

## 1 Funktionsbeschreibung

Der Stillstandswächter KFD2-SR2-\*\*.W.SM kann in der Funktion als Stillstandsmonitor mit Anlaufüberbrückung oder als Stillstandsmonitor mit Drehrichtungsmeldung betrieben werden. Die Auswahl der Funktion erfolgt mittels DIP-Schalter 3.

Die Grenzwerte zur Stillstandserkennung können über die DIP-Schalter 1 und 2 ausgewählt werden (Details siehe Datenblatt).

Das Gerät ist mit 2 Eingängen ausgestattet und hat eine maximale Eingangsfrequenz von 2000 Hz

- Die aktuelle Firmwareversion ist 2v0.
- Die aktuelle Hardwareversion ist 1v0.

### Funktion Anlaufüberbrückung

Die Eingangspulse am Eingang 1 werden für die Stillstandsüberwachung verwendet. Der Eingang wird auf Leitungsfehler (LB – Leitungsbruch/LK – Leitungskurzschluss) überwacht (in der Ex-Version).

Eingang 2 wird zur Triggerung der Anlaufüberbrückung verwendet. Es stehen 2 Zeiten (5 s und 20 s) zur Verfügung. Damit wird für die Dauer der Anlaufüberbrückung das Gerät in den Zustand „kein Stillstand“ versetzt. Hier erfolgt keine Leitungsüberwachung.

### Funktion Drehrichtungsmeldung

Hier werden beide Eingänge für die Stillstandsüberwachung verwendet. Fällt einer der beiden Kanäle aus, so wird der noch funktionierende Eingang für die Stillstandsüberwachung verwendet. Zusätzlich wird über die Reihenfolge der Eingangssignale der beiden sich überlappenden Eingangssignale eine Drehrichtung ermittelt. Diese Drehrichtung wird über das Relais 2 ausgegeben. Beide Eingänge werden auf Leitungsfehler überwacht (in der Ex-Version).

### Verhalten bei Störung

- Überwachung auf Leitungsfehler (in der Ex-Version)
- ständige Überwachung des Gerätes auf Fehler des internen Speichers

Bei Auftreten eines Fehlers gehen beide Relais in den sicheren Zustand, die roten LEDs signalisieren den Fehler und über das Power Rail wird ein Sammelfehler (nur Ex-Gerät) ausgegeben

## 2 Beschaltung des KFD2-SR2-\*\*2.W.SM in Zusammenhang mit SIL2-Anwendungen

Achten Sie darauf, dass die Relais im kritischen Zustand der Anwendung abgefallen (passiv) sind. Somit kann bei Stromausfall (abgefallenes Relais) kein sicherheitstechnischer „Gut-Zustand“ (angezogenes Relais) erreicht werden.

Dieses Verhalten ist vor Inbetriebnahme der Anlage zu testen.

### Beispiel 1

Das Schutzgitter einer sich drehenden Welle soll so lange verriegelt bleiben, bis die Welle sich im Stillstand befindet. Der sicherheitstechnisch kritische Zustand ist die sich drehende Welle (Verletzungsgefahr). Aus diesem Grund ist das Verriegeln des Schutzgitters durch ein abgefallenes (passives) Relais zu realisieren. Erst wenn die Welle steht (sicherheitstechnischer Gut-Zustand), zieht das Relais an (aktiv). Diese Gerätefunktion wird nur mit „Stillstandsüberwachung mit Anlaufüberbrückung“ (S3 = I) und Steuerung des Schutzgitters mit Relais 2 erreicht.

### Beispiel 2

Die Kühlung eines kritischen Prozesses mittels Lüfter/Kühlmittelpumpe soll überwacht werden. Der sicherheitstechnisch kritische Zustand ist der Stillstand von Lüfter/Pumpe (Überhitzung). Aus diesem Grund ist das Auslösen eines Alarms durch ein abgefallenes (passives) Relais zu realisieren. Solange der Lüfter bzw. die Pumpe läuft (sicherheitstechnischer Gut-Zustand), zieht das Relais an (aktiv). Diese Gerätefunktion kann mit „Stillstandsüberwachung mit Anlaufüberbrückung“ (S3 = I) und „Stillstandsüberwachung mit Drehrichtungsmeldung“ (S3 = II) mit Relais 1 erreicht werden.

Weitere Angaben zu Rand- und Umgebungsbedingungen sind dem zugehörigen Datenblatt zu entnehmen.

### 3 Sicherheits- und Installationshinweise

Die Stillstandswächter KFD2-SR2-\*\*2.W.SM dürfen nur von eingewiesenem Fachpersonal entsprechend dem Datenblatt betrieben werden.

Der Schutz des Betriebspersonals und der Anlage ist nur gewährleistet, wenn die Geräte entsprechend ihrer bestimmungsgemäßen Verwendung eingesetzt werden. Ein anderer Betrieb als der in dem Datenblatt oder der Sicherheitsanweisung beschriebene stellt die Sicherheit und Funktion der Geräte und angeschlossenen Systeme in Frage.

Können Störungen nicht beseitigt werden, sind die Geräte außer Betrieb zu setzen und gegen versehentliche Inbetriebnahme zu schützen. Die Geräte dürfen nur direkt vom Hersteller Pepperl+Fuchs repariert werden. Eingriffe und Veränderungen in den Geräten sind gefährlich und daher unzulässig. Sie machen jeden Anspruch auf Garantie nichtig und heben die Zulassung nach SIL2 auf.

Fehlfunktionen der Geräte sind an den Hersteller Pepperl+Fuchs zu melden.

Die Stillstandswächter sind in der Schutzart IP21 aufgebaut und müssen dementsprechend bei widrigen Umgebungsbedingungen (Wasser, kleine Fremdkörper) geschützt werden.

