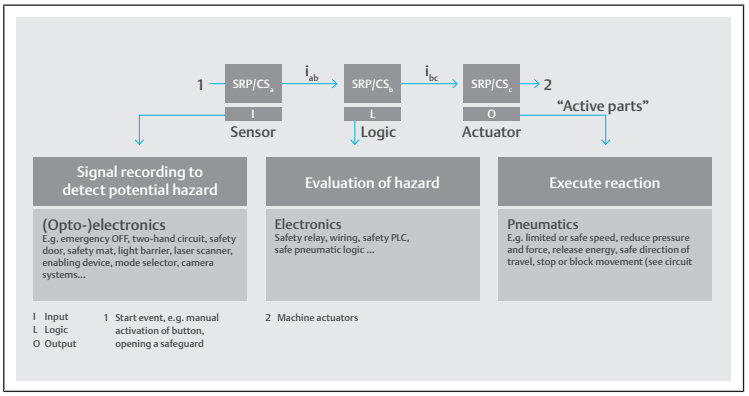


Fig. 2: Concentration sur les parties d'une commande relatives à la sécurité (SRP/CS selon la norme ISO 13849-1)

3.4 Exemple 1 avec PLr = e

Exemple 1, d'après VDMA 66416:2016-01, Numéros 2.1.1.1 et 2.2.1.1

Remarque préliminaire

Description des conditions périphériques :

- Mode de fonctionnement : automatique (BA1)
- Temps de cycle de la machine : 5 à 15 secondes
- Risque dû à un démarrage inattendu
- PL_r = e

Mesures techniques de commande (fonctions de sécurité) :

- Arrêt sécurisé du couple (STO) ou
- Arrêt sécurisé de l'apport en énergie (SEC)
- Prévention du démarrage inattendu (PUS)

Entrée

Événement déclencheur :

- Barrière lumineuse interrompue ou portes de protection verrouillées ouvertes ou non maintenues fermées

Logique

Évaluation de la fonction de sécurité :

- Arrêt des apports en énergie

Sortie

Réaction de sécurité :

- Coupure de l'apport en énergie fluidique : $PL_r \geq d$ => à 2 canaux
  et de l'apport en énergie électrique : $PL_r \geq d$ => à 2 canaux recommandé

3.4.1 Mise en œuvre de l'exemple 1

Selon ISO 13849, PL = e peut être atteint avec la catégorie 3, si les conditions suivantes sont remplies :

- DC_{avg} = moyen
- MTTF = haut

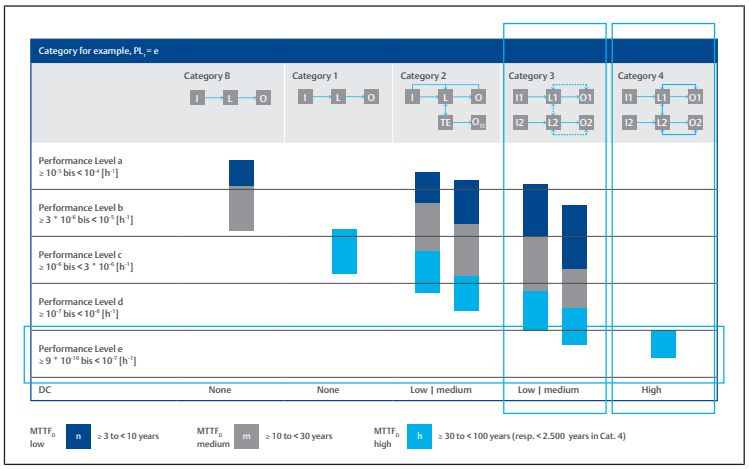


Fig. 3: Mise en œuvre de l'exemple 1 : PL_e avec la catégorie 3, DC = moyen, $MTTF_D$ = haut

Selon l'approche simplifiée de la norme ISO 13849-1, les quatre classes pour le degré de couverture de diagnostic DC sont définies comme suit :

- aucun : DC < 60 %
- faible : 60 % < DC < 90 %
- moyen : 90 % < DC < 99 %
- haut : 99 % < DC

Conception et réalisation technique de la fonction de sécurité

Poste de travail manuel
TM=20 ans
d/a=320 jours
h/d=24 h / durée de cycle min. 10 s = 55.296.000 cycles de commutation pour distributeur d'air de service et principal

En mode réglage, les dispositifs de protection mobiles de coupure doivent être pontés et ouverts et les dispositifs de protection fixes de coupure doivent être montés.

INFO: Un seul défaut n'entraîne pas la perte de la fonction de sécurité. Certains défauts (pas tous) sont détectés. Cependant une accumulation de défauts inconnus peut conduire à la perte de la fonction de sécurité.

Sélection des distributeurs

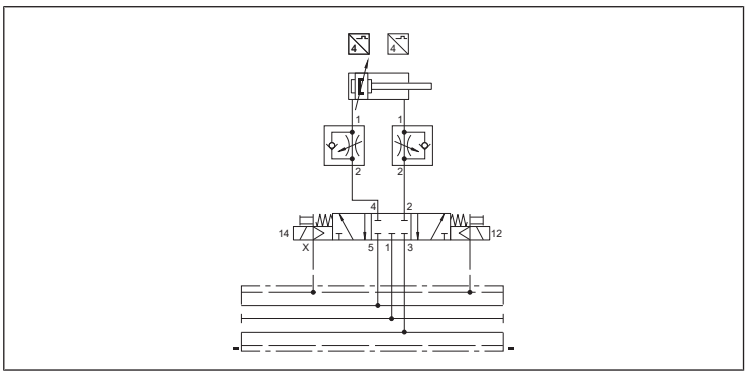


Fig. 4: Schéma de connexion : sélection des distributeurs

- Position de commutation sûre définie à l'état sans courant par ressort mécanique
- Les conduites de pression sont bloquées à l'état sans courant
- Les conduites d'échappement d'air ne sont pas ouvertes
- Le vérin après un ARRÊT D'URGENCE ne peut plus être déplacé, c'est-à-dire que le dégagement de la personne est nécessaire
- Possibilité de freiner les masses qui s'échappent
- Arrêt sécurisé en cas de mouvements verticaux avec des masses (à partir de PL_d seulement avec des mesures supplémentaires -> à 2 canaux)
- Mode JOG possible (course de vérin par impulsions)
- Influence transversale par l'évacuation de l'air des grands vérins voisins impossible
- Adapté jusqu'au niveau de performance PL_e (mesures supplémentaires, voir → Fig. 5.)
- Sens de déplacement dangereux autorisé du vérin vers l'extérieur et vers l'intérieur
- La durée de vie des distributeurs a été testée selon la norme ISO 19973-1 et -2

Commutation de sécurité pneumatique catégorie 3 PL_e

Désignation :
Prévention d'un démarrage inattendu (Prevention of unexpected start-up, PUS) selon la fiche unifiée VDMA 24584.

Blocage des débits volumétriques entrant et sortant des deux chambres de piston.

INFO: À noter au redémarrage :
Les chambres de vérin peuvent purger l'air en raison de fuites de certains composants.

INFO: Des impulsions de contrôle peuvent entraîner la commutation des distributeurs.

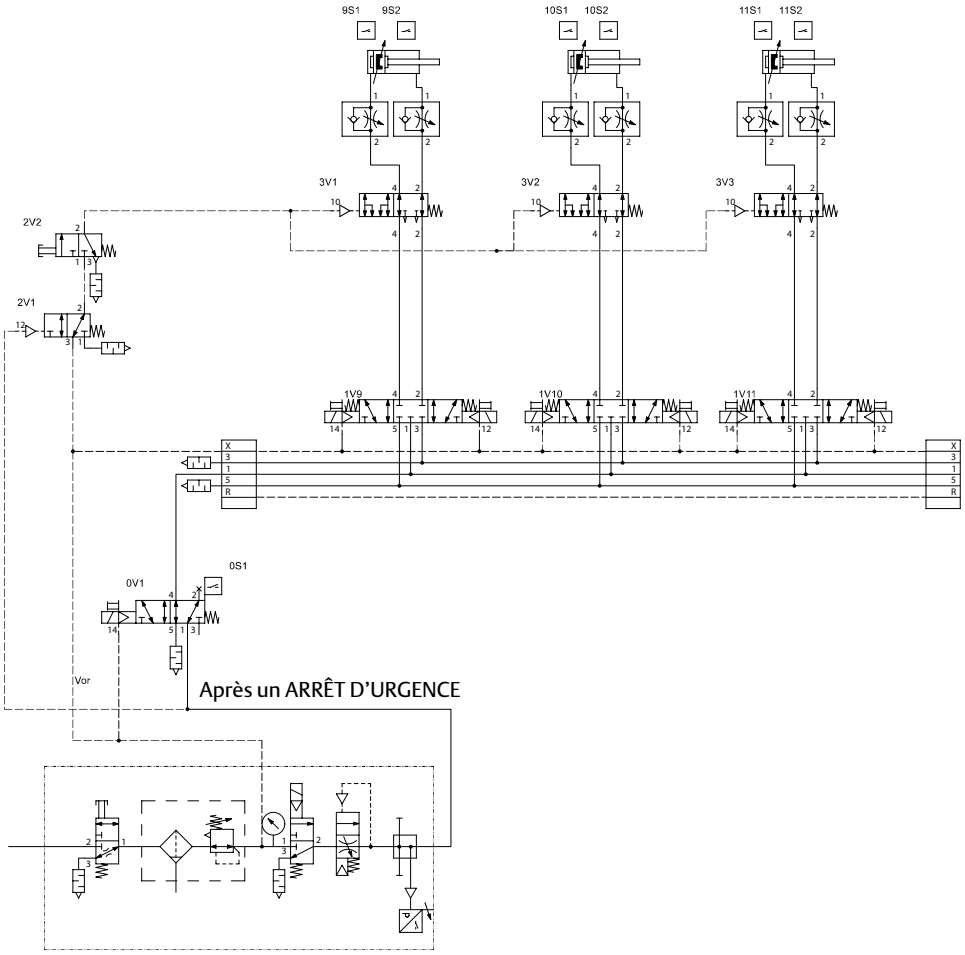


Fig. 5: Schéma de principe : canaux de fonction et de test

INFO: En cas de ventilation / d'échappement simultanée de plus de 8 distributeurs, veiller à une ventilation / un échappement supplémentaire par le biais de plaques d'alimentation.

Dégagement de la personne par la purge (pour les circuits avec maintien de position)

Pour mouvements verticaux et horizontaux :

- Gravité de la blessure = S2 (blessure généralement irréversible, décès inclus)
- La zone dangereuse se situe dans le périmètre accessible
- l'opérateur n'est pas en mesure de se dégager lui-même
- la purge ne doit pas occasionner de danger supplémentaire

Le dégagement de la personne peut être réalisé seulement dans les conditions suivantes :

- Uniquement à l'état hors pression
- Après arrêt d'urgence actif par 2V1 (un 2V1 peut alimenter plusieurs 2V2), celui-ci doit être monté à proximité de la zone dangereuse
- Prévoir un dégagement de personne commun pour des groupes de vérins (un 2V2 peut purger plusieurs vérins)

Schéma de principe

La figure suivante montre le schéma fonctionnel de sécurité pour l'exemple 1.

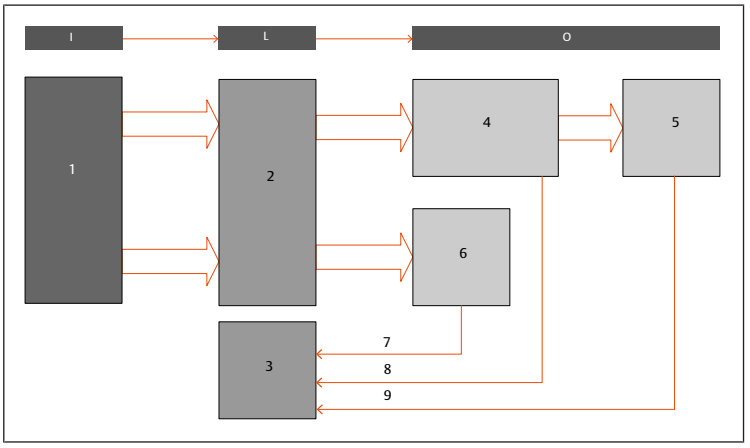


Fig. 6: Schéma fonctionnel de sécurité, exemple 1

1 Interrupteur de porte de protection (par ex. BOUTON CHAMPIGNON PSEN cs3.1 ou PSEN sl-0.5p 1.1)

2 Module de sécurité (par ex. BOUTON CHAMPIGNON PNOZ)

3 API (Automate programmable industriel)

4 Partie électrique de l'îlot de distribution AV alimentation UA via une plaque d'alimentation électrique

5 Partie pneumatique de l'îlot de distribution AV

6 Distributeur d'air principal avec interrogation sur la position du tiroir (par ex. IS12-PD)

7 Diagnostic « Interrogation de la position du tiroir du distributeur d'air principal »

8 Message de diagnostic « La tension de distributeur UA est inférieure à la tension d'arrêt (UA < UAoff) »

9 Diagnostic « Interrogation indirecte du distributeur de service »

Schéma de connexion pneumatique

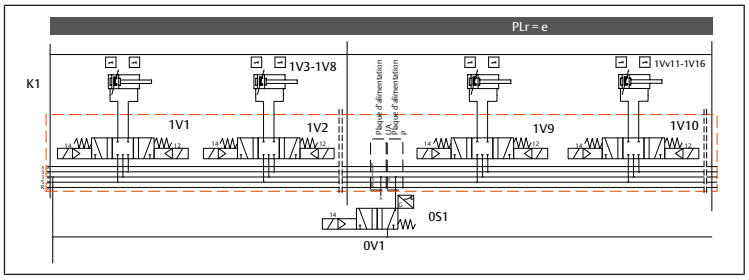


Fig. 7: Schéma de connexion pneumatique, exemple 1

K1	Système de distributeurs	1V1 – 1V8	Distributeurs en dehors de la chaîne de commande de sécurité
1V3 – 1V8	Non représenté	1V9 – 1V16	Distributeurs pour entraînements avec PL_r = e
1V1 – 1V16	Non représenté	0S1	Détection de position de 0V1
0V1	Distributeur d'air principal		

Îlot de distribution complet avec composants externes

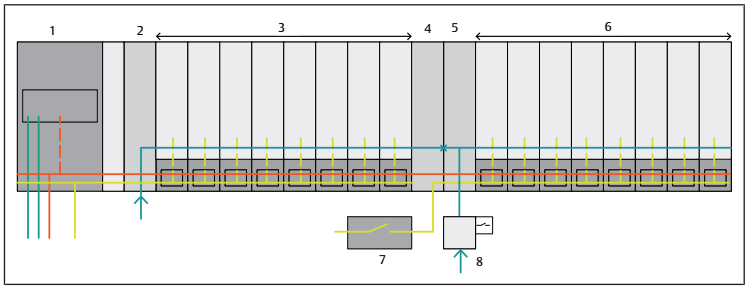


Fig. 8: Îlot de distribution et composants externes

1 Coupleur de bus
2 Plaque d'alimentation pneumatique
3 Distributeurs (pas dans le circuit de sécurité)
4 Plaque d'alimentation électrique - correspond au bloc 4 dans le schéma fonctionnel de sécurité
5 Plaque d'alimentation pneumatique, - pas de surveillance (UAoff) requise, pas de circuit électronique intégré
6 Distributeurs (circuit de sécurité) - correspond au bloc 5 dans le schéma fonctionnel de sécurité - la partie électrique des distributeurs (pilotes de distributeurs) correspond au bloc 4 dans le schéma fonctionnel de sécurité
7 Module de sécurité, correspond au bloc 2 dans le schéma fonctionnel de sécurité
8 Le distributeur d'air principal correspond aux blocs 6 et 7 dans le schéma fonctionnel de sécurité

3.4.2 Fonctions de sécurité

Prévention de sécurité du démarrage inattendu à partir de la position de repos, avec option de dégagement de la personne.

La présente documentation ne montre que la partie de commande pneumatique comme sous-système. Pour la réalisation de la fonction de sécurité complète, d'autres parties du système de commande relatives à la sécurité (tels que les moyens de protection et la logique électrique) doivent être prises en compte en tant que sous-systèmes.

- Gravité de la blessure = S2
- La zone dangereuse se situe dans le périmètre accessible et l'opérateur ne peut pas se dégager lui-même
- la purge ne doit pas occasionner de danger supplémentaire
- étant donné que les dégagements de personne 2V1, 2V2, 3V1 et 3Vn après l'arrêt d'urgence, c'est-à-dire après la purge du distributeur 3/2 dans l'unité de traitement d'air sont entièrement fonctionnels et n'ont aucune influence sur la fonction de sécurité, ils ne sont pas pris en compte dans le calcul.

Cela ne peut être réalisé que dans les conditions suivantes :

- Uniquement à l'état hors pression
- Après arrêt d'urgence actif par 2V1 (un 2V1 peut alimenter plusieurs 2V2), celui-ci doit être monté à proximité de la zone dangereuse
- Prévoir un dégagement de personne commun pour des groupes de vérins (un 2V2 peut purger plusieurs vérins)

Description fonctionnelle de la commutation PL c, d, e_Kat-3_02 en cas d'utilisation dans un poste de travail manuel

- Les mouvements sont commandés de manière redondante par le distributeur d'air principal 0V1 et le distributeur de service 1Vn
- Le distributeur 0V1 doit être commandé en permanence pour que 1Vn puisse être commandé
- Un défaut unique de l'un des distributeurs mentionnés n'entraîne pas la perte de la fonction de sécurité
- tous les distributeurs sont commandés de manière cyclique dans le process
- la fonction du distributeur d'air principal 0V1 est surveillée par une interrogation de la position du distributeur 0S1
- la fonction du distributeur de service 1Vn est détectée indirectement par les commutateurs nS1 et nS2 pendant le process
- l'accumulation de défauts non détectés peut entraîner la perte de la fonction de sécurité
- en cas de risque lié à l'énergie accumulée (pression, masse, ressort), des mesures supplémentaires sont nécessaires

Caractéristiques de construction

- Les principes de sécurité fondamentaux et éprouvés ainsi que l'exigence de la catégorie B sont respectés
- Le distributeur d'air principal 0V1 est placé dans la position de commutation sûre par un ressort
- Le distributeur de service nV1 a une position centrale bloquée (sans chevauchement) avec centrage du ressort
- la position de commutation sûre est atteinte aux deux distributeurs après suppression de la tension de commande
- le traitement du signal des interrogations sur les distributeurs et des surveillances s'effectue dans une commande API à 1 canal
- Commande ON et porte de chargement fermée :
  - le distributeur d'air principal 0V1 est activé et la tension est présente à l'îlot de distribution
- Mode automatique ON et porte de chargement ouverte :
  - pas de tension au distributeur d'air principal 0V1 et à l'îlot de distribution
- Mode réglage et porte de protection pontée avec interrupteur à clé :
  - pas de tension au distributeur d'air principal 0V1 et à l'îlot de distribution
  - la conduite pneumatique entre le distributeur d'air principal 0V1 et le distributeur de travail nV1 est purgée
  - les mouvements sont possibles uniquement avec un interrupteur de validation supplémentaire
  - l'interrupteur de validation commute le distributeur d'air principal 0V1 et la tension est présente à l'îlot de distribution
  - Les mouvements dangereux sans mesures supplémentaires justifiées ne sont autorisés que lorsque la porte de protection est fermée

Calcul de la probabilité d'une défaillance et durée de vie

Durée de vie exigée :
20 ans / 320 jours / 24 h / temps de cycle de 10 sec. (nop = 2764800 cycles/an)

- Distributeur 0V1 B_{10D} = 79,2 M (IS12-PD)
- Distributeur nV1 B_{10D} = 39,6 M (AV05) ou distributeur nV1 B_{10D} = 105,8 M (AV03)

3.4.3 Calcul du MTTF pour les parties électrique et pneumatique de l'îlot de distribution

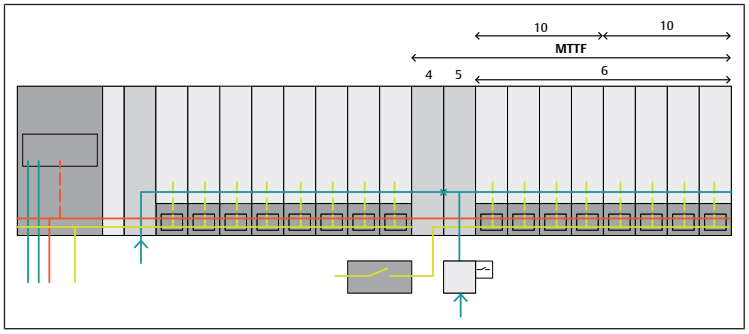


Fig. 9: Composants importants pour le calcul du $MTTF_D$ de la partie électrique

4 Plaque d'alimentation électrique avec surveillance UAon, correspond au bloc 4 dans le schéma fonctionnel de sécurité

5 Plaque d'alimentation pneumatique avec surveillance UAoff, la fonction électrique = surveillance UAoff correspond aux blocs 4 et 8 dans le schéma fonctionnel de sécurité

6 Distributeurs (circuit de sécurité) correspond au bloc 5 dans le schéma fonctionnel de sécurité la partie électrique des distributeurs (pilotes de distributeurs) correspond au bloc 4 dans le schéma fonctionnel de sécurité

10 Quadruple platine pilote de distributeurs

Voir → 6. Indicateurs de fiabilité et → Fig. 9

Il en résulte :

- Plaque d'alimentation électrique (**4**) MTTF = 854 ans
- Surveillance UAoff (**5**) MTTF = 1094 ans
- Quadruple platine pilote de distributeurs (**10**) MTTF = 630 ans
- Distributeurs AV03 5/3 rappel par ressort (**6**) MTTF = 382,7 ans

$$MTTF_{ges} = \frac{1}{\frac{1}{854\ [a]} + \frac{1}{1094\ [a]} + \frac{1}{630\ [a]} + \frac{1}{630\ [a]} + \frac{1}{382{,}7\ [a]}} = 127\ [a]$$

Les valeurs MTTF des modules AES ont été calculées à l'aide des taux de défaillance figurant dans une base de données.

Selon DIN EN 13849-1, Annexe C, chaque défaillance n'est pas considérée comme une défaillance dangereuse. Dans ce cas, on peut définir $MTTF_D = 2 \times MTTF_{ges}$ pour le calcul de l'ensemble du système.

$MTTF_D = 2x\ MTTF_{ges} = 2 \times 127\ [a] = 254\ [a]$

3.4.4 Diagnostic

La plaque d'alimentation pneumatique surveille la tension de l'actionneur UA et envoie le bit de diagnostic UAoff, lorsque UA n'atteint pas la tension d'arrêt.

