Sicherheitshandbuch

A-Druckschalterserie

Dokument: I&M009-10210
REV. A - Fassung vom 19/04/2013

Inhaltsverzeichnis:

1 EINLEITUNG

Dieses Sicherheitshandbuch enthält Informationen für die Entwicklung, Installation, Überprüfung und Wartung einer sicherheitstechnischen Funktion (SIF) unter Verwendung der A-Druckschalterserie. Das Handbuch erläutert die Anforderungen hinsichtlich der Einhaltung der Normen IEC 61508 und IEC 61511 zur funktionalen Sicherheit.

1.1 Begriffe und Abkürzungen

Sicherheit — Nichtvorliegen einer inakzeptablen Gefährdung

Funktionale Sicherheit — Die Fähigkeit eines Systems, die Verfahren zur Erreichung oder Aufrechterhaltung eines definierten sicheren Zustands der Geräte / Anlage / Apparatur unter Steuerung durch das System durchzuführen.

Grundlegende Sicherheit — Das Gerät muss so konzipiert und hergestellt werden, dass Personen vor jeglicher vom System ausgehender Gefährdung durch elektrische Schläge und sonstige Risiken sowie auch daraus resultierenden Bränden und Explosionen geschützt werden. Der Schutz muss bei allen nominellen Betriebsbedingungen und bei Erstauftreten eines Fehlers wirksam sein.

Sicherheitsbeurteilung — Eine Untersuchung der Sicherheitsaspekte von die Sicherheit betreffenden Systemen, die in einer evidenz-basierten Bewertung resultiert.

Fail-Safe-Zustand — Zustand, in dem das Magnetventil spannungsfrei und die Feder ausgedehnt sind.

Fail Safe (Ungefährlicher Ausfall) — Ein Fehler, der bewirkt, dass sich das Ventil ohne prozessabhängigen Befehl in den Fail-Safe-Zustand begibt.

Fail Dangerous (Gefährlicher Ausfall) — Fehler, der nicht auf einen prozessabhängigen Befehl reagiert (d.h. der definierte Fail-Safe-Zustand kann nicht hergestellt werden).

Fail Dangerous Undetected (Unerkannter gefährlicher Ausfall) — Fehler, der eine Gefährdung darstellt und durch die automatischen Hubtests nicht erkannt wird.

Fail Dangerous Detected (Erkannter gefährlicher Ausfall) — Fehler, der eine Gefährdung darstellt, jedoch durch die automatischen Hubtests erkannt wird.

Fail Annunciation Undetected (Ausfall Meldung unerkannt) — Fehler, der nicht zu Fehlauslösungen führt oder die Sicherheitsfunktion behindert, der jedoch zu einem Verlust der automatischen Diagnose führt und nicht von anderen Diagnosen erkannt wird.

Fail Annunciation Detected (Ausfall Meldung erkannt) Fehler, der nicht zu Fehlauslösungen führt oder die Sicherheitsfunktion behindert, der jedoch zu einem Verlust der automatischen Diagnose oder zu einer falschen Diagnosemeldung führt.

Fail No Effect (Ausfall ohne Auswirkung) Fehler einer Komponente, die Bestandteil der Sicherheitsfunktion ist, jedoch keine Auswirkung auf die Sicherfunktion hat.

Low demand mode (Betriebsart mit niedriger Anforderungsrate) Modus, in dem die Anforderungsrate an ein sicherheitsrelevantes System nicht höher ist als das Doppelte der Wiederholungs-prüfungsfrequenz.

1.2 Abkürzungen

FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware-Fehlertoleranz
MOC	Management of Change, Änderungsmanagement Hierbei handelt es sich um bestimmte Verfahren, die oft bei Arbeiten angewendet werden, die behördlichen Bestimmungen unterliegen.
PFDavg	Average Probability of Failure on Demand (Mittlere Ausfallwahrscheinlichkeit der Funktion im Anforderungsfall)
SFF	Safe Failure Fraction (Anteil ungefährlicher Ausfälle), der Anteil an der gesamten Ausfallquote eines Geräts, der entweder zu einem ungefährlichen Ausfall oder einem diagnostizierten ungefährlichen Ausfall führt.
SIF	Sicherheitstechnische Funktion, eine Reihe an Geräten/Vorrichtungen, die das Risiko aufgrund einer bestimmten Gefährdung reduzieren sollen (eine Sicherheitsschleife).
SIL	Safety Integrity Level (Sicherheitsintegritätslevel), eine bestimmte Stufe (eine von möglichen vier Stufen) zur Festlegung der Anforderungen an die Sicherheitsintegrität einer Sicherheitsfunktion, die sicherheitsrelevanten E/E/PE-Systemen zugewiesen wird; Sicherheitsintegritätslevel 4 entspricht der höchsten Stufe der Sicherheitsintegrität, während Sicherheitsintegritätslevel 1 der niedrigsten Stufe entspricht.
SIS	Safety Instrumented System (Sicherheitstechnisches System) Implementierung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus einer beliebigen Kombination aus Sensor(en), Logiksystem(en) und finalem (finalen) Element(en).

