

MANUFACTURER DOCUMENT PACKAGE

Manufacturer's Manual

Selected original pages for procurement and maintenance review

PRODUCT BRAND

Siemens

PRODUCT MODEL

6ES7138-4FB03-0AB0

PROFIsafe Digital Output Module

SOURCE EDITIONS AND SCOPE

03/10/2017; historical technical data, not a current lifecycle assertion (PDF 1,2,3); 08/2008, A5E00888115-07 (PDF 2,3,46,48,71,193,194,195,201,202,203,204); 10/2015, A5E03310062-AE (PDF 9,13,15)

Selected original Siemens pages combine the complete English exact-model datasheet (2017), Chinese operating-manual extracts (08/2008, A5E00888115-07) and the English safety-value supplement (10/2015, A5E03310062-AE). Inductive-voltage limitation differs between historical manufacturer documents and remains unresolved; it is not an approved design value. This reference package is not an installation guide. Installation Instructions are omitted pending resolution.

Open identified Siemens source (complete document)

AMIKON PRODUCT SUPPORT

+86-18020776786 INFO@AMIKON.CN

AMIKONG.COM

Amikon prepared this independent reference package. Siemens remains the author of the appended original pages; original page numbers and manufacturer notices are retained.

*** SPARE PART*** SIMATIC DP, ELECTRON. MODULE F.
ET200S, 4 F-DO PROFISAFE, DC 24V/2A, 30 MM WIDTH UP TO
CATEGORY 4 (EN954-1)/ SIL3 (IEC61508)/PLE (ISO13849), ALSO
USEABLE IN PROFINET- NETWORKS WITH IM151-3 HF



Figure similar

Supply voltage	
Load voltage L+	
• Rated value (DC)	24 V
• Reverse polarity protection	No
Input current	
From load voltage L+ (no load), typ.	100 mA
from backplane bus 3.3 V DC, max.	28 mA
Power loss	
Power loss, typ.	3.5 W
Digital outputs	
Number of digital outputs	4
Short-circuit protection	Yes
Limitation of inductive shutdown voltage to	Typ. (2L+) -47 V
Controlling a digital input	No
Switching capacity of the outputs	
• on lamp load, max.	10 W

Load resistance range	
• lower limit	12 Ω
• upper limit	1 k Ω
Output voltage	
• for signal "1", min.	L+ (-2,0 V), current sourcing switch: L+ (-1,5 V), voltage drop on current sinking switch: max. 0.5 V
Output current	
• for signal "1" rated value	2 A
• for signal "1" permissible range, min.	20 mA
• for signal "1" permissible range, max.	2.4 A
• for signal "0" residual current, max.	0.5 mA; Current-sourcing: max. 0.5 mA; Current sinking: max. 4 mA
Parallel switching of two outputs	
• for uprating	No
• for redundant control of a load	No
Switching frequency	
• with resistive load, max.	30 Hz
• with inductive load, max.	0.1 Hz
• on lamp load, max.	10 Hz
Total current of the outputs	
• Current per module, max.	6 A
Total current of the outputs (per group)	
horizontal installation	
— up to 40 °C, max.	6 A
— up to 55 °C, max.	5 A
— up to 60 °C, max.	4 A
vertical installation	
— up to 40 °C, max.	4 A
Cable length	
• shielded, max.	200 m
• unshielded, max.	200 m
Interrupts/diagnostics/status information	
Diagnostic functions	Yes
Diagnostic messages	
• Wire-break	Yes
• Short-circuit	Yes
Diagnostics indication LED	
• Group error SF (red)	Yes
• Status indicator digital output (green)	Yes
Potential separation	
Potential separation digital outputs	

- between the channels
- between the channels and backplane bus
- Between the channels and load voltage L+

No
Yes
No

Isolation

Isolation tested with 500 V DC

tested with

- Channels against backplane bus and load voltage L+ 1500 V AC

Standards, approvals, certificates

Highest safety class achievable in safety mode

- acc. to EN 954 4
- Performance level according to ISO 13849-1 e
- SIL acc. to IEC 61508 SIL 3

Dimensions

Width 30 mm

Height 81 mm

Depth 52 mm

Weights

Weight, approx. 85 g

last modified: 03/09/2017 

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

 危险
表示如果不采取相应的小心措施， 将会 导致死亡或者严重的人身伤害。

 警告
表示如果不采取相应的小心措施， 可能 导致死亡或者严重的人身伤害。

 小心
带有警告三角，表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

小心
不带警告三角，表示如果不采取相应的小心措施，可能导致财产损失。

注意
表示如果不注意相应的提示，可能会出现不希望的结果或状态。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