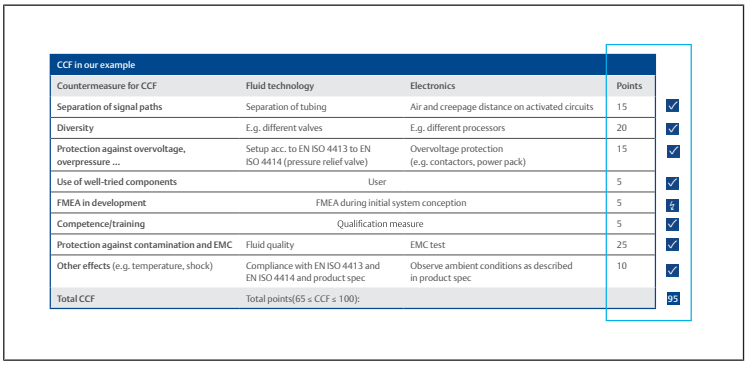
La plaque d'alimentation électrique surveille la tension de l'actionneur UA et envoie le bit de diagnostic UAon, lorsque UA n'atteint pas la tension de mise en marche.

Le bit de diagnostic (UAoff) doit être surveillé. Pour cela, un changement de signal est nécessaire, réalisé par ex. à la mise en marche de la machine ou par des cycles tests spécifiques.

Interrogation directe de la fonction de la position du tiroir sur le distributeur principal 99 %.

Interrogation indirecte de la fonction du distributeur de service 90 %.

DC = 94,4 % $MTTF_D$ = haut (100 J) CCF = 95



CCF in our example			
Countermeasure for CCF	Fluid technology	Electronics	Points
Separation of signal paths	Separation of tubing	Air and creepage distance on activated circuits	15
Diversity	E.g. different valves	E.g. different processors	20
Protection against overvoltage, overpressure ...	Setup acc. to EN ISO 4413 to EN ISO 4414 (pressure relief valve)	Overvoltage protection (e.g. contactors, power pack)	15
Use of well-tried components	User		5
FMEA in development	FMEA during initial system conception		5
Competence/training	Qualification measure		5
Protection against contamination and EMC	Fluid quality	EMC test	25
Other effects (e.g. temperature, shock)	Compliance with EN ISO 4413 and EN ISO 4414 and product spec	Observe ambient conditions as described in product spec	10
Total CCF	Total points(65 ≤ CCF ≤ 100):		95

Fig. 10: Exemple : CCF - Défaillance de cause commune

Niveau de performance = PL_e / Catégorie = 3

Remplacement du distributeur d'air principal 0V1 (IS12-PD) non requis.

Remplacement du distributeur nV1 (AV03) non requis.

Remplacement du distributeur nV1 (AV05) après 14,3 ans - avec un temps de cycle ≥ 14 sec. non requis ou durée d'utilisation 20 ans.

3.4.5 Vérification du bit de diagnostic

Pour une description détaillée de la surveillance, se reporter au chapitre → 3.11 Description de la surveillance UAoff / UAon.

Lorsque la tension UA est coupée, aussi bien le message de diagnostic UAon que UAoff doit être envoyé.

Tab. 3: Vérification du bit de diagnostic

UA = 0, coupée	Diagnostic de mise en marche UAon	Diagnostic d'arrêt UAoff
valide	1	1
non valide	1	0
non valide	0	1

Lorsque les conditions précitées sont prises en compte, les données des normes suivantes permettent d'estimer la surveillance de la tension de distributeur coupée avec un DC = 90 % à < 99 % (moyen) :

- DIN EN ISO 13849-1 Annexe E : « Estimations pour la couverture du diagnostic (DC) pour les fonctions et les modules »
- DIN EN 61508-2 : « Tableau A.14 – Actionneurs »
- DIN EN 61508-2 : « Tableau A.7 – Unités E/S et interfaces (communication externe) »

3.5 Exemple 2 avec PLr = c

Exemple 2, d'après 66416:2016-01, Numéros 1.1.2.1 et 2.1.2.3

Remarque préliminaire

Description des conditions périphériques :

- Mode de fonctionnement BA2 mode réglage ou service
- Risque dû à un démarrage inattendu, à une énergie cinétique résiduelle
- $PL_r = c$

Mesures techniques de commande (fonctions de sécurité) (voir remarque) :

- Arrêt sécurisé du couple (STO)
- Arrêt sécurisé de l'apport en énergie (SEC)
- Prévention du démarrage inattendu (PUS)

Entrée

Événement déclencheur :

- Sélecteur de mode de fonctionnement, dispositif de validation

Logique

Évaluation de la fonction de sécurité :

- Arrêt des apports en énergie

Sortie

Réaction de sécurité :

- Arrêt à 1 canal du média fluidique. Les mises en œuvre suivantes sont possibles :
  - Distributeur en position d'arrêt
  - Commande de valve(s) de blocage

– S1 possible, car l'énergie résiduelle n'entraîne que des blessures réversibles

- Coupure de l'apport en énergie électrique : $PL_r \geq d$ => à 2 canaux recommandé

Remarque

Le thème de l'énergie résiduelle est abordé plus en détail dans les documents suivants :

- Projet VDMA 66416 : chapitre 5.1.3 Mode réglage / mode service (BA2) « Des vitesses réduites sont à prévoir comme suit ... »
- Projet VDMA 66416 : Tableau A2 - Code d'identification des estimations des paramètres du graphique de risque du tableau A7

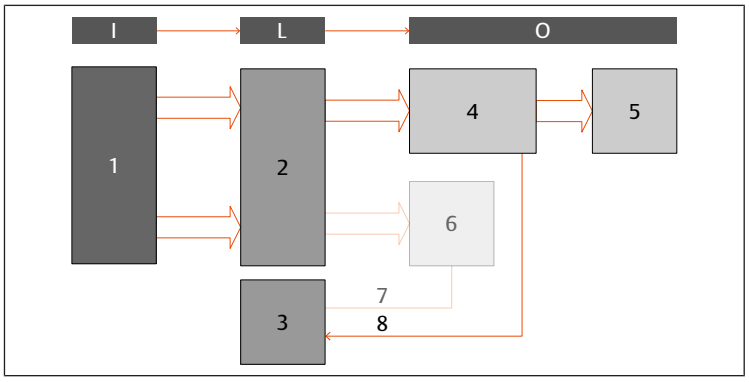


Fig. 11: Schéma fonctionnel de sécurité, exemple 2

1 Dispositif de validation
2 Module de sécurité (par ex. BOUTON CHAMPIGNON PNOZ)
3 API (Automate programmable industriel)
4 Partie électrique de l'îlot de distribution AV, alimentation UA via une plaque d'alimentation électrique
5 Distributeurs de l'îlot de distribution AV
6 Distributeur d'air principal avec interrogation sur la position du tiroir (par ex. IS12-PD, ...)
pas actif pour cette fonction de sécurité
7 Diagnostic « Interrogation de la position du tiroir du distributeur d'air principal »
pas actif pour cette fonction de sécurité
8 Diagnostic « La tension de distributeur UA est inférieure à la tension d'arrêt (UA < UAoff) »

3.6 Exemple 3 avec PLr = d

Exemple 3, d'après VDMA 66416, numéros 2.1.1.1 et 2.2.1.1

Cet exemple est similaire à l'exemple 1, le PL_r exigé est cependant d.

Remarque préliminaire

Description des conditions périphériques :

- Mode de fonctionnement automatique (BA1)
- Risque dû à un démarrage inattendu
- $PL_r = d$

Mesures techniques de commande (fonctions de sécurité) :

- Arrêt sécurisé du couple (STO)
- Arrêt sécurisé de l'apport en énergie (SEC)
- Prévention du démarrage inattendu (PUS)

Entrée

Événement déclencheur :

- Barrière lumineuse interrompue ou portes de protection verrouillées ouvertes ou non maintenues fermées

Logique

Évaluation de la fonction de sécurité :

- Arrêt des apports en énergie

Sortie

Réaction de sécurité :

- Coupure de l'apport en énergie fluidique : $PL_r \geq d$ => à 2 canaux et de l'apport en énergie électrique : $PL_r \geq d$ => à 2 canaux recommandé

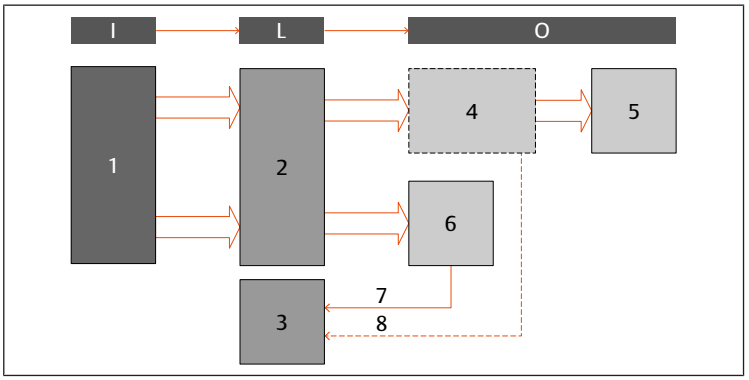


Fig. 12: Schéma fonctionnel de sécurité, exemple 3

1 Interrupteur de porte de protection (par ex. BOUTON CHAMPIGNON PSEN cs3.1 ou PSEN sl-0.5p 1.1)
2 Module de sécurité (par ex. BOUTON CHAMPIGNON PNOZ)
3 API (Automate programmable industriel)
4 Partie électrique de l'îlot de distribution AV
Soit alimentation UA par plaque d'alimentation électrique. Une exclusion des défauts est possible pour ce bloc (voir → 3.6.1 Exclusion des défauts).
Soit alimentation UA par coupleur de bus. Aucune exclusion des défauts possible (voir → 3.6.2 Aucune exclusion des défauts).
5 Distributeurs de l'îlot de distribution AV
6 Distributeur d'air principal avec interrogation sur la position du tiroir (par ex. IS12-PD, ...)
7 Diagnostic « Interrogation de la position du tiroir du distributeur d'air principal »
8 Diagnostic « La tension de distributeur UA est inférieure à la tension d'arrêt (UA < UAoff) »
Si une exclusion des défaut est utilisée pour (**4**), ce diagnostic n'est pas requis.

3.6.1 Exclusion des défauts

Si l'îlot de distribution est conçu et utilisé comme décrit dans les chapitres suivants, le circuit électronique de distribution ne doit pas être inclus dans le calcul des valeurs MTTF d'une chaîne de commande de sécurité.

La condition préalable pour l'utilisation de l'exclusion des défauts est

- qu'au maximum PL d soit applicable (PL e doit être calculé comme dans l'exemple 1),
- que l'îlot de distribution soit conçu avec une ou plusieurs plaques d'alimentation électriques,
- que les distributeurs devant être coupés soient alimentés par ces plaques d'alimentation électriques,
- que les plaques d'alimentation électriques soient câblées conformément aux concepts de câblage 1-3,
- que le câble de raccordement de la plaque d'alimentation ne contienne que la tension d'alimentation 24 V UA,
- que le câble soit conçu conformément à la norme DIN EN 60204.

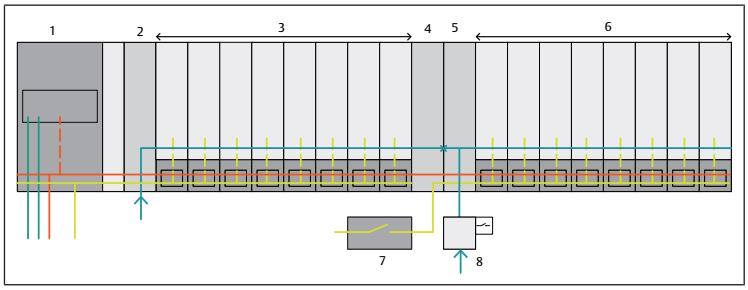


Fig. 13: Îlot de distribution et composants externes

1 Coupleur de bus
2 Plaque d'alimentation pneumatique
3 Distributeurs (pas dans le circuit de sécurité)
4 Plaque d'alimentation électrique - correspond au bloc 4 dans le schéma fonctionnel de sécurité
5 Plaque d'alimentation pneumatique, - pas de surveillance (UAoff) requise, pas de circuit électronique intégré
6 Distributeurs (circuit de sécurité) - correspond au bloc 5 dans le schéma fonctionnel de sécurité - la partie électrique des distributeurs (pilotes de distributeurs) correspond au bloc 4 dans le schéma fonctionnel de sécurité
7 Module de sécurité, correspond au bloc 2 dans le schéma fonctionnel de sécurité
8 Le distributeur d'air principal correspond aux blocs 6 et 7 dans le schéma fonctionnel de sécurité

3.6.2 Aucune exclusion des défauts

Si l'alimentation UA est assurée par un coupleur de bus, aucune exclusion des défauts n'est possible. La probabilité d'une défaillance doit être calculée.

Autres mesures :

- L'alimentation UA via le coupleur de bus doit être coupée de façon sûre afin d'éviter toute commutation inattendue des distributeurs.
- Les câbles doivent être posés selon la norme DIN EN 60204.
- Le diagnostic du coupleur de bus (UAon et UAoff) doit être évalué.

Selon le niveau de performance requis, d'autres mesures doivent être prises.

3.7 Vue d'ensemble des différentes possibilités d'alimentation

Tab. 4: Différentes possibilités d'alimentation

	Alimentation UA par coupleur de bus	Alimentation UA par plaque d'alimentation électrique
PL_r maximal pouvant être atteint	d (e non recommandé)	e
Exclusion des défauts possible	Non Voir → 3.6.2 Aucune exclusion des défauts	$PL_r \leq$ d : oui PL_r = e : non
Évaluation du diagnostic	Oui (UAon et UAoff du coupleur de bus)	$PL_r \leq$ d : non (non requis en raison de l'exclusion des défauts) PL_r = e : oui (UAon et UAoff) La plaque d'alimentation pneumatique doit être équipée d'une surveillance UAoff.
CC	90 % ... < 99 %	90 % ... < 99 %
Limitation du courant de démarrage	Oui	Oui
Test possible (test croisé)	Non	Oui

Limitation du courant de démarrage

Le courant de démarrage très élevé de l'unité, comme c'est normalement le cas pour les charges capacitives, est limité à une valeur de 5 A maximum.

Définition de l'impulsion de test

Une impulsion de test est une modification limitée dans le temps d'un niveau de tension de signal pour vérifier le bon fonctionnement de la sortie ou de l'appareil ou pour contrôler le parcours de transmission.
[Source : ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V., document de position « Classification des interfaces binaires 24 V avec test dans le domaine de la sécurité fonctionnelle »]

Test possible

Des sorties et/ou des modules de sécurité sûr(e)s génèrent des signaux d'horloge ou des impulsions de test à leurs sorties. Lorsqu'une telle sortie est connectée à la plaque d'alimentation électrique, il n'y a pas d'interprétation erronée du test de connexion croisée. Si une telle sortie est utilisée pour l'alimentation UA sur le coupleur de bus, cela entraîne une interprétation erronée du test de connexion croisée.

Remarque

Seul le parcours de transmission jusqu'à la plaque d'alimentation électrique peut être contrôlé.

3.8 Affectation des tensions d'alimentation dans l'îlot de distribution

La figure suivante montre l'affectation des tensions d'alimentation aux fonctions à l'intérieur de l'îlot de distribution.

- La tension d'alimentation **UL** alimentée au coupleur de bus (**1**) alimente tout le circuit électronique de l'îlot de distribution.
- La tension d'alimentation **UA** alimentée au coupleur de bus alimente les sorties du module DO (**6**) (sortie numérique, digital output) et tous les distributeurs entre le coupleur de bus et l'alimentation UA.

Le composant « plaque d'alimentation électrique » (**5**) interrompt la tension d'alimentation entrante **UA**. Pour tous les distributeurs situés à droite de la plaque d'alimentation électrique, c'est la tension d'alimentation de ce composant qui est utilisée. Le composant « Plaque d'alimentation électrique » peut être utilisé plusieurs fois dans la zone des distributeurs.

La tension **UL** est en principe isolée galvaniquement de la tension **UA** dans l'îlot de distribution.

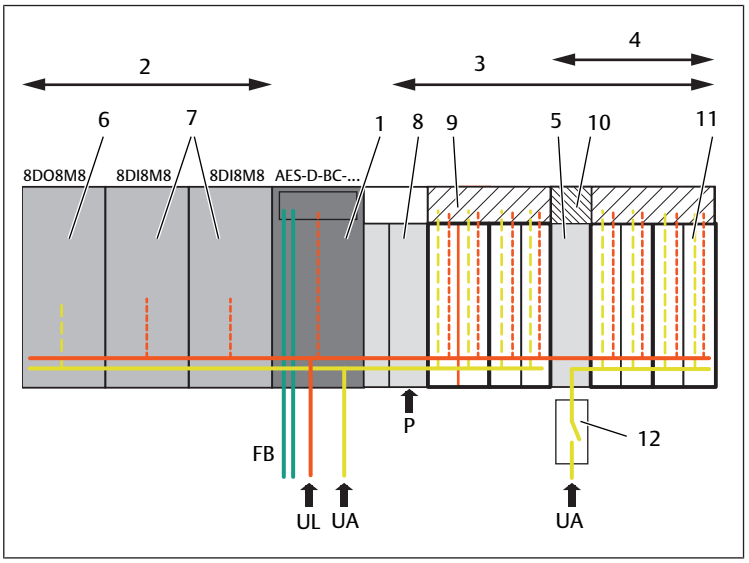


Fig. 14: Affectation des tensions d'alimentation UL et UA

1 Coupleur de bus
2 Modules E/S
3 Zone des distributeurs
4 Partie de la chaîne de commande de sécurité
5 Plaque d'alimentation électrique
6 Module de sortie
7 Module d'entrée
8 Plaque d'alimentation pneumatique
9 Quadruple platine pilote de distributeurs
10 Platine d'alimentation
11 Distributeur
12 Module de sécurité
UL Tension d'alimentation 24 V pour l'électronique et la logique
UA Tension d'alimentation 24 V pour les actionneurs
FB Bus de terrain

3.9 Concept de câblage de l'îlot de distribution

Les trois figures ci-dessous montrent les différents concepts de câblage de l'îlot de distribution.

Pour les trois représentations :

- L'alimentation en tension au coupleur de bus (K1) pour **UL** et **UA** s'effectue par connecteur **X1S1**.
- L'alimentation de la tension d'alimentation sûre pour les distributeurs s'effectue en principe via le raccordement de la plaque d'alimentation électrique supplémentaire (**X1S2**) des distributeurs.

Pour les concepts de câblage suivants, on utilise les équipements avec les codes de référence s'appuyant sur la norme EN 81346. Les exemples montrent uniquement l'extrait pertinent de l'alimentation électrique et ne sont pas exhaustifs. Des équipements supplémentaires sont nécessaires pour une utilisation à l'intérieur d'une machine.

Voir → Fig. 14. Un bloc d'alimentation commun (**L01**) est utilisé dans le schéma de connexion pour les deux tensions **UL** et **UA**. La tension pour les distributeurs au raccord **X1S2** est coupée de manière bipolaire (c'est-à-dire **UA+** et **UA-**) par le module de sécurité.

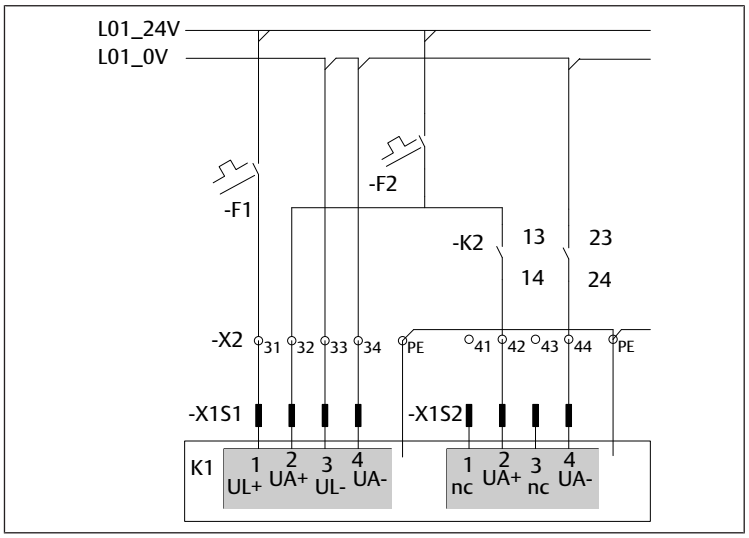


Fig. 15: Concept de câblage 1

-K1	Îlot de distribution avec deux connecteurs pour l'alimentation électrique	**-K2**	Module de sécurité
-X1S1	Raccord pour l'alimentation électrique du coupleur de bus	**-X1S2**	Raccord pour l'alimentation électrique de la plaque d'alimentation électrique
-F1	Protection de la tension **UL**	**-F2**	Protection de la tension **UA**
-X2	Pièce de fixation	**L0x**	Alimentation électrique

Dans l'exemple suivant, deux blocs d'alimentation séparés sont utilisés pour les deux tensions **UL** (**L01**) et **UA** (**L02**). La tension pour les distributeurs au raccord **X1S2** est coupée de manière bipolaire (c'est-à-dire **UA+** et **UA-**) par le module de sécurité.

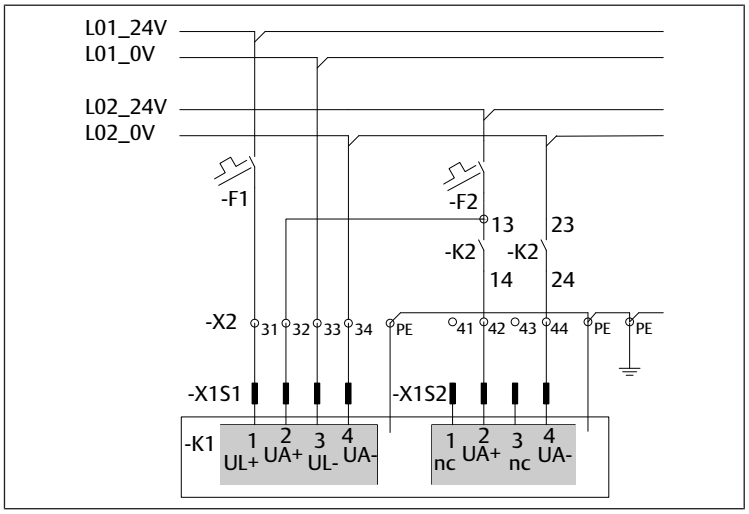


Fig. 16: Concept de câblage 2

-K1	Îlot de distribution avec deux connecteurs pour l'alimentation électrique	**-K2**	Module de sécurité
-X1S1	Raccord pour l'alimentation électrique du coupleur de bus	**-X1S2**	Raccord pour l'alimentation électrique de la plaque d'alimentation électrique
-F1	Protection de la tension **UL**	**-F2**	Protection de la tension **UA**
-X2	Pièce de fixation	**L0x**	Alimentation électrique

Dans l'exemple suivant, un bloc d'alimentation commun (**L01**) est utilisé pour les deux tensions **UL** et **UA**. La tension pour les distributeurs au raccord **X1S2** est coupée de manière unipolaire **UA+** par le module de sécurité.

