

安全系统评估 Safety Evaluation

演讲人：杨光

安全系统评估 Safety Evaluation

SIEMENS
Ingenuity for life



- 安全系统概念

- 安全评估

- 安全系统的评估

- 机械设备安全评估

安全系统概念

安全功能

针对特定的危险事件，为达到或保持EUC的安全状态，由E/E/PE安全相关系统、其它技术安全相关系统或外部风险降低设施实现的功能。





















安全完整性

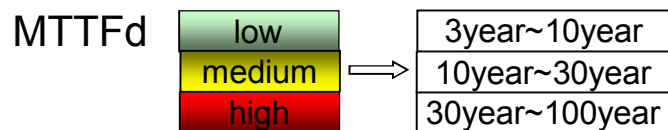
在规定的条件下、规定的时间内，安全相关系统成功实现所要求的安全功能的概率。

- 安全完整性等级越高，安全相关系统不能实现所要求的安全功能的概率越低；
- 安全完整性等级有4种
- 在确定安全完整性的过程中，应包括导致非安全状态的所有失效的起因，例如随机硬件失效，软件导致的失效以及由电气干扰引起的失效。
- 安全完整性由硬件安全完整性和系统安全完整性构成。其中随机硬件失效，在危险失效模式中，可用失效率这样的量进行量化，但系统的安全完整性取决于许多因素，一般只能进行定性的考虑。
- 这一定义着重于安全相关系统执行安全功能的可靠性。

安全系统评估 Safety Evaluation

安全系统的“安全等级”

PL a					
PL b			 	 	 
PL c			 	 	  
PL d				 	
PL e					
DC avg=	0 Cat. B	1 Cat. 1	Low Medium Cat. 2	Low Medium Cat. 3	high Cat. 4



失效概率的计算

1 E/E/PE安全相关系统的安全功能在要求时的平均失效概率，是通过计算和组合提供安全功能的所有子系统在要求时的平均失效概率确定的。由于失效概率很低，故可以表示为：

$$PFDSYS= PFDS+ PFDL+ PFDFE$$

式中：

PFDSYS—E/E/PE安全相关系统的安全功能在要求时的平均失效概率；

PFDS—传感器子系统要求的平均失效概率；

PFDL—逻辑子系统要求的平均失效概率；

PFDFE—最终元件子系统要求的平均失效概率。

失效概率的计算

2 针对各个子系统进行计算

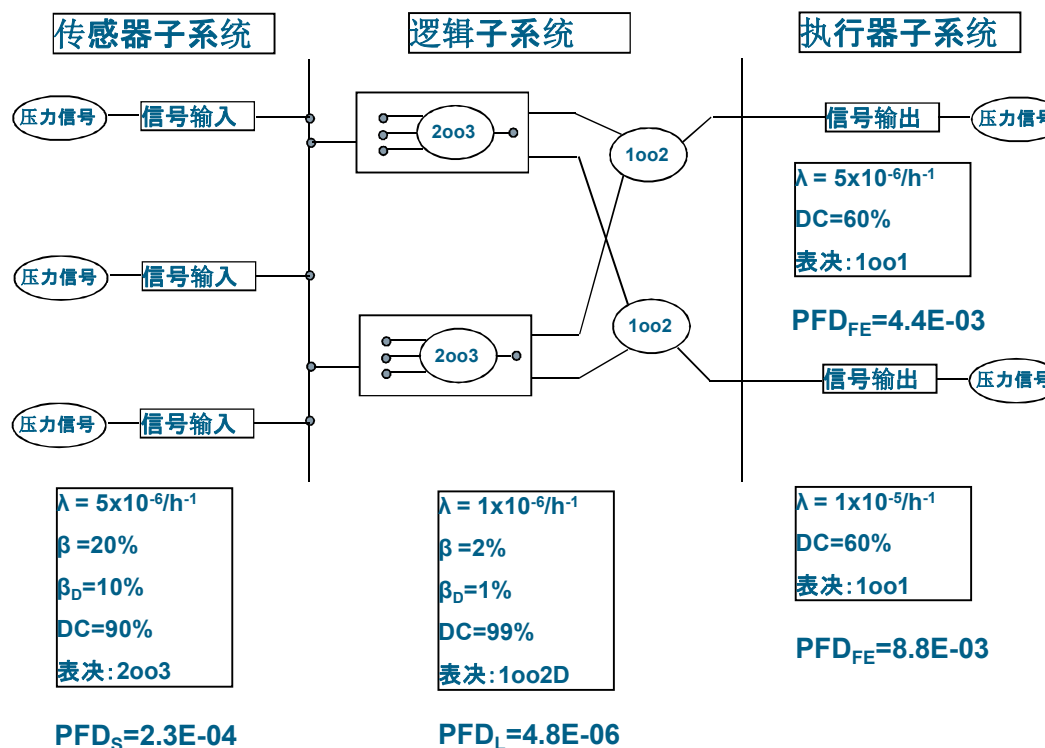
- (1) 画出各子系统的块图，确定每个子系统的表决组：1oo1/1oo2/2oo2/1oo2D/2oo3等；
- (2) 确定检验测试的时间间隔，确定每次失效的平均恢复时间，如8小时。
- (3) 对每个子系统的表决组，确定：
 - 结构（如2oo3）
 - 每个通道的诊断覆盖率（如90%）
 - 每个通道的失效率（小时） λ （例如2.0E-06）
 - 共因失效系数 β
- (4) 将确定的参数带入数学模型计算结果。
- (5) 如果安全功能依赖于传感器或执行器的多个表决组，传感器或最终元件子系统在要求时的组合平均失效概率PFDS或PFDfE为每个表决组平均失效概率之和：

