

TURCK

**Industrielle
Automation**

SICHERHEITS- HANDBUCH

**RELAIS-
KOPPLER**

**IM73-12-R/230VAC
IM73-12-R/24VUC**



**HFT SFF
MTBF PFD
 λ_{safe}
FMEDA**

Sense it! Connect it! Bus it! Solve it!

1	Über dieses Sicherheitshandbuch	5
1.1	Zielgruppen	5
1.2	Symbolerläuterung	5
1.3	Abkürzungen und Benennungen	5
1.4	Dokumentenhistorie	6
2	Hinweise zu den Geräten	6
2.1	Gerätevarianten	6
2.2	Lieferumfang	6
2.3	Hersteller und Service	7
3	Zu Ihrer Sicherheit	7
3.1	Bestimmungsgemäße Verwendung	7
3.2	Naheliegende Fehlanwendung	7
3.3	SIL-Registrierkarte	7
3.4	Allgemeine Sicherheitsvorschriften	8
4	Gerätespezifische Informationen zu Sicherheitsanwendungen	8
4.1	Sicherheitsfunktion	8
4.2	Sicherer Zustand	8
4.3	Funktionen und Betriebsarten	8
4.3.1	Pegelumschaltung	8
4.3.2	Fehler quittieren	9
4.4	Fehler- und Ausfallarten	9
4.5	Sicherheitstechnische Kennwerte	9
4.5.1	Annahmen FMEDA	9
4.5.2	Hardwarearchitektur	9
4.5.3	Kennwerte – Gerätetyp IM73-12-R/24VUC	10
4.5.4	Kennwerte – Gerätetyp IM73-12-R/230VAC	10
4.6	Wiederkehrende Funktionstests	10
4.6.1	Wiederkehrende Funktionstests für IM73-12-R/24VUC	10
4.6.2	Wiederkehrende Funktionstests für IM73-12-R/230VAC	11
4.7	Nutzungsdauer	11
4.8	Besondere Vorschriften und Einschränkungen	11
5	Installation und Inbetriebnahme	11
5.1	Montieren	11
5.2	Anschließen	12
5.2.1	Anschlussbilder	12
5.3	In Betrieb nehmen	12
6	Betrieb, Instandhaltung und Reparatur	13
6.1	Störungen beseitigen	13
6.2	Instand halten	13
6.3	Reparieren	13
6.3.1	Geräte zurücksenden	13
7	Außerbetriebnahme und Ausmusterung	13
7.1	Außer Betrieb nehmen	13
7.2	Ausmustern	13
8	Anhang – EXIDA-Report FMEDA Turck 04/07-14 R006	15

1 Über dieses Sicherheitshandbuch

Dieses Sicherheitshandbuch enthält Vorschriften zur Anwendung der Geräte in sicherheitstechnischen Systemen (Safety Instrumented Systems SIS). Die Betrachtung der sicherheitsrelevanten Werte basiert auf der IEC 61508. Das Sicherheitshandbuch beschreibt die zur SIL-Beurteilung ermittelten Werte und ist nur im Zusammenhang mit dem anhängenden EXIDA-Report FMEDA Turck 04/07-14 R006 gültig. Lesen Sie dieses Dokument vor dem Gebrauch des Geräts aufmerksam durch. So vermeiden Sie mögliche Personen-, Sach- oder Geräteschäden. Bewahren Sie das Sicherheitshandbuch auf, solange das Gerät genutzt wird. Falls Sie das Gerät weitergeben, geben Sie auch dieses Sicherheitshandbuch mit.



GEFAHR

Fehlfunktion durch Bedienfehler

Lebensgefahr durch Ausfall der Sicherheitsfunktion!

- Die in diesem Sicherheitshandbuch enthaltenen Vorschriften unbedingt einhalten, wenn das Gerät in sicherheitsgerichteten Anwendungen eingesetzt wird.

1.1 Zielgruppen

Das Sicherheitshandbuch richtet sich an Fachpersonal oder fachlich geschultes Personal. Es muss von jeder Person gelesen und verstanden werden, die für eine der folgenden Arbeiten verantwortlich ist:

- Auspacken und Montage
- Inbetriebnahme
- Prüfung und Wartung
- Störungsbehebung
- Demontage und Entsorgung

1.2 Symbolerläuterung

In diesem Sicherheitshandbuch werden folgende Symbole verwendet:



GEFAHR

GEFAHR kennzeichnet eine unmittelbar gefährliche Situation mit hohem Risiko, die zu Tod oder schwerer Verletzung führt, wenn sie nicht vermieden wird.



HINWEIS

Unter HINWEIS finden Sie Tipps, Empfehlungen und wichtige Informationen. Die Hinweise erleichtern die Arbeit, enthalten Infos zu speziellen Handlungsschritten und helfen, Mehrarbeit durch falsches Vorgehen zu vermeiden.



HANDLUNGSAUFFORDERUNG

Dieses Zeichen kennzeichnet Handlungsschritte, die der Anwender auszuführen hat.



HANDLUNGSRISIKO

Dieses Zeichen kennzeichnet relevante Resultate von Handlungen und Handlungsabfolgen.

1.3 Abkürzungen und Benennungen

Begriffserklärungen siehe IEC 61508-4

DC	diagnostic coverage	Diagnosedeckungsgrad
E/E/PE-System	electrical/electronic/programmable electronic system	elektrisch/elektronisch/programmierbares elektronisches System
EUC	equipment under control	EUC-Einrichtung
	dangerous failure	gefährlicher Ausfall
	no effect failure	Ausfall ohne Auswirkung
	no part failure	Ausfall eines unbeteiligten Bauteils
	safe failure	ungefährlicher Ausfall

Sicherheitshandbuch – Relaiskoppler

	safe state	sicherer Zustand
HFT	hardware fault tolerance	Hardwarefehlertoleranz
	high demand mode	Betriebsart mit hoher Anforderungsrate
	low demand mode	Betriebsart mit niedriger Anforderungsrate
MooN	M out of N channel architecture	Architektur mit M-aus-N Kanälen
MTBF	mean time between failures	mittlere Betriebsdauer zwischen Ausfällen
MTTR	mean time to restauration	mittlere Dauer bis zur Wiederherstellung
PFD	probability of dangerous failure on demand	Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung
PFD_{AVG}	average probability of dangerous failure on demand)	mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung
PFH	average frequency of a dangerous failure per hour	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde
SFF	safe failure fraction	Anteil sicherer Ausfälle
SIF	safety instrumented function	Sicherheitsfunktion
SIS	safety instrumented system	das sicherheitstechnische System
SIL	safety integrity level	Sicherheits-Integritätslevel
	proof test	Wiederholungsprüfung
	proof test interval	Intervall für die Wiederholungsprüfung

1.4 Dokumentenhistorie

Rev.	Beschreibung	Datum
1.0.0	Erstausgabe	02.04.2015

Die deutschsprachige Version gilt als das führende Dokument. Sämtliche Übersetzungen wurden mit großer Sorgfalt erstellt. Sollten Sie unsicher sein hinsichtlich der Auslegung, verwenden Sie das deutschsprachige Sicherheitshandbuch oder wenden sich direkt an TURCK.



HINWEIS

Benutzen Sie grundsätzlich das neueste Sicherheitshandbuch. Prüfen Sie, ob eine neuere Version zur Verfügung steht.