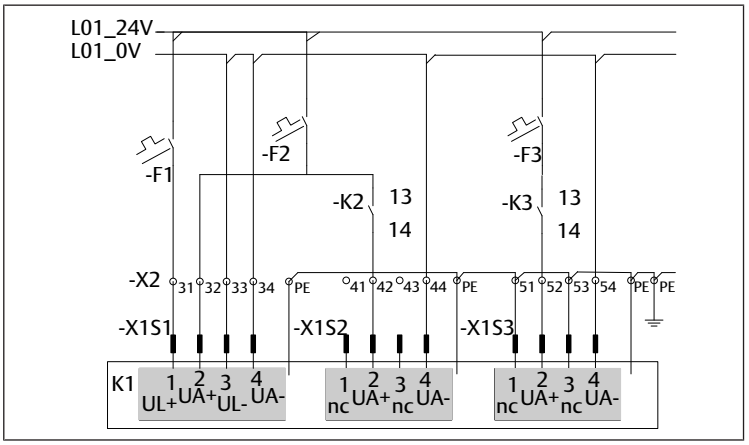


Fig. 17: Concept de câblage 3

-K1	Îlot de distribution avec trois connecteurs pour l'alimentation électrique	**-K2**	Module de sécurité
-X1S1	Raccord pour l'alimentation électrique du coupleur de bus	**-X1S2**	Raccord pour l'alimentation électrique de la plaque d'alimentation électrique
-X1S3	Raccord pour l'alimentation électrique de la plaque d'alimentation électrique	**-F1**	Protection de la tension **UL**
-F3	Protection de la tension **UA**	**-F2**	Protection de la tension **UA**
-K3	Module de sécurité	**-X2**	Pièce de fixation
L0x	Alimentation électrique		

3.10 Remarques sur le câblage

Pour l'utilisation des concepts de câblage susmentionnés, il convient de tenir compte des remarques suivantes :

1. Raccordez l'îlot de distribution comme représenté dans les trois concepts de câblage.
2. Assurez-vous que les distributeurs devant être coupés de manière sûre se trouvent en aval de la plaque d'alimentation électrique.
3. Raccordez **X1S2** avec un câble à 2 fils.

En cas d'utilisation d'un câble avec plus de 2 conducteurs, les conditions suivantes doivent être remplies. Voir → Fig. 17 :

- les fils non utilisés sont reliés à PE pour des raisons de CEM
- aucune autre tension présente dans le câble.

En cas de coupure unipolaire de la tension UA, le câble correspondant doit être posé de manière à éviter les courts-circuits transversaux.

3.11 Description de la surveillance UAoff / UAon

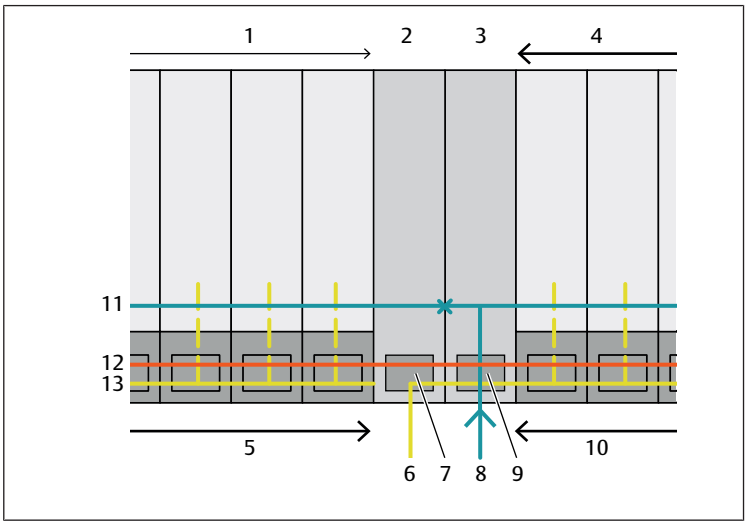


Fig. 18: Image détaillée UAoff / UAon

1 distributeurs précédents
2 plaque d'alimentation électrique
3 plaque d'alimentation pneumatique
4 distributeurs suivants
5 pilotes de distributeurs
6 Tension de l'actionneur UA de la plaque d'alimentation électrique
7 Surveillance UAon dans la plaque d'alimentation électrique
8 Alimentation en air comprimé de la plaque d'alimentation pneumatique
9 Surveillance UAoff dans la plaque d'alimentation pneumatique
10 pilotes de distributeurs
11 Alimentation P existante
12 Tension UL continue
13 Tension UA existante

La plaque d'alimentation électrique (**2**) interrompt l'alimentation UA des distributeurs. Les distributeurs précédents (**1**) sont alimentés par la tension de distribution existante. Les distributeurs suivants (**4**) sont alimentés par la nouvelle tension de distributeur (**6**).

Dans la plaque d'alimentation électrique, la nouvelle tension issue de (**6**) est surveillée à la limite UAon.

Si la tension UA n'atteint pas la tension de mise en marche UAon, la plaque d'alimentation électrique envoie le bit de diagnostic UAon.

La plaque d'alimentation pneumatique (**3**) interrompt l'alimentation P (**11**) des distributeurs. Les distributeurs précédents (**1**) sont alimentés avec l'air comprimé existant. Les distributeurs suivants (**4**) sont alimentés avec de l'air comprimé nouveau (**8**).

Dans la plaque d'alimentation pneumatique, la tension UA existante est surveillée à la limite UAoff.

Si la tension UA n'atteint pas la tension de coupure UAoff, la plaque d'alimentation pneumatique envoie le bit de diagnostic UAoff.

La surveillance de la tension UA dans la plaque d'alimentation pneumatique n'est disponible que si l'îlot de distribution a été configuré en conséquence. La position des bits de diagnostic dans la plage de données pour les commandes est indiquée dans les descriptions correspondantes des coupleurs de bus de la série AES.

4 Transformation et réparation

Vous avez le droit de transformer et de réparer l'îlot de distribution, comme décrit dans les descriptions systèmes des coupleurs de bus AES et des pilotes de distributeurs AV.

▶ Voir également aux chapitres → 2. Consignes de sécurité et → 2.2 Qualification du personnel

5 Données techniques

Les données techniques pour l'îlot de distribution figurent dans les descriptions systèmes correspondantes.

▶ Pour les données nécessaires à la fonction de sécurité, adressez-vous à AVENTICS GmbH (pour l'adresse, voir au dos).

6 Indicateurs de fiabilité

Les explications (concernant les indicateurs de fiabilité ainsi que les informations relatives à l'application de la norme ISO 13849-1) sont également disponibles au téléchargement sur notre site Web : www.emerson.com/de-de/expertise/automation/improving-safety-security/machine-safety.

Les valeurs indiquées dans le tableau correspondent à la version valable à la clôture de la rédaction. Les données sont régulièrement actualisées et peuvent aussi être téléchargées sur notre site Web.

Indice

1 Sulla presente documentazione 35
1.1 Validità della documentazione 35
1.2 Documentazione necessaria e complementare 35
1.3 Presentazione delle informazioni 35
1.3.1 Avvertenze 35
1.3.2 Simboli 35
1.4 Denominazioni 35
1.5 Abbreviazioni 35

2 Indicazioni di sicurezza 35
2.1 Sul presente capitolo 35
2.2 Qualifica del personale 35
2.3 Impiego in catene di comando rilevanti per la sicurezza 35

3 Sistema valvole AV in una catena di comando orientata alla sicurezza 36
3.1 Preambolo generale (responsabilità) 36
3.2 Il processo verso una macchina sicura: la valutazione dei rischi 36
3.3 Informazioni relative agli esempi 36
3.3.1 Sistematica degli esempi 36
3.3.2 Misure tecniche preventive 36
3.4 Esempio 1 con PLr = e 36
3.4.1 Implementazione dell'esempio 1 37
3.4.2 Funzioni di sicurezza 39
3.4.3 Calcolo del MTTF per la parte elettrica e pneumatica del sistema valvole 40
3.4.4 Diagnosi 40
3.4.5 Verifica del bit di diagnosi 40
3.5 Esempio 2 con PLr = c 40
3.6 Esempio 3 con PLr = d 41
3.6.1 Esclusione di guasto 41
3.6.2 Nessuna esclusione di guasto 42
3.7 Panoramica delle diverse possibilità di alimentazione 42
3.8 Assegnazione delle tensioni di alimentazione nel sistema valvole 42
3.9 Principi di cablaggio del sistema valvole 42
3.10 Indicazioni per il cablaggio 43
3.11 Descrizione del monitoraggio UAoff / UAon 43

4 Trasformazione e riparazione 44

5 Dati tecnici 44

6 Parametri di affidabilità 44

1 Sulla presente documentazione

1.1 Validità della documentazione

La presente documentazione è valida per componenti della serie AV utilizzati in catene di comando orientate alla sicurezza. Questa documentazione è indirizzata a programmatori, progettisti elettrotecnici, esperti di pneumatica, personale del Servizio Assistenza e gestori di impianti.

La presente documentazione contiene importanti informazioni per valutare l'esclusione di guasto nei sistemi valvole della serie AV in determinate condizioni.

1.2 Documentazione necessaria e complementare

- ▶ Mettere in funzione i sistemi valvole della serie AV in catene di comando orientate alla sicurezza soltanto se si dispone della documentazione relativa al sistema valvole e ai singoli componenti e dopo aver compreso e seguito le indicazioni.

Tutte le istruzioni di montaggio, le descrizioni del sistema delle serie AES e AV e i file di configurazione del PLC si trovano nel CD R412018133.

1.3 Presentazione delle informazioni

1.3.1 Avvertenze

In queste istruzioni le azioni da eseguire sono precedute da note di avviso, se esiste pericolo di danni a cose o persone. Le misure descritte per la prevenzione di pericoli devono essere rispettate.

Struttura delle avvertenze

⚠ PAROLA DI SEGNALAZIONE

Natura e fonte del pericolo

Conseguenze di una mancata osservanza

- ▶ Precauzioni

Significato delle parole di segnalazione

⚠ PERICOLO

Pericolo immediato per la vita e la salute delle persone.

La mancata osservanza di queste avvertenze causa gravi conseguenze per la salute, inclusa la morte.

⚠ AVVERTENZA

Possibile pericolo per la vita e la salute delle persone.

La mancata osservanza di queste avvertenze può causare gravi conseguenze per la salute, inclusa la morte.

⚠ ATTENZIONE

Possibile situazione pericolosa.

La mancata osservanza di questi avvertimenti può causare lesioni di lieve entità o danni materiali.

NOTA

Possibilità di danni materiali o malfunzionamenti.

La mancata osservanza di questi avvisi può causare danni materiali o malfunzionamenti, ma non lesioni alle persone.

1.3.2 Simboli

Si raccomanda di attenersi al corretto utilizzo dei nostri prodotti.

Rispettare il presente documento al fine di garantire il funzionamento regolare.

1.4 Denominazioni

In questa documentazione vengono utilizzate le seguenti denominazioni:

Tab. 1: Denominazioni

Definizione	Significato
Backplane	Collegamento elettrico interno dell'accoppiatore bus ai driver valvole e ai moduli I/O
Lato sinistro	Campo I/O, a sinistra dell'accoppiatore bus, guardando i suoi attacchi elettrici
Lato destro	Campo valvole, a destra dell'accoppiatore bus, guardando i suoi attacchi elettrici
Driver valvole	Parte elettrica del pilotaggio valvole che trasforma il segnale proveniente dal backplane in corrente per la bobina magnetica.

1.5 Abbreviazioni

Nella presente documentazione sono utilizzate le seguenti abbreviazioni:

Tab. 2: Abbreviazioni

Abbreviazione	Significato
AES	**A**dvanced **E**lectronic **S**ystem
AV	**A**dvanced **V**alve
Modulo I/O	Modulo **I**nput/**O**utput
IS12-PD	Valvola ISO con posizionatore
PL	**P**erformance **L**evel
PLC	**P**rogrammable **L**ogic **C**ontroller o PC che esegue funzioni di comando
UA	Tensione attuatori (alimentazione di tensione delle valvole e delle uscite)
UAoff	Segnalazione che la tensione attuatori UA è scesa sotto il valore della tensione di spegnimento delle valvole. Le valvole sono scollegate dalla corrente.
UAon	Segnalazione che la tensione attuatori UA è scesa sotto il valore della tensione di accensione delle valvole. Le valvole non possono essere attivate elettricamente.
UL	Tensione logica (alimentazione di tensione dell'elettronica e dei sensori)

2 Indicazioni di sicurezza

2.1 Sul presente capitolo

Il prodotto è stato realizzato in base alle regole della tecnica generalmente riconosciute. Ciononostante sussiste il pericolo di lesioni personali e danni materiali, qualora non vengano rispettate le indicazioni di questo capitolo e le indicazioni di sicurezza contenute nella presente documentazione.

1. Leggere la presente documentazione attentamente e completamente prima di utilizzare il prodotto.
2. Conservare la documentazione in modo che sia sempre accessibile a tutti gli utenti.
3. Cedere il prodotto a terzi sempre unitamente alle documentazioni necessarie.
4. Osservare la norma ISO 4414 per l'utilizzo sicuro della pneumatica.

2.2 Qualifica del personale

Le attività descritte nella presente documentazione richiedono conoscenze di base in ambito elettrico e pneumatico e conoscenze dei termini specifici appartenenti a questi campi. Per garantire la sicurezza operativa, queste attività devono essere eseguite esclusivamente da personale specializzato o da persone istruite sotto la guida di personale specializzato.

Per personale specializzato si intendono coloro i quali, grazie alla propria formazione professionale, alle proprie conoscenze ed esperienze e alle conoscenze delle disposizioni vigenti, sono in grado di valutare i lavori commissionati, individuare i possibili pericoli e adottare le misure di sicurezza adeguate. Il personale specializzato deve rispettare le norme in vigore specifiche del settore.

2.3 Impiego in catene di comando rilevanti per la sicurezza

Accoppiatore bus e driver valvole possono essere utilizzati in catene di comando orientate alla sicurezza per la **"Funzione di arresto legata alla sicurezza e altre funzioni di sicurezza legate a un dispositivo di protezione"** se l'intero impianto è predisposto di conseguenza.

3 Sistema valvole AV in una catena di comando orientata alla sicurezza

3.1 Preambolo generale (responsabilità)

Gli esempi riportanti in queste istruzioni rappresentano un estratto di un comando rilevante per la sicurezza. Questi esempi mostrano i principi, ma non sempre tutti i componenti necessari. Per applicazioni nelle macchine possono essere necessari ulteriori elementi e valutazioni. I dati forniti non esonerano l'utente da proprie valutazioni e controlli. Si deve considerare che i nostri prodotti sono soggetti ad un processo naturale di usura e di invecchiamento.

3.2 Il processo verso una macchina sicura: la valutazione dei rischi

La valutazione dei rischi

- deve essere eseguita dal produttore della macchina; i suoi risultati restano presso il produttore
- deve tenere conto dell'uso conforme e anche di qualsiasi applicazione errata prevedibile
- rappresenta un'importante fonte di prova, in caso di eventuali responsabilità a seguito di un incidente

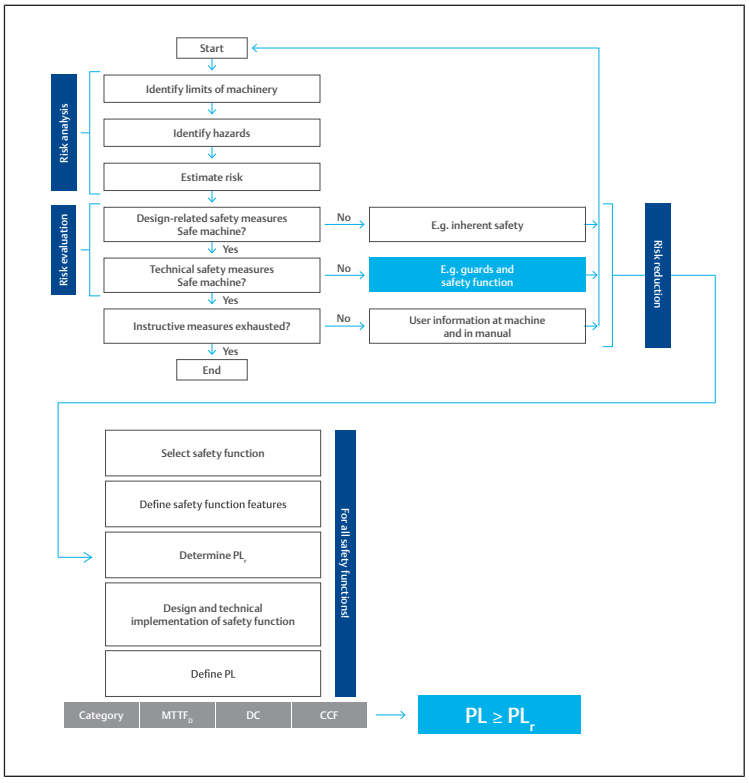


Fig. 1: Processo per la valutazione dei rischi e la determinazione del PL_r

Le informazioni contenute in queste istruzioni consentono la valutazione dei rischi, l'applicazione di misure di protezione tecniche per la riduzione dei rischi, la valutazione delle funzioni di sicurezza e la determinazione del performance level. La figura mostra il processo necessario per la valutazione dei rischi. Il Performance Level (PL) deve corrispondere almeno al Performance Level richiesto (PL_r) e dipende dall'architettura di comando (categoria), dal Mean Time To dangerous Failure ($MTTF_D$), dal grado di copertura diagnostica (DC) e dai guasti per causa comune (CCF).

3.3 Informazioni relative agli esempi

I tre esempi seguenti mostrano:

- Esempio 1: pericolo dovuto ad avviamento improvviso, PL_r = e
- Esempio 2: pericolo dovuto ad avviamento improvviso, energia cinetica residua, PL_r = c
- Esempio 3: pericolo dovuto ad avviamento improvviso, PL_r = d con esclusione di guasto

3.3.1 Sistematica degli esempi

La sistematica degli esempi si orienta alla chiave di identificazione delle parti delle funzioni di sicurezza riportate nella norma VDMA 66416:2016-01.

La descrizione generale è la seguente:

Premessa

Descrizione delle condizioni marginali:

- Tipo di macchina, modo di funzionamento, ...
- Pericolo dovuto a ...
- Parametri di rischio secondo DIN EN ISO 13849-1:2016-06
- PL_r

Misure di controllo tecniche (funzioni di sicurezza) e ulteriori misure per la riduzione dei rischi:

- Nome della funzione di sicurezza
- Nome della funzione di sicurezza
- ...

Input

Evento scatenante:

- Interrogazione degli stati dei dispositivi di sicurezza e
- Monitoraggio degli eventi
  Esempi: dispositivo di consenso, arresto di emergenza, interruttore di sicurezza, interruttore a chiave,
- Barriera fotoelettrica, pressostato di sicurezza, ...

Logica

Valutazione della funzione di sicurezza:

- Spegnimento delle forniture di energia, relè di sicurezza, PLC di sicurezza

Output

Reazioni orientate alla sicurezza:

- Esempi: valvole dei fluidi, contattori, riduttori, freni, ...

3.3.2 Misure tecniche preventive

Se la sicurezza di una macchina dipende da un comando correttamente funzionante si parla di "sicurezza funzionale". Le parti "attive" del comando sono il focus principale, cioè componenti che monitorano la situazione pericolosa (rilevamento del segnale "I" = Input), ne deducono le reazioni adatte (valutazione, "L" = Logica) e implementano azioni affidabili (esecuzione, "O" = Output). Il termine "comando" comprende quindi l'intero sistema di elaborazione dei segnali.

Gli "elementi di un comando legati alla sicurezza (SRP/CS)" non sono necessariamente "componenti di sicurezza" in base alla direttiva macchine. Gli SRP/CS (Safety Related Part of a Control System) possono però essere considerati tali, ad es. dispositivi di comando a due mani oppure unità logiche con funzione di sicurezza. Gli azionamenti (cilindri), l'approvvigionamento energetico (come alimentazione di pressione o gruppi di trattamento dell'aria) e i raccordi non rientrano direttamente nella stima delle probabilità di guasto pericolose.

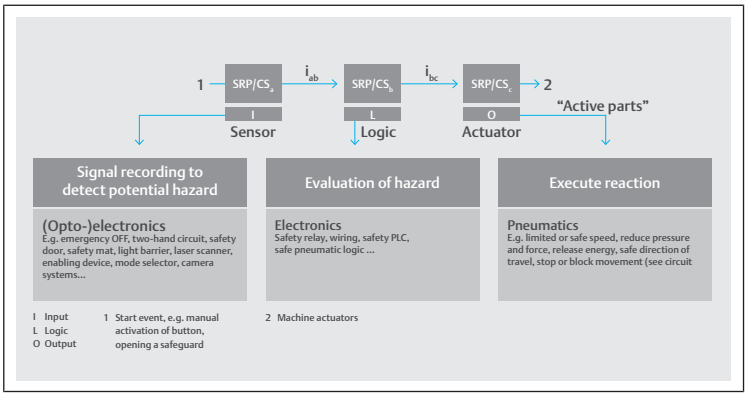


Fig. 2: Focus nelle parti di un sistema di comando legate alla sicurezza (SRP/CS secondo ISO 13849-1)

3.4 Esempio 1 con PLr = e

Esempio 1, in conformità con VDMA 66416:2016-01, numero 2.1.1.1 e 2.2.1.1

Premessa

Descrizione delle condizioni marginali:

- Modo di funzionamento: automatico (BA1)
- Tempo di ciclo della macchina: da 5 a 15 secondi
- Pericolo dovuto ad avviamento improvviso

- PL_r = e

Misure di controllo tecniche (funzioni di sicurezza):

- Disattivazione sicura della coppia (STO) o
- Spegnimento sicuro dell'apporto energetico (SEC)
- Protezione dal riavvio accidentale (PUS)

Input

Evento scatenante:

- Barriera fotoelettrica interrotta o porte di sicurezza aperte o non tenute

Logica

Valutazione della funzione di sicurezza:

- Spegnimento delle forniture di energia

Output

Reazioni orientate alla sicurezza:

- Separazione dall'alimentazione di energia fluida: $PL_r \geq d$ => a 2 canali
  e dall'alimentazione elettrica: $PL_r \geq d$ = > 2 canali consigliati

3.4.1 Implementazione dell'esempio 1

Secondo ISO 13849 può essere raggiunto PL = e con categoria 3 se vale quanto segue:

- DC_{avg} = medio
- MTTF = alto

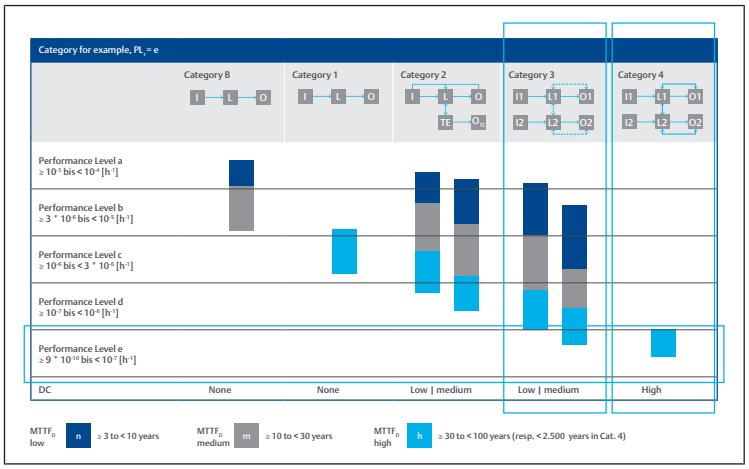


Fig. 3: Implementazione dell'esempio 1: PL_e con categoria 3, DC = medio, $MTTF_D$ = alto

Secondo il metodo semplificato della ISO 13849-1 le quattro classi per il grado di copertura diagnostica DC sono definite nel modo seguente:

- nulla: DC < 60 %
- bassa: 60 % < DC < 90 %
- media: 90 % < DC < 99 %
- alta: 99 % < DC

Progettazione e implementazione della funzione di sicurezza

Posto di lavoro manuale
TM=20 anni
d/a=320 giorni
h/d=24 h / tempo di ciclo min. 10 sec = 55.296.000 cicli di commutazione per valvola aria di lavoro e principale

Nella modalità di regolazione i ripari mobili di protezione devono essere bypassati e aperti e quelli fissi devono essere montati.