Siemens 产品

请注意下列说明：

 警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号 ® 的都是西门子股份有限公司的注册商标。标签中的其他符号可能是一些其他商标，这是出于保护所有权利的目的由第三方使用而特别标示的。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

前言

本手册用途

本手册中的信息是有关 ET 200S 分布式 I/O 系统故障安全模块的操作、功能说明和技术规范的参考源。

基本知识要求

本手册是对《ET 200S 分布式 I/O 系统》(ET 200S Distributed I/O System) 手册的补充。使用本手册需要具有自动化工程的基本知识。还需要具有使用 STEP 7 基本软件和 ET 200S 分布式 I/O 系统的经验。

本手册适用范围

模块	订货号	版本号和更高版本
电源模块 PM-E F pm DC24V PROFIsafe	6ES7138-4CF03-0AB0	01
电源模块 PM-E F pp DC24V PROFIsafe	6ES7138-4CF42-0AB0	01
电源模块 PM-D F DC24V PROFIsafe	3RK1903-3BA02	01
数字电子模块 4/8 F-DI DC24V PROFIsafe	6ES7138-4FA04-0AB0	01
数字电子模块 4 F-DI/3 F-DO DC24V PROFIsafe	6ES7138-4FC01-0AB0	01
数字电子模块 4 F-DO DC24V/2A PROFIsafe	6ES7138-4FB03-0AB0	01
数字电子模块 1 F-RO DC24V/AC24..230V/5A	6ES7138-4FR00-0AA0	01

4.5 对于传感器和执行器的要求

对于传感器和执行器的常规要求

对于传感器和执行器的安全相关的使用，请注意以下重要信息：

警告

传感器和执行器的使用超出我们的影响范围。我们在电子器件中配有安全工程功能，使您能消除最大 85% 的传感器和执行器可能发生的危险故障（这对应于安全工程中传感设备、执行设备和用于输入、处理、输出的电子开关之间建议的负载共享）。

因此请注意，使用带有传感器和执行器的仪器要承担很大的**安全责任**。另请牢记，传感器和执行器的寿命通常不会达到 IEC 61508 中定义的检测测试间隔（没有显著安全损失的情况下，间隔为 10 年）。

安全功能发生危险故障的概率和发生危险故障的严重度必须符合 SIL 定义的上限。可在 F 模块技术规范中的“故障安全性能特性”下找到 F 模块达到的值的列表。

要达到 SIL3（Cat.4/PLe），需要使用相应的合格传感器。

附加传感器要求

一般规则： 使用单通道传感器足可达到 SIL2/Cat.3/PLd。但传感器必须连接到两个通道才可达到 SIL3/Cat.4/PLe。但是，要使用单通道传感器达到 SIL2/Cat.3/PLd，传感器本身必须达到 SIL2/Cat.3/PLd，否则，传感器必须连接到两个通道才能达到此安全级别。

4.5 对于传感器和执行器的要求

对于执行器的附加要求

F 模块定期测试输出。要执行此操作，F 模块将暂时关闭激活的输出。这些测试脉冲的持续时间：

- 暂时禁用期 < 1 ms

在测试期间，快速响应执行器可能会暂时断开。如果过程不容许这样做，则必须使用具有足够延迟(> 1 ms)的执行器。



警告

如果执行器的工作电压高于 24 VDC（例如，230 VDC），或者当执行器用于切换更高电压时，必须确保在故障安全输出模块和承载更高电压（符合 EN 50178）组件的输出之间进行安全隔离。

对于继电器和接触器通常如此。对于半导体开关设备，必须特别注意此方面。

参见

使用 ET 200S 故障安全模块 (页 17)

分配 PROFIsafe 地址 (页 37)

PM-E F pm DC24V PROFIsafe 的技术规范 (页 91)

PM-E F pp DC24V PROFIsafe 的技术规范 (页 108)

PM-D F DC24V PROFIsafe 的技术规范 (页 120)

EM 4/8 F-DI DC24V PROFIsafe 的应用 (页 132)

EM 4/8 F-DI DC24V PROFIsafe 的技术规范 (页 157)

EM 4 F-DI/3 F-DO DC24V PROFIsafe 的输入应用 (页 173)

EM 4 F-DI/3 F-DO DC24V PROFIsafe 的技术规范 (页 188)