2 Hinweise zu den Geräten

2.1 Gerätevarianten

Dieses Sicherheitshandbuch gilt für die folgenden TURCK-Trennschaltverstärker:

IM73-12-R/230VAC

IM73-12-R/24VUC

2.2 Lieferumfang

Im Lieferumfang sind das Gerät und die SIL-Registrierkarte enthalten.

2.3 Hersteller und Service

TURCK unterstützt Sie bei Ihren Projekten von der ersten Analyse bis zur Inbetriebnahme Ihrer Applikation. In der TURCK-Produktdatenbank finden Sie Software-Tools für Programmierung, Konfiguration oder Inbetriebnahme, Datenblätter und CAD-Dateien in vielen Exportformaten. Über folgende Adresse gelangen Sie direkt in die Produktdatenbank: www.turck.de/produkte

Für weitere Fragen ist das Sales-und-Service-Team in Deutschland telefonisch unter folgenden Nummern zu erreichen:

Vertrieb: +49 208 4952-380

Technik: +49 208 4952-390

Im Ausland wenden Sie sich bitte an Ihre TURCK-Landesvertretung.

Hans Turck GmbH & Co. KG
45466 Mülheim an der Ruhr
Germany

3 Zu Ihrer Sicherheit

Das Gerät ist nach dem Stand der Technik konzipiert. Dennoch gibt es Restgefahren.

Um Personen- und Sachschäden zu vermeiden, müssen Sie die Warnhinweis und Sicherheitsvorschriften beachten. Für Schäden durch Nichtbeachtung von Vorschriften übernimmt TURCK keine Haftung.

3.1 Bestimmungsgemäße Verwendung

Die Relais-Koppler IM73-12-R/24VUC und IM73-12-R/230VAC dienen zur sicheren Trennung binärer Signale. Ausgangsseitig sind zwei synchrongesteuerte Relais mit je einem Umschalter vorhanden.

Mit diesen Geräten lassen sich auch sicherheitsgerichtete Systeme bis einschließlich SIL3 gemäß IEC 61508 aufbauen (Eingangselektronik: Hardwarefehlertoleranz HFT = 0; Ausgangselektronik: Hardwarefehlertoleranz HFT = 1). Die Geräte dürfen nur in sicherheitsgerichteten Kreisen verwendet werden, wenn alle Anforderungen strikt eingehalten werden, die sich aus diesem Sicherheitshandbuch und dem EXIDA-Bericht ergeben. Die Angaben im EXIDA-Bericht gelten bei Anwendung der IEC 61508 für Einsatzfälle mit niedriger Anforderungsrate (Gerätetyp A für Low-Demand-Betrieb). Beim Einsatz in Sicherheitssystemen ist die Ausfallwahrscheinlichkeit (PFD) für den gesamten Kreis zu ermitteln und zu berücksichtigen.

3.2 Naheliegende Fehlanwendung

Bei Einsatz in Sicherheitskreisen müssen die beiden Relais (Umschalter) in Reihe geschaltet werden; darüber hinaus muss der Kontaktstromkreis durch eine Sicherung auf 60 % des Nennstroms ($5 \text{ A} \times 0,6 = 3 \text{ A}$) begrenzt sein.

3.3 SIL-Registrierkarte



HINWEIS

Die dem Gerät beiliegende SIL-Registrierkarte muss im Falle sicherheitsgerichteter Anwendungen der Geräte vom Anwender ausgefüllt und an TURCK zurückgeschickt werden.

3.4 Allgemeine Sicherheitsvorschriften

- Der Anwender ist dafür verantwortlich, dass das Gerät jeweils in Übereinstimmung mit den geltenden Bestimmungen, Normen und Gesetzen eingesetzt wird.
- Die Eignung für bestimmte Einsatzfälle muss durch die Betrachtung des jeweiligen sicherheitsgerichteten Gesamtsystems im Hinblick auf die Anforderungen der IEC 61508 bewertet werden.
- Das Gerät darf nur von geschultem Personal montiert und installiert werden.
- Das Gerät darf nur von erfahrenen Anwendern in Betrieb genommen und betrieben werden.
- Vor dem ersten Betrieb, nach Reparatur und Austausch sowie im vorgeschriebenen Zeitabstand T[Proof] muss ein Funktionstest durchgeführt werden
- Beim Betrieb des Gerätes ist sicherzustellen, dass die Spannungsversorgung dem angegebenen Spannungsbereich entspricht.
- Der ordnungsgemäße Zustand der Verbindungen und Kabel muss regelmäßig überprüft werden.
- Besondere applikationsspezifische Einflüsse, wie z. B. chemische und physikalische Belastungen, können zur vorzeitigen Abnutzung der Geräte führen und müssen bereits bei der Anlagenplanung berücksichtigt werden; fehlende Erfahrungswerte durch besondere Maßnahmen ausgleichen, z. B. durch verkürzte Prüfintervalle.
- Bei Fehlern innerhalb des Gerätes, die zum Übergang in den als sicher definierten Zustand führen, müssen Maßnahmen getroffen werden, die bei Weiterbetrieb der Gesamtsteuerung den sicheren Zustand erhalten.
- Gefährliche Ausfälle müssen umgehend an TURCK gemeldet werden.
- Ein defektes Gerät muss umgehend ausgetauscht und darf nicht repariert werden.
- Bei defekten Klemmen sowie bei sichtbaren Fehlern am Gerät ist ein sofortiger Austausch notwendig.
- Eingriffe und Umbauten am Gerät sind unzulässig. Reparaturen dürfen ausschließlich von TURCK ausgeführt werden. Senden Sie das Gerät zu diesem Zweck an TURCK (siehe Abschnitt „Reparieren“).
- Vor dem Einsatz des Produktes in sicherheitsbezogenen Anwendungen müssen die Angaben dieses Sicherheitshandbuches immer auf ihre Anwendbarkeit für die jeweilige Applikation (z. B. auf besondere, branchenspezifische Anforderungen und Gepflogenheiten) geprüft werden. Im Zweifelsfall kontaktieren Sie bitte die angegebene Herstelleradresse.

4 Gerätespezifische Informationen zu Sicherheitsanwendungen

4.1 Sicherheitsfunktion

Die Ausgangsrelais sind abgeschaltet, wenn die Eingangsspannung kleiner als die Schaltschwelle ($< 5\text{ V}$) ist.



GEFAHR

Fehler bei der Installation und Inbetriebnahme

Lebensgefahr durch Ausfall der Sicherheitsfunktion

- Die beiden Relais (Umschalter) müssen in Reihe geschaltet werden. Setzen Sie dazu eine Brücke zwischen Klemme 21 und 14.
- Stellen Sie sicher, dass der Kontaktstromkreis durch eine Sicherung auf 60 % des Nennstroms ($5\text{ A} \times 0,6 = 3\text{ A}$) begrenzt ist.
- Falls das Gerät direkt durch ein Schütz angesteuert wird, versehen Sie das Schütz mit einer Schutzbeschaltung.

4.2 Sicherer Zustand

Der sichere Zustand ist so definiert, dass der Ausgang LOW ist (Relais abgefallen).