INFO: Un singolo errore non comporta la perdita della funzione di sicurezza. Il problema è che alcuni errori vengono riconosciuti, ma non tutti. Un accumulo di errori sconosciuti può quindi portare alla perdita della funzione di sicurezza.

Selezione delle valvole

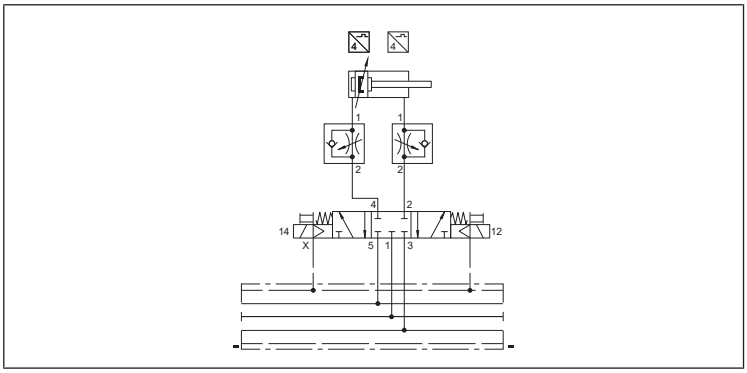


Fig. 4: Schema di collegamento: selezione delle valvole

- Posizione di commutazione sicura e definita in assenza di corrente tramite molla meccanica
- I tubi di mandata sono bloccati in assenza di corrente
- Le condutture aria di scarico non sono aperte
- Il cilindro non è spostabile dopo un arresto di emergenza, il che significa che è necessario liberare persone
- Possibilità di decelerazione di masse sporgenti
- Arresto sicuro dei movimenti verticali con masse (a partire da PL_d solo con misure aggiuntive ->a 2 canali)
- Modalità JOG possibile (corsa cilindro a impulsi)
- Possibilità di contaminazione con aria di scarico di cilindri confinanti più grandi
- Adatto fino al Performance Level PL_e (per misure aggiuntive vedere → Fig. 5.)
- Estrazione e rientro consentite della direzione di movimento del cilindro pericolosa
- La durata delle valvole è stata testata secondo ISO 19973-1 e 2

Interruttore di sicurezza pneumatico categoria 3 PL_e

Definizione:
Protezione dal riavvio accidentale (Prevention of unexpected start-up, PUS) secondo VDMA scheda standard 24584.

Blocco delle portate in entrata e in uscita dalle due camere dei pistoni.

INFO: In caso di riavvio osservare quanto segue:
Le camere del cilindro possono sfiatare a seguito di perdite di singoli elementi.

INFO: Impulsi di prova possono portare allo spegnimento delle valvole.

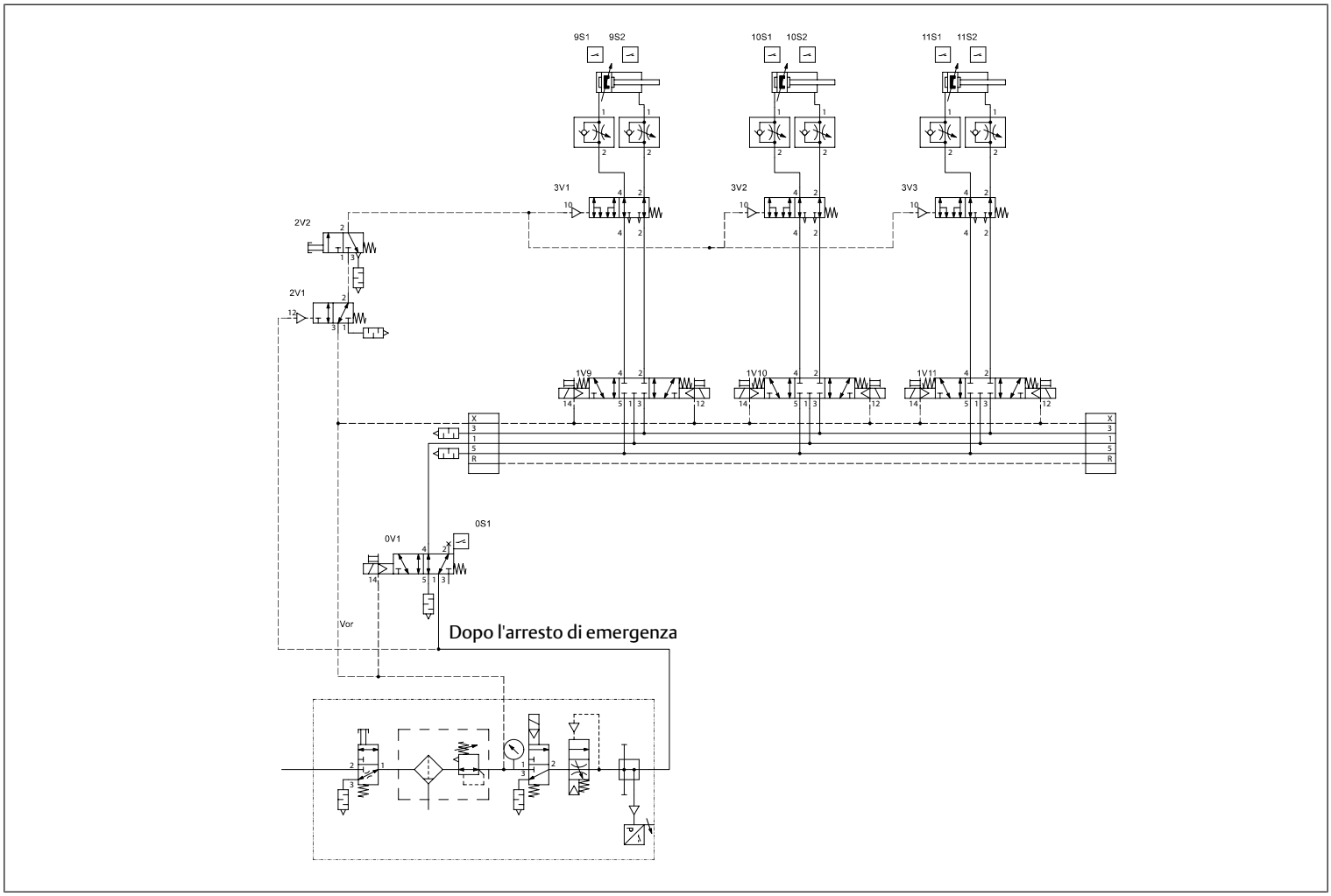


Fig. 5: Schema: canali di funzione e di prova

INFO: In caso di aerazione/scarico contemporaneo di più di 8 valvole, fare attenzione all'aerazione/scarico supplementari attraverso le piastre di alimentazione.

Liberazione di persone tramite scarico dell'aria (per circuiti con mantenimento di posizione)

Per movimenti verticali e orizzontali:

- Gravità della lesione = S2 (lesione di norma irreversibile, inclusa la morte)
- Il punto di pericolo si trova nell'area accessibile
- L'operatore non può liberarsi da solo
- Lo sfiato non deve rappresentare un ulteriore pericolo

La liberazione delle persone può avvenire solo nei modi seguenti:

- Solo in assenza di pressione
- Dopo un arresto di emergenza attivato da 2V1 (un 2V1 può alimentare più 2V2), che deve essere montato nelle vicinanze del punto pericoloso
- Per gruppi di cilindri prevedere una liberazione di persone congiunta (un 2V2 può sfiatare diversi cilindri)

Schema a blocchi

Nella figura seguente è rappresentato il diagramma a blocchi relativo alla sicurezza per l'esempio 1.

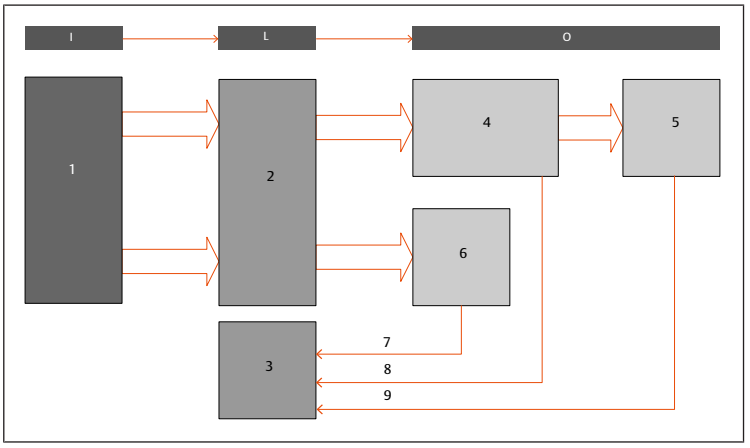


Fig. 6: Diagramma a blocchi relativo alla sicurezza, esempio 1

1 Interruttore porta di sicurezza (ad es. PILZ PSEN cs3.1 o PSEN sl-0.5p 1.1)
2 Modulo di sicurezza (ad es. PILZ PNOZ)
3 PLC (controller logico programmabile)
4 Parte elettrica del sistema valvole AV, alimentazione UA tramite piastra di alimentazione elettrica
5 Parte pneumatica del sistema valvole AV
6 Valvola aria principale con posizionatore (ad es. IS12-PD)
7 Diagnosi "Richiesta posizionatore della valvola aria principale"
8 Messaggio di diagnosi "La tensione valvola UA è più bassa della tensione di spegnimento (UA < UAoff)"
9 Diagnosi "Richiesta indiretta della valvola di lavoro"

Schema pneumatico

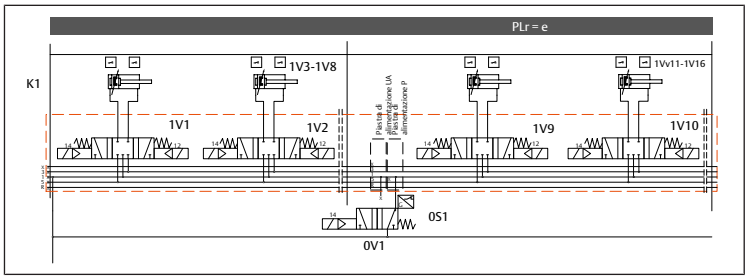


Fig. 7: Schema pneumatico, esempio 1

K1	Batteria di valvole	1V1 – 1V8	Valvole fuori dalla catena di comando orientata alla sicurezza
1V3 – 1V8	Non disegnato	1V9 – 1V16	Valvole per azionamenti con PL_r = e
1V1 – 1V16	Non disegnato	0S1	Rilevamento posizione di 0V1
0V1	Valvola aria principale		

Sistema valvole completo con componenti esterni

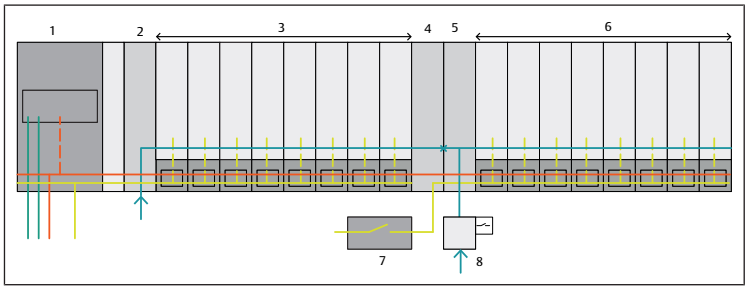


Fig. 8: Sistema valvole e componenti esterni

1 Accoppiatore bus

2 Piastra di alimentazione pneumatica

3 Valvole (non nel circuito di sicurezza)

4 Piastra di alimentazione - corrisponde al blocco 4 nel diagramma a blocchi relativo alla sicurezza

5 Piastra di alimentazione pneumatica, - nessun monitoraggio necessario (UAoff), nessuna elettronica attiva integrata

6 Valvole (circuito di sicurezza) - corrisponde al blocco 5 nel diagramma a blocchi relativo alla sicurezza - la parte elettrica delle valvole (driver valvole) corrisponde al blocco 4 nel diagramma a blocchi relativo alla sicurezza

7 Modulo di sicurezza, corrisponde al blocco 2 nel diagramma a blocchi relativo alla sicurezza

8 La valvola aria principale corrisponde al blocco 6 e 7 nel diagramma a blocchi relativo alla sicurezza

3.4.2 Funzioni di sicurezza

Protezione di sicurezza dal riavvio accidentale a partire dalla posizione di riposo con opzione di liberazione delle persone.

Nella presente documentazione è rappresentato solo l'elemento di comando pneumatico come sottosistema. Per la funzione di sicurezza completa devono essere aggiunti come sottosistemi ulteriori componenti di comando legati alla sicurezza (ad es. ripari e logica elettrica).

- Gravità della lesione = S2
- Il punto di pericolo si trova nell'area accessibile e l'operatore non può liberarsi da solo
- Lo sfiato non deve rappresentare un ulteriore pericolo
- Dato che la liberazione di persone 2V1, 2V2, 3V1 e 3Vn dopo un arresto di emergenza e quindi dopo lo sfiato della valvola 3/2 nel gruppo di trattamento dell'aria è pienamente operativa e non interferisce con la funzione di sicurezza, non viene inclusa nel calcolo.

Questa può essere realizzata solo nel modo seguente:

- Solo in assenza di pressione
- Dopo un arresto di emergenza attivato da 2V1 (un 2V1 può alimentare più 2V2), che deve essere montato nelle vicinanze del punto pericoloso
- Per gruppi di cilindri prevedere una liberazione di persone congiunta (un 2V2 può sfiatare diversi cilindri)

Descrizione delle funzioni del circuito PL c, d, e_Kat-3_02 utilizzate in un posto di lavoro manuale

- I movimenti sono comandati con ridondanza dalla valvola aria principale 0V1 e dalla valvola di lavoro 1Vn
- La valvola 0V1 deve essere pilotata continuamente affinché sia pilotato 1Vn
- Il guasto di una delle suddette valvole non comporta la perdita della funzione di sicurezza
- Tutte le valvole sono pilotate ciclicamente nel processo
- La funzione della valvola aria principale 0V1 è sorvegliata tramite richiesta di posizione valvola 0S1
- La funzione della valvola di lavoro 1Vn viene riconosciuta indirettamente dagli interruttori nS1 e nS2 durante il processo
- Un accumulo di errori non rilevati può portare alla perdita della funzione di sicurezza
- Per pericoli associati all'energia accumulata (pressione, massa, molla) sono necessarie ulteriori misure

Caratteristiche costruttive

- Sono stati rispettati i principi di sicurezza di base e ben provati e i requisiti della categoria B
- La valvola aria principale 0V1 è portata nella posizione di commutazione sicura tramite una molla
- La valvola di lavoro nV1 ha una posizione centrale bloccata (senza intersezione) con centraggio a molla
- La posizione di commutazione sicura di entrambi le valvole viene raggiunta dopo avere tolto la tensione di comando
- L'elaborazione segnale delle richieste valvola e dei monitoraggi avviene in un comando PLC a un canale
- Comando ON e sportello di caricamento chiuso:
  - La valvola aria principale 0V1 è attivata e sul sistema valvole è presente tensione
- Funzionamento automatico ON e sportello di caricamento aperto:
  - Sulla valvola aria principale 0V1 e sul sistema valvole non è presente tensione
- Modalità di regolazione e porta di sicurezza bypassata con interruttore a chiave:
  - Sulla valvola aria principale 0V1 e sul sistema valvole non è presente tensione
  - Il cavo pneumatico tra valvola aria principale 0V1 e valvola di lavoro nV1 è scaricato
  - I movimenti sono possibili solo con ulteriore interruttore di consenso
  - L'interruttore di consenso aziona la valvola aria principale 0V1 e sul sistema valvole è presente tensione
  - Movimenti pericolosi senza misure aggiuntive con relativa giustificazione sono consentiti solo con porta di sicurezza chiusa

Calcolo della probabilità di default e della durata

Durata richiesta:
20 anni / 320 giorni / 24 h / tempo di ciclo 10 sec. (nop = 2764800 cicli/anno)

- Valvola 0V1 B_{10D} = 79,2 milioni (IS12-PD)
- Valvola nV1 B_{10D} = 39,6 milioni (AV05) o valvola nV1 B_{10D} = 105,8 milioni (AV03)

3.4.3 Calcolo del MTTF per la parte elettrica e pneumatica del sistema valvole

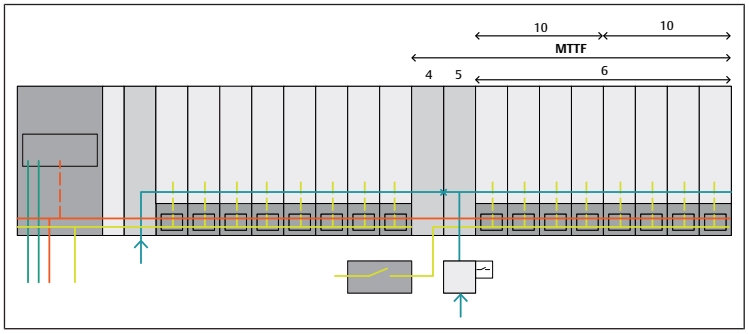


Fig. 9: Componenti rilevanti per il calcolo del $MTTF_D$ per la parte elettrica

4 Piastra di alimentazione elettrica con monitoraggio UAon, corrisponde al blocco 4 nel diagramma a blocchi relativo alla sicurezza

5 Piastra di alimentazione pneumatica con monitoraggio UAoff, la funzione elettrica = monitoraggio UAoff corrisponde al blocco 4 e 8 nel diagramma a blocchi relativo alla sicurezza

6 Valvole (circuito di sicurezza) corrispondono al blocco 5 nel diagramma a blocchi relativo alla sicurezza La parte elettrica delle valvole (driver valvole) corrisponde al blocco 4 nel diagramma a blocchi relativo alla sicurezza

10 Scheda driver per 4 valvole

Vedere → 6. Parametri di affidabilità e vedere → Fig. 9

Ciò significa:

- Piastra di alimentazione elettrica (**4**) MTTF = 854 anni
- Monitoraggio UAoff (**5**) MTTF = 1094 anni
- Scheda driver per 4 valvole (**10**) MTTF = 630 anni
- Valvole AV03 5/3 con ritorno a molla (**6**) MTTF = 382,7 anni

$$MTTF_{ges} = \frac{1}{\frac{1}{854\,[a]} + \frac{1}{1094\,[a]} + \frac{1}{630\,[a]} + \frac{1}{630\,[a]} + \frac{1}{382{,}7\,[a]}} = 127\,[a]$$

I valori MTTF dei moduli AES sono stati calcolati con l'ausilio dei tassi di guasto ripresi da una banca dati.

Secondo DIN EN 13849-1, allegato C non tutti i guasti sono da considerarsi pericolosi. In questo caso può essere applicata la formula $MTTF_D = 2 \times MTTF_{tot}$ per il calcolo del tasso dei guasti pericolosi in tutto l'impianto.

$MTTF_D = 2x\ MTTF_{tot} = 2 \times 127\,[a] = 254\,[a]$

3.4.4 Diagnosi

La piastra di alimentazione pneumatica monitora la tensione attuatori UA e invia il bit di diagnosi UAoff se UA è inferiore alla tensione di spegnimento.

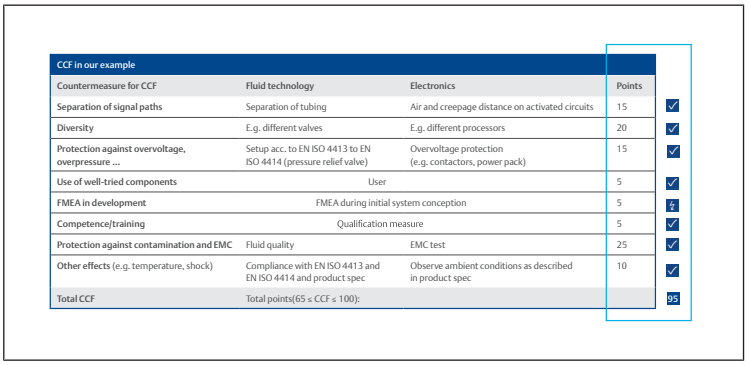
La piastra di alimentazione elettrica monitora la tensione attuatori UA e invia il bit di diagnosi UAon, se UA è inferiore alla tensione di accensione.

Il bit di diagnosi (UAoff) deve essere monitorato. Per farlo è necessario un cambio di segnale. Questo può essere eseguito ad es. all'accensione della macchina oppure con cicli di prova speciali.

Richiesta di funzione diretta del posizionatore sulla valvola principale 99 %.

Richiesta di funzione indiretta della valvola di lavoro 90 %.

DC = 94,4 % $MTTF_D$ = alto (100 anni) CCF = 95



CCF in our example			
Countermeasure for CCF	Fluid technology	Electronics	Points
Separation of signal paths	Separation of tubing	Air and creepage distance on activated circuits	15
Diversity	E.g. different valves	E.g. different processors	20
Protection against overvoltage, overpressure ...	Setup acc. to EN ISO 4413 to EN ISO 4414 (pressure relief valve)	Overvoltage protection (e.g. contactors, power pack)	15
Use of well-tried components	User		5
FMEA in development	FMEA during initial system conception		5
Competence/training	Qualification measure		5
Protection against contamination and EMC	Fluid quality	EMC test	25
Other effects (e.g. temperature, shock)	Compliance with EN ISO 4413 and EN ISO 4414 and product spec	Observe ambient conditions as described in product spec	10
Total CCF	Total points(65 ≤ CCF ≤ 100):		95

Fig. 10: Esempio: CCF – cause comuni di guasto

Performance Level = PL_e / categoria = 3

Sostituzione della valvola aria principale 0V1 (IS12-PD) non necessaria.

Sostituzione della valvola nV1 (AV03) non necessaria.

Sostituzione della valvola nV1 (AV05) dopo 14,3 anni - con tempo di ciclo ≥ 14 sec. non necessaria o durata di utilizzo 20 anni.

