Sicherheitshandbuch für Fisher™ GX Stellgerät mit Antrieb

Zweck

Dieses Sicherheitshandbuch bietet Informationen an, die zur Konstruktion, Installation, Prüfung und Wartung von Safety Instrumented Function (SIF) erforderlich sind, die das Fisher Stellgerät GX mit Antrieb betreffen.

⚠ WARNUNG

Dieser Anhang zur Betriebsanleitung ist nicht zur Verwendung als selbstständiges Dokument vorgesehen. Er muss zusammen mit dem folgenden Handbuch verwendet werden:
Betriebsanleitung für die Fisher GX Stellgerät- und Antriebssysteme (D103175X0DE)
Wenn dieser Anhang zur Betriebsanleitung nicht zusammen mit der o.g. Betriebsanleitung verwendet wird, kann dies zu Personen- oder Sachschäden führen. Wenn Sie Fragen zu diesen Anweisungen haben oder Hilfe für den Bezug eines dieser Dokumente benötigen, wenden Sie sich an Ihr zuständiges Emerson Vertriebsbüro oder an den lokalen Geschäftspartner von Emerson.

Einführung

Dieses Handbuch bietet Informationen, die für die Erfüllung der Normen IEC 61508 oder IEC 61511 für funktionale Sicherheit erforderlich sind.

Abbildung 1. Fisher Stellgerät GX, Antrieb und digitaler Stellungsregler FIELDVUE™ DVC2000

W8861

Begriffe und Abkürzungen

Sicherheit: Frei von nicht akzeptablen Verletzungsrisiken.

Funktionale Sicherheit: Die Fähigkeit eines Systems, die Aktionen auszuführen, die notwendig sind, um einen definierten sicheren Status zu erreichen oder für die Ausrüstung/Maschinen/Anlage/Vorrichtung unter Kontrolle durch das System aufrechtzuerhalten.

Basissicherheit: Ausrüstung muss so konzipiert und gefertigt sein, dass sie vor Verletzungsrisiken durch elektrischen Schock oder sonstige Gefahren sowie gegen Brand- und Explosionsgefahr schützt. Der Schutz muss unter allen normalen Betriebsbedingungen und bei Einzelfehlern gewährleistet sein.

Sicherheitsbewertung: Die Untersuchung, um zu einem Urteil zu kommen-, das auf den Tatsachen der Sicherheit basiert, die durch dazugehörige Systeme erreicht wird.

Ausfallsicherer Zustand (Fail-Safe): Zustand, in dem der Ventilstellantrieb stromlos und die Federn bis zum Endanschlag entspannt sind.

Ausfallsicher (Fail Safe): Ein Fehler, der veranlasst, dass das Ventil ohne Prozessanforderung in den definierten ausfallsicheren Zustand übergeht.

Gefährlicher Fehler (Fail dangerous): Ein Fehler, der nicht auf eine Prozessanforderung reagiert (d. h. es wird nicht in den ausfallsicheren Zustand geschaltet).

Gefährlicher Fehler unerkannt (Fail Dangerous Undetected): Ein gefährlicher Fehler, der vom automatischen Hubtest nicht erkannt worden ist.

Gefährlicher Fehler erkannt (Fail Dangerous Detected): Ein Fehler, der gefährlich ist, aber vom automatischen Hubtest erkannt worden ist.

Fehlermeldung unerkannt: Fehler, der keine Fehlauslösung verursacht oder die Sicherheitsfunktion nicht blockiert, aber eine automatische Diagnose verhindert und nicht von einer anderen Diagnosefunktion erfasst wird.

Fehlermeldung erkannt: Fehler, der keine Fehlauslösung verursacht oder die Sicherheitsfunktion nicht blockiert, aber eine automatische Diagnose oder falsche Diagnoseanzeige verhindert.