4.3 Funktionen und Betriebsarten

4.3.1 Pegelumschaltung

Eine Pegelumschaltung am Eingang verursacht eine Pegelumschaltung am zugehörigen Ausgang.

Pegelumschaltung – Gerätetyp IM73-12-R/24VUC

- Am Ausgang liegt ein HIGH-Pegel an, wenn das Eingangssignal 19...29 V ist.
- Am Ausgang liegt ein LOW-Pegel an, wenn das Eingangssignal 0...5 V ist.

Pegelumschaltung – Gerätetyp IM73-12-R/230VAC

- Am Ausgang liegt ein HIGH-Pegel an, wenn das Eingangssignal 184...276 VAC ist.
- Am Ausgang liegt ein LOW-Pegel an, wenn das Eingangssignal 0...5 V ist.

4.3.2 Fehler quittieren

Fehler müssen nicht quittiert werden. Ist der Fehler beseitigt, nimmt das Gerät den Betrieb selbstständig wieder auf.

4.4 Fehler- und Ausfallarten

Fehler müssen im Zusammenhang mit der Applikation in sichere (nicht gefährliche) und unsichere (gefährliche) Fehler klassifiziert werden. Dafür sind Sie als Betreiber verantwortlich.



HINWEIS

Sämtliche Schäden, die durch einen gefährlichen unentdeckten Ausfall verursacht werden, müssen umgehend an TURCK gemeldet werden.

4.5 Sicherheitstechnische Kennwerte

4.5.1 Annahmen FMEDA

Die sicherheitstechnischen Kennwerte wurden auf Basis einer FMEDA nach IEC 61508 ermittelt. Die FMEDA beruht auf folgenden Annahmen:

- Die Ausfallraten sind konstant.
- Der mechanische Verschleiß ist nicht betrachtet.
- Die Ausbreitung von Ausfällen ist nicht relevant.
- Die Reparaturzeit MTTR nach einem ungefährlichen Fehler beträgt 8 Stunden (Austausch des Gerätes).
- Das Gerät wird in der Betriebsart mit niedriger Anforderungsrate betrieben (Low Demand Mode).
- Die Ausfallraten einer externen Spannungsversorgung sind nicht berücksichtigt.
- Die beiden Ausgangsrelais sind in Reihe geschaltet.
- Bei den verwendeten Ausfallraten handelt es sich um die Siemens-Standards SN 29500 bei 40 °C .
- Die Umgebungsbedingungen entsprechen einer durchschnittlichen industriellen Umgebung, definiert in MIL-HNBK-217-F oder der IEC 60654-1, Class C (sheltered location).
 - Die Umgebungstemperatur beträgt in der Regel 40 °C.
 - Bei Umgebungstemperaturen von 60 °C und bei häufigen Temperaturschwankungen ist ein Sicherheitsfaktor von 2,5 zu verwenden.

4.5.2 Hardwarearchitektur

Das Gerät wird als Komponente des Typs A betrachtet (nicht-komplexes Gerät). Der Abschaltpfad ist redundant aufgebaut. Daher kann die Elektronik in zwei Subsysteme unterteilt und differenziert betrachtet werden:

- Eingangselektronik: Die Hardwarefehlertoleranz HFT ist 0.
- Ausgangselektronik: Die Hardwarefehlertoleranz HFT ist 1.

Aus Gründen der Vereinfachung wurde bei der Analyse das zweite Relais als „Diagnose“ für das erste Relais betrachtet werden kann. Als Diagnostic Coverage DC wurde eine Wert von 90 % festgelegt; damit sind auch Fehler gemeinsamer Ursache berücksichtigt.

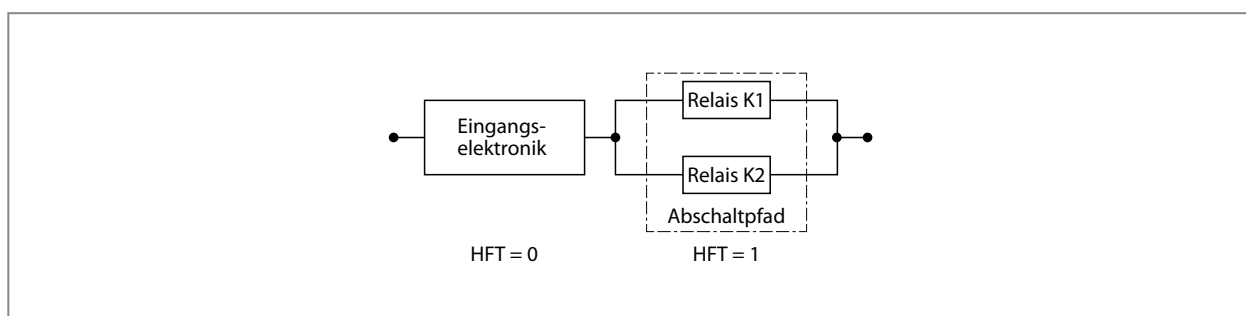


Abb. 1: Relaiskoppler IM73-12-R – Aufteilung der Elektronik in zwei Subsysteme

Sicherheitshandbuch – Relaiskoppler

4.5.3 Kennwerte – Gerätetyp IM73-12-R/24VUC

Das Gerät ist einsetzbar für Anwendungen bis zu SIL 3.

$$MTBF = MTTF + MTTR = 1/(\lambda_{\text{total}} + \lambda_{\text{not part}}) + 8 \text{ h} = 963 \text{ Jahre}$$

Rate ungefährlicher und gefährlicher Ausfälle

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
114 FIT	2 FIT	98,08 %

Mittlere Ausfallwahrscheinlichkeit im Anforderungsfall

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{\text{AVG}} = 9,82 \times 10^{-6}$	$PFD_{\text{AVG}} = 4,91 \times 10^{-5}$	$PFD_{\text{AVG}} = 9,81 \times 10^{-5}$

4.5.4 Kennwerte – Gerätetyp IM73-12-R/230VAC

Die Geräte sind einsetzbar für Anwendungen bis zu SIL 3.

$$MTBF = MTTF + MTTR = 1/(\lambda_{\text{total}} + \lambda_{\text{not part}}) + 8 \text{ h} = 947 \text{ Jahre}$$

Rate ungefährlicher und gefährlicher Ausfälle

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
116 FIT	2 FIT	98,11 %

Mittlere Ausfallwahrscheinlichkeit im Anforderungsfall

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{\text{AVG}} = 9,82 \times 10^{-6}$	$PFD_{\text{AVG}} = 4,91 \times 10^{-5}$	$PFD_{\text{AVG}} = 9,81 \times 10^{-5}$



HINWEIS

Der PFD_{AVG} -Wert der Relaiskoppler ist auf max. 10 % des zulässigen PFD_{AVG} -Gesamtwertes für den Sicherheits-Integritätslevel SIL3 beschränkt. Ein grün unterlegter PFD_{AVG} -Wert besagt, dass der PFD-Anteil nach IEC 61508-1 im Rahmen des SIL3-Bereiches liegt und weniger als 10 % des Gesamtwertes für SIL3 beträgt.