3.4.5 Verifica del bit di diagnosi

Una descrizione dettagliata del monitoraggio è riportata al capitolo → 3.11 Descrizione del monitoraggio UAoff / UAon.

Se la tensione UA viene disattivata, deve essere inviata sia la segnalazione di diagnosi UAon sia UAoff.

Tab. 3: Verifica del bit di diagnosi

UA = 0, spento	Diagnosi dell'accensione UAon	Diagnosi dello spegnimento UAoff
valida	1	1
non valida	1	0
non valida	0	1

Se vengono rispettare le condizioni di cui sopra, con le informazioni fornite dalle norme seguenti si può presumere che il monitoraggio della tensione valvole spenta sia di DC = dal 90 % al < 99 % (medio):

- DIN EN ISO 13849-1 allegato E: “Stime di copertura diagnostica (DC) per funzioni e moduli”
- DIN EN 61508-2: “Tabella A.14 – elementi finali (attuatori)”
- DIN EN 61508-2: “Tabella A.7 – unità I/O e interfacce (comunicazione esterna)”

3.5 Esempio 2 con PLr = c

Esempio 2, in conformità con 66416:2016-01, numero 1.1.2.1 e 2.1.2.3

Premessa

Descrizione delle condizioni marginali:

- Modo di funzionamento BA2 Modalità di regolazione e di servizio
- Pericolo dovuto ad avviamento improvviso, energia cinetica residua
- PL_r = c

Misure di controllo tecniche (funzioni di sicurezza) (vedere la nota):

- Disattivazione sicura della coppia (STO)
- Spegnimento sicuro dell'apporto energetico (SEC)
- Protezione dal riavvio accidentale (PUS)

Input

Evento scatenante:

- Selettore modi operativi, dispositivo di consenso

Logica

Valutazione della funzione di sicurezza:

- Spegnimento delle forniture di energia

Output

Reazioni orientate alla sicurezza:

- Bloccaggio a 1 canale del fluido. Sono possibili le seguenti attuazioni:
  - Valvola in posizione chiusa
  - Comando di valvola(e) di blocco
  - S1 possibile, perchè l'energia residua provoca solo lesioni reversibili

- Separazione dell'alimentazione di energia elettrica: $PL_r \geq d$ =>consigliata a 2 canali

Nota

Il tema energia residua viene descritto più da vicino nelle documentazioni seguenti:

- Norma VDMA 66416: capitolo 5.1.3 Modalità di regolazione / modalità di servizio (BA2) “Le velocità ridotte devono essere previste nel modo seguente ...“
- Norma VDMA 66416: tabella A2 - Chiave di identificazione per le valutazioni dei parametri del grafico dei rischi nella tabella A7

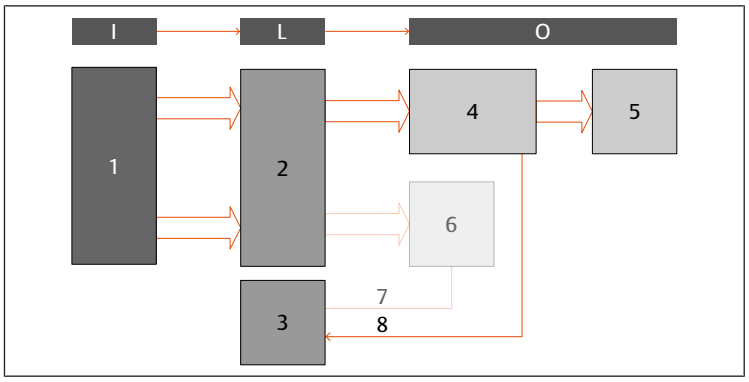


Fig. 11: Diagramma a blocchi relativo alla sicurezza, esempio 2

1 Dispositivo di consenso
2 Modulo di sicurezza (ad es. PILZ PNOZ)
3 PLC (controller logico programmabile)
4 Parte elettrica del sistema valvole AV, alimentazione UA tramite piastra di alimentazione elettrica
5 Valvole del sistema valvole AV
6 Valvola aria principale con posizionatore (ad es. IS12-PD, ...) non attiva per questa funzione di sicurezza
7 Diagnosi “Richiesta posizionatore della valvola aria principale” non attiva per questa funzione di sicurezza
8 Diagnosi “La tensione valvola UA è più bassa della tensione di spegnimento (UA < UAoff)”

3.6 Esempio 3 con PLr = d

Esempio 3, in conformità con VDMA 66416, numero 2.1.1.1 e 2.2.1.1

Questo esempio è simile all'esempio 1, il PL_r richiesto è tuttavia d.

Premessa

Descrizione delle condizioni marginali:

- Modo di funzionamento automatico (BA1)
- Pericolo dovuto ad avviamento improvviso
- $PL_r = d$

Misure di controllo tecniche (funzioni di sicurezza):

- Disattivazione sicura della coppia (STO)
- Spegnimento sicuro dell'apporto energetico (SEC)
- Protezione dal riavvio accidentale (PUS)

Input

Evento scatenante:

- Barriera fotoelettrica interrotta o porte di sicurezza aperte o non tenute

Logica

Valutazione della funzione di sicurezza:

- Spegnimento delle forniture di energia

Output

Reazioni orientate alla sicurezza:

- Separazione dall'alimentazione di energia fluida: $PL_r \geq d$ => a 2 canali e dall'alimentazione elettrica: $PL_r \geq d$ => a 2 canali consigliate

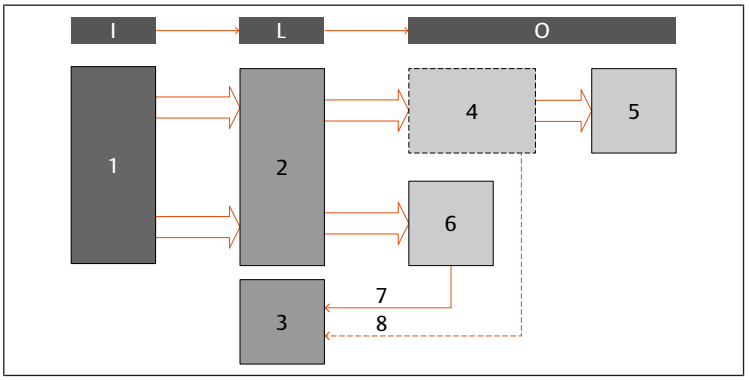


Fig. 12: Diagramma a blocchi relativo alla sicurezza, esempio 3

1 Interruttore porta di sicurezza (ad. es. PILZ PSEN cs3.1 o PSEN sl-0.5p 1.1)
2 Modulo di sicurezza (ad es.
3 PLC (controller logico programmabile)
4 Parte elettrica del sistema valvole AV

O Alimentazione UA tramite piastra di alimentazione elettrica. Per questo blocco è possibile un'esclusione di guasto (vedere → 3.6.1 Esclusione di guasto).

Oppure alimentazione UA tramite accoppiatore bus. Nessuna possibilità di esclusione di guasto (vedere → 3.6.2 Nessuna esclusione di guasto).

5 Valvole del sistema valvole AV
6 Valvola aria principale con posizionatore (ad es. IS12-PD, ...)
7 Diagnosi “Richiesta posizionatore della valvola aria principale”
8 Diagnosi “La tensione valvola UA è più bassa della tensione di spegnimento (UA < UAoff)”

Se per (4) viene utilizzata l'esclusione di guasto, questa diagnosi non è necessaria.

3.6.1 Esclusione di guasto

Se il sistema valvole è montato e utilizzato come descritto nei capitoli seguenti, l'elettronica delle valvole non deve essere inclusa nel calcolo dei valori MTTF di una catena di comando orientata alla sicurezza.

La condizione per l'applicazione dell'esclusione di guasto è,

- che sia applicabile massimo il PL d (PL e deve essere calcolato come nell'esempio 1),
- che il sistema valvole sia realizzato con una o più piastre di alimentazione elettriche,
- che le valvole, che devono essere disattivate, siano alimentate tramite queste piastre di alimentazione elettriche,
- che le piastre di alimentazione elettriche siano cablate in base ai principi di cablaggio 1–3,
- che il cavo per il collegamento della piastra di alimentazione includa solo la tensione di alimentazione UA da 24 V,
- che il cavo sia cablato ai sensi della norma DIN EN 60204.

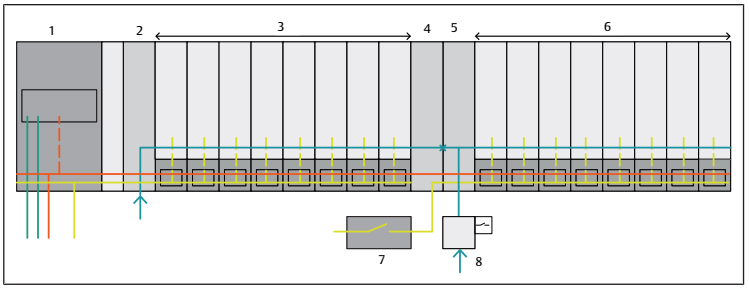


Fig. 13: Sistema valvole e componenti esterni

1 Accoppiatore bus
2 Piastra di alimentazione pneumatica
3 Valvole (non nel circuito di sicurezza)
4 Piastra di alimentazione - corrisponde al blocco 4 nel diagramma a blocchi relativo alla sicurezza
5 Piastra di alimentazione pneumatica, - nessun monitoraggio necessario (UAoff), nessuna elettronica attiva integrata
6 Valvole (circuito di sicurezza) - corrisponde al blocco 5 nel diagramma a blocchi relativo alla sicurezza - la parte elettrica delle valvole (driver valvole) corrisponde al blocco 4 nel diagramma a blocchi relativo alla sicurezza
7 Modulo di sicurezza, corrisponde al blocco 2 nel diagramma a blocchi relativo alla sicurezza
8 La valvola aria principale corrisponde al blocco 6 e 7 nel diagramma a blocchi relativo alla sicurezza

3.6.2 Nessuna esclusione di guasto

Se si utilizza l'alimentazione UA tramite l'accoppiatore bus non è possibile un'esclusione di guasto. È necessario calcolare la probabilità di guasto.

Ulteriori misure sono le seguenti:

- L'alimentazione UA tramite l'accoppiatore bus deve essere disattivata in modo sicuro per evitare un'accensione inaspettata delle valvole.
- I cavi devono essere cablati ai sensi della norma DIN EN 60204.
- La diagnosi dell'accoppiatore bus (UAon e UAoff) deve essere valutata.

A seconda del Performance Level richiesto è necessario adottare ulteriori misure.

3.7 Panoramica delle diverse possibilità di alimentazione

Tab. 4: Diverse possibilità di alimentazione

	Alimentazione UA tramite accoppiatore bus	Alimentazione UA tramite piastra di alimentazione elettrica
PL_r massimo raggiungibile	d (e non consigliato)	e
È possibile l'esclusione di guasto	no ved. → 3.6.2 Nessuna esclusione di guasto	$PL_r \leq$ d: sì PL_r = e: no
Valutazione della diagnosi	sì (UAon e UAoff dell'accoppiatore bus)	$PL_r \leq$ d: no (non necessario a causa dell'esclusione di guasto) PL_r = e: sì (UAon e UAoff) La piastra di alimentazione pneumatica deve essere dotata di monitoraggio UAoff.
DC	90 % ... < 99 %	90 % ... < 99 %
Limitazione di corrente di inserzione	sì	sì
Prova possibile (cortocircuito trasversale)	no	sì

Limitazione di corrente di inserzione

La corrente di inserzione molto alta dell'unità, solitamente presente nei carichi capacitivi, viene limitata a un valore di massimo 5 A.

Definizione di impulso di prova

Un impulso di prova è una modifica temporanea del livello di tensione del segnale per controllare il funzionamento dell'uscita o dell'apparecchio oppure per verificare la distanza di trasmissione.
[Fonte: ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (Associazione generale delle industrie elettroniche ed elettrotecniche), documento di sintesi “Classificazione di interfacce binarie da 24 V con test nel campo della sicurezza funzionale”]

Prova possibile

Uscite sicure e/o moduli di sicurezza creano segnali di ciclo o impulsi di prova sulle loro uscite. Se una di queste uscite viene collegata con la piastra di alimentazione elettrica, è possibile escludere un'interpretazione errata del controllo di cortocircuito trasversale. Se una di queste uscite viene utilizzata per l'alimentazione UA sull'accoppiatore bus, ciò porta ad un'interpretazione errata del controllo di cortocircuito trasversale.

Nota

Può essere controllata solo la distanza di trasmissione fino alla piastra di alimentazione.

3.8 Assegnazione delle tensioni di alimentazione nel sistema valvole

La figura seguente mostra l'assegnazione delle tensioni di alimentazione alle funzioni all'interno del sistema valvole.

- La tensione di alimentazione **UL** immessa nell'accoppiatore bus (**1**) alimenta l'elettronica completa del sistema valvole.
- La tensione di alimentazione **UA** immessa nell'accoppiatore bus alimenta le uscite del modulo DO (**6**) (uscita digitale, digital output) e tutte le valvole tra accoppiatore bus e alimentazione UA.

Il modulo “piastra di alimentazione elettrica” (**5**) interrompe la tensione di alimentazione **UA** in arrivo. Per tutte le valvole alla destra della piastra di alimentazione elettrica viene utilizzata la tensione di alimentazione di questo modulo. Il modulo “piastra di alimentazione elettrica” può essere utilizzato più volte nel campo valvole.

La tensione **UL** nel sistema valvole è normalmente separata galvanicamente dalla tensione **UA**.

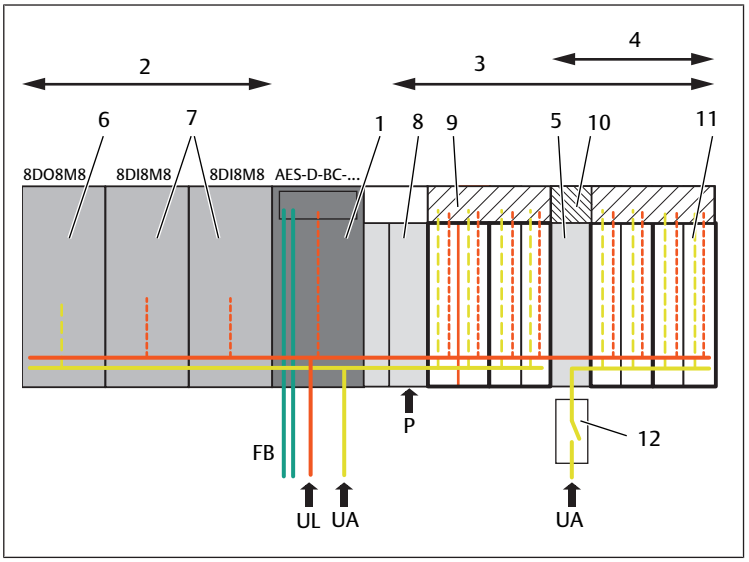


Fig. 14: Assegnazione delle tensioni di alimentazione UL e UA

1	Accoppiatore bus	2	Moduli I/O
3	Campo valvole	4	Parte della catena di comandi orientata alla sicurezza
5	Piastra di alimentazione elettrica	6	Modulo di uscita
7	Modulo d'ingresso	8	Piastra di alimentazione pneumatica
9	Scheda driver per 4 valvole	10	Scheda di alimentazione
11	Valvola	12	Modulo di sicurezza
UL	Tensione di alimentazione 24 V per elettronica e logica	UA	Tensione di alimentazione a 24 V per attuatori
FB	Bus di campo		

3.9 Principi di cablaggio del sistema valvole

Le tre figure seguenti mostrano i diversi principi di cablaggio del sistema valvole.

Per tutte e tre le rappresentazioni vale quanto segue:

- L'alimentazione di tensione sull'accoppiatore bus (K1) per **UL** e **UA** avviene tramite connettore **X1S1**.
- L'immissione della tensione di alimentazione sicura per le valvole avviene principalmente tramite l'attacco della piastra di alimentazione elettrica aggiuntiva (**X1S2**) delle valvole.

Per i principi di cablaggio seguenti vengono utilizzati i mezzi di esercizio con designatori di riferimento ai sensi di EN 81346. Gli esempi mostrano solo la parte rilevante dell'alimentazione di tensione e non sono esaustivi. Per l'applicazione all'interno di una macchina sono necessari ulteriori mezzi di esercizio.

Vedere → Fig. 14. Nello schema elettrico viene utilizzato un alimentatore in comune (**L01**) per le due tensioni **UL** e **UA**. La tensione per le valvole sull'attacco **X1S2** viene spenta a due poli (ossia **UA+** e **UA-**) tramite il modulo di sicurezza.

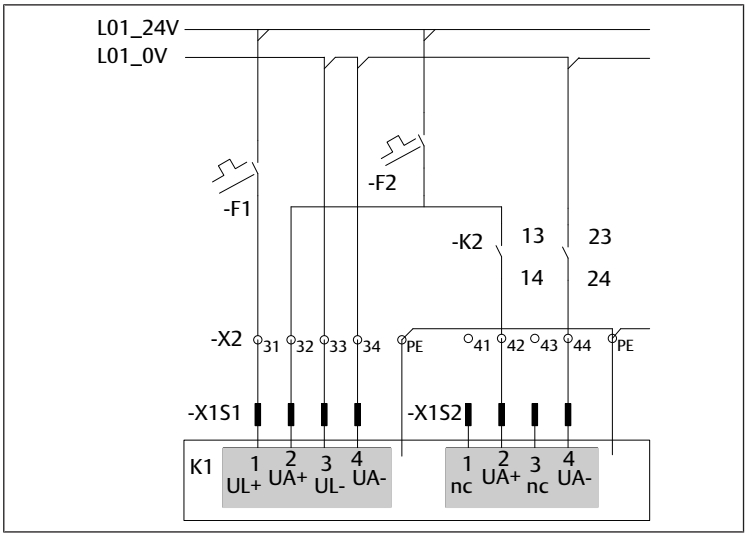


Fig. 15: Concetto di cablaggio 1

-K1	Sistema valvole con due connettori per l'alimentazione di tensione	**-K2**	Modulo di sicurezza
-X1S1	Attacco per l'alimentazione di tensione dell'accoppiatore bus	**-X1S2**	Attacco per l'alimentazione di tensione della piastra di alimentazione elettrica
-F1	Fusibile della tensione **UL**	**-F2**	Fusibile della tensione **UA**
-X2	Morsettiera a listello	**L0x**	Alimentazione di tensione

Nell'esempio seguente vengono utilizzati due alimentatori separati per entrambe le tensioni **UL** (**L01**) e **UA** (**L02**). La tensione per le valvole sull'attacco **X1S2** viene spenta a due poli (ossia **UA+** e **UA-**) tramite il modulo di sicurezza.

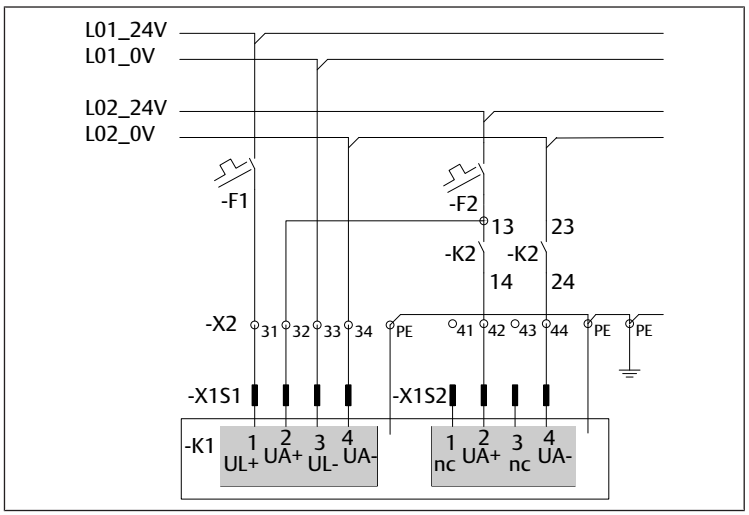


Fig. 16: Concetto di cablaggio 2

-K1	Sistema valvole con due connettori per l'alimentazione di tensione	**-K2**	Modulo di sicurezza
-X1S1	Attacco per l'alimentazione di tensione dell'accoppiatore bus	**-X1S2**	Attacco per l'alimentazione di tensione della piastra di alimentazione elettrica
-F1	Fusibile della tensione **UL**	**-F2**	Fusibile della tensione **UA**
-X2	Morsettiera a listello	**L0x**	Alimentazione di tensione

Nell'esempio seguente viene utilizzato un alimentatore in comune (**L01**) per entrambe le tensioni **UL** e **UA**. La tensione per le valvole sull'attacco **X1S2** viene spenta a un polo **UA+** tramite il modulo di sicurezza.

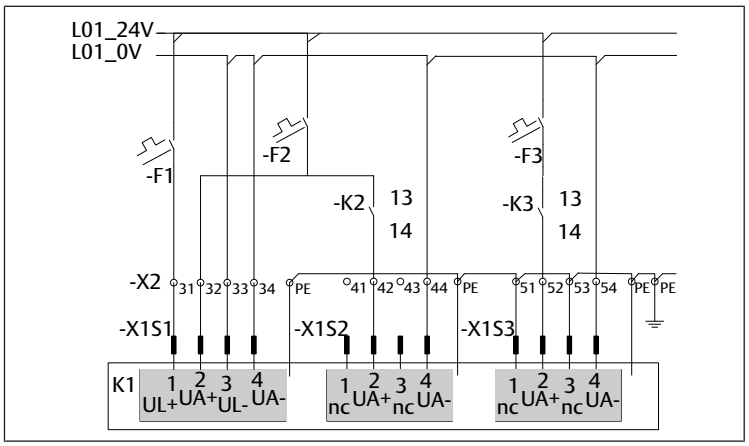


Fig. 17: Concetto di cablaggio 3

-K1	Sistema valvole con tre connettori per l'alimentazione di tensione	**-K2**	Modulo di sicurezza
-X1S1	Attacco per l'alimentazione di tensione dell'accoppiatore bus	**-X1S2**	Attacco per l'alimentazione di tensione della piastra di alimentazione elettrica
-X1S3	Attacco per l'alimentazione di tensione della piastra di alimentazione elettrica	**-F1**	Fusibile della tensione **UL**
-F3	Fusibile della tensione **UA**	**-F2**	Fusibile della tensione **UA**
-K3	Modulo di sicurezza	**-X2**	Morsettiera a listello
L0x	Alimentazione di tensione		

3.10 Indicazioni per il cablaggio

Durante l'utilizzo dei suddetti principi di cablaggio devono essere osservate le indicazioni seguenti:

1. Collegare il sistema valvole come rappresentato nei tre principi di cablaggio.
2. Assicurarsi che le valvole che devono essere disattivate in sicurezza si trovino dietro la piastra di alimentazione elettrica.
3. Collegare **X1S2** tramite un cavo a 2 fili.

Se si utilizza un cavo con più di 2 fili valgono i punti seguenti. Vedere → Fig. 17:

- i fili non utilizzati sono collegati con PE per motivi di compatibilità elettromagnetica
- non è presente alcuna tensione nel cavo.

