DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

DGUV-Information

Manuelle Rückstelleinrichtung

der Rückstellfunktion nach DIN EN ISO 13849-1

Ausgabe 02/2015 FB HM-067

Das Quittieren einer Schutzeinrichtung nach Auslösen eines Stoppbefehls wird gemäß DIN EN ISO 13849-1 als manuelle Rückstellfunktion (Manual Reset) bezeichnet. Derzeit existieren unterschiedliche Auffassungen über die Signalauswertung der manuellen Rückstelleinrichtung („Reset-Taster"). Diese DGUV-Information beschränkt sich auf die möglichen Prinzipien zur Realisierung des Rückstellsignales. Die Umsetzung der gesamten Sicherheitsfunktion „Manual Reset" ist nicht Gegenstand dieses Informationsblattes.

Inhaltsverzeichnis

1 Anforderung an Signalauswertung des Reset

Gemäß DIN EN ISO 13849-1 Abschnitt 5.2.2 [1] sind für die Signal-Auswertung des Reset nachfolgende Anforderungen zu erfüllen:

„Nach der Einleitung eines Stoppbefehls durch eine Schutzeinrichtung muss der Stoppzustand aufrechterhalten bleiben, bis eine manuelle Rückstelleinrichtung betätigt wird und der sichere Zustand für einen Wiederanlauf gegeben ist.

Die Wiederherstellung der Sicherheitsfunktion durch die Rückstellung der Schutzeinrichtung unterbricht den Stoppbefehl. Wenn durch die Risikobeurteilung angezeigt, muss diese Aufhebung des Stoppbefehls durch eine manuelle, separate und beabsichtigte Handlung (manuelle Rückstellung) bestätigt werden.

Die manuelle Rückstellfunktion:

- *muss durch ein getrenntes, manuell zu bedienendes Gerät in dem SRP/CS bereitgestellt werden,*
- *darf nur dann erreicht werden, wenn alle Sicherheitsfunktionen und Schutzeinrichtungen funktionsfähig sind,*
- *darf selbst keine Bewegung oder Gefährdungssituation einleiten,*
- *muss eine beabsichtigte Handlung sein,*
- *muss der Steuerung ermöglichen, einen separaten Startbefehl anzunehmen,*
- *darf nur erfolgen durch das Loslassen des Antriebselements in seiner betätigten (Ein)Position.*

Der Performance Level der sicherheitsbezogenen Teile für die manuelle Rückstellfunktion muss so ausgewählt werden, dass die Einbeziehung der manuellen Rückstellfunktion die erforderliche Sicherheit der zugehörigen Sicherheitsfunktion nicht mindert".

2 Fragestellung / Lösungsansatz

- Muss die manuelle Rückstellfunktion bei Drücken oder Loslassen des Betätigungselementes erfolgen?
- Ist bei elektrotechnischen Realisierungen die Auswertung des Rückstellsignales ausschließlich über die fallende Flanke zulässig oder kann eine Auswertung auch über eine steigende Flanke erfolgen?

  Wenn ja, unter welchen Bedingungen?

Lösungsansatz:

Zur Beantwortung der o.g. Fragestellung wird zunächst eine FMEA (**F**ehler **M**ode **E**ffekt **A**nalyse) durchgeführt, in welcher beide Möglichkeiten gegenübergestellt und bewertet werden. Die nachfolgende FMEA beschreibt jedoch nicht die Beurteilung der gesamten Sicherheitsfunktion „Manual Reset", sondern bezieht sich lediglich auf das Rückstellsignal selbst.

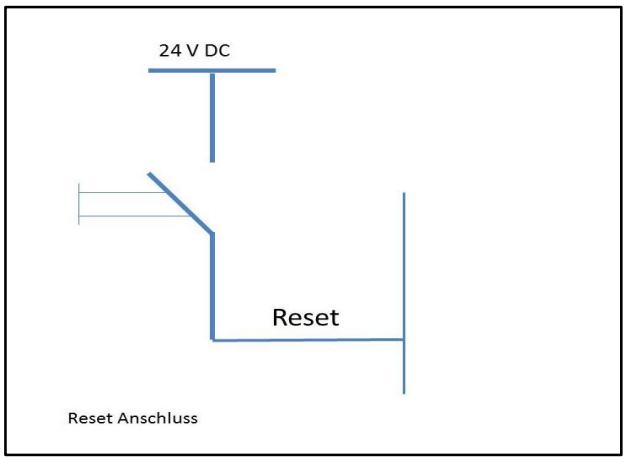

Abb. 1: Reset Anschluss

Vorausgesetzt wird hierbei, dass die Auswertung der *steigenden* oder *fallenden* Flanke mit sicherheitsgerichteten

Komponenten z.B. Sicherheits-SPS, Sicherheitsschaltgerät u.a. erfolgt und der Reset-Taster entsprechend den Abbildungen 1 und 2 verwendet wird.