4.6 Wiederkehrende Funktionstests

Vor dem ersten Betrieb, nach jeder Parametrierung, nach Reparatur und Austausch sowie im vorgeschriebenen Zeitabstand T[Proof] ist ein Funktionstest durchzuführen:

4.6.1 Wiederkehrende Funktionstests für IM73-12-R/24VUC

- Stellen Sie sicher, dass der Funktionstest nur von qualifiziertem Personal durchgeführt wird.
- Denken Sie zuerst an Ihre Sicherheit und die Sicherheit Ihrer Umgebung. Tauschen Sie im Zweifelsfall das Gerät aus.
- Brücken Sie den Relaiskoppler in der Sicherheitssteuerung (PLT) und stellen Sie sicher, dass die Sicherheit gewährleistet bleibt. Für die Gewährleistung der Sicherheit sind Sie als Betreiber verantwortlich.
- Simulieren Sie am Eingang eine Spannung $< 3 \text{ V}$ und prüfen Sie, ob der Ausgang auf LOW wechselt.
- Simulieren Sie am Eingang eine Spannung von 24 V und prüfen Sie, ob der Ausgang auf HIGH wechselt.
- Sind alle Prüfungen abgeschlossen und wurden keine Fehler festgestellt, nehmen Sie den Sicherheitskreis wieder in Betrieb.
- Dokumentieren und archivieren Sie nach der Durchführung des Tests die Ergebnisse.

4.6.2 Wiederkehrende Funktionstests für IM73-12-R/230VAC

- Stellen Sie sicher, dass der Funktionstest nur von qualifiziertem Personal durchgeführt wird.
- Denken Sie zuerst an Ihre Sicherheit und die Sicherheit Ihrer Umgebung. Tauschen Sie im Zweifelsfall das Gerät aus.
- Brücken Sie den Relaiskoppler in der Sicherheitssteuerung (PLT) und stellen Sie sicher, dass die Sicherheit gewährleistet bleibt. Für die Gewährleistung der Sicherheit sind Sie als Betreiber verantwortlich.
- Simulieren Sie am Eingang eine Spannung <10 VAC und prüfen Sie, ob der Ausgang auf LOW wechselt.
- Simulieren Sie am Eingang eine Spannung von 230 VAC und prüfen Sie, ob der Ausgang auf HIGH wechselt.
- Sind alle Prüfungen abgeschlossen und wurden keine Fehler festgestellt, nehmen Sie den Sicherheitskreis wieder in Betrieb.
- Dokumentieren und archivieren Sie nach der Durchführung des Tests die Ergebnisse.



HINWEIS

Durch den Funktionstest werden mehr als 90 % der unerkannten Gefahr bringenden Fehler (Du) des Gerätes aufgedeckt

4.7 Nutzungsdauer

Die berechneten Ausfallraten des Gerätes gelten für eine Nutzungsdauer (Useful Lifetime) von 100 000 Schaltzyklen bei 40 °C.

4.8 Besondere Vorschriften und Einschränkungen



HINWEIS

Jede Anwendung hat ihre besonderen Einsatz- und Umgebungsbedingungen. Daher muss bei der sicherheitstechnischen Beurteilung einer Anlage – neben den allgemeinen Aussagen zu Ausfallwahrscheinlichkeiten, Toleranzen und Fehlerraten der Komponenten – immer auch der konkrete Prozess betrachtet werden. So können beispielsweise besondere chemische und physikalische Belastungen zur vorzeitigen Abnutzung der Geräte führen, deren Einflüsse bereits bei der Anlagenplanung berücksichtigt werden müssen. Fehlende Erfahrungswerte lassen sich durch besondere Maßnahmen ausgleichen, zum Beispiel durch verkürzte Prüfintervalle. Die Einschätzung des Diagnosedeckungsgrads (DC) kann von Anwendung zu Anwendung variieren. Die Einschätzung der Hardwarefehlertoleranz (HFT) kann nur erfolgen, wenn Einschränkungen zur Anwendung des konformen Objektes gemacht werden.

5 Installation und Inbetriebnahme



GEFAHR

Fehlfunktion durch Fehler bei der Inbetriebnahme und Bedienung

Lebensgefahr durch Ausfall der Sicherheitsfunktion!

- Stellen Sie sicher, dass das Produkt nur durch fachlich geschultes und erfahrenes Personal montiert, installiert, betrieben und gewartet wird.



GEFAHR

Fehler bei der Installation und Inbetriebnahme

Lebensgefahr durch Ausfall der Sicherheitsfunktion

- Die beiden Relais (Umschalter) müssen in Reihe geschaltet werden. Setzen Sie dazu eine Brücke zwischen Klemme 21 und 14.
- Stellen Sie sicher, dass der Kontaktstromkreis durch eine Sicherung auf 60 % des Nennstroms ($5 \text{ A} \times 0,6 = 3 \text{ A}$) begrenzt ist.
- Falls das Gerät direkt durch ein Schütz angesteuert wird, versehen Sie das Schütz mit einer Schutzbeschaltung.

5.1 Montieren

Beachten Sie die Montagehinweise in der Betriebsanleitung.

Sicherheitshandbuch – Relaiskoppler

5.2 Anschließen

Beachten Sie die Installationshinweise in der Betriebsanleitung.