In caso di spegnimento monopolare della tensione UA il cavo corrispondente deve essere cablato a prova di cortocircuito trasversale.

3.11 Descrizione del monitoraggio UAoff / UAon

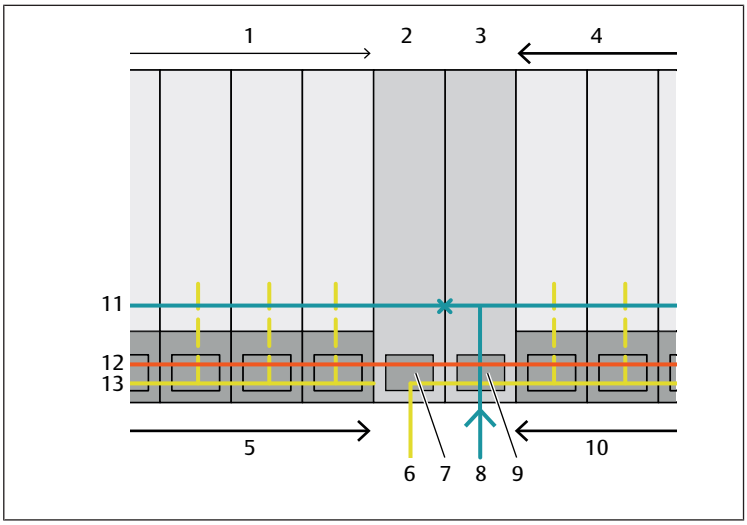


Fig. 18: Immagine dettagliata UAoff / UAon

1	Valvole a monte
2	Piastra di alimentazione elettrica
3	Piastra di alimentazione pneumatica
4	Valvole a valle
5	Driver valvole
6	Tensione attuatori UA della piastra di alimentazione elettrica
7	Monitoraggio UAon nella piastra di alimentazione elettrica
8	Alimentazione ad aria compressa della piastra di alimentazione pneumatica
9	Monitoraggio UAoff nella piastra di alimentazione pneumatica
10	Driver valvole
11	Alimentazione P presente
12	Tensione continua UL
13	Tensione UA presente

La piastra di alimentazione elettrica (**2**) interrompe l'alimentazione UA delle valvole. Le valvole a monte (**1**) sono alimentate con la tensione valvole presente. Le valvole a valle (**4**) sono alimentate con la nuova tensione valvole (**6**).

Nella piastra di alimentazione elettrica viene sorvegliato il limite UAon della nuova tensione proveniente da (**6**).

Se la tensione UA è inferiore alla tensione di accensione UAon, la piastra di alimentazione elettrica invia il bit di diagnosi UAon.

La piastra di alimentazione pneumatica (**3**) interrompe l'alimentazione P (**11**) delle valvole. Le valvole a monte (**1**) sono alimentate con l'aria compressa presente. Le valvole a valle (**4**) sono alimentate con la nuova aria compressa (**8**).

Nella piastra di alimentazione pneumatica viene sorvegliato il limite UAoff della tensione UA presente.

Se la tensione UA è inferiore alla tensione di spegnimento UAoff, la piastra di alimentazione pneumatica invia il bit di diagnosi UAoff.

> **i** Il monitoraggio della tensione UA nella piastra di alimentazione pneumatica è a disposizione solo se la batteria valvole è configurata di conseguenza. La posizione dei bit di diagnosi per i comandi è riportata nelle relative descrizioni degli accoppiatori bus della serie AES.

4 Trasformazione e riparazione

Il sistema valvole può essere trasformato e riparato come riportato nelle descrizioni dei sistemi accoppiatore bus AES e driver valvole AV.

▶ Vedere anche capitolo → 2. Indicazioni di sicurezza e → 2.2 Qualifica del personale

5 Dati tecnici

I dati tecnici del sistema valvole sono riportati nella descrizione dei singoli sistemi.

▶ Rivolgersi ad AVENTICS GmbH per richiedere i dati necessari per la funzione di sicurezza, l'indirizzo è riportato sul retro.

6 Parametri di affidabilità

Sul nostro sito web è inoltre possibile scaricare le spiegazioni (parametri di affidabilità e indicazioni per l'applicazione della norma ISO 13849-1): www.emerson.com/de-de/expertise/automation/improving-safety-security/machine-safety.

I valori nella tabella corrispondono allo stato al momento della chiusura redazionale. I dati vengono aggiornati regolarmente e possono anche essere scaricati sul nostro sito web.

Índice

1 Acerca de esta documentación ... 46

1.1 Validez de la documentación ... 46

1.2 Documentación necesaria y complementaria ... 46

1.3 Presentación de la información ... 46

1.3.1 Advertencias ... 46

1.3.2 Símbolos ... 46

1.4 Denominaciones ... 46

1.5 Abreviaturas ... 46

2 Indicaciones de seguridad ... 46

2.1 Acerca de este capítulo ... 46

2.2 Cualificación del personal ... 46

2.3 Ubicación en cadenas de control relevantes para la seguridad ... 46

3 Sistema de válvulas en una cadena de control con función de seguridad ... 47

3.1 Preámbulo general (exoneración de responsabilidad) ... 47

3.2 El proceso para una máquina segura: la evaluación de riesgos ... 47

3.3 Información sobre los ejemplos ... 47

3.3.1 Sistematización de los ejemplos ... 47

3.3.2 Medidas de protección técnicas ... 47

3.4 Ejemplo 1 con PLr = e ... 47

3.4.1 Aplicación del ejemplo 1 ... 48

3.4.2 Funciones de seguridad ... 50

3.4.3 Cálculo del MTTF de la parte eléctrica y neumática del sistema de válvulas ... 51

3.4.4 Diagnóstico ... 51

3.4.5 Verificación del bit de diagnóstico ... 51

3.5 Ejemplo 2 con PLr = c ... 51

3.6 Ejemplo 3 con PLr = d ... 52

3.6.1 Exclusión de fallos ... 52

3.6.2 Sin exclusión de fallos ... 52

3.7 Resumen de las distintas opciones de alimentación ... 53

3.8 Asignación de las tensiones de alimentación en el sistema de válvulas ... 53

3.9 Conceptos de cableado del sistema de válvulas ... 53

3.10 Notas sobre el cableado ... 54

3.11 Descripción de la monitorización UAoff / UAon ... 54

4 Transformación y reparación ... 55

5 Datos técnicos ... 55

6 Parámetros de fiabilidad ... 55

1 Acerca de esta documentación

1.1 Validez de la documentación

Esta documentación se aplica a los componentes de la serie AV que se utilizan en cadenas de control relacionadas con la seguridad. Esta documentación va dirigida a programadores, planificadores de instalaciones eléctricas, reparadores de sistemas neumáticos, personal de servicio y operadores de sistemas.

Esta documentación contiene información importante para evaluar la exclusión de fallos para los sistemas de válvulas de la serie AV en determinadas condiciones.

1.2 Documentación necesaria y complementaria

- ▶ No ponga en funcionamiento los sistemas de válvulas de la serie AV en cadenas de control con función de seguridad hasta que disponga de la documentación del sistema de válvulas y de los componentes individuales y haya entendido su contenido.

Todas las instrucciones de montaje y las descripciones del sistema de las series AES y AV, así como los archivos de configuración del CLP, se encuentran en el CD R412018133.

1.3 Presentación de la información

1.3.1 Advertencias

Esta documentación incluye avisos de advertencia antes de los pasos siempre que exista riesgo de daños personales o materiales en el equipo. Se deberán cumplir las medidas descritas para evitar dichos peligros.

Estructura de las advertencias

⚠ PALABRA DE ADVERTENCIA

Tipo de peligro y origen

Consecuencias derivadas de la no observancia

- ▶ Precauciones

Significado de las palabras de advertencia

⚠ PELIGRO

Riesgo inmediato para la vida y la salud de las personas.

No respetar estas indicaciones tendrá consecuencias graves, incluida la muerte.

⚠ ADVERTENCIA

Posible riesgo para la vida y la salud de las personas.

No respetar estas indicaciones puede tener consecuencias graves, incluida la muerte.

⚠ ATENCIÓN

Posible situación peligrosa.

No respetar estas indicaciones podría ocasionar lesiones personales leves o daños materiales.

NOTA

Posibilidad de averías o daños materiales.

No respetar estas indicaciones podría ocasionar averías o daños materiales, pero no lesiones personales.

1.3.2 Símbolos

Recomendaciones para una utilización óptima de nuestros productos.

Tenga en cuenta esta información para garantizar el mejor funcionamiento posible.

1.4 Denominaciones

En esta documentación se utilizan las siguientes denominaciones:

Tab. 1: Denominaciones

Denominación	Significado
Bus backplane	Unión eléctrica interna del acoplador de bus con los controladores de válvula y los módulos E/S
Lado izquierdo	Zona E/S, a la izquierda del acoplador de bus mirando a sus conexiones eléctricas
Lado derecho	Zona de válvulas, a la derecha del acoplador de bus mirando a sus conexiones eléctricas
Controlador de válvula	Componente eléctrico del pilotaje de válvulas que transforma la señal procedente del bus backplane en corriente para la bobina magnética.

1.5 Abreviaturas

En esta documentación se utilizan las siguientes abreviaturas:

Tab. 2: Abreviaturas

Abreviatura	Significado
AES	**A**dvanced **E**lectronic **S**ystem
AV	**A**dvanced **V**alve
Módulo E/S	Módulo de **e**ntrada y **s**alida
IS12-PD	Válvula ISO con consulta de posición de la corredera
PL	**P**erformance **L**evel (Nivel de rendimiento)
CLP	**P**rogrammable **L**ogic **C**ontrol (pilotaje programable de memoria) o PC encargado de las funciones de control
UA	Tensión de actuadores (alimentación de tensión de las válvulas y las salidas)
UAoff	Mensaje de que la tensión del actuador UA ha caído por debajo del valor de la tensión de desconexión de las válvulas. Las válvulas están desconectadas eléctricamente.
UAon	Mensaje de que la tensión del actuador UA ha caído por debajo del valor de la tensión de conexión de las válvulas. Las válvulas no pueden conectarse eléctricamente.
UL	Tensión lógica (alimentación de tensión de la electrónica y los sensores)

2 Indicaciones de seguridad

2.1 Acerca de este capítulo

Este producto ha sido fabricado conforme a las reglas de la técnica generalmente conocidas. No obstante, existe riesgo de sufrir daños personales y materiales si no se tienen en cuenta este capítulo ni las indicaciones de seguridad contenidas en la documentación.

1. Lea esta documentación con detenimiento y por completo antes de trabajar con el producto.
2. Guarde esta documentación en un lugar al que siempre puedan acceder fácilmente todos los usuarios.
3. Transmita el producto a terceros siempre junto con la documentación requerida.
4. Respete la norma ISO 4414 para la manipulación segura de la neumática.

2.2 Cualificación del personal

Las actividades descritas en esta documentación requieren disponer de conocimientos básicos de electrónica y neumática, así como de la terminología correspondiente. Para garantizar un uso seguro, solamente el personal cualificado o bien otra persona supervisada por una persona cualificada podrá realizar estas actividades.

Por personal cualificado se entiende una persona que, en virtud de su formación especializada, sus conocimientos y experiencia, así como su conocimiento acerca de las normas vigentes, puede evaluar los trabajos que se le han encomendado, detectar potenciales peligros y adoptar medidas de seguridad adecuadas. Una persona cualificada debe cumplir las normas técnicas pertinentes.

2.3 Ubicación en cadenas de control relevantes para la seguridad

Los acopladores de bus y los controladores de válvula se pueden utilizar en cadenas de control con función de seguridad para la función de seguridad **"Función de parada relativa a la seguridad y otras funciones de seguridad iniciadas por un dispositivo de protección"** si el conjunto de la instalación está diseñado para ello.

3 Sistema de válvulas en una cadena de control con función de seguridad

3.1 Preámbulo general (exoneración de responsabilidad)

Los ejemplos mostrados en estas instrucciones representan una sección de un sistema de control relacionado con la seguridad. Estos ejemplos muestran los principios y no siempre todos los componentes necesarios. Para las aplicaciones en máquinas pueden ser necesarios otros componentes y evaluaciones. Las especificaciones no eximen al usuario de realizar sus propias evaluaciones y verificaciones. Debe tenerse en cuenta que nuestros productos están sometidos a un proceso natural de desgaste y envejecimiento.

3.2 El proceso para una máquina segura: la evaluación de riesgos

La evaluación de riesgos

- debe ser realizada por el fabricante de la máquina, los resultados son conservados por el fabricante
- debe considerar la utilización conforme a las especificaciones y también todo uso erróneo previsible de la máquina
- constituye una fuente de evidencia importante para el fabricante de la máquina en caso de posibles demandas de responsabilidad a causa de un accidente

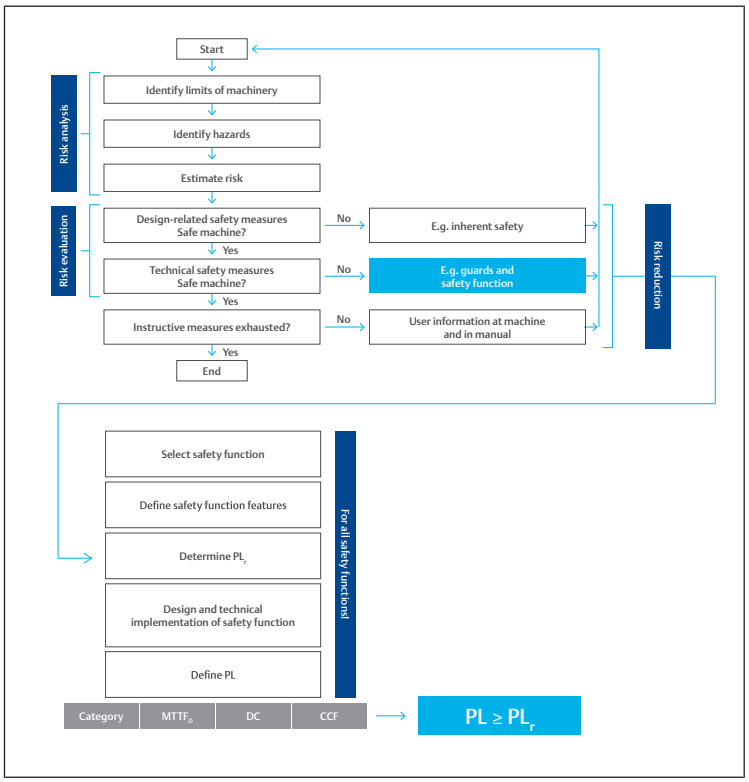


Fig. 1: Proceso de evaluación de riesgos y determinación del PL_r

En esta guía nos concentramos dentro del proceso de la evaluación de riesgos en la aplicación de medidas de protección técnicas para la reducción de riesgos, en la evaluación de la función de seguridad y en la determinación de su nivel de rendimiento. La figura muestra el proceso necesario para la evaluación de riesgos. En función de la arquitectura de control (categoría) del Mean Time To dangerous Failure ($MTTF_D$), del grado de cobertura de diagnóstico (DC) y del error resultante de una causa común (CCF), el nivel de rendimiento (PL) debe cumplir por lo menos el nivel de rendimiento (PL_r) necesario.

3.3 Información sobre los ejemplos

Los 3 ejemplos siguientes muestran:

- Ejemplo 1: Peligro debido a un arranque inesperado, PL_r = e
- Ejemplo 2: Peligro debido a un arranque inesperado, energía cinética restante, PL_r = c
- Ejemplo 3: Peligro debido a un arranque inesperado, PL_r = d con exclusión de fallos

3.3.1 Sistematización de los ejemplos

La sistematización de los ejemplos se basa en la clave para la identificación de partes de las funciones de seguridad del borrador VDMA 66416:2016-01.

La descripción general es la siguiente:

Observación preliminar

Descripción de las condiciones marginales:

- Tipo de máquina, tipo de funcionamiento...
- Peligro por...
- Parámetros de riesgo según la norma DIN EN ISO 13849-1:2016-06
- PL_r

Medidas de control (funciones de seguridad) y otras medidas de reducción de riesgos:

- Nombre de la función de seguridad
- Nombre de la función de seguridad
- ...

Entrada

Evento desencadenante:

- Consulta de los estados de los dispositivos de seguridad y
- Supervisión de los eventos
  Ejemplos: dispositivo de habilitación, parada de emergencia, interruptor de seguridad, interruptor llave,
- Rejilla de luz, presostato de seguridad...

Lógica

Evaluación de la función de seguridad:

- Desconexión de los suministros de energía, relé de seguridad, CLP de seguridad

Output

Respuesta orientada a la seguridad:

- Ejemplos: válvulas de fluidos, contactores, controladores, frenos...

3.3.2 Medidas de protección técnicas

Si la seguridad de una máquina depende de un control que funcione correctamente, se habla entonces de una “seguridad funcional”. Las piezas “activas” del control están en primer plano, es decir, los componentes que reconocen la situación peligrosa (detección de señales, “I” = Input), que deducen las reacciones adecuadas (evaluación, “L” = lógica) y que después aplican medidas de manera confiable (ejecución, “O” = Output). El término “control” contiene también el sistema de procesamiento de señales completo.

Las “piezas relacionadas con la seguridad de un control (SRP/CS)” no son necesariamente “componentes de seguridad” conforme a la directiva de máquinas. Sin embargo, la SRP/CS (Safety Related Part of a Control System) puede ser dichos componentes de seguridad, por ejemplo, controles bimanuales o unidades lógicas con función de seguridad. Los accionamientos (cilindro), el suministro de energía (como la alimentación de presión o las unidades de mantenimiento) y las conexiones no se consideran directamente en la estimación de las probabilidades de fallos que conlleven peligro.

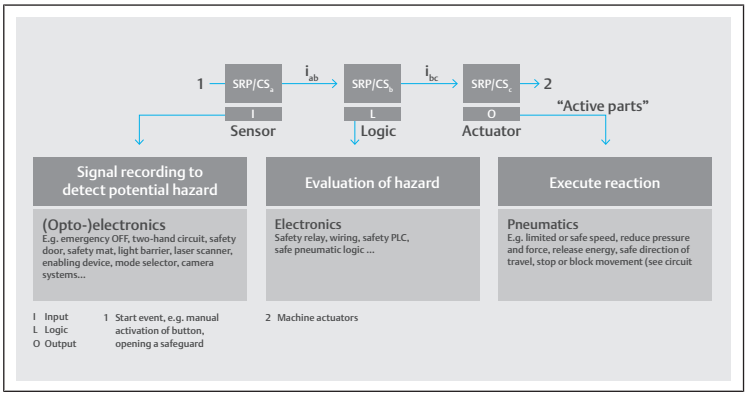


Fig. 2: Enfoque en piezas relacionadas con la seguridad de un control (SRP/CS conforme la ISO 13849-1)

3.4 Ejemplo 1 con PLr = e

Ejemplo 1, basado en VDMA 66416:2016-01, sección 2.1.1.1 y 2.2.1.1

Observación preliminar

Descripción de las condiciones marginales:

- Tipo de servicio: automático (BA1)
- Tiempo de ciclo de la máquina: de 5 a 15 segundos
- Peligro debido a un arranque inesperado
- PL_r = e

Medidas de control (funciones de seguridad):

- Desconexión de par segura (STO) o
- Desconexión segura del suministro de energía (SEC)
- Prevención del arranque inesperado (PUS)

Entrada

Evento desencadenante:

- Rejilla fotoeléctrica interrumpida o puertas de seguridad abiertas o que no se han mantenido cerradas

Lógica

Evaluación de la función de seguridad:

- Desconexión del suministro de energía

Output

Respuesta orientada a la seguridad:

- Desconexión del suministro de energía del fluido: $PL_r \geq d$ => 2 canales y del suministro de energía eléctrica: $PL_r \geq d$ => 2 canales recomendados

3.4.1 Aplicación del ejemplo 1

Según la norma ISO 13849, PL = e puede alcanzarse con la categoría 3 si se dan las siguientes circunstancias:

- CD_{avg} = medio
- MTTF = alto

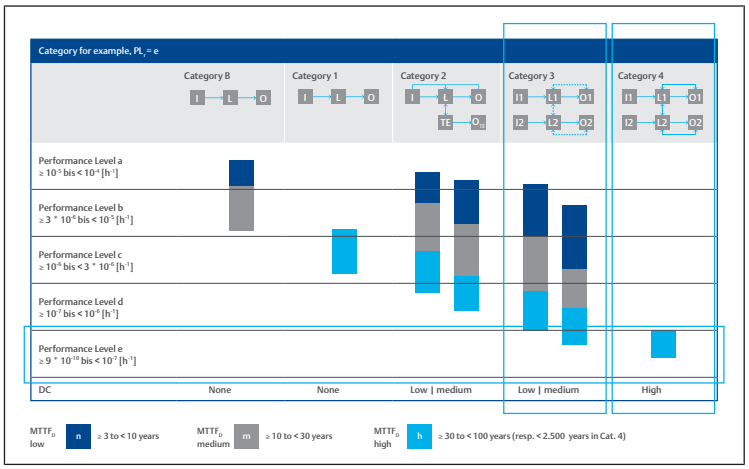


Fig. 3: Aplicación del ejemplo 1: PL_e con categoría 3, CD = medio, $MTTF_D$ = alto

Según el enfoque simplificado de la norma ISO 13849-1, las 4 clases de CD de cobertura de diagnóstico se definen del siguiente modo:

- ninguna: CD < 60 %
- baja: 60 % < CD < 90 %
- media: 90 % < CD < 99 %
- alta: 99 % < CD

Diseño e implementación técnica de la función de seguridad

Puesto de trabajo manual
TM=20 años
d/a=320 días
h/d=24 h/min. 10 sec duración del ciclo = 55.296.000 ciclos de conmutación para la válvula de aire de trabajo y principal

En el modo de preparación, los resguardos móviles deben puentearse y abrirse y los resguardos fijos deben instalarse.

INFO: Un único error no ocasiona la pérdida de la función de seguridad. Se detectan algunos errores, pero no todos. Sin embargo, una acumulación de errores desconocidos puede provocar la pérdida de la función de seguridad.