Ausfall ohne Auswirkung (Fail No Effect): Ein Fehler einer Komponente, die Teil der Sicherheitsfunktion ist, aber die keine Auswirkung auf die Sicherheitsfunktion hat.

Niedriger Anforderungsmodus: Modus, bei dem die Häufigkeit der Anforderungen für den Betrieb, die auf einem sicherheitsbezogenen System gestellt werden, nicht größer ist als zweimal die Abnahmeprüfungsfrequenz.

β: Beta-Faktor, Ausfallwahrscheinlichkeit durch einen Common Caused Failure. (CCF – Ausfall mehrerer Komponenten durch dieselbe Fehlerursache).

λ: Fehlerrate. λDD: erkannt, gefährlich; λDU: unerkannt, gefährlich; λSD: erkannt, sicher; λSU: unerkannt, sicher.

Akronyme

FMEDA: Failure Modes, Effects and Diagnostic Analysis (Fehlermodi, Effekte und Diagnoseanalyse)

HFT: Hardware Fault Tolerance (Hardware-Fehlertoleranz)

MOC: Management of Change (Management von Änderungen). Diese speziellen Verfahren werden oft angewandt, wenn Arbeitsmaßnahmen in Übereinstimmung mit Regulierungsbehörden durchgeführt werden.

PFD_{AVG}: Average Probability of Failure on Demand (Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung)

SFF: Safe Failure Fraction (Anteile ungefährlicher Fehler). Der Anteil der Gesamtfehlerrate eines Gerätes, der entweder zu einem ungefährlichen Fehler oder einem diagnostizierten gefährlichen Fehler führt.

SIF: Safety Instrumented Function (sicherheitsgerichtete Instrumentierungsfunktion). Eine Gruppe von Geräten zur Verringerung des Risikos einer bestimmten Gefahr (eine Sicherheitsschleife).

SIL: Safety Integrity Level (Sicherheitsintegritätsstufe), diskrete Stufe (eine aus vier möglichen) zur Festlegung der Sicherheitsintegritätsanforderungen für die Sicherheitsfunktionen von E/E/PE-sicherheitsrelevanten Systemen, wobei die Sicherheitsintegritätsstufe 4 (SIL 4) die höchste Stufe der Sicherheitsintegrität ist und SIL 1 die niedrigste.

SIS: Safety Instrumented System (Sicherheitsgerichtetes System) – Implementierung einer oder mehrerer sicherheitsgerichteter Funktionen. Ein SIS setzt sich zusammen aus beliebigen Kombinationen von Sensor(en), Logikbaustein(en) und Endgerät(en).

Weiterführende Literatur

Hardware-Dokumente:

Datenblatt:

Datenblatt 51.1:Produktdatenblatt für GX, Fisher Stellgerät GX mit Antrieb: D103171X0DE

Betriebsanleitung:

Betriebsanleitung des Fisher GX Stellgeräts- und Antriebssystems: D103175X0DE

Richtlinien/Verweise:

- Safety Integrity Level Selection — Systematic Methods Including Layer of Protection Analysis (Sicherheitsintegritätsstufen-Auswahl — Systematische Methoden einschließlich Schutzschichtanalyse), ISBN 1-55617-777-1, ISA
- Control System Safety Evaluation and Reliability (Steuersystem-Sicherheitsbeurteilung und -zuverlässigkeit), 2. Ausgabe, ISBN 1-55617-638-8, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations (Instrumentierte Sicherheitssystemprüfung, praktische Wahrscheinlichkeitsberechnungen), ISBN 1-55617-909-9, ISA

Referenzstandards

Funktionale Sicherheit

- IEC 61508: 2000 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Funktionale Sicherheit — Sicherheitsgerichtete Systeme für die Prozessindustrie

Produktbeschreibung

Das Fisher Stellgerät Typ GX (Abbildung 1) ist ein kompaktes und modernes System aus Stellglied und Antrieb, das für die Regelung einer Vielzahl von Prozessflüssigkeiten, Gasen und Dämpfen entwickelt wurde.