1.3 Produktsupport

Produktsupport kann angefordert werden bei:

Ashcroft Inc., 250 East Main St., Stratford Ct. 06614

www.ashcroft.com

(203) 378-8281

1.4 Bezugsquellen

Hardwaredokumente:

- Ashcroft A-Series Switch Installation, Operation and Maintenance Instructions (Installations-, Betriebs- und Wartungsanleitung für die Ashcroft A-Schalterserie)

Richtlinien/Referenzen:

- Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis (Auswahl des Sicherheitsintegritätslevels – Systematische Methoden einschließlich Analyse der Sicherheitsebene), ISBN 1-55617-777-1, ISA
- Control System Safety Evaluation and Reliability (Sicherheitsbeurteilung und Zuverlässigkeit von Steuersystemen), 2nd Edition, ISBN 1-55617-638-8, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations (Überprüfung von sicherheitstechnischen Systemen, Wahrscheinlichkeitsberechnungen), ISBN 1-55617-909-9, ISA

1.5 Referenznormen

Funktionale Sicherheit

- IEC 61508: 2010 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector (Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie)

2 GERÄTEBESCHREIBUNG

Der Druckschalter der Serie A ist ein elektrischer Schalter, der durch den Eingangsdruck ausgelöst wird. Bei steigendem Druck wechselt der Schalter vom Zustand „Normally Closed (NC)“ (Ruhekontakt (R)) in den Zustand „Normally Open (NO)“ (Arbeitskontakt (A)). Bei Druckabfall wechselt der Zustand erneut von A zu R.

Der Schalter ist in mehreren Konfigurationen erhältlich. Die Komponente kann als werksseitig eingestelltes Modell (APS) erworben werden, bei welcher der Schaltpunkt bei der Herstellung festgelegt wird und nicht verändert werden kann, oder aber als vom Kunden einstellbares Modell (APA), das vom Endbenutzer justiert werden kann. Jede Ausführung wird mit einem wasserdichten oder einem explosionssicheren Gehäuse geliefert. Es sind unterschiedliche Drucknschlüsse mit Innen- oder Außengewinde lieferbar. Ferner sind mehrere elektrische Anschlüsse lieferbar (18-AWG-Drahtleitungen, 1/2-Zoll-Kabelverschraubung, Kabel, Kabelschuhe, Micro-DIN-Steckverbinder mit C-Form). Der Schalter kann als SPDT-Schalter (Single-Pole Double-Throw, einpoliger Wechselschalter) oder als DPDT-Schalter (Double-Pole Double-Throw; zweipoliger Wechselschalter) erworben werden. Die elektrischen Nennwerte reichen je nach dem bestellten Schaltertyp von 1 A bei 125 VDC bis zu 5 A bei 250 VDC. Als Druckbereiche stehen Werte von -15 psi bis 7500 psi zur Verfügung, wobei die Schaltpunkte jeweils nicht größer als der maximale Wertebereich des Produkts sind.

3 EINRICHTEN EINER SIF MIT EINEM HERSTELLERPRODUKT

3.1 Sicherheitsfunktion

Der Schalter der A-Serie wechselt seinen Zustand bei Veränderung des Eingangsdrucks. Sobald ein Ansprechdruck erreicht wird, ändert der Schalter seinen Status, wie in Abschnitt 2 dieses Dokuments erläutert. Der Konstrukteur der SIF muss beachten, ob die Alarmbedingung bei fallendem Druck oder bei steigendem Druck besteht, und den Schalter entsprechend anpassen. Bei Verwendung eines werksseitig eingestellten Produkts muss für dieses eine Spezifikation vorgegeben werden, so dass der Status bei einem vordefinierten Druck und in der gewünschten Richtung geändert wird. Bei Auswahl des Produktes der A-Serie mit Zweifach-Schalter kann nur ein Schaltpunkt für den Druck verwendet werden. Dieser Druck löst beide Schalter aus.