5.2.1 Anschlussbilder

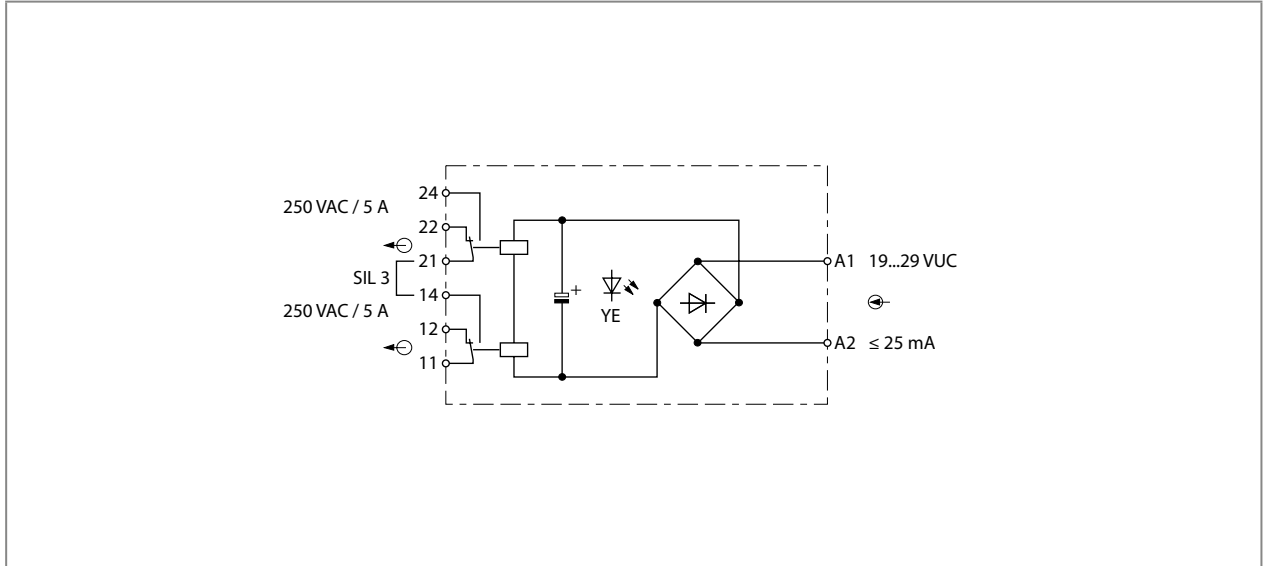


Abb. 2: Blockschaltbild IM73-12-R/24VUC

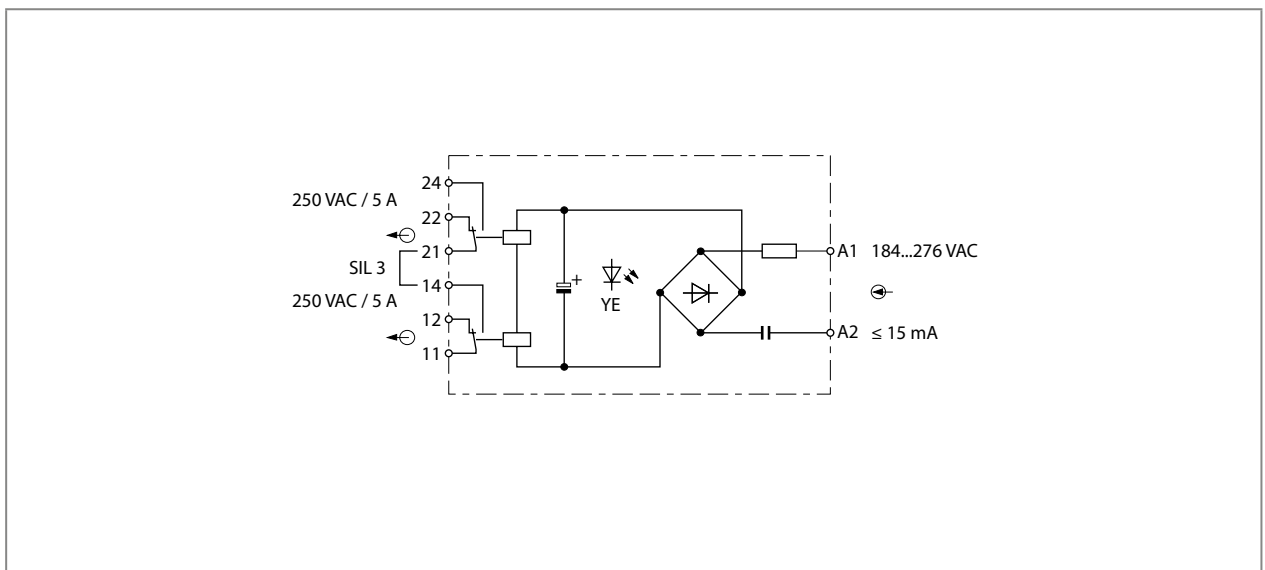


Abb. 3: Blockschaltbild IM73-12-R/230VAC

5.3 In Betrieb nehmen

Beim Betrieb des Gerätes ist sicherzustellen, dass die Spannungsversorgung dem angegebenen Spannungsbereich entspricht. Die Inbetriebnahme ist in der Betriebsanleitung des jeweiligen Gerätes beschrieben.



GEFAHR

Fehlfunktion durch Bedien- und Gerätefehler

Lebensgefahr durch Ausfall der Sicherheitsfunktion!

► Vor dem ersten Betrieb, nach Reparatur und Austausch sowie im vorgeschriebenen Zeitabstand T[Proof] Funktionstest durchführen.

6 Betrieb, Instandhaltung und Reparatur

Die Angaben gelten für die Betriebsbedingungen in einem industriellen Umfeld gemäß IEC 606541-1 Class C (geschützte Lage) mit einer Umgebungstemperatur von 40 °C über einen langen Zeitraum.

6.1 Störungen beseitigen

Die Behebung von Störungen ist in der Betriebsanleitung des jeweiligen Gerätes beschrieben.



HINWEIS

Der Anwender muss sämtliche Störungen am Gerät, die bei Einsatz des Gerätes in sicherheitstechnischen Anwendungen auftreten, umgehend an TURCK melden.

6.2 Instand halten

Der ordnungsgemäße Zustand der Verbindungen und Kabel muss regelmäßig überprüft werden. Die Geräte sind wartungsfrei, bei Bedarf trocken reinigen.



GEFAHR

Fehlfunktion durch leitende Medien oder statische Aufladung

Lebensgefahr durch Ausfall der Sicherheitsfunktion!

► Verwenden Sie bei der Reinigung keine flüssigen Medien oder statisch aufladenden Reinigungsmittel.



GEFAHR

Unbeabsichtigtes Verstellen der Parameter

Lebensgefahr durch Ausfall der Sicherheitsfunktion!

► Führen Sie nach jeder Reinigung einen Funktionstest durch.

6.3 Reparieren



GEFAHR

Das Gerät darf nicht repariert werden.

Lebensgefahr durch Fehlfunktion!

► Senden Sie das Gerät zur Reparatur an TURCK. Beachten Sie hierbei die spezifischen, mit der Lieferung vereinbarten Garantiebedingungen.

6.3.1 Geräte zurücksenden

Ist die Rücksendung eines Gerätes erforderlich, so können nur Geräte entgegengenommen werden, die mit einer Dekontaminationserklärung versehen sind. Diese steht unter http://www.turck.de/static/media/downloads/Dekontamination_de.pdf zum Download zur Verfügung und muss vollständig ausgefüllt, wetter- und transport-sicher an der Außenseite der Verpackung angebracht sein.

7 Außerbetriebnahme und Ausmusterung

7.1 Außer Betrieb nehmen

Die Außerbetriebnahme ist in der Betriebsanleitung des jeweiligen Gerätes beschrieben.

7.2 Ausmustern

Die Geräte müssen nach dem Ablauf der Useful Lifetime von 100.000 Schaltzyklen ausgemustert werden. Die Geräte sind für den Einbau in industrielle Großanlagen und Großwerkzeuge bestimmt. Für die Entsorgung gelten die für diese Anlagen und Werkzeuge maßgeblichen Gesetze und Vorgaben. Die Geräte gehören nicht in den normalen Hausmüll.

8 Anhang – EXIDA-Report FMEDA Turck 04/07-14 R006



Failure Modes, Effects and Diagnostic Analysis

Project:
Relay couplers
IM73-12-R/24VUC and IM73-12-R/230VAC

Customer:
Hans Turck GmbH & Co. KG
Mühlheim
Germany

Contract No.: TURCK 06/02-16
Report No.: TURCK 06/02-16 R006
Version V1, Revision R1.1, March 2006
Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights on the format of this technical report reserved.



Management summary

This report summarizes the results of the hardware assessment carried out on the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC with the two output relays connected in series.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-4}$ to $< 10^{-3}$ for SIL 3 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to $1,00E-04$.

The shut-down path of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC is carried out redundant. Therefore they could be split into two separate subsystems, one representing the input electronics having a hardware fault tolerance of 0, and one representing the shut-down path having a hardware fault tolerance of 1.

For simplicity reasons the analysis, however, was done by considering one of the two relays to be the "diagnostics" for the "primary" relay. A Diagnostic Coverage (DC) of 90% was considered to account for possible common cause failures.

The Relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC are considered to be Type A¹ components with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 90% and 99% according to table 2 of IEC 61508-2 for SIL 3 (sub-) systems with a hardware fault tolerance of 0.