Das GX erfüllt sowohl EN- als auch ASME-Normen. Das System ist mit einem kompletten Zubehörpaket lieferbar, einschließlich eines integrierten digitalen Stellungsreglers FIELDVUE DVC2000.

Gestaltung eines SIF mittels eines Fisher GX Stellgeräts mit Antrieb

Sicherheitsfunktion

Wenn der Ventilstellantrieb stromlos ist, müssen sich Stellantrieb und Ventil in die ausfallsichere Position bewegen. Je nach spezifizierter Konfiguration – bei Ausfall schließen/öffnen – bewegt der Stellantrieb den Ventilkegel, um den Fließweg durch das Ventil abzusperren bzw. zu öffnen.

Das GX Stellgerät mit Antrieb ist als Teil des letzten Element-Teilsystems vorgesehen, wie es gemäß IEC 61508 definiert ist, und die erreichte SIL-Ebene der konstruierten Funktion muss vom Konstrukteur überprüft werden.

Druck- und Temperaturgrenzen

Der SIF-Designer muss prüfen, dass das Produkt für den Einsatz innerhalb der voraussichtlichen Druck- und Temperaturgrenzwerte klassifiziert ist. Beziehen Sie sich bzgl. Druck und Grenztemperaturen auf das Produktdatenblatt des GX Stellgeräts mit Antrieb (51.1:GX).

Anwendungsgrenzen

Die Konstruktionswerkstoffe des GX Stellgeräts mit Antrieb sind in den jeweiligen Produktdatenblättern angegeben. Eine Reihe von Werkstoffen sind für verschiedene Anwendungen erhältlich. Die Serienkarte führt für ein gegebenes Ventil die verwendeten Konstruktionswerkstoffe auf. Es ist besonders wichtig, dass der Designer die Werkstoffkompatibilität mit potenziellen -chemischen Verunreinigungen und Umgebungsbedingungen der Anlage prüft. Wenn das GX Stellgerät mit Antrieb außerhalb der Anwendungsgrenzen oder mit inkompatiblen Materialien verwendet wird, werden hierdurch die bereitgestellten Zuverlässigkeitsdaten ungültig.

Ansprechzeit der Diagnosefunktion

Das GX Stellgerät mit Antrieb führt selbst keine automatischen Diagnosefunktionen aus und hat deshalb keine eigene Diagnose-Ansprechzeit. Möglicherweise werden jedoch automatische Diagnosefunktionen des Stellgerät-Teilsystems, wie z. B. Teilhubtests (PVST), durchgeführt. Auf diese Weise wird das Ventil in einem kleinen Prozentbereich seines normalen Stellweges bewegt, ohne den Durchfluss durch das Ventil zu beeinträchtigen. Sollten Fehler bei diesem PVST automatisch erfasst und gemeldet werden, entspricht die Ansprechzeit der Diagnosefunktion der PVST-Intervallzeit. Damit dieser Test aussagekräftig ist, muss der PVST 10 mal häufiger durchgeführt werden als eine voraussichtliche Anforderung.

Designprüfung

Von Emerson kann ein detaillierter FMEDA-Bericht angefordert werden. Dieser Bericht detailliert alle Fehlerraten und Fehlermodi sowie auch die erwartete Lebensdauer.

Das erreichte Sicherheitsintegritätslevel (SIL) eines ganzen SIF-Designs muss vom Designer anhand einer PFD_{AVG}-Berechnung unter Berücksichtigung der Architektur, des Intervalls der Abnahmeprüfung, der Wirksamkeit der Abnahmeprüfung, jeder automatischen Diagnose, der durchschnittlichen Reparaturzeit und der spezifischen Fehlerraten aller in der SIF enthaltenen Produkte geprüft werden. Jedes Teilsystem muss geprüft werden, um die Konformität mit den minimalen HFT-Anforderungen sicherzustellen.