Der Schalter der A-Serie ist als Komponente des Subsystems mit finalen Elementen gemäß IEC 61508 vorgesehen; und der erzielte SIL der eingerichteten Funktion muss vom Konstrukteur überprüft werden.

3.2 Grenzwerte der Umgebungsbedingungen

Der Konstrukteur einer SIF muss sicherstellen, dass das Produkt im Hinblick auf eine Verwendung innerhalb der vorgegebenen Umgebungsbedingungen ausgelegt wird. Beachten Sie die Temperaturgrenzwerte auf der Produktkennzeichnung oder im Datenblatt der A-Druckschalterserie, das unter www.Ashcroft.com abgerufen werden kann.

3.3 Anwendungsgrenzwerte

Die Werkstoffe, aus denen ein Schalter der A-Serie gefertigt wird, werden im Datenblatt der Ashcroft A-Druckschalterserie aufgeführt. Es ist unbedingt erforderlich, dass der Konstrukteur die Werkstoffkompatibilität unter Beachtung möglicher chemischer Verunreinigungen und der Luftzufuhrbedingungen am Standort überprüft. Sollte der Schalter der A-Serie unter Bedingungen eingesetzt werden, die die Anwendungsgrenzwerte über- bzw. unterschreiten, oder mit inkompatiblen Werkstoffen, so verlieren die angegebenen Zuverlässigkeitsdaten ihre Gültigkeit.

3.4 Überprüfung der Konstruktion

Ashcroft Inc. stellt einen FMEDA-Bericht (Failure Mode, Effects, and Diagnostics Analysis) zur Verfügung. Hierin sind alle Ausfallquoten und Ausfallmodi sowie die erwartete Lebensdauer aufgeführt.

Der erzielte Sicherheitsintegritätslevel (SIL) einer ganzen eingerichteten sicherheitstechnischen Funktion muss vom Konstrukteur durch folgende Berechnungen/Testverfahren überprüft werden: PFDavg unter Berücksichtigung der Architektur, Wiederholungsprüfungsintervall, Effektivität der Wiederholungsprüfung, automatische Diagnosen, durchschnittliche Reparaturzeit und spezifische Ausfallquoten aller in der SIF enthaltenen Produkte. Jedes Subsystem muss im Hinblick auf seine Einhaltung der Mindestanforderungen an die Hardware-Fehlertoleranz überprüft werden. Zu diesem Zweck wird die Verwendung des exida exSILentia® Tools empfohlen, das passende Modelle für den Druckschalter der A-Serie und die entsprechenden Ausfallquoten enthält.

Bei Verwendung eines Druckschalters der A-Serie in einer redundanten Konfiguration müssen die Sicherheitsintegritätsberechnungen einen CCF-Faktor (Common Cause Failure) von mindestens 5 % enthalten.

Die im FMEDA-Bericht aufgelisteten Daten zur Ausfallquote gelten nur für die Nutzlebensdauer eines Druckschalters der A-Serie. Nach Ablauf dieser Zeit können die Ausfallquoten mitunter steigen. Zuverlässigkeitsberechnungen basierend auf den im FMEDA-Bericht aufgelisteten Daten für Einsatzzeiten, die über die Nutzlebensdauer hinausgehen, ergeben möglicherweise zu optimistische Ergebnisse, d.h. der berechnete Sicherheitsintegritätslevel wird dann nicht erreicht.

3.5 SIL-Fähigkeit

3.5.1 Systematische Integrität

Das Produkt entspricht hinsichtlich des Herstellerkonstruktionsprozesses den Anforderungen von Sicherheitsintegritätslevel (SIL) 3. Diese Anforderungen sollen eine ausreichende Stabilität des Produkts gegenüber vom Hersteller induzierten systematischen Konstruktionsfehlern erzielen. Eine in dieses Produkt integrierte sicherheitstechnische Funktion (SIF) darf ohne Begründung des Endbenutzers vor der Anwendung oder ohne entsprechende Technologieredundanz in der Konstruktion nicht mit einem höheren SIL als in der Erklärung eingesetzt werden.

3.5.2 Zufallsintegrität

Der Druckschalter der Serie A ist ein Gerät vom Typ A. Aus diesem Grund kann eine Konstruktion, basierend auf einer SFF zwischen 60 % und 90 % bei Verwendung des Druckschalters der A-Serie in Low-Trip-Anwendungen und als einzige Komponente eines Subsystems mit finalen Elementen, SIL 2 bei HFT=0 entsprechen. Bei Verwendung in High-Trip-Anwendungen beträgt die SFF <60 %; deshalb gelten für die Einschränkungen bezüglich der Architektur SIL 1 bei HFT=0 und SIL 2 bei HFT=1.