Selección de la válvula

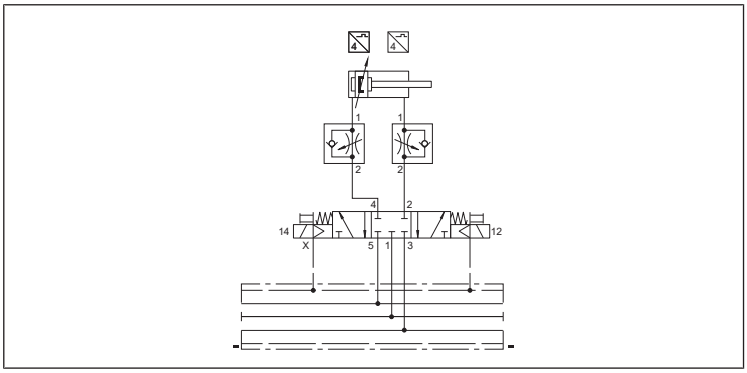


Fig. 4: Diagrama de conexiones: selección de la válvula

- Posición de conmutación definida y segura en estado sin corriente mediante resorte mecánico
- Los conductos de presión están bloqueados en estado sin corriente
- Los conductos de aire de escape no están abiertos
- El cilindro después de la PARADA DE EMERGENCIA no se puede mover, es decir, se requiere la liberación por parte de la persona
- Posibilidad de frenado de masas derramadas
- Parada segura durante movimientos verticales con masas (a partir de PL_d solo con medidas adicionales -> 2 canales)
- Es posible el funcionamiento JOG (golpeteo de la carrera del cilindro)
- No es posible la influencia transversal del aire de escape de cilindros vecinos de gran tamaño
- Adecuado hasta el Performance Level PL_e (medidas adicionales véase → Fig. 5.)
- Dirección de movimiento peligrosa permitida del cilindro en extensión y retracción
- La vida útil de las válvulas ha sido probada según la norma ISO 19973-1 y -2

Desconexión de seguridad neumática categoría 3 PL_e

Denominación:
Prevención de arranques inesperados (PUS) según la hoja de normas 24584 de VDMA.

Bloqueo de los flujos de volumen que entran y salen de ambas cámaras del pistón.

INFO: Al reiniciar, tener en cuenta:
Las cámaras de los cilindros pueden purgarse debido a fugas de componentes individuales.

INFO: Los impulsos de prueba pueden provocar la conmutación de las válvulas.

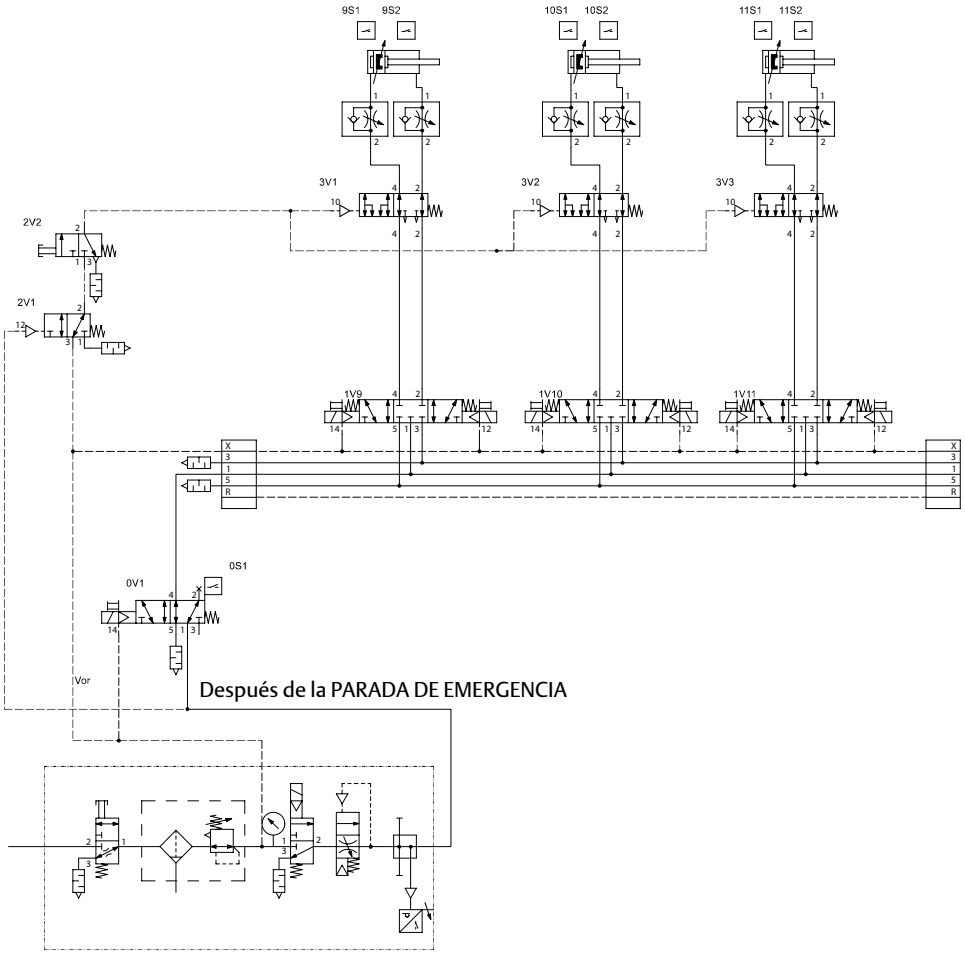


Fig. 5: Diagrama esquemático: canales de función y de prueba

INFO: Si realiza simultáneamente la aplicación de aire/el escape de más de 8 válvulas, observe que se disponga de aplicación de aire/escape adicional por medio de placas de alimentación.

Liberación de personas por escape (para circuitos con mantenimiento de posición)

Para movimientos verticales y horizontales:

- Gravedad de la lesión = S2 (lesión normalmente irreversible, incluyendo la muerte)
- La zona de peligro está en el área accesible
- El personal de manejo no puede liberarse por sí mismo
- El escape no debe causar ningún peligro adicional

La liberación de personas solo puede realizarse en las siguientes circunstancias:

- Solo en estado sin presión
- Tras la parada de emergencia activa por 2V1 (un 2V1 puede alimentar varios 2V2), este debe montarse cerca del punto de peligro
- Prever un desbloqueo personal común para los grupos de cilindros (un 2V2 puede purgar varios cilindros)

Diagrama de bloques

La siguiente figura muestra el diagrama de bloques de seguridad del ejemplo 1.

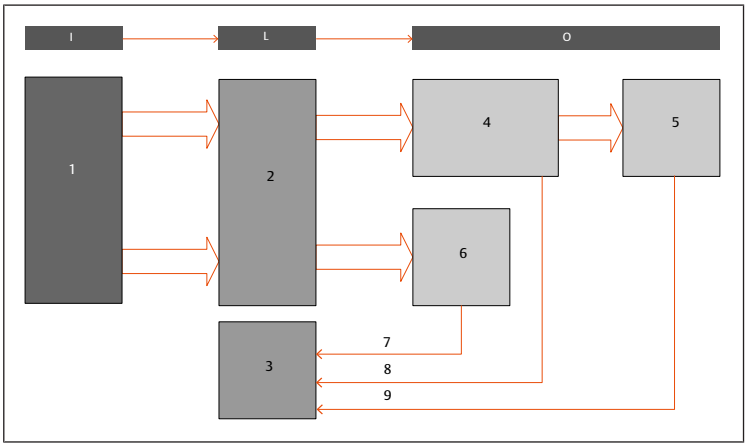


Fig. 6: Diagrama de bloques de seguridad, ejemplo 1

1 Interruptor de puerta protectora (por ejemplo, PILZ PSEN cs3.1 o PSEN sl-0.5p 1.1)

2 Elemento de seguridad (por ejemplo, PILZ PNOZ)

3 CLP (controlador lógico programable)

4 Parte eléctrica del sistema de válvulas AV Alimentación UA mediante placa de alimentación eléctrica

5 Parte neumática del sistema de válvulas AV

6 Válvula de aire principal con consulta de la posición de la corredera (por ejemplo, IS12-PD)

7 Diagnóstico “Consulta de la posición de la corredera de la válvula de aire principal”

8 Mensaje de diagnóstico “La tensión de la válvula UA es inferior a la tensión de desconexión (UA < UAoff)”

9 Diagnóstico “Consulta indirecta de la válvula de trabajo”

Diagrama de conexiones neumático

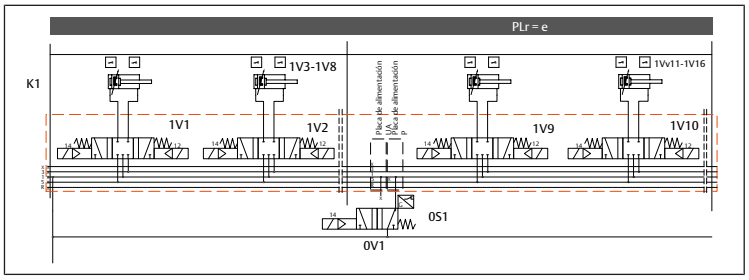


Fig. 7: Diagrama de conexiones neumático, ejemplo 1

K1	Sistema portaválvulas	1V1 – 1V8	Válvulas fuera de la cadena de control de seguridad
1V3 – 1V8	No dibujado	1V9 – 1V16	Válvulas para accionamientos con PL_r = e
1V1 – 1V16	No dibujado	0S1	Detección de posición desde 0V1
0V1	Válvula de aire principal		

Sistema de válvulas completo con componentes externos

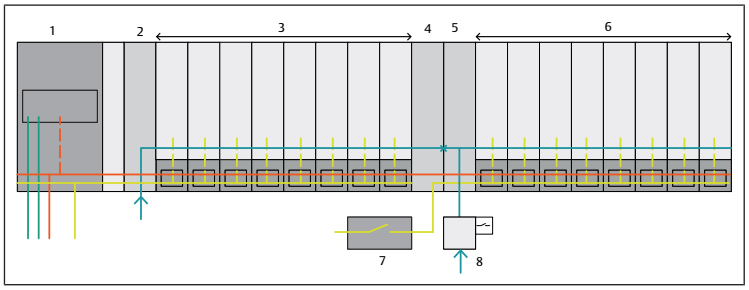


Fig. 8: Sistema de válvulas y componentes externos

1 Acoplador de bus
2 Placa de alimentación neumática
3 Válvulas (no en el circuito de seguridad)
4 Placa de alimentación eléctrica - corresponde al bloque 4 del diagrama de bloques de seguridad
5 Placa de alimentación neumática, - No es necesaria la supervisión (UA-off), sin electrónica activa instalada
6 Válvulas (circuito de seguridad) - Corresponde al bloque 5 del diagrama de bloques de seguridad - La parte eléctrica de las válvulas (controlador de válvulas) corresponde al bloque 4 del diagrama de bloques de seguridad
7 Módulo de control de seguridad, corresponde al bloque 2 del diagrama de bloques de seguridad
8 La válvula de aire principal corresponde a los bloques 6 y 7 del diagrama de bloques de seguridad

3.4.2 Funciones de seguridad

Evitar, por motivos de seguridad, el arranque inesperado desde la posición de reposo, con opción de liberación del personal.

En esta documentación solo se muestra la pieza de control neumático como subsistema. Para la función de seguridad completa, se deben agregar otras piezas de control de seguridad (por ejemplo, dispositivos protectores y lógica eléctrica) como subsistemas.

- Gravedad de la lesión = S2
- El punto peligroso se encuentra en la zona accesible y el personal de montaje no puede liberarse
- El escape no debe causar ningún peligro adicional
- Como el desbloqueo personal 2V1, 2V2, 3V1 y 3Vn después de la parada de emergencia, es decir, después de purgar la válvula de 3/2 válvulas distribuidoras en la unidad de preparación de aire, es totalmente funcional y no influye en la función de seguridad, no se tienen en cuenta en el cálculo.

Esto solo se puede realizar por la siguiente circunstancia:

- Solo en estado sin presión
- Tras la parada de emergencia activa por 2V1 (un 2V1 puede alimentar varios 2V2), este debe montarse cerca del punto de peligro
- Prever un desbloqueo personal común para los grupos de cilindros (un 2V2 puede purgar varios cilindros)

Descripción funcional de la conexión PL c, d, e_Kat-3_02 cuando se utiliza en un puesto de trabajo manual

- Los movimientos se pilotan de forma redundante mediante la válvula neumática principal 0V1 y la válvula de trabajo 1Vn
- La válvula 0V1 debe estar controlada constantemente para poder pilotar 1Vn
- Tan solo el fallo de una de las válvulas mencionadas no ocasiona la pérdida de la función de seguridad
- Todas las válvulas se pilotan cíclicamente en el proceso
- El funcionamiento de la válvula de aire principal 0V1 se controla mediante una consulta de posición de la válvula 0S1
- La función de la válvula de trabajo 1Vn se detecta indirectamente durante el proceso mediante los interruptores nS1 y nS2
- La acumulación de errores no detectados puede provocar la pérdida de la función de seguridad
- Se requieren medidas adicionales si existe un peligro debido a la energía almacenada (presión, masa, muelle)

Características constructivas

- Se cumplen los principios de seguridad básicos y probados, así como los requisitos de la categoría B
- La válvula neumática principal 0V1 se desplaza a la posición de conmutación de seguridad mediante un resorte
- La válvula de trabajo nV1 tiene una posición central bloqueada (sin intersecciones) con centrado por muelle
- La posición de conmutación segura se alcanza para ambas válvulas después de desconectar la tensión de mando
- El procesamiento de señales de las consultas y la supervisión de las válvulas se realiza en un pilotaje de PLC de un canal
- Control en ON y puerta de carga cerrada:
  - La válvula de aire principal 0V1 se conmuta y se aplica tensión al sistema de válvulas.
- Modo automático ON y puerta de carga abierta:
  - No hay tensión en la válvula de aire principal 0V1 ni en el sistema de válvulas
- Modo de puesta en marcha y puerta de seguridad puenteada con interruptor llave:
  - No hay tensión en la válvula de aire principal 0V1 ni en el sistema de válvulas
  - El conducto neumático entre la válvula de aire principal 0V1 y la válvula de trabajo nV1 está purgado
  - Los movimientos solo son posibles con un interruptor de habilitación adicional
  - El interruptor de habilitación conmuta la válvula de aire principal 0V1 y se aplica tensión al sistema de válvulas
  - Los movimientos peligrosos sin medidas adicionales justificadas solo se permiten si la puerta protectora está cerrada

Cálculo de la probabilidad de fallo y de la vida útil

Vida útil requerida:
20 años / 320 días / 24 h / 10 seg. Duración del ciclo (nop = 2764800 ciclos/año)

- Válvula 0V1 B_{10D} = 79,2 millones (IS12-PD)
- Válvula nV1 B_{10D} = 39,6 millones (AV05) o válvula nV1 B_{10D} = 105,8 millones (AV03)

3.4.3 Cálculo del MTTF de la parte eléctrica y neumática del sistema de válvulas

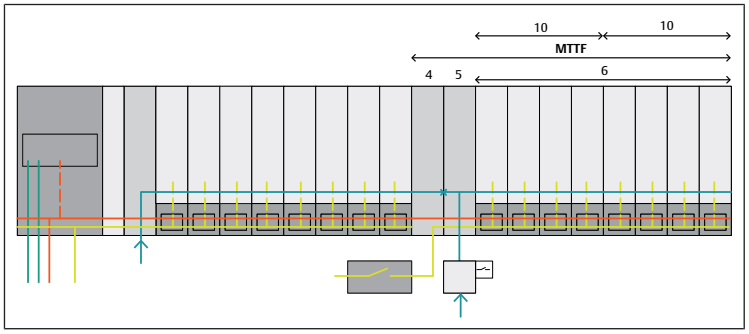


Fig. 9: Componentes relevantes para el cálculo del $MTTF_D$ para la parte eléctrica

4 Placa de alimentación eléctrica con control UAon, corresponde al bloque 4 del diagrama de bloques de seguridad

5 Placa de alimentación neumática con control UAoff, la función eléctrica = supervisión de UAoff corresponde a los bloques 4 y 8 del diagrama de bloques de seguridad

6 Válvulas (circuito de seguridad) corresponde al bloque 5 del diagrama de bloques de seguridad la parte eléctrica de las válvulas (controlador de válvulas) corresponde al bloque 4 del diagrama de bloques de seguridad

10 Placa de controlador de 4 válvulas

Véase → 6. Parámetros de fiabilidad y → Fig. 9

De esto se deduce:

- Placa de alimentación eléctrica (**4**) MTTF = 854 años
- Supervisión de UAoff (**5**) MTTF = 1094 años
- Placa de controlador de 4 válvulas (**10**) MTTF = 630 años
- Válvulas AV03 5/3 retorno por muelle (**6**) MTTF = 382,7 años

$$MTTF_{ges} = \frac{1}{\frac{1}{854\ [a]} + \frac{1}{1094\ [a]} + \frac{1}{630\ [a]} + \frac{1}{630\ [a]} + \frac{1}{382{,}7\ [a]}} = 127\ [a]$$

Los valores MTTF de los módulos AES se calcularon utilizando las tasas de fallo de una base de datos.

Según la norma DIN EN 13849-1, anexo C, no todo fallo es un fallo peligroso. En este caso, se puede establecer $MTTF_D = 2 \times MTTF_{ges}$ para el cálculo de todo el sistema.

$MTTF_D = 2x\ MTTF_{ges} = 2 \times 127\ [a] = 254\ [a]$

3.4.4 Diagnóstico

La placa de alimentación neumática supervisa la tensión UA del actuador y envía el bit de diagnóstico UAoff si UA cae por debajo de la tensión de desconexión.

La placa de alimentación eléctrica supervisa la tensión UA del actuador y envía el bit de diagnóstico UAon si UA cae por debajo de la tensión de conexión.

Debe controlarse el bit de diagnóstico (UAoff). Para ello es necesario cambiar la señal. Esto puede hacerse, por ejemplo, al encender la máquina o con ciclos de prueba especiales.

Consulta directa de la posición de la corredera en la válvula principal 99 %.

Consulta de funcionamiento indirecto de la válvula de trabajo 90 %.

CD = 94,4 % $MTTF_D$ = alto (100 J) CCF = 95

CCF in our example				
Countermeasure for CCF	Fluid technology	Electronics	Points	
Separation of signal paths	Separation of tubing	Air and creepage distance on activated circuits	15	✓
Diversity	E.g. different valves	E.g. different processors	20	✓
Protection against overvoltage, overpressure ...	Setup acc. to EN ISO 4413 to EN ISO 4414 (pressure relief valve)	Overvoltage protection (e.g. contactors, power pack)	15	✓
Use of well-tried components	User		5	✓
FMEA in development	FMEA during initial system conception		5	½
Competence/training	Qualification measure		5	✓
Protection against contamination and EMC	Fluid quality	EMC test	25	✓
Other effects (e.g. temperature, shock)	Compliance with EN ISO 4413 and EN ISO 4414 and product spec	Observe ambient conditions as described in product spec	10	✓
Total CCF	Total points(65 ≤ CCF ≤ 100):			95

Fig. 10: Ejemplo: CCF – Errores por causa común

Performance Level = PL_e / categoría = 3

No es necesario sustituir la válvula de aire principal 0V1 (IS12-PD).

No es necesario sustituir la válvula nV1 (AV03).

Sustitución de la válvula nV1 (AV05) después de 14,3 J; no es necesario para tiempos de ciclo ≥ 14 seg. o vida útil de 20 años.

3.4.5 Verificación del bit de diagnóstico

Encontrará una descripción detallada del seguimiento en el capítulo → 3.11 Descripción de la monitorización UAoff / UAon.

Cuando se desconecta la tensión UA, deben enviarse tanto el mensaje de diagnóstico UAon como UAoff.

Tab. 3: Verificación del bit de diagnóstico

UA = 0, desconectado	Diagnóstico de encendido UA-on	Diagnóstico de desconexión UAoff
válido	1	1
no válido	1	0
no válido	0	1

Si se tienen en cuenta las condiciones mencionadas, se pueden utilizar las siguientes normas para estimar el control de la tensión de la válvula de desconexión con una CD = del 90 % al < 99 % (media):

- DIN EN ISO 13849-1 Anexo E: “Estimaciones de la cobertura de diagnóstico (CD) para funciones y módulos”
- DIN EN 61508-2: “Tabla A.14 - Elementos de mando (actuadores)”
- DIN EN 61508-2: “Tabla A.7. Unidades de E/S e interfaces (comunicación externa)”

3.5 Ejemplo 2 con PLr = c

Ejemplo 2, basado en 66416:2016-01, número 1.1.2.1 y 2.1.2.3

Observación preliminar

Descripción de las condiciones marginales:

- Modo de funcionamiento BA2 Modo de configuración o tipo de servicio
- Peligro por arranque inesperado, energía cinética restante
- $PL_r = c$

Medidas de control (funciones de seguridad) (véase la observación):

- Desconexión de par segura (STO)
- Desconexión segura del suministro de energía (SEC)
- Prevención del arranque inesperado (PUS)

Entrada

Evento desencadenante:

- Conmutador de modo de funcionamiento, dispositivo de habilitación

Lógica

Evaluación de la función de seguridad:

- Desconexión del suministro de energía

Output

Respuesta orientada a la seguridad:

- Contención de 1 canal de medio fluido. Son posibles las siguientes conversiones:
  - Válvula distribuidora en posición de bloqueo
  - Pilotaje de válvula(s) de bloqueo
  - S1 posible porque la energía residual solo produce lesiones reversibles
- Desconexión del suministro de energía eléctrica: $PL_r \geq d$ => 2 canales recomendados

Observación

El tema de la energía residual se describe con más detalle en los siguientes documentos:

- Borrador VDMA 66416: Capítulo 5.1.3 Modo de configuración o tipo de servicio (BA2) “Las velocidades reducidas se proporcionarán como sigue...”
- Borrador VDMA 66416: Tabla A2. Clave para la identificación de las estimaciones de los parámetros del gráfico de riesgo de la tabla A7

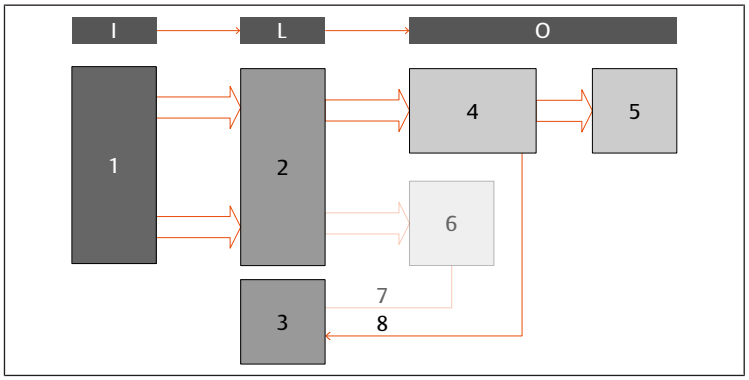


Fig. 11: Diagrama de bloques de seguridad, ejemplo 2

1 Dispositivo de habilitación
2 Elemento de seguridad (por ejemplo, PILZ PNOZ)
3 CLP (controlador lógico programable)
4 Parte eléctrica del sistema de válvulas AV, alimentación UA mediante placa de alimentación eléctrica
5 Válvula distribuidora del sistema de válvulas AV
6 Válvula de aire principal con consulta de la posición de la corredera (por ejemplo, IS12-PD...)
No activo para esta función de seguridad
7 Diagnóstico "Consulta de la posición deslizante de la válvula de aire principal"
No activo para esta función de seguridad
8 Diagnóstico "La tensión de válvula UA es inferior a la tensión de desconexión (UA < UAoff)"

3.6 Ejemplo 3 con PLr = d

Ejemplo 3, basado en VDMA 66416, número 2.1.1.1 y 2.2.1.1

Este ejemplo es similar al ejemplo 1, pero el PL_r requerido es d.