Wenn ein GX Stellgerät mit Antrieb in einer redundanten Konfiguration verwendet wird, sollte ein gebräuchlicher Ursachenfaktor von mindestens 5 % in die Berechnung der Sicherheitsintegrität mit einbezogen werden.

Die im FMEDA-Bericht aufgelisteten Fehlerratendaten sind nur für die Nutzungsdauer eines GX Stellgeräts mit Antrieb hilfreich. Die Fehlerraten nehmen nach dieser Zeitspanne zu. Zuverlässigkeitsberechnungen basieren auf den Daten, die im FMEDA-Bericht aufgelistet sind. Für Einsatzzeiten jenseits der Lebensdauer können sich zu optimistische Ergebnisse ergeben, d. h. die berechnete Sicherheitsintegritätsstufe wird nicht erreicht.

SIL-Fähigkeit

Systematische Integrität

Abbildung 2. exida SIL 3-fähig

Das Produkt hat die Herstellerentwurfsprozessanforderungen von IEC-61508 Sicherheitsintegritätsstufe 3 erfüllt. Diese sollen hinreichende Integrität gegen systematische Konstruktionsfehler durch den Hersteller erreichen. Eine mit diesem Produkt konzipierte SIF darf ohne Begründung „vor der Benutzung" durch den Endanwender oder diverse technische Redundanz im Design nicht auf einer höheren SIL-Stufe als angegeben verwendet werden.

Zufällige Integrität

Das GX Stellgerät mit Antrieb ist als Typ-A-Gerät gemäß IEC 61508 klassifiziert und hat eine Hardwarefehlertoleranz von 0. Das vollständige Schlusselement-Teilsystem, mit einem Fisher-Ventil als letztes Steuerelement, muss ausgewertet werden, um den sicheren Ausfallanteil des Teilsystems zu bestimmen. Wenn SFF für das gesamte Stellgerät-Teilsystem zwischen 60 % und 90 % liegt, kann das Design SIL 2 bei HFT = 0 erfüllen.

Sicherheitsparameter

Für detaillierte Fehlerrateninformationen siehe Fehlermodi, Auswirkungen und diagnostischer Analysebericht für das GX Stellgerät mit Antrieb.

Verbindung vom Fisher GX Stellgerät mit Antrieb zum SIS-Logikbaustein

Das Stellgerät-Teilsystem (bestehend aus einem Stellungsregler, einem GX Stellgerät mit Antrieb) wird am sicherheitsbewerteten Logikbaustein angeschlossen, der die Sicherheitsfunktion aktiv ausführt sowie alle automatischen Diagnosefunktionen für die Erfassung potenziell gefährlicher Fehler des GX Stellgeräts mit Antrieb und aller anderen Komponenten des Stellgeräts (z. B. Teilhubtest des Ventils).

Allgemeine Anforderungen

Die Ansprechzeit des Systems sollte geringer als die Prozess-Sicherheitszeit sein. Das Stellglied-Teilsystem muss entsprechend dimensioniert sein, um sicherzustellen, dass die Ansprechzeit geringer als die erforderliche Prozess-Sicherheitszeit ist. Das GX Stellgerät mit Antrieb geht innerhalb von weniger als der Sicherheitszeit der erforderlichen SIF unter den spezifizierten Bedingungen in seinen sicheren Zustand über.

Alle SIS-Komponenten, einschließlich des GX Stellgeräts mit Antrieb müssen vor dem Prozessbeginn betriebsbereit sein.

Der Benutzer muss überprüfen, dass das GX Stellgerät mit Antrieb sich für die Verwendung in Sicherheitsanwendungen eignet.

Wartungs- und Prüfpersonal am GX Stellgerät mit Antrieb muss die erforderlichen Kompetenzen besitzen.

Die Ergebnisse der Abnahmeprüfungen müssen regelmäßig aufgezeichnet und überprüft werden.