Wenn die Elementgruppe aus vielen Komponenten besteht, muss der SIL für die gesamte Gruppe anhand der Ausfallquoten aller Komponenten überprüft werden. Bei dieser Analyse müssen alle Hardware-Fehlertoleranzen und die Einschränkungen bezüglich der Architektur berücksichtigt werden.

3.5.3 Sicherheitsparameter

Detaillierte Informationen zu den Ausfallquoten entnehmen Sie bitte dem Failure Modes, Effects and Diagnostics Analysis-Bericht für den Druckschalter der Serie A.

3.6 Allgemeine Anforderungen

Die Ansprechzeit des Systems sollte kürzer sein als die Prozess-Sicherheitszeit. Der Druckschalter der Serie A ändert seinen Zustand unter bestimmten Bedingungen in weniger als 1 s.

Alle SIS-Komponenten einschließlich des Druckschalters der Serie A müssen vor Prozessstart operationell sein.

Der Anwender muss sicherstellen, dass der Druckschalter der Serie A für die Verwendung in Sicherheitsanwendungen geeignet ist, indem er das Typenschild des Druckschalters der Serie A auf seine richtige Kennzeichnung hin überprüft.

Personen, die Instandhaltungs- und Prüfverfahren am Druckschalter ausführen, müssen hierfür entsprechend qualifiziert sein.

Die Ergebnisse der Wiederholprüfungen werden aufgezeichnet und regelmäßig kontrolliert.

Die Nutzlebensdauer des Druckschalters der A-Serie wird im Failure Modes, Effects and Diagnostics Analysis-Bericht für den Druckschalter der A-Serie erläutert.

4 INSTALLATION UND INBETRIEBNAHME

4.1 Installation

Der Druckschalter der A-Serie muss gemäß der im Installationshandbuch erläuterten Standardverfahren installiert werden.

Die Umgebung muss überprüft werden, um sicherzustellen, dass die Umgebungsbedingungen die angegebenen Grenzwerte nicht über- bzw. unterschreiten.

Der Druckschalter der A-Serie muss so angebracht werden, dass er für die physische Inspektion zugänglich ist.

4.2 Physische Anbringung und Positionierung

Der Druckschalter der A-Serie muss so angebracht werden, dass ausreichend Platz für Druck- und elektrische Anschlüsse vorhanden ist und manuelle Prüfungen möglich sind.

Der Druckschalter der A-Serie muss in einer vibrationsarmen Umgebung installiert werden. Ist übermäßige Vibration zu erwarten, müssen besondere Vorkehrungen getroffen werden, um die Integrität der pneumatischen Anschlüsse sicherzustellen, oder aber die Vibration muss mithilfe geeigneter Dämpfvorrichtungen verringert werden.

4.3 Druckanschlüsse

Es obliegt der Verantwortung des Konstrukteurs der SIF, sicherzustellen, dass die bei der Installation des Schalters verwendeten Druckschläuche und -anschlüsse für den angegebenen Betriebsdruck des Systems ausgelegt sind und den Druck zum Schalter nicht begrenzen.

5 BETRIEB UND WARTUNG

5.1 Prüfverfahren ohne automatische Prüfungen

Ziel der Prüfverfahren ist es, Ausfälle innerhalb des Ashcroft Schalters zu erkennen, die durch die automatische Diagnose des Systems nicht erkannt werden. Von besonderer Bedeutung sind hierbei unerkannte Ausfälle, die die ordnungsgemäße Funktionsweise der sicherheitstechnischen Funktion verhindern.

Die Frequenz dieser Prüfverfahren, d.h. das Wiederholungsprüfungsintervall, muss anhand von Zuverlässigkeitsberechnungen für die sicherheitstechnischen Funktionen bestimmt werden, für die der Ashcroft Schalter eingesetzt wird. Die Wiederholungsprüfungen müssen mindestens so häufig durchgeführt werden, wie im Berechnungsergebnis angegeben, um die erforderliche Sicherheitsintegrität der sicherheitstechnischen Funktion aufrecht zu erhalten.

Das folgende Prüfverfahren wird hierfür empfohlen. Die Ergebnisse des Wiederholungstests werden aufgezeichnet, und jegliche erkannte Ausfälle, die die funktionale Sicherheit beeinträchtigen, müssen an Ashcroft gemeldet werden.