$$PFDS = \sum PFDG_i$$

$$PFDfE = \sum PFDG_j$$

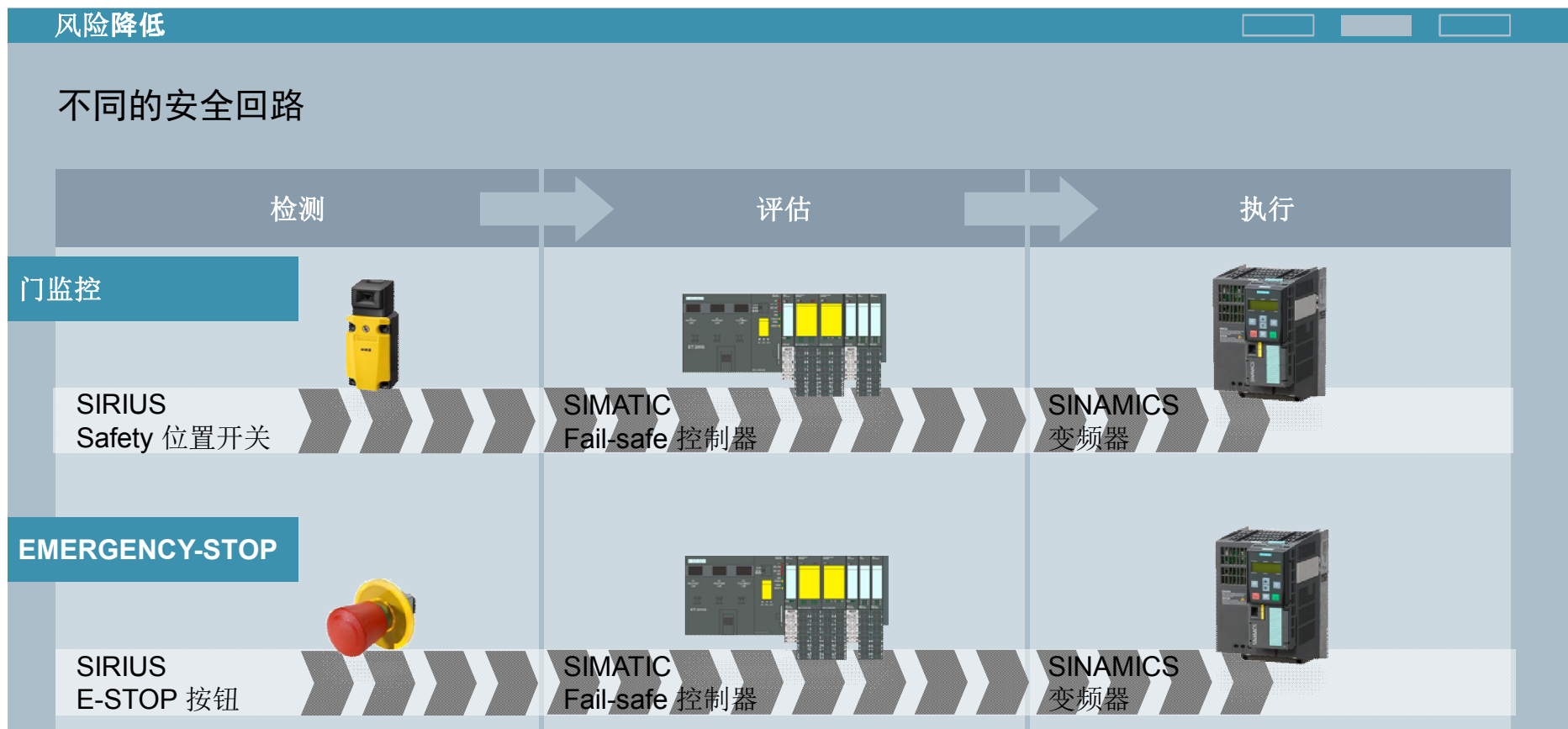
安全系统评估 Safety Evaluation

失效概率的计算



则 $PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} = 1.3 \times 10^{-2} \longrightarrow \text{SIL1}$

安全系统评估 Safety Evaluation



安全系统评估 Safety Evaluation



安全系统评估

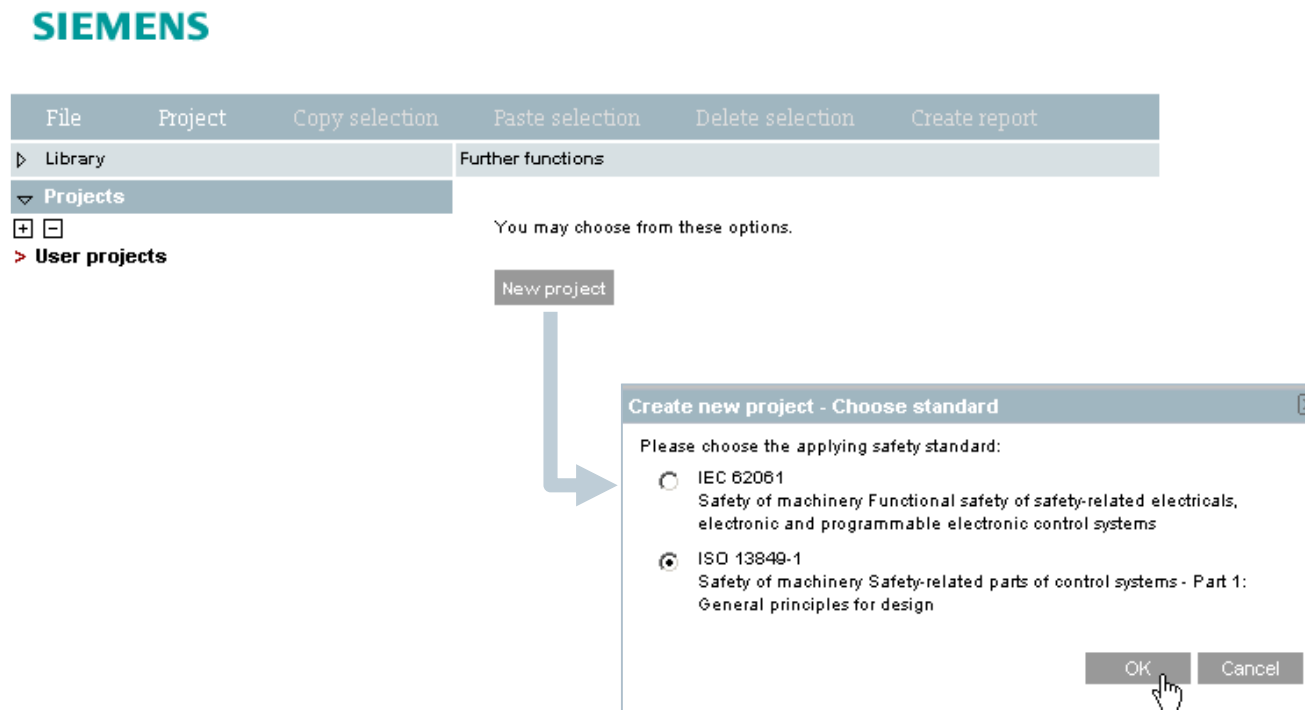
Safety 评估工具

- 免费的基于internet的工具，无需安装，用来评估功能安全，评估标准：
 - ISO 13849-1（替代EN 954-1）
 - IEC 62061
- 报表方式产生文档
- 为两个标准提供简单相同的处理方式
- 使用西门子产品可优化处理

安全系统评估 Safety Evaluation



创建一个新的项目，选择需要的标准



安全系统评估 Safety Evaluation

分配一个项目名称并创建一个Safety区域

The screenshot displays the 'Project - General description' configuration window. The 'Name' field is highlighted with a red box and contains the text 'Project'. Below it, the 'Safety standard' is set to 'ISO 13849-1'. Other fields for 'Manager', 'Inspector', 'Systemtype', and 'Document risk analysis' are present but empty. A large text area for 'Description' is at the bottom. In the 'Further functions' section, a red box highlights the 'New safety area' button, which is accompanied by a tooltip that reads 'Create a new safety area in the selected project'.