Die Nutzungsdauer des GX Stellgeräts mit Antrieb wird im „Bericht bzgl. Fehlermodi, Auswirkungen und Diagnoseanalysen“ für das Fisher GX Stellgerät mit Antrieb aufgezeigt.

Installation und Inbetriebnahme

Installation

Das Fisher GX Stellgerät mit Antrieb muss entsprechend den in der jeweiligen Betriebsanleitung aufgeführten Standardverfahren installiert werden.

Die Betriebsumgebung muss darauf überprüft werden, dass Druck- und Temperaturbedingungen die Nennwerte nicht überschreiten.

Das GX Stellgerät mit Antrieb muss für physikalische Inspektionen zugänglich sein.

Tabelle 1. Empfohlene Abnahmeprüfung für vollen Hub

Schritt	Maßnahme
1	Die Sicherheitsfunktion umgehen und entsprechende Maßnahmen einleiten, um eine falsche Auslösung zu vermeiden.
2	Signal/Versorgung zum Stellantrieb unterbrechen oder verändern, um einen zwangsweisen vollen Hub des Stellantriebs und Ventils in den ausfallsicheren Status auszuführen und überprüfen, dass der sichere Status in der richtigen Zeit erreicht worden ist.
3	Signal/Versorgung zum Stellantrieb wiederherstellen und überprüfen, dass der normale Betriebsmodus erreicht worden ist.
4	Untersuchen Sie das GX Stellgerät mit Antrieb und die anderen Stellglied-Komponenten auf Leckagen, sichtbare Schäden oder Verunreinigung.
5	Die Prüfergebnisse und alle Fehler in der SIF-Inspektionsdatenbank Ihres Unternehmens aufzeichnen.
6	Den Bypass entfernen und den Normalbetrieb wiederherstellen.

Physikalischer Ort und Platzierung

Das Fisher GX Stellgerät mit Antrieb muss mit ausreichendem Platz für den Stellantrieb, die pneumatischen Anschlüsse und sämtliche andere Komponenten des Stellglieds zugänglich sein. Es müssen Vorkehrungen für manuelle Abnahmeprüfungen getroffen werden.

Das pneumatische Rohrleitungssystem zum Stellantrieb muss so kurz und gerade wie möglich gehalten werden, um die Luftströmungsbeschränkungen und das Verstopfungspotenzial zu minimieren. Lange oder gebogene pneumatische Leitungen können auch die Ventilschließzeit erhöhen.

Das GX Stellgerät mit Antrieb muss in einer Umgebung mit niedriger Vibration montiert werden. Bei voraussichtlich starken Vibrationen müssen spezielle Vorsichtsmaßnahmen ergriffen werden, um die Integrität von pneumatischen Anschlüssen sicherzustellen oder die Vibrationen müssen mit geeigneten Dämpfungshalterungen reduziert werden.

Betrieb und Wartung

Empfohlene Abnahmeprüfung

Das Ziel der Abnahmeprüfung ist es, Fehler innerhalb eines GX Stellgeräts mit Antrieb zu erkennen, die nicht von einer automatischen Diagnose des Systems entdeckt wurden. Das Hauptanliegen sind unerkannte Fehler, die die sicherheitsgerichtete Instrumentierungsfunktion an der Ausführung der beabsichtigten Funktion hindern.

Die Frequenz der Abnahmeprüfung oder das Abnahmeprüfungsintervall muss anhand von Zuverlässigkeitsberechnungen der sicherheitsgerichteten Instrumentierungsfunktionen bestimmt werden, für die ein GX Stellgerät mit Antrieb eingesetzt wird. Die Abnahmeprüfungen müssen mindestens gemäß der in der Berechnung spezifizierten Frequenz durchgeführt werden, um die erforderliche Integrität der Sicherheit für die sicherheitsgerichtete Instrumentierungsfunktion (SIF) zu erhalten.