It is important to realize that the "no effect" failures are included in the "safe" failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The following failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

¹ Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.



Table 1: Summary IM73-12-R/24VUC – Failure rates

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
114 FIT	2 FIT	98% ²

Table 2: Summary IM73-12-R/24VUC – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 9,82E-06	PFD _{AVG} = 4,91E-05	PFD _{AVG} = 9,81E-05

Table 3: Summary IM73-12-R/230VAC – Failure rates

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
116 FIT	2 FIT	98% ³

Table 4: Summary IM73-12-R/230VAC – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 9,82E-06	PFD _{AVG} = 4,91E-05	PFD _{AVG} = 9,81E-05

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-04.

Because the Safe Failure Fraction (SFF) is above 90%, also the architectural constraints requirements of table 2 of IEC 61508-2 for Type A subsystems with a Hardware Fault Tolerance (HFT) of 0 are fulfilled.

A user of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 5.1 and 5.2 along with all assumptions.

The failure rates are valid for the useful life of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC (see Appendix 2).

² If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 69% and $\lambda_{\text{dangerous}}$ = 20 FIT per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

³ If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 70% and $\lambda_{\text{dangerous}}$ = 20 FIT per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.



Table of Contents

Management summary	2
1 Purpose and Scope	5
2 Project management	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved	6
2.3 Standards / Literature used	6
2.4 Reference documents	7
2.4.1 Documentation provided by the customer	7
2.4.2 Documentation generated by <i>exida</i>	7
3 Description of the analyzed modules	8
4 Failure Modes, Effects, and Diagnostic Analysis	9
4.1 Description of the failure categories	9
4.2 Methodology – FMEDA, Failure rates	10
4.2.1 FMEDA	10
4.2.2 Failure rates	10
4.2.3 Assumptions	10
5 Results of the assessment	11
5.1 Relay coupler IM73-12-R/24VUC	13
5.2 Relay coupler IM73-12-R/230VAC	15
6 Terms and Definitions	17
7 Status of the document	18
7.1 Liability	18
7.2 Releases	18
7.3 Release Signatures	18
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	18
Appendix 2: Impact of lifetime of critical components on the failure rate	20



1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the software development process

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition this option consists of an assessment of the proven-in-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment carried out on the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC.

It shall be assessed whether the described devices meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 3 sub-systems according to IEC 61508.

It **does not** consider any calculations necessary for proving intrinsic safety.



2 Project management

2.1 exida

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Werner Turck GmbH & Co. KG Manufacturer of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC.

exida Performed the hardware assessment according to option 1 (see section 1).

Werner Turck GmbH & Co. KG contracted *exida* in February 2006 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N3]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N4]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N5]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components



2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	d200555.pdf	Data sheet relay couplers
[D2]	12188900.tif	Circuit diagram "MK73-12-R/...v.c" SP 121 889 00 index A of 23.07.97
[D3]	1364366700.pdf	Parts list 12188907 for MK73-12-R/230VAC/K10 index F of 04.03.97
[D4]	1541124992.pdf	Parts list 12188903 for MK73-12-R/24VUC/K10 index E of 20.08.03
[D5]	FMEDA V6 IM73-12-R24VUC V1R1.xls of 20.01.06	
[D6]	FMEDA V6 IM73-12-R230VUC V1R1 Review SA.xls of 02.03.06	
[D7]	FMEDA V6 IM73-12-R230VUC V1R1 HFT1 Review SA.xls of 02.03.06	

2.4.2 Documentation generated by exida

[R1]	FMEDA V6 IM73-12-R24VUC V1R1 Review SA.xls of 02.02.06	
[R2]	FMEDA V6 IM73-12-R24VUC V1R1 HFT1 Review SA.xls of 02.02.06	
[R3]	FMEDA V6 IM73-12-R24VUC V1R2.xls of 02.03.06	
[R4]	FMEDA V6 IM73-12-R24VUC V1R2 HFT1.xls of 02.03.06	
[R5]	FMEDA V6 IM73-12-R230VAC V1R2.xls of 02.03.06	
[R6]	FMEDA V6 IM73-12-R230VAC V1R2 HFT1.xls of 02.03.06	



3 Description of the analyzed modules

The two single channel relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC are used to securely isolate binary signals.

Both couplers are equipped with two synchronized output relays with one SPDT contact each.

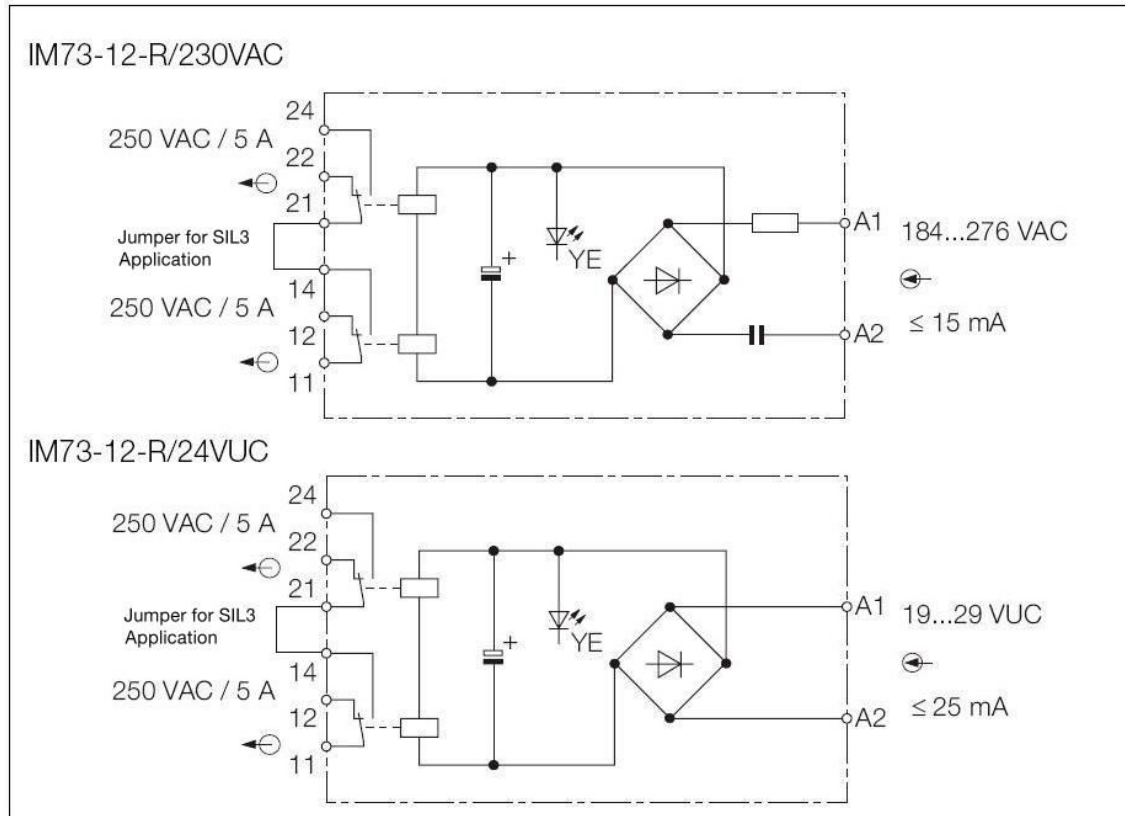


Figure 1: Block diagram of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC

The relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC are considered to be Type A components with a hardware fault tolerance of 0.