Tabelle 1: Empfohlenes Prüfverfahren

Schritt	Maßnahme
1	Die Sicherheitsfunktion umgehen und geeignete Maßnahmen treffen, um eine falsche Aktivierung zu vermeiden.
2	Den Druck zum Schalter anpassen, und überprüfen, ob der Schalter unter den festgelegten Bedingungen ausgelöst wird.
3	Den Druckschalter der A-Serie auf mögliche sichtbare Beschädigung oder Verunreinigung inspizieren. Darauf achten, dass die weiße Gehäusebelüftung noch immer an ihrem Platz sitzt. (Ein fehlender Entlüftungsstopfen weist auf ein mögliches Druckleck im Schalter hin.)
4	Jegliche Fehler in der SIF-Inspektionsdatenbank Ihres Unternehmens dokumentieren.
5	Den Bypass entfernen, und ansonsten den Normalbetrieb wiederherstellen.

Mit diesem Test werden >90 % der möglichen DU-Ausfälle am Druckschalter der A-Serie erkannt.

Die Person(en), die die Prüfverfahren am Druckschalter der A-Serie ausführt (ausführen), muss (müssen) im Hinblick auf den Betrieb von SIS, einschließlich der Bypassverfahren, Schalterinstandhaltung und Änderungsmanagement-verfahren des Unternehmens geschult sein. Es sind keine speziellen Werkzeuge erforderlich.

5.2 Reparatur und Austausch

Ein Schalter der A-Serie ist einstellbar (nur die APA-Ausführung), kann jedoch nicht repariert werden. Beim Auftreten eines Ausfalls muss der Schalter ausgetauscht werden. Die Person(en), die den Austausch des Druckschalters der A-Serie vornimmt (vornehmen), muss (müssen) im Hinblick auf den Betrieb von SIS, einschließlich der Bypassverfahren, Schalterinstandhaltung und Änderungsmanagementverfahren des Unternehmens geschult sein.

5.3 Nutzlebensdauer

Die Nutzlebensdauer des Druckschalters der A-Serie beträgt 10 bis 15 Jahre oder 10.000 Zyklen.

5.4 Benachrichtigung des HERSTELLERS

Jeglicher Fehler, der erkannt wird und die funktionale Sicherheit gefährdet, muss an Ashcroft gemeldet werden. Bitte wenden Sie sich an den Ashcroft Kundendienst.

6 CHECKLISTE FÜR DAS STARTVERFAHREN

Die folgende Checkliste kann als Hilfe verwendet werden, um den Druckschalter der A-Serie gemäß IEC 61508 in einer sicherheitskritischen SIF zu integrieren.

#	Maßnahme	Ergebnis	Überprüft	
			Durch	Datum
	Konstruktion			
	Erforderlicher Sicherheitsintegritätslevel und PFDavg bestimmt			
	Richtige Ventil-Betriebsart ausgewählt (Fehler-geschlossen, Fehler-geöffnet)			
	Konstruktionsentscheidung dokumentiert			
	Pneumatische Kompatibilität und Eignung überprüft			
	Anforderungen an SIS-Logiksystem für Ventilprüfungen definiert und dokumentiert			
	Führung der pneumatischen Anschlüsse bestimmt			
	Anforderungen an SIS-Logiksystem für Teilhubtests definiert und dokumentiert			
	Konstruktion formell geprüft und Eignung formell bewertet			
	Implementierung			
	Physischer Anbringungsort geeignet			
	Pneumatische Anschlüsse geeignet und konform mit anwendbaren Vorschriften			
	Ventilbetätigungsprüfung für SIS-Logiksystem implementiert			
	Instandhaltungsanweisungen für Wiederholungsprüfung herausgegeben			
	Überprüfungs- und Testplan herausgegeben			
	Implementierung formell geprüft und Eignung formell bewertet			

#	Maßnahme	Ergebnis	Überprüft	
			Durch	Datum
	Überprüfung und Tests			
	Elektrische Anschlüsse überprüft und getestet			
	Pneumatischer Anschluss überprüft und getestet			
	Ventilbetätigungstest für SIS-Logiksystem überprüft			
	Sicherheitsschleifenfunktion überprüft			
	Zeiten der Sicherheitsschleife gemessen			
	Bypassfunktion getestet			
	Überprüfungs- und Testergebnisse formell kontrolliert und Eignung formell bewertet			
	Instandhaltung			
	Druckzuführungsblockage / -teilblockage getestet			
	Sicherheitsschleifenfunktion getestet			