EM 4 F-DO DC24V/2A PROFIsafe 的技术规范 (页 205)

EM 1 F-RO DC24V/AC24..230V/5A 的技术规范 (页 217)

故障安全模块

7.1 简介

本章

故障安全电源模块和故障安全数字模块可用于将数字传感器/编码器以及执行器/负载连接到 ET 200S。本章为每个故障安全模块提供了以下信息：

- 属性和特殊功能
- 前视图、端子模块的端子分配和方框图
- 接线图和可编程参数
- 诊断功能（包括纠正措施）
- 技术规范



警告

技术规范中的安全特性适用于为期 20 年的检测测试间隔和 100 小时的修复时间。如果在 100 小时之内无法修复，则在到达 100 小时前从端子模块上拆下相应模块或切断其电源。

然后按照“对故障的响应 (页 49)”一章所述继续进行。

可用的标准电源模块和端子模块的描述

可用的标准电源模块和端子模块在《ET 200S 分布式 I/O 系统》(ET 200S distributed I/O system) 操作说明中介绍。

7.7 EM 4 F-DO DC24V/2A PROFIsafe 数字电子模块

7.7.1 EM 4 F-DO DC24V/2A PROFIsafe 数字电子模块的属性

订货号

6ES7138-4FB03-0AB0

特性

EM 4 F-DO DC24V/2A PROFIsafe 数字电子模块具有下列特性：

- 四个输出，P/M 开关
- 2 A 输出电流
- 额定负载电压为 24 VDC
- 适用于电磁阀、DC 接触器和指示灯
- 组故障显示（SF；红色 LED）
- 每次输出的状态显示（绿色 LED）
- 可分配的诊断
- 可达到安全级别 SIL3

适用于 SIL2 或 SIL3 的电源模块

表格 7- 34 EM 4 F-DO DC24V/2A PROFIsafe： 可达到 SIL/Cat./PL 的电源模块

电源模块	可达到的 SIL/Cat./PL
通过 PM-E DC24V、PM-E DC24V/AC120/230V 或 PM-E DC24..48V 供电	SIL3/Cat.4/PLe

切换接地负载

如果 EM 4 F-DO DC24V/2A PROFIsafe 切换带有机壳接地连接的负载（例如，为了改善 EMC 特性）并且如果机壳在正在使用的电源处接地，则会检测到“短路”。