4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Werner Turck GmbH & Co. KG and is documented in [D5] to [D7] and [R1] to [R6]. Failures can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized.
Fail Safe	Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state).
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics. For the calculation of the SFF it is treated like a safe undetected failure.
Not part	Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The "No Effect" failures and the "Annunciation Undetected" failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the "No Effect" and "Annunciation Undetected" failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.



4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is a FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates are considered to be appropriate for safety integrity level verification calculations. The rates match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The two relays are connected in series.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
 - IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.



5 Results of the assessment

exida did the FMEDAs together with Werner Turck GmbH & Co. KG.

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

λ_{total} consists of the sum of all component failure rates. This means:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$$

$$SFF = 1 - \lambda_{du} / \lambda_{total}$$

For the FMEDAs failure modes and distributions were used based on information gained from [N3] to [N5].

The shut-down path for the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC is carried out redundant. Therefore they could be split into two separate subsystems, one representing the input electronics having a hardware fault tolerance of 0, and one representing the shut-down path having a hardware fault tolerance of 1.

For simplicity reasons the analysis, however, was done by considering one of the two relays to be the "diagnostics" for the "primary" relay. A Diagnostic Coverage (DC) of 90% was considered to account for possible common cause failures.

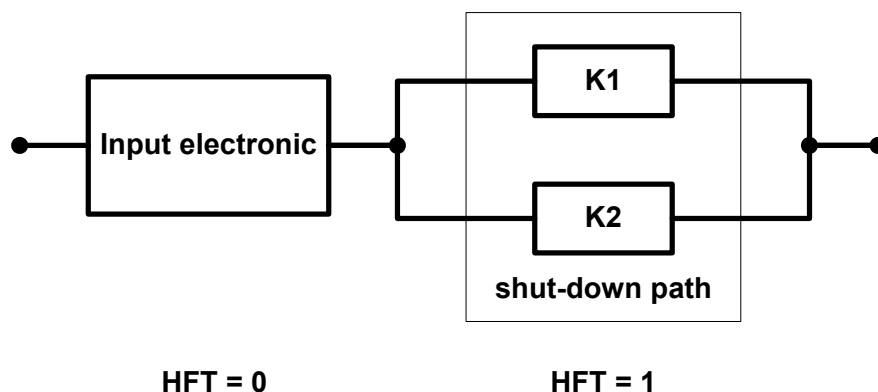


Figure 2: Separation of the relay couplers IM73-12-R into two subsystems

For the calculation of the PFD_{AVG} the following Markov model for 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

The proof test time was changed using the Microsoft® Excel 2000 based FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.

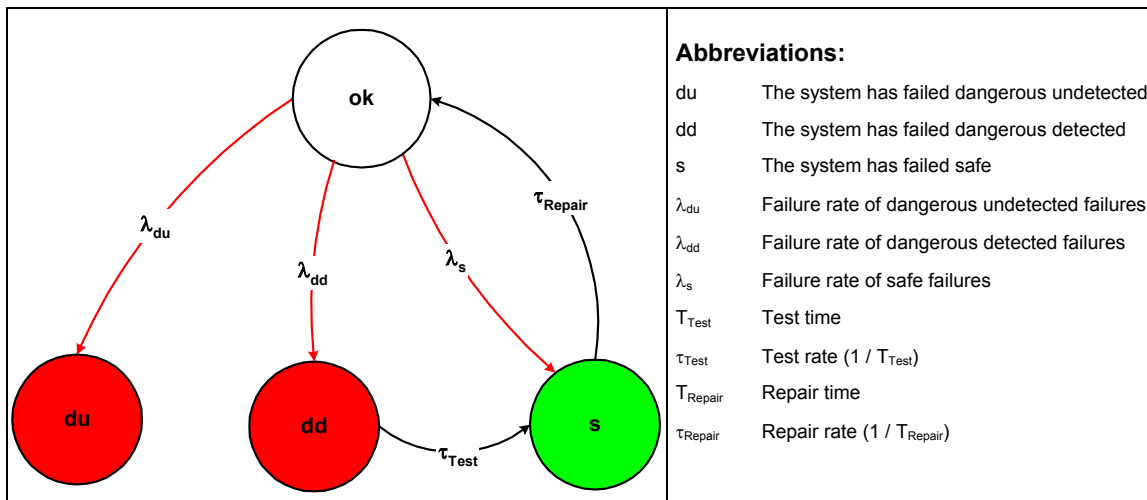


Figure 3: Markov model for a 1oo1D structure



5.1 Relay coupler IM73-12-R/24VUC

The FMEDA carried out on the relay coupler IM73-12-R/24VUC leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

$$\lambda_{SD} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{SU} = 7,21E-08 \text{ 1/h}$$

$$\lambda_{DD} = 1,80E-08 \text{ 1/h}^4$$

$$\lambda_{DU} = 2,24E-09 \text{ 1/h}$$

$$\lambda_{\text{annunciation}} = 2,00E-08 \text{ 1/h}^4$$

$$\lambda_{\text{no effect}} = 4,06E-09 \text{ 1/h}$$

$$\lambda_{\text{total}} = 1,16E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 2,20E-09 \text{ 1/h}$$

$$\text{MTBF} = \text{MTTF} + \text{MTTR} = 1 / (\lambda_{\text{total}} + \lambda_{\text{not part}}) + 8 \text{ h} = 963 \text{ years}$$

Under the assumptions described in section 5 and the definitions given in section 4.1 the following table shows the failure rates according to IEC 61508:

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
114 FIT	2 FIT	98,08% ⁵

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 3.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 9,82E-06$	$\text{PFD}_{\text{AVG}} = 4,91E-05$	$\text{PFD}_{\text{AVG}} = 9,81E-05$

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-04$. Figure 4 shows the time dependent curve of PFD_{AVG} .

⁴ The reason for having "dd" and "annunciation" failures comes from the fact that one of the two relays is considered to be the "diagnostic" for the "primary" relay. A DC of 90% was considered to account for possible common cause failures. The DD and Annunciation failures will actually lead to the fail-safe state and should therefore be considered in spurious trip calculations.