Die in Tabelle 1 dargestellte Abnahmeprüfung wird empfohlen. Die Ergebnisse der Abnahmeprüfung sollten protokolliert werden und jegliche Fehler, die erkannt werden oder solche, die die funktionelle Sicherheit gefährden, sollten Emerson Automation Solutions gemeldet werden. Die vorgeschlagene Abnahmeprüfung besteht aus einem vollen Hub des GX Stellgeräts mit Antrieb.

Das die Abnahmeprüfung eines GX Stellgeräts mit Antrieb durchführende Personal sollte in SIS-Verfahren, einschließlich Bypass-Prozeduren, Ventilwartung und firmeneigenem Management von Veränderungen, geschult sein. Besondere Werkzeuge werden nicht benötigt.

Reparatur und Austausch

Die Reparaturverfahren in der zutreffenden Ventil-Betriebsanleitung müssen befolgt werden.

Benachrichtigung des Herstellers

Ausfälle, die erkannt werden und die die funktionale Sicherheit gefährden, müssen Emerson gemeldet werden. Bitte wenden Sie sich an Ihr Emerson-Vertriebsbüro oder lokalen Geschäftspartner.

Dokumentenstatus

Veröffentlichungen

Versionsgeschichte: (Version, Status, Datum)

Anhang A

Beispiel für eine Inbetriebnahme-Checkliste

Dieser Anhang enthält ein Beispiel für eine Inbetriebnahme-Checkliste für ein Fisher GX Stellgerät mit Antrieb. Eine Inbetriebnahme-Checkliste bietet eine Anleitung für den Einsatz des Stellglieds.

Inbetriebnahme-Checkliste

Die folgende Checkliste kann als eine Anleitung zum Einsatz des GX Stellgeräts mit Antrieb in einer mit IEC61508 konformen sicherheitskritischen SIF verwendet werden.

#	Tätigkeit	Ergebnis	Überprüft	
			Von	Datum
	Design			
	Ziel-Sicherheitsintegritätsstufe und PFD_{AVG} bestimmt			
	Korrekter Ventilmodus ausgewählt (bei Fehler geschlossen, bei Fehler offen)			
	Designentscheidung dokumentiert			
	Pneumatik-Kompatibilität und Eignung geprüft			
	Anforderungen des SIS-Logikbausteins für Ventilprüfungen definiert und dokumentiert			
	Verlegung von pneumatischen Anschlüssen bestimmt			
	Anforderungen des SIS-Logikbausteins für Teilhubtests definiert und dokumentiert			
	Design formal überprüft und Eignung formal bewertet			
	Implementierung			
	Physikalischer Ort geeignet			
	Pneumatische Anschlüsse geeignet und entsprechend den anwendbaren Normen			
	SIS-Logikbaustein Ventilbetätigungstest implementiert			
	Wartungsanweisungen für Abnahmeprüfung veröffentlicht			
	Verifizierungs- und Prüfungsplan veröffentlicht			
	Implementierung formal überprüft und Eignung formal bewertet			
	Verifizierung und Prüfung			
	Elektrische Anschlüsse verifiziert und getestet			
	Pneumatische Anschlüsse verifiziert und getestet			
	SIS-Logikbaustein Ventilbetätigungstest verifiziert			
	Funktion der Sicherheitsschleife verifiziert			
	Timing der Sicherheitsschleife gemessen			
	Bypass-Funktion geprüft			
	Verifizierungs- und Testergebnisse formal überprüft und Eignung formal bewertet			
	Wartung			
	Auf Rohrverstopfung/teilweise Verstopfung getestet			
	Funktion der Sicherheitsschleife getestet			

Emerson Automation Solutions
Marshalltown, Iowa 50158 USA
Sorocaba, 18087 Brazil
Cernay, 68700 France
Dubai, United Arab Emirates
Singapore 128461 Singapore

www.Fisher.com