从 F 模块的角度来看，M 开关通过机壳接地的方式被跨接（请参考下图中的 EM 4 F-DO DC24V/2A PROFIsafe 示例）。

解决方法：

- 使用 PM-E F pp DC24V PROFIsafe
- 在负载端，机壳和接地之间的电阻值必须大于 100 kΩ

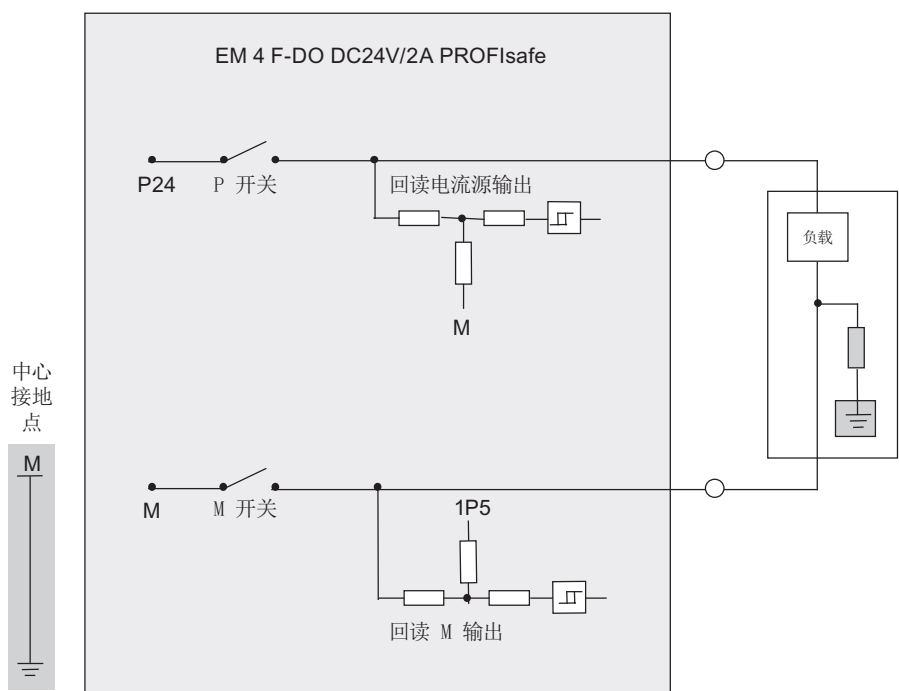


图 7-47 切换接地负载（机壳和接地之间存在电阻）

数字量输入/输出信号的电容串扰

请参见“PM-E F pm DC24V PROFIsafe 电源模块特性”。

电感负载时的磁容量

说明

请注意，连接到 DO 通道的电感负载在强磁场电磁干扰时会引起感应电压。这可能引起短路错误消息。

解决方法：

- 空间上将电感负载与磁场隔断或采用屏蔽层来抵抗磁场。
- 将回读时间参数的值设置为 50 ms 或更高。

7.7.2 EM 4 F-DO DC24V/2A PROFIsafe 端子分配

前视图

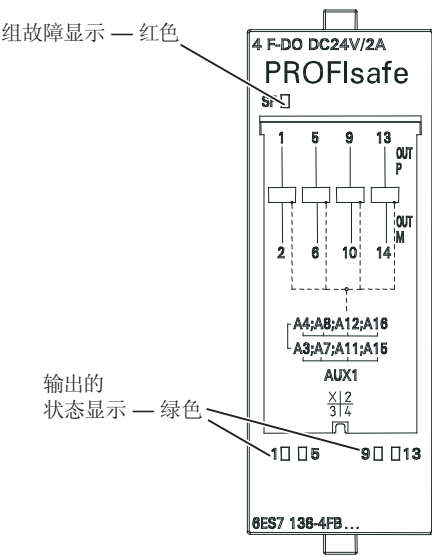


图 7-48 EM 4 F-DO DC24V/2A PROFIsafe 的前视图

 警告

SF LED 和输入/输出的状态显示并非专用于安全相关的功能，因此可能不会针对安全相关的活动对其进行评估。

7.7.4 EM 4 F-DO DC24V/2A PROFIsafe 的参数

STEP 7 中的参数

下表列出了可为 F-DO 模块分配的参数（请参见『组态和编程』）。

表格 7- 35 F-DO 模块的参数

参数	范围	默认	参数类型	有效范围
F 参数:				
F_destination_address	1 到 1022	由 STEP 7 分配	静态	模块
F 监视时间	10 到 10000 ms	150 ms	静态	模块
模块参数:				
通道发生故障后的特性*	钝化整个模块/钝化通道	钝化整个模块	静态	模块
DO 通道 n	激活/取消激活	激活	静态	通道
回读时间	1 到 400 ms	1 ms	静态	通道
诊断: 断线	激活/取消激活	取消激活	静态	通道
* 仅在安装 S7 Distributed Safety V5.4 或更高版本时，此设置才适用。				

回读时间参数

每个输出通道都有其各自可选的回读时间。该时间指定相应通道关闭测试的最长持续时间，从而也可指定关闭通道的回读时间。

可以设置以下回读时间：1 ms、5 ms、10 ms、50 ms、100 ms、200 ms 和 400 ms。

如果通道涉及切换高电容负载，则应设置足够高的回读时间。如果控制电容负载的回读时间设置得太低，由于在关闭测试中不发生电容放电，则输出通道将被钝化。

如果回读信号不正确，则仅当回读时间结束后“短路”故障才会导致输出通道钝化。

 警告
如果回读时间值组态为 50 ms 或更高，则在干扰信号频率大于 10 Hz（50:50 占空因数）时，可以抑制短路（交叉电路）。 将检测同一模块的输出上的短路（交叉电路）。

7.7.5 EM 4 F-DO DC24V/2A PROFIsafe 的诊断功能

在发生电源电压故障时的行为

外部辅助电压出现电压突降时，SF LED 点亮并钝化该模块。

随后电源恢复（电平必须保持高于指定值至少 1 分钟（请参见技术规范：电压、电流、电位））后，SF LED 将再次熄灭而模块保持钝化。如果没有其它错误，则在确认该错误前，SF LED 将一直闪烁。