3 FMEA des Reset - Signales mit steigender Flanke

3.1 Fehlerannahme Nr. 1: Ständiges High-Signal des Reset

Kontakt des Tasters bleibt geschlossen z. B. der Taster klemmt, der Taster bleibt gedrückt,

Bewertung:

Ein Reset kann einmalig erfolgen, d.h. die Schutzeinrichtung wird zurückgesetzt. Der Fehler wird beim nächsten Ansprechen der Schutzeinrichtung erkannt, sofern bei Auslösen der Schutzeinrichtung zunächst eine Abfrage auf “Reset = Low“ erfolgt.

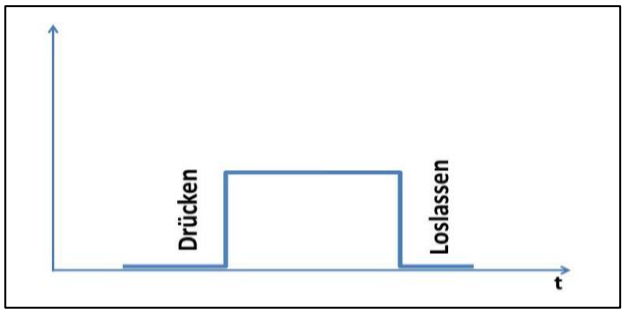

Abb. 2: Reset-Signal

3.2 Fehlerannahme Nr. 2: Ständiges High Signal des Reset

z.B. Kurzschluss der 2 Adern auf der Leitung zwischen Reset-Taster und Schaltgerät, Kurzschluss zur 24V Leitung, Fremdspannung, Stuck at High.

Bewertung:

a. Sicheres Verhalten, wenn der Fehler außerhalb des Zeitraumes „Reset Required“ erfolgt, sofern bei Auslösen der Schutzeinrichtung zunächst eine Abfrage auf: “Reset = Low“ erfolgt. Ein Reset kann nicht ausgelöst werden.

b. Unsicheres Verhalten, wenn der Fehler während des Zeitraumes „Reset Required“ auftritt, da dann ungewollt ein Reset ausgelöst wird.

Bemerkung: Fehler kann bei geschützter Kabelverlegung ausgeschlossen werden.

3.3 Fehlerannahme Nr. 3: Ständiges Low Signal des Reset

z.B. Leitungsunterbrechung, Nichtschließen des Reset-Kontaktes.

Bewertung:

Ein Reset kann nicht erfolgen, d.h. die Schutzeinrichtung kann nicht zurückgesetzt werden, da der Signalwechsel von Low nach High erwartet und ausgewertet wird. **(Sicherer Zustand)**

3.4 Fehlerannahme Nr. 4: Kurzzeitiger Impuls (Edge) des Reset

Bewertung:

Ein kurzzeitiger Impuls spiegelt einen Flankenwechsel von Low nach High und wieder nach Low vor. Dies bedeutet theoretisch, dass ein gültiges Reset-Signal vorgetäuscht werden kann. (unsicheres Verhalten während des Zeitraumes „Reset required“). Mögliche Maßnahmen und Nachweise, siehe Hinweis „Achtung“, Seite 3.

4 FMEA des Reset - Signales mit fallender Flanke

4.1 Fehlerannahme Nr. 1: Ständiges High Signal des Reset

z. B. Reset-Taster klemmt, Kurzschluss der 2 Adern auf der Leitung zwischen Reset-Taster und Schaltgerät, Kurzschluss zur 24V Leitung, Fremdspannung.

Bewertung:

Ein Reset kann nicht erfolgen, d.h. die Schutzeinrichtung kann nicht zurückgesetzt werden, da kein Signalwechsel von High nach Low erfolgt.

Sicherheitskritisch, wenn als Zweitfehler der klemmende Taster sich wieder löst oder eine Leitungsunterbrechung während des Zeitraumes „Reset Required“ erfolgt

4.2 Fehlerannahme Nr. 2: Ständiges Low Signal des Reset

z.B. Leitungsunterbrechung, Nichtschließen des Reset-Kontaktes.

Bewertung:

Ein Reset kann nicht erfolgen.

4.3 Fehlerannahme Nr. 3: Kurzzeitiger Impuls (Edge) des Reset

Bewertung:

Ein kurzzeitiger Impuls spiegelt einen Flankenwechsel von Low nach High und wieder nach Low vor. Dies bedeutet, dass ein gültiges Reset-Signal erkannt werden könnte.

5 Zusammenfassung und Anwendungsgrenzen

Die jeweils durchgeführte FMEA zeigt, dass **beide Varianten** durch die Flankenauswertung bei Auftreten eines Fehlers sicher funktionieren. Es werden jedoch **in beiden Lösungen** gleichermaßen nicht alle Fehler sofort erkannt. Dadurch kann es bei einem Auftreten eines weiteren Fehlers zu einer Fehlreaktion kommen.

Entscheidend für die Realisierung eines Reset-Signales ist nicht die Art der Flankenerkennung (High-Low oder Low-High), sondern die richtige Auswertung des dynamischen Verhaltens, sowie der notwendigen Fehlererkennung in der Auswerteeinrichtung.