Observación preliminar

Descripción de las condiciones marginales:

- Tipo de servicio automático (BA1)
- Peligro debido a un arranque inesperado
- PL_r = d

Medidas de control (funciones de seguridad):

- Desconexión de par segura (STO)
- Desconexión segura del suministro de energía (SEC)
- Prevención del arranque inesperado (PUS)

Entrada

Evento desencadenante:

- Rejilla fotoeléctrica interrumpida o puertas de seguridad abiertas o que no se han mantenido cerradas

Lógica

Evaluación de la función de seguridad:

- Desconexión del suministro de energía

Output

Respuesta orientada a la seguridad:

- Desconexión de suministro de energía de fluido: $PL_r \geq d$ => 2 canales y suministro de energía eléctrica: $PL_r \geq d$ => 2 canales recomendados

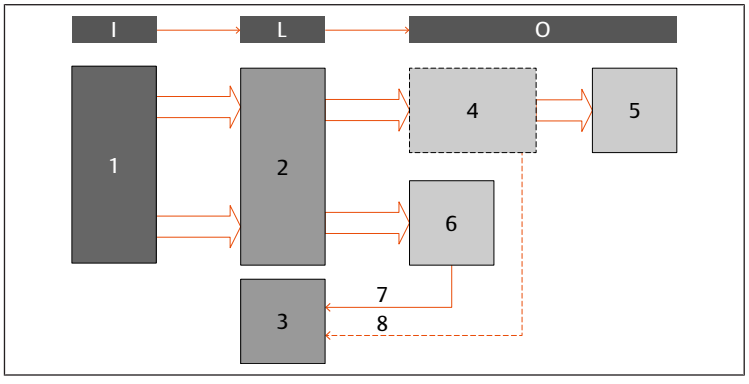


Fig. 12: Diagrama de bloques de seguridad, ejemplo 3

1 Interruptor de puerta protectora (por ejemplo, PILZ PSEN cs3.1 o PSEN sl-0.5p 1.1)
2 Elemento de seguridad (por ejemplo, PILZ PNOZ)
3 CLP (controlador lógico programable)
4 Pieza eléctrica del sistema de válvulas AV
O alimentación UA mediante placa de alimentación eléctrica. Es posible excluir fallos de este bloque (véase → 3.6.1 Exclusión de fallos).
O alimentación UA mediante acoplador de bus. No se pueden excluir fallos (véase → 3.6.2 Sin exclusión de fallos).
5 Válvula distribuidora del sistema de válvulas AV
6 Válvula de aire principal con consulta de la posición de la corredera (por ejemplo, IS12-PD...)
7 Diagnóstico "Consulta de la posición de la corredera de la válvula de aire principal"
8 Diagnóstico "La tensión de válvula UA es inferior a la tensión de desconexión (UA < UAoff)"
Si se aplica la exclusión de fallos para (**4**), este diagnóstico no es necesario.

3.6.1 Exclusión de fallos

Si el sistema de válvulas se configura y aplica como se describe en los capítulos siguientes, no es necesario incluir la electrónica de la válvula en el cálculo de los valores MTTF de una cadena de control relacionada con la seguridad.

El requisito previo para la aplicación de la exclusión de fallos es:

- que se aplique un máximo de PL d (PL e debe calcularse como en el ejemplo 1),
- que el sistema de válvulas esté configurado con una o varias placas de alimentación eléctrica,
- que las válvulas que deben desconectarse se alimenten a través de estas placas de alimentación eléctrica,
- que las placas de alimentación eléctrica estén cableados de acuerdo con los conceptos de cableado 1-3,
- que el cable de conexión de la placa de alimentación solo contenga la tensión de alimentación de 24 V UA y
- que el cable esté tendido de acuerdo con la norma DIN EN 60204.

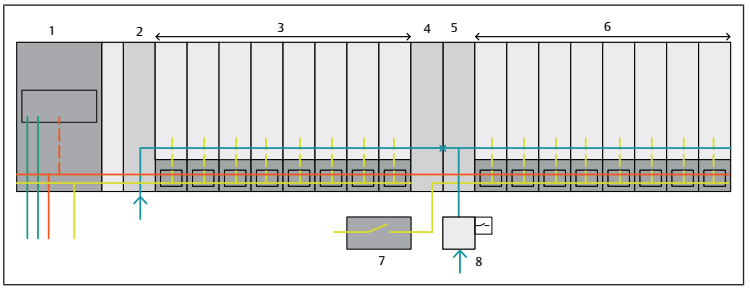


Fig. 13: Sistema de válvulas y componentes externos

1 Acoplador de bus
2 Placa de alimentación neumática
3 Válvulas (no en el circuito de seguridad)
4 Placa de alimentación eléctrica - corresponde al bloque 4 del diagrama de bloques de seguridad
5 Placa de alimentación neumática, - No es necesaria la supervisión (UA-off), sin electrónica activa instalada
6 Válvulas (circuito de seguridad) - Corresponde al bloque 5 del diagrama de bloques de seguridad - La parte eléctrica de las válvulas (controlador de válvulas) corresponde al bloque 4 del diagrama de bloques de seguridad
7 Módulo de control de seguridad, corresponde al bloque 2 del diagrama de bloques de seguridad
8 La válvula de aire principal corresponde a los bloques 6 y 7 del diagrama de bloques de seguridad

3.6.2 Sin exclusión de fallos

Si se aplicara la alimentación UA mediante acoplador de bus, no se podrán excluir fallos. Debe contarse con la probabilidad de fallo.

Observar las medidas siguientes:

- La alimentación UA mediante acoplador de bus debe desconectarse con seguridad para evitar que las válvulas se conecten de forma inesperada.
- El cableado debe tenderse conforme a la norma DIN EN 60204.
- Deberá evaluarse el diagnóstico del acoplador de bus (UAon y UAoff).

En función del rendimiento necesario, podrían requerirse otras medidas.

3.7 Resumen de las distintas opciones de alimentación

Tab. 4: Varias opciones de alimentación

	Alimentación UA mediante acoplador de bus	Alimentación UA mediante placa de alimentación eléctrica
PL_r máximo alcanzable	d (e no recomendado)	e
¿Es posible la exclusión de fallos?	no véase → 3.6.2 Sin exclusión de fallos	$PL_r \leq$ d: sí PL_r = e: no
Evaluación del diagnóstico	sí (UAon y UAoff del acoplador de bus)	$PL_r \leq$ d: no (no es necesario debido a la exclusión de fallos) PL_r = e: sí (UAon y UAoff) La placa de alimentación neumática debe estar equipada con supervisión UAoff.
CD	90 % ... < 99 %	90 % ... < 99 %
Limitación de la corriente de arranque	sí	sí
Posibilidad de pruebas (conexión cruzada)	no	sí

Limitación de la corriente de arranque

La elevadísima corriente de irrupción de la unidad, como suele ocurrir con las cargas capacitivas, está limitada a un valor máximo de 5 A.

Definición impulso de prueba

Un impulso de prueba es un cambio limitado en el tiempo del nivel de tensión de una señal para comprobar el funcionamiento de la salida o el aparato o para comprobar la ruta de transmisión.
[Fuente: ZVEI (Asociación Alemana de Fabricantes de Material Eléctrico y Electrónico), documento de posición Clasificación de interfaces binarias de 24 V con pruebas en el ámbito de la seguridad funcional]

Posibilidad de pruebas

Las salidas seguras y/o los módulos de seguridad generan señales de reloj o impulsos de prueba en sus salidas. Si se conecta una salida de este tipo a la placa de alimentación eléctrica, no se produce una interpretación errónea de la prueba de circuito cruzado. Si se utiliza una salida de este tipo para la alimentación de UA en el acoplador de bus, se produce una interpretación errónea de la comprobación de conexión cruzada.

Observación

Solo puede probarse la línea de transmisión hasta la placa de alimentación eléctrica.

3.8 Asignación de las tensiones de alimentación en el sistema de válvulas

La siguiente figura muestra la asignación de las tensiones de alimentación a las funciones dentro del sistema de válvulas.

- La tensión de alimentación **UL** introducida en el acoplador de bus (**1**) alimenta toda la electrónica del sistema de válvulas.
- La tensión de alimentación **UA** alimentada en el acoplador de bus alimenta las salidas del módulo DO (**6**) (salida digital) y todas las válvulas entre el acoplador de bus y la alimentación UA.

El módulo “placa de alimentación eléctrica” (**5**) interrumpe la tensión de alimentación entrante **UA** . La tensión de alimentación de este módulo se utiliza para todas las válvulas situadas a la derecha de la placa de alimentación eléctrica. El módulo “placa de alimentación eléctrica” puede utilizarse varias veces en la zona de válvulas.

La tensión **UL** siempre está aislada galvánicamente de la tensión **UA** en la unidad de válvulas.

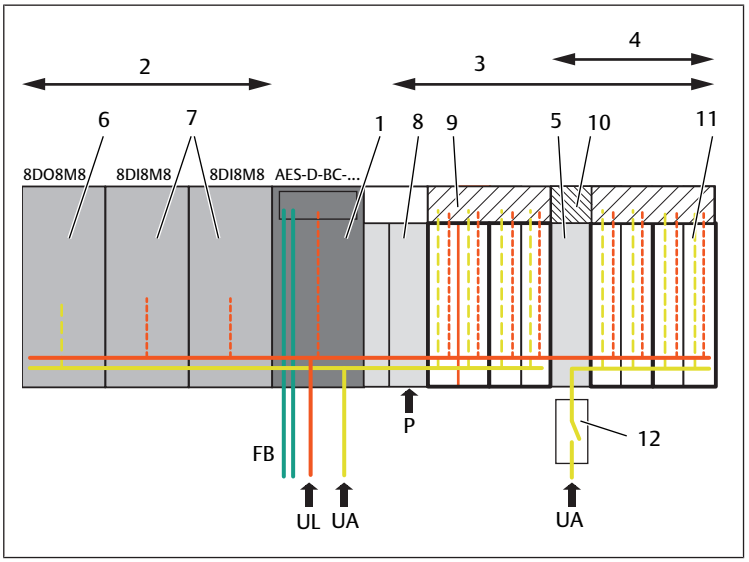


Fig. 14: Asignación de las tensiones de alimentación UL y UA

1	Acoplador de bus	2	Módulos E/S
3	Zona de válvulas	4	Parte de la cadena de control de seguridad
5	Placa de alimentación eléctrica	6	Módulo de salida
7	Módulo de entrada	8	Placa de alimentación neumática
9	Placa de controlador de 4 válvulas	10	Placa de alimentación
11	Válvula	12	Elemento de seguridad
UL	Tensión de alimentación de 24 V para la electrónica y la lógica	UA	Tensión de alimentación de 24 V para los actuadores
FB	Bus de campo		

3.9 Conceptos de cableado del sistema de válvulas

Las 3 ilustraciones siguientes muestran los diferentes conceptos de cableado del sistema de válvulas.

Para las 3 representaciones se aplica lo siguiente:

- La alimentación de tensión en el acoplador de bus (K1) para **UL** y **UA** se realiza a través del conector **X1S1**.
- La tensión de alimentación segura de las válvulas se alimenta siempre a través de la conexión de la placa de alimentación eléctrica adicional (**X1S2**) de las válvulas.

Para los siguientes conceptos de cableado, se utilizan los equipos con las designaciones de referencia basadas en la norma EN 81346. Los ejemplos solo muestran el recorte correspondiente de la alimentación de tensión y no están completos. Se requiere equipo adicional para su uso dentro de una máquina.

Véase → Fig. 14. En el diagrama de conexiones, se utiliza un bloque de alimentación común (**L01**) para ambas tensiones **UL** y **UA**. La tensión de las válvulas en la conexión **X1S2** se desconecta en ambos polos (es decir, **UA+** y **UA–**) a través del módulo de control de seguridad.

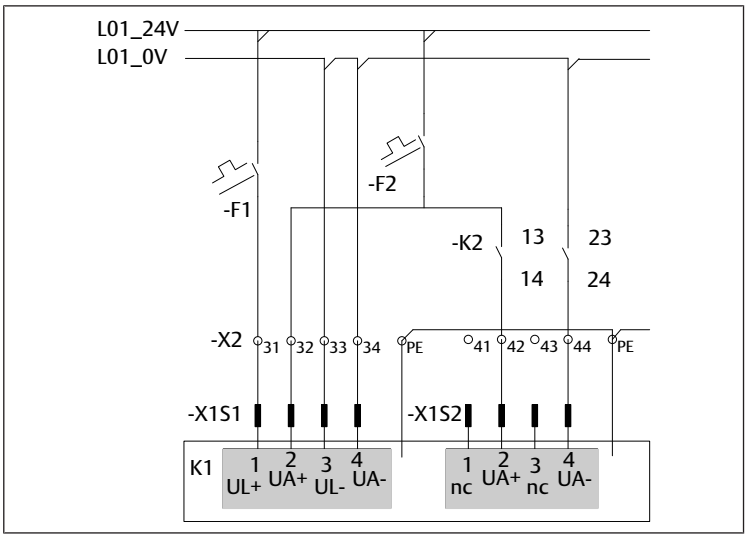


Fig. 15: Concepto de cableado 1

-K1	Sistema de válvulas con 2 conectores para alimentación de tensión	**-K2**	Elemento de seguridad
-X1S1	Conexión para la alimentación de tensión del acoplador de bus	**-X1S2**	Conexión para la alimentación de tensión de la placa de alimentación eléctrica
-F1	Protección por fusible de la tensión **UL**	**-F2**	Protección por fusible de la tensión **UA**
-X2	Abrazadera	**L0x**	Alimentación de tensión

En el siguiente ejemplo, se utilizan 2 bloques de alimentación con separación para ambas tensiones **UL** (**L01**) y **UA** (**L02**). La tensión de las válvulas en la conexión **X1S2** se desconecta en ambos polos (es decir, **UA+** y **UA–**) a través del módulo de control de seguridad.

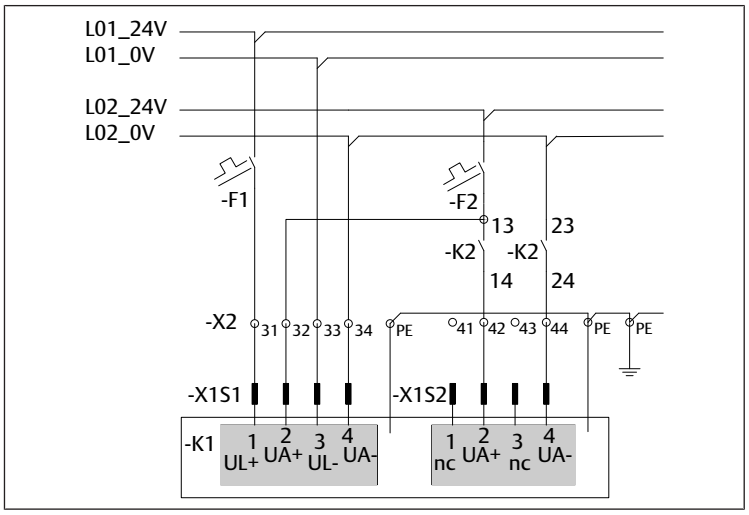


Fig. 16: Concepto de cableado 2

-K1	Sistema de válvulas con 2 conectores para alimentación de tensión	**-K2**	Elemento de seguridad
-X1S1	Conexión para la alimentación de tensión del acoplador de bus	**-X1S2**	Conexión para la alimentación de tensión de la placa de alimentación eléctrica
-F1	Protección por fusible de la tensión **UL**	**-F2**	Protección por fusible de la tensión **UA**
-X2	Abrazadera	**L0x**	Alimentación de tensión

En el siguiente ejemplo, se utiliza un bloque de alimentación común (**L01**) para ambas tensiones **UL** y **UA**. La tensión para las válvulas en la conexión **X1S2** se desconecta unipolarmente **UA+** a través del módulo de control de seguridad.

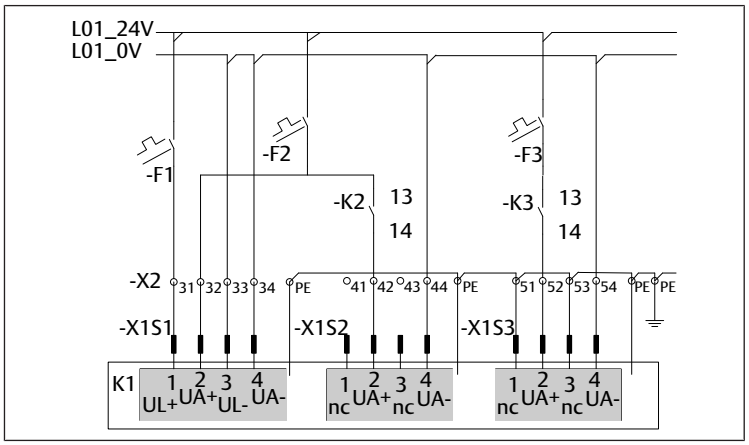


Fig. 17: Concepto de cableado 3

-K1	Sistema de válvulas con 3 conectores para alimentación de tensión	**-K2**	Elemento de seguridad
-X1S1	Conexión para la alimentación de tensión del acoplador de bus	**-X1S2**	Conexión para la alimentación de tensión de la placa de alimentación eléctrica
-X1S3	Conexión para la alimentación de tensión de la placa de alimentación eléctrica	**-F1**	Protección por fusible de la tensión **UL**
-F3	Protección por fusible de la tensión **UA**	**-F2**	Protección por fusible de la tensión **UA**
-K3	Elemento de seguridad	**-X2**	Abrazadera
L0x	Alimentación de tensión		

3.10 Notas sobre el cableado

Al utilizar los conceptos de cableado mencionados, se deben tener en cuenta las siguientes notas:

1. Conecte el sistema de válvulas como se muestra en los 3 conceptos de cableado.
2. Asegúrese de que las válvulas que deben desconectarse de forma segura se encuentran detrás de la placa de alimentación eléctrica.
3. Conecte **X1S2** a través de un cable de 2 hilos.

Cuando se utiliza un cable con más de 2 núcleos, se deben tener en cuenta los siguientes hechos. Véase → Fig. 17:

- Los núcleos no utilizados se conectan a PE por razones de EMC
- No hay más tensión en el cable.

En caso de desconexión unipolar de la tensión UA, el cable correspondiente debe tenderse a prueba de cortocircuitos.

3.11 Descripción de la monitorización UAoff / UAon

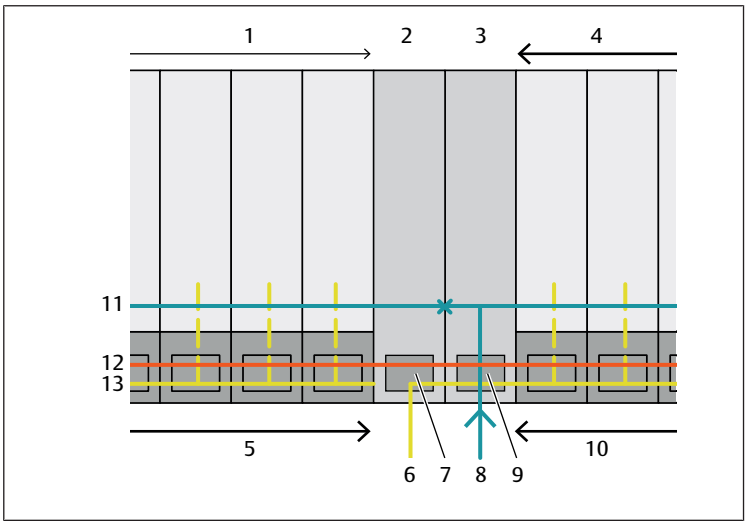


Fig. 18: Detalle de la imagen UAoff / UAon

1	Válvulas anteriores
2	Placa de alimentación eléctrica
3	Placa de alimentación neumática
4	Válvulas siguientes
5	Controlador de válvula
6	Tensión del actuador UA de la placa de alimentación eléctrica
7	Supervisión de UAon en la placa de alimentación eléctrica
8	Alimentación de aire comprimido de la placa de alimentación neumática
9	Supervisión de UAoff en la placa de alimentación neumática
10	Controlador de válvula
11	Suministro de P existente
12	Tensión UL pasante
13	Tensión UA actual

La placa de alimentación eléctrica (**2**) interrumpe el suministro de UA a las válvulas. Las válvulas anteriores (**1**) se suministran con la tensión de válvula existente. Las siguientes válvulas (**4**) se suministran con la nueva tensión de válvula (**6**).

En la placa de alimentación eléctrica, la nueva tensión (**6**) se controla para el límite UAon.

Si la tensión UA cae por debajo de la tensión de conexión UAon, la placa de alimentación eléctrica envía el bit de diagnóstico UAon.

La placa de alimentación neumática (**3**) interrumpe la alimentación P (**11**) de las válvulas. Las válvulas anteriores (**1**) se alimentan con el aire comprimido existente. Las siguientes válvulas (**4**) se suministran con el nuevo aire comprimido de (**8**).

En la placa de alimentación neumática se supervisa la tensión UA existente para el límite UAoff.

Si la tensión UA cae por debajo de la tensión de desconexión UAoff, la placa de alimentación neumática envía el bit de diagnóstico UAoff.

La supervisión de la tensión UA en la placa de alimentación neumática solo está disponible si el sistema del terminal de válvulas se ha configurado en consecuencia. La posición de los bits de diagnóstico en el área de datos de los controladores puede consultarse en las descripciones correspondientes de los acopladores de bus de la serie AES.

4 Transformación y reparación

Puede modificar y reparar el sistema de válvulas como se describe en las descripciones del sistema del acoplador de bus AES y del controlador de válvulas AV.

▶ Véanse también los capítulos → 2. Indicaciones de seguridad y → 2.2 Cualificación del personal

5 Datos técnicos

Los datos técnicos del sistema de válvulas pueden encontrarse en las respectivas descripciones de sistema.

▶ Póngase en contacto con AVENTICS GmbH para obtener los datos necesarios para la función de seguridad; consulte la dirección en la contraportada.

6 Parámetros de fiabilidad

Puede obtener las explicaciones (valores característicos de fiabilidad y otra información sobre la aplicación de la ISO 13849-1) descargándolas de nuestra página Web: www.emerson.com/de-de/expertise/automation/improving-safety-security/machine-safety.

Los valores en la tabla corresponden al estado al cierre de la publicación. Además, los datos se actualizan regularmente y se pueden descargar de nuestra página Web.

Emerson Automation Solutions

AVENTICS GmbH
Ulmer Straße 4
30880 Laatzen, GERMANY
phone +49 511 2136-0
fax +49 511 2136-269
www.emerson.com/aventics
aventics@emerson.com

Further addresses:
www.emerson.com/contactus

The data specified above only serve to describe the product. No statements concerning a certain condition or suitability for a certain application can be derived from our information. The given information does not release the user from the obligation of own judgement and verification. It must be remembered that our products are subject to a natural process of wear and aging.

An example configuration is depicted on the title page. The delivered product may thus vary from that in the illustration.

Translation of the original operating instructions. The original operating instructions were created in the German language.

EMERSON