诊断功能

下表概述了 EM 4 F-DO DC24V/2A PROFIsafe 的诊断功能。诊断功能被分配给一个通道或整个模块。

表格 7- 36 EM 4 F-DO DC24V/2A PROFIsafe 的诊断功能

诊断功能*	故障编号	LED	诊断的有效范围	是否可为其分配参数
短路	1 _H	SF	通道	否
过载	4 _H	SF	通道	否
过热	5 _H	SF	模块	否
断线	6 _H	SF	通道	是
内部错误	9 _H	SF	模块	否
参数分配错误	10 _H	SF	模块	否
传感器或负载失电	11 _H	SF	模块	否
通信错误	13 _H	SF	模块	否
安全相关的关闭	19 _H	SF	通道	否
*: 特别适用于 F 模块；在 STEP 7 中显示，请参见“通道特定诊断，故障安全模块的故障类型”表				

警告

确认短路诊断前，消除相应的错误并验证安全功能。此时，请按“对故障的响应 (页 49)”一章中所述的步骤操作。

故障原因和纠正措施

下表包含 EM 4 F-DO DC24V/2A PROFIsafe 的各诊断消息所述故障的可能原因和解决方法。

表格 7- 37 EM 4 F-DO DC24V/2A PROFIsafe 的诊断消息、出错原因和解决方法

诊断消息	故障检测	可能的原因	纠正措施
短路	始终	执行器中发生短路	消除短路
		执行器中有交叉电路	在发生错误的 100 小时内消除交叉电路。
		内部错误	更换模块
过载	仅针对输出信号“1”	输出级过载并且过热	消除过载故障
过热	始终	由于模块箱内的温度超出上限值或低于下限值而关闭	检查负载接线，检查环境温度，检查是否超过环境温度下允许的输出电流（总电流）。消除故障后，必须拆下模块后再插入，或者关闭电源后再接通。
断线	仅针对输出信号“1”	断线	消除断线，确保规定的最小负载（请参见技术规范）
内部错误	始终	发生内部模块故障	更换模块
参数分配错误	始终	插入的模块与组态不匹配。参数分配不正确。	纠正组态（比较实际组态与预设组态），然后检查通信路径 纠正组态
		PROFIsafe 地址在 F 模块中设置不正确	检查该模块的 PROFIsafe 地址与 <i>HW Config</i> 中的组态是否匹配
传感器或负载失电	始终	无电源电压或电源电压过低	检查互连的 PM 的电源电压并检查模块是否正确接触

诊断消息	故障检测	可能的原因	纠正措施
通信错误	始终	例如，F-CPU 和模块之间的通信由于 PROFIBUS 连接故障或 EMI 高于允许值而发生错误	测试 PROFIBUS/PROFINET 连接。纠正故障
		PROFIsafe 监视时间设置得过低	在 <i>HW Config</i> 中将模块的“F 监视时间”(F monitoring time) 参数的值设置得高一些
		F 模块的组态与安全程序不匹配	重新生成安全程序；然后将组态和安全程序再次加载到 F-CPU
安全相关的关闭	始终	切换频率超出限制	降低切换频率

有关诊断的一般适用信息

有关适合所有故障安全模块的诊断信息（例如，关于读取诊断功能或钝化通道的信息），请参考本手册中的『[诊断](#)』一章。

参见

故障诊断 (页 51)

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security on the Internet (<http://www.siemens.com/industrialsecurity>).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find more information on the Internet (<http://support.automation.siemens.com>).

PFDavg and PFH values for components with use in SIMATIC Safety, Distributed Safety and F/FH Systems

This product information contains **important information on the F-systems SIMATIC Safety, Distributed Safety and F/FH Systems**. The Product Information is part of the product supplied.

PFDavg and PFH values

The following tables contain the PFDavg and PFH values for individual components with use in SIMATIC Safety (S), Distributed Safety (D) and F/FH Systems (F) with a repair time of 100 hours:

F-CPU S7-1200/1500	Operation in low demand mode low demand mode According to IEC 61508:2010: PFDavg = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h ⁻¹]	With a mission time of	S	D	F
For all F-CPU S	< 2E-05	< 1E-09	20 years	x	-	-