Auch mit einer steigenden Flanke des Reset-Signales können bei richtiger Umsetzung die Anforderungen gemäß DIN EN ISO 13849-1 sinngemäß erfüllt werden.

Fehler-annahme	**ohne Abfrage**	**mit Abfrage**		
Taster klemmt		OK	OK	OK
Fremd-spannung, Stuck at High			OK	OK

OK Die Maßnahme ist geeignet

steigende Flanke

fallende Flanke

Rücksetzen mit steigender, Fehlererkennung mit fallender Flanke

Tabelle 1: FMEA, Übersicht

Die Kombination steigende und fallende Flanke des Reset-Signales beinhaltet das Zurücksetzen der Schutzeinrichtung mit der steigenden Flanke und Fehlererkennung mit der fallenden Flanke, wenn in der Steuerungssoftware hiermit eine weitere Signalverarbeitung erfolgen würde. (z.B. Startfreigabe setzen, Fehlererkennung kann sofort erfolgen und ein Maschinenstart kann verhindert werden.)

Die manuelle Rückstellfunktion trägt nicht allein zur Risikoreduzierung bei. Sie ist vielmehr immer im Zusammenhang mit einer Schutzeinrichtung als überwachte Startfunktion zu sehen, so dass für die manuelle Rückstellfunktion eine Bewertung eines PL oder SIL nicht zwingend durchzuführen ist. Die Anforderung der DIN EN ISO 13849-1 Kap. 5.2.2 „durch die manuelle Rückstellfunktion darf die erforderliche Sicherheit nicht gemindert werden“ kann durch die dynamische Flankenauswertung - wie oben beschrieben - erfüllt werden. Die von der Europäischen Kommission verabschiedete Recommendation for Use (RfU (11.053 Rev.03) bestätigt diesen Sachverhalt.

In der Praxis ist eine manuelle Rückstelleinrichtung bei nicht trennenden hintertretbaren Schutzeinrichtungen (insbesondere BWS, Schaltmatten als Zugangsabsicherung) sowie bei verriegelten trennenden Schutzeinrichtungen erforderlich.

Hinweis:

Abhängig vom Typ der eingesetzten BWS gelten für die Rücksetzfunktion funktionale Anforderungen an die Verwendung der Anlauf- bzw. Wiederanlaufsperre (DIN EN 61496-1). Anforderungen an die Verwendung einer Rückstelleinrichtung können für konkrete Applikationen oder Maschinen u.a. durch Typ-C-Normen geregelt sein.

In den Fällen wo aus der Risikobeurteilung eine manuelle Rückstelleinrichtung zur Verhinderung des unerwarteten Anlaufs nicht abgeleitet werden kann (z.B. bei Einsatz von geeigneten Maßnahmen zur Personendetektion, Hintertretsicherung oder Verhinderung des Zugangs zum Gefahrenbereich durch konstruktive Maßnahmen) müssen keine besonderen Maßnahmen z.B. in Form einer Flankenerkennung hinsichtlich des Resetkreises erfüllt werden.

Achtung:

Störimpulse auf der Reset-Leitung (z.B. Surge, Burst, eingekoppelte HF) können grundsätzlich zu einer Reset Auslösung führen, während das Reset angefordert wird (required).

Es muss durch Hardware- und/oder Software-Filtermaßnahmen dafür gesorgt werden, dass diese Störimpulse keinen Einfluss haben. Ein Nachweis kann z.B. durch EMV-Prüfungen mit erhöhten Störpegeln erfolgen.

Der Fachbereich Holz und Metall setzt sich u. a. zusammen aus Vertretern der Unfallversicherungsträger, staatlichen Stellen, Sozialpartnern, Herstellern und Betreibern. Dieses Informationsblatt beruht auf dem durch den Fachbereich zusammengeführten Erfahrungswissen.

Diese DGUV-Information wurde vom Fachbereich Holz und Metall, Sachgebiet Maschinen, Anlagen, Fertigungsautomation erstellt. Diese DGUV-Information ersetzt das Fachbereichs-Informationsblatt „Manuelle Rückstellfunktion gemäß DIN EN ISO 13849-1, Signal-Verarbeitung“, herausgegeben als Entwurf 04/2013. Weitere DGUV-Informationen bzw. Informationsblätter vom Fachbereich Holz und Metall stehen im Internet zum Download bereit [2].

Zu den Zielen der DGUV-Information siehe DGUV-Information FB HM-001 „Ziele der DGUV-Information herausgegeben vom Fachbereich Holz und Metall“.

Literatur:

[1] DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006); Deutsche Fassung DIN EN ISO 13849-1:2008)

[2] Internet: www.dguv.de/fb-holzundmetall Publikationen oder www.bghm.de Webcode: <626>

Bildnachweis

Die in dieser DGUV-Information gezeigten Abbildungen wurden freundlicherweise vom Herausgeber zur Verfügung gestellt.

Herausgeber

Fachbereich Holz und Metall der DGUV
Sachgebiet Maschinen, Anlagen, Fertigungsautomation
Postfach 37 80
55027 Mainz