⁵ If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 69,52% and $\lambda_{\text{dangerous}} = 20 \text{ FIT}$ per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

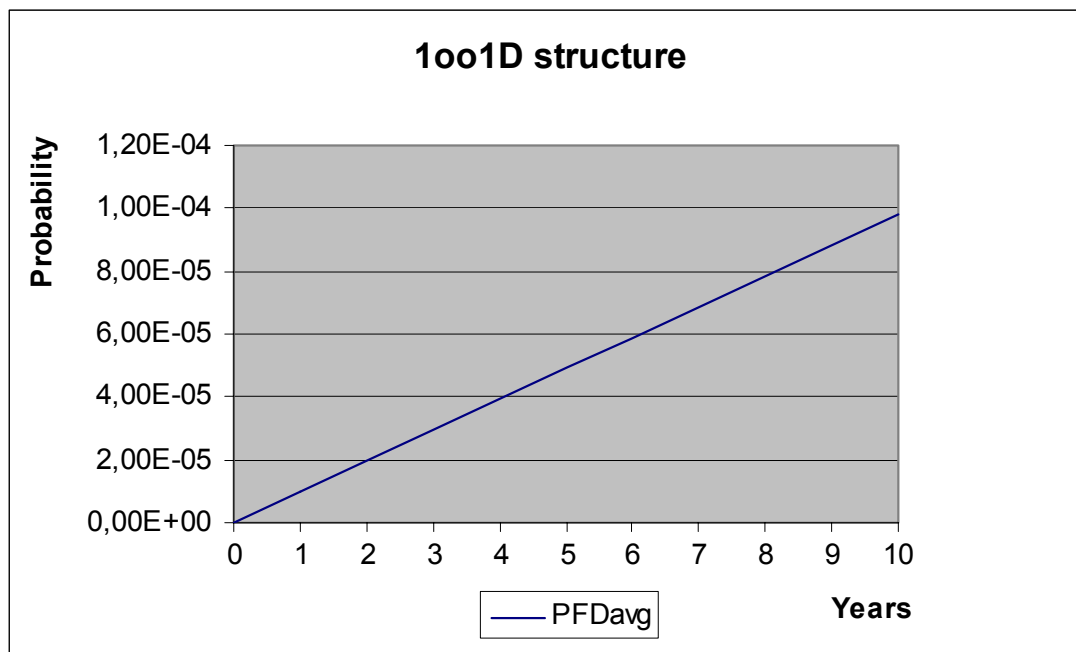


Figure 4: PFD_{AVG}(t)



5.2 Relay coupler IM73-12-R/230VAC

The FMEDA carried out on the relay coupler IM73-12-R/230VAC leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

$$\lambda_{SD} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{SU} = 7,35E-08 \text{ 1/h}$$

$$\lambda_{DD} = 1,80E-08 \text{ 1/h}^6$$

$$\lambda_{DU} = 2,24E-09 \text{ 1/h}$$

$$\lambda_{annunciation} = 2,00E-08 \text{ 1/h}^6$$

$$\lambda_{no \text{ effect}} = 4,57E-09 \text{ 1/h}$$

$$\lambda_{total} = 1,18E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,20E-09 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 947 \text{ years}$$

Under the assumptions described in section 5 and the definitions given in section 4.1 the following table shows the failure rates according to IEC 61508:

λ_{safe}	$\lambda_{dangerous}$	SFF
116 FIT	2 FIT	98,11% ⁷

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 3.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{AVG} = 9,82E-06$	$PFD_{AVG} = 4,91E-05$	$PFD_{AVG} = 9,81E-05$

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-04$. Figure 5 shows the time dependent curve of PFD_{AVG} .

⁶ The reason for having "dd" and "annunciation" failures comes from the fact that one of the two relays is considered to be the "diagnostic" for the "primary" relay. A DC of 90% was considered to account for possible common cause failures. The DD and Annunciation failures will actually lead to the fail-safe state and should therefore be considered in spurious trip calculations.

⁷ If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 70,37% and $\lambda_{dangerous} = 20 \text{ FIT}$ per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

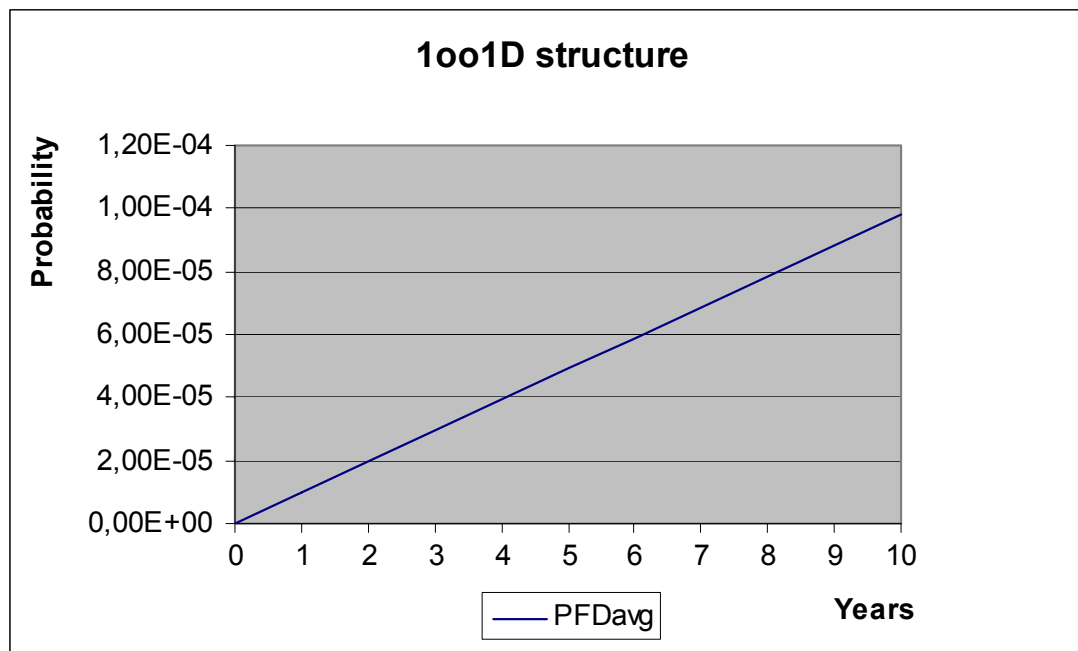


Figure 5: PFD_{AVG}(t)



6 Terms and Definitions

FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A component	"Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval



7 Status of the document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version: V1
Revision: R1.1
Version History: V0, R1.0: Initial version; March 3, 2006
V1, R1.0: Review comments incorporated; March 24, 2006
V1, R1.1: Footnotes 4 and 6 corrected; March 27, 2006
Authors: Stephan Aschenbrenner
Review: V0, R1.0: Review by Frank Seeler (Turck); March 6, 2006
V0, R1.0: Review by Rachel Amkreutz (*exida*); March 24, 2006
Release status: Released to Werner Turck GmbH & Co. KG

7.3 Release Signatures

A handwritten signature in black ink, appearing to read "S. Aschenbrenner", written over a horizontal line.

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

A handwritten signature in black ink, appearing to read "R. Faller", written over a horizontal line.

Dipl.-Ing. (Univ.) Rainer Faller, Principal Partner



Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Table 5 shows an importance analysis of the most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Table 5: Importance Analysis of “du” failures

Component	% of total λ_{du}	Detection through
K1 (K2)	89,29%	100% functional test with monitoring of the output signal of each relay
X1, X2 , X3, X4	10,71%	100% functional test with monitoring of the output signal of each relay



Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime⁸ of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

Table 6 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 6: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life at 40°C
Relay	K1 (K2)	100.000 switching cycles

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

⁸ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

TURCK

**Industrielle
Automation**



www.turck.com

**Your Global
Automation Partner!**

WORLDWIDE HEADQUARTERS

Hans Turck GmbH & Co. KG
Witzlebenstr. 7
45472 Muelheim an der Ruhr
Germany
Tel. +49 208 4952-0
Fax +49 208 4952-264
E-Mail more@turck.com
Internet www.turck.com

D201456 2015/04



Irrtümer und Änderungen vorbehalten