### 4 Fehlerraten

Die Fehlerraten und entsprechende zugehörige Kenngrößen sind Abschnitt 6 und der FMEDA zu entnehmen. Die mittlere Ausfallwahrscheinlichkeit PFD entnehmen Sie Abschnitt 5.

Der Stillstandswächter KFD2-SR2-\*\*2.W.SM ist mit dem Sicherheits-Integritätslevel SIL2 eingestuft. Bei der Beurteilung des Gesamtsystems in dem der Stillstandswächter eingesetzt werden soll, ist die Fehlerrate des gesamten Loops zu betrachten.

## 5 Produktlebenszeit und Wartung

Die Produktlebenszeit wird durch folgende Parameter begrenzt:

- Mechanische Lebensdauer der Relais von mindestens  $2,5 \times 10^5$  Schaltspielen bei maximal zulässiger Last (500 VA) entsprechend dem Datenblatt.  
Bei einer Belastung der Kontakte mit ca. 50 mW beträgt die Lebensdauer ca.  $5 \times 10^6$  Schaltspiele.
- Lebensdauer des Flashspeichers ca. 12 Jahre
- Lebensdauer der Elkos ca. 15 Jahre

Bei Geräten die im „Low Demand Mode“ eingesetzt werden, hat die Überprüfung im Rahmen der Wartung der Gesamtanlage zu erfolgen, spätestens aber nach 5 Jahren.

PFD für Geräte mit Leitungsfehlererkennung nach 5 Jahren: **5,62E-4**

PFD für Geräte ohne Leitungsfehlererkennung nach 5 Jahren: **5,81E-4**

Zur Erkennung von zufälligen Fehlern die bei der FMEDA als „undetected dangerous“ eingestuft wurden, sind während der Wartungsintervalle folgende Tests durchzuführen:

- Anlegen einer Frequenz kleiner 10 % der eingestellten Grenzfrequenz -> Relais muss entsprechend den Angaben im Datenblatt schalten.
- Anlegen einer Frequenz größer 10 % der eingestellten Grenzfrequenz + zugehöriger Hysterese -> Relais muss entsprechend den Angaben im Datenblatt schalten.
- Bei der Überprüfung der Schaltzustände der Relais ist im abgefallenen Zustand zu prüfen, ob der Ruhekontakt (Öffner, NC) niederohmig ist und der Arbeitskontakt (Schließer, NO) hochohmig (Kontaktverschweißen).
- Bei der Überprüfung der Schaltzustände der Relais ist im angezogenen Zustand zu prüfen, ob der Ruhekontakt (Öffner, NC) hochohmig (Kontaktverschweißen) ist und der Arbeitskontakt (Schließer, NO) niederohmig (Ist nur im Sinne der Verfügbarkeit notwendig).

Durch diese Tests können 95 % aller Fehler die als „undetected dangerous“ eingestuft wurden erkannt werden.

Eine Fehlerfrüherkennung ist in der Funktionalität des KFD2-SR2-\*\*2.W.SM nicht enthalten.

Rekalibrierungen sind nicht erforderlich.

## 6 Validierung

Die Validierung der SIL2-Tauglichkeit der Stillstandswächter KFD2-SR2-\*\*2.W.SM erfolgte im Rahmen eines Assessments mit EXIDA. Die entsprechenden Dokumente sind im Internet oder direkt bei Pepperl+Fuchs zu beziehen.

Als Hardware-Fehlertoleranz wurde entsprechend Tabelle in EN 61508-2 (7.4.3.1.3) Tabelle B der Wert 0 angenommen.

Die verwendeten Fehlerraten beziehen sich auf die „Basic Failure Rates“ aus dem Siemens-Standard SN29500.

Weiterhin wurden folgende Annahmen getroffen:

- Fehlerraten sind konstant, Abnutzung wurde nicht betrachtet.
- Fehlerfortpflanzungen sind nicht relevant.
- Nach einem „sicheren Fehler“ beträgt die Reparaturzeit 8 Stunden.
- Es wird der „Low Demand Mode“ angenommen.
- Fehlerraten von externen Stromversorgungen sind nicht mit eingerechnet.
- Angeschlossene Sensoren wurden nicht in die Fehlerraten mit eingerechnet
- Ausgang 1 wurde als sicherheitsrelevanter Ausgang betrachtet.
- Als Umgebungsbedingung kann entweder die Klassifizierung MIL-HNBK-217F oder IEC 645-1 Klasse C (max. Temperatur entspricht den Herstellerangaben) bei einer durchschnittlichen Umgebungstemperatur von 40°C angenommen werden.
- Die Testzeit innerhalb der die logische Auswerteeinheit auf einen „Dangerous Detected“-Fehler reagieren muss, beträgt eine Stunde.

Folgende SFF und Fehlerraten wurden für den Stillstandswächter KFD2-SR2-\*\*2.W.SM ermittelt:

**mit  
Leitungsfehlererkennung**

$$\lambda_{sd} = 11 \text{ FIT}$$

$$\lambda_{su} = 248 \text{ FIT}$$

$$\lambda_{dd} = 90 \text{ FIT}$$

$$\lambda_{du} = 26 \text{ FIT}$$

$$\text{SFF} = 91,25 \%$$

$$\text{DC}_S = 4,25 \%$$

$$\text{DC}_D = 77,59 \%$$

**ohne  
Leitungsfehlererkennung**

$$\lambda_{sd} = 9 \text{ FIT}$$

$$\lambda_{su} = 247 \text{ FIT}$$

$$\lambda_{dd} = 90 \text{ FIT}$$

$$\lambda_{du} = 27 \text{ FIT}$$

$$\text{SFF} = 90,91 \%$$

$$\text{DC}_S = 3,52 \%$$

$$\text{DC}_D = 76,92 \%$$