F-I/O ET 200SP	Article number	Operation in low demand mode low demand mode According to IEC 61508:2010: PFD_{avg} = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h⁻¹]	With a mission time of	S	D	F
F-DI 8x24VDC HF	6ES7136-6BA00-0CA0	SIL 3: < 2E-05	SIL 3: < 1E-09	20 years	x	x	-
F-DQ 4x24VDC/2A PM HF	6ES7136-6DB00-0CA0	SIL 3: < 2E-05	SIL 3: < 1E-09	20 years	x	x	-
F-PM-E 24VDC/8A PPM ST	6ES7136-6PA00-0BC0	SIL 3: < 2E-05	SIL 3: < 1E-09	20 years	x	x	-
F-RQ 1x24VDC/24..230V AC/5A	6ES7136-6RA00-0BF0	SIL 2: < 1E-04, with function test 1x per year	SIL 2: < 1E-08, with function test 1x per year	20 years	x	x	-
		SIL 3: < 1E-05, with function test 1x per month	SIL 3: < 6E-09, with function test 1x per month	20 years	x	x	-

F-I/O ET 200S	Article number	Operation in low demand mode low demand mode (PFD = average probability of failure on demand)	Operation in high demand or continuous mode high demand/continuous mode (PFH = probability of a dangerous failure per hour)	With a mission time of	S	D	F
4/8 F-DI DC24V PROFIsafe	6ES7138-4FA03-0AB0	SIL 2: < 1E-03 SIL 3: < 1E-05	SIL 2: < 1E-08 SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FA04-0AB0	SIL 2: < 1E-03 SIL 3: < 1E-05	SIL 2: < 1E-08 SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FA05-0AB0	SIL 2: < 1E-03 SIL 3: < 1E-05	SIL 2: < 1E-08 SIL 3: < 1E-10	20 years	x	x	x
4 F-DO DC24V/2A PROFIsafe	6ES7138-4FB02-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FB03-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4FB04-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
4 F-DI/3 F-DO DC24V PROFIsafe	6ES7138-4FC00-0AB0	SIL 2: < 1E-04	SIL 2: < 1E-08	20 years	x	x	x
	6ES7138-4FC01-0AB0	SIL 2: < 1E-04	SIL 2: < 1E-08	20 years	x	x	x
PM-E F pm DC24V PROFIsafe	6ES7138-4CF02-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4CF03-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
PM-E F pp DC24V PROFIsafe	6ES7138-4CF41-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
	6ES7138-4CF42-0AB0	SIL 3: < 1E-05	SIL 3: < 1E-10	20 years	x	x	x
1 F-RO DC24V/AC24..230V /5A	6ES7138-4FR00-0AA0	SIL 3: < 1E-05	SIL 3: < 1E-09	20 years	x	x	x

Fail-safe GSD based DP slaves Fail-safe GSD based IO devices Fail-safe PA field devices Fail-safe HMI devices	Operation in low demand mode low demand mode According to IEC 61508:2010: PFD_{avg} = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode high demand/continuous mode According to IEC 61508:2010: PFH = Average frequency of a dangerous failure [h⁻¹]	With a mission time of	S	D	F
Fail-safe GSD based DP slaves: See Technical Data for fail-safe GSD based DP slave						
Fail-safe GSD based IO devices: See Technical Data for fail-safe GSD based IO device						
Fail-safe PA field devices: See Technical Data for fail-safe PA field device						
Fail-safe HMI devices: See technical specifications on the fail-safe HMI device						
Other fail-safe devices: See technical specifications on the fail-safe device						

Determine the contribution of the F-system to the PFD_{avg} and PFH values

The contribution of the fail-safe system to the PFD_{avg} and PFH values of a safety function is determined by adding the PFD_{avg}- and PFH values of the F-CPU and F-I/Os involved.

The contribution of the safety-related communication is added to this. Please note that several F-systems can be involved in a safety function.

You determine the PFD_{avg} and PFH values of a safety function by adding the contribution of the fail-safe system to the contribution of the encoders and actuators involved in the safety function.

Calculation example

A safety function is implemented with a SIMATIC Safety F-system. The F-CPU and F-I/O listed in the following table are involved in the safety function.

20 years was selected as the mission time. The fail-safe signal modules operate in safety mode for SIL3/Kat.4/PL_e. Operation is in high demand mode:

F-CPU, F-SMs and safety-related communication involved in the safety function	Quantity	Probability of a dangerous failure per hour
CPU 319F-3 PN/DP 6ES7318-3FL01-0AB0	1	3E-09
SM 326; DO 10 × DC 24V/2A 6ES7326-2BF01-0AB0	1	1E-09
SM 326; DI 24 × DC 24V 6ES7326-1BK02-0AB0	2	2E-09
Safety-related communication		1E-09
Total		7E-09

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG

PFD_{avg} and PFH values for components with use in SIMATIC Safety, Distributed Safety and F/FH Systems
A5E03310062-AE, 10/2015