Field	Value
Name	Project
Safety standard	ISO 13849-1
Manager	
Inspector	
Systemtype	
Document risk analysis	
Description	

Further functions

You may choose from these options.

New safety area

Create a new safety area in the selected project

安全系统评估 Safety Evaluation

分配安全区域

The screenshot displays the Siemens Safety Integrated software interface. On the left, a tree view shows the project structure: Library > Projects > User projects > Project > Safety area 1. The main window is titled 'Safety area - General description' and contains a form with the following fields:

- Name:** Safety area 1
- Safety standard:** ISO 13849-1
- Description:** (Empty text area)

Below the form, under the heading 'Further functions', there is a section titled 'You may choose from these options.' containing two buttons: 'New safety function' and 'Create a new safety function'. A blue arrow points from the 'New safety function' button to a dialog box titled 'Create new safety function - Choose layout'. This dialog box offers the following options for the layout of the safety function:

- DETECTION > EVALUATION > REACTION
- DETECTION+EVALUATION > REACTION
- DETECTION > EVALUATION+REACTION
- DETECTION+EVALUATION+REACTION

The dialog box also includes 'OK', 'Cancel', and 'Help' buttons at the bottom.

构建功能安全的架构

安全系统评估 Safety Evaluation

Safety 功能 „ESTOP conveyor “ 设定所需安全等级

Safety function - General description

Name	ESTOP conveyor	Status	open
Project name	Project	Version	
Operation mode	automatic mode	Creation date	
Last editor	Name	Last edit date	
Inspector	Siemens, Industry		
Description			

⚠ Required PL: No value selected.

Consideration of safety integrity acc. to ISO 13849-1

Required PL: Please choose Evaluate

Further functions

Required PL: Please choose
PL a
PL b
PL c
PL d
PL e

Further functions

常规数据

输入:

- 名字
- 操作模式, 如自动模式等

安全系统评估 Safety Evaluation



部署子系统

包括子系统传感器（E-STOP）、评估单元（CPU）和执行机构（接触器）

Sensor group - ISO 13849-1 - General description

Name: local E-STOP conveyer

Type: Customerdata required

Manufacturer: Siemens

Productgroup: SPS/US Commanding and Signaling Devices

Producttype: EMERGENCY STOP pushbutton, Turn-to-Release (rotate to unlatch)

Order number: 5SE3 0-1 A20

PL: PL e

PFHD: 2.47 E-08

Logic group - ISO 13849-1 - General description

Name: Failsafe CPU

Manufacturer: Siemens

Productgroup: SIMATIC S7 F-CPU

Producttype: CPU 319F 3PN/DP

Order number: 6ES7318-3FL00-0AB0

PL: PL e

PFHD: 4.00 E-09

PFHD PROFIsafe incl.: 1.00 E-09

Actuator group - ISO 13849-1 - General description

Name: Contactors

Type: Customerdata required

Manufacturer: Siemens

Productgroup: SPS/US Contactors / Motor Starters

Producttype: Contactor 3RT

Order number: 3RT10

PL: PL e

PFHD: 2.47 E-08

安全系统评估 Safety Evaluation



系统安全等级评估结果

File	Project	Copy selection	Paste selection	Delete selection	Create report
Library					
Projects					
<ul style="list-style-type: none"> [-] User projects <ul style="list-style-type: none"> [-] Project <ul style="list-style-type: none"> [-] Safety area 1 <ul style="list-style-type: none"> [-] ESTOP conveyor <ul style="list-style-type: none"> [+] DETECTION <ul style="list-style-type: none"> [>] local ESTOP conveyor [+] EVALUATION <ul style="list-style-type: none"> [>] Failsafe CPU [+] REACTION <ul style="list-style-type: none"> [>] Contactors 					
Safetyfunction - General description					
Name		ESTOP conveyor	Status		open
Project name		Project	Version		
Operation mode		automatic mode	Creation date		
Last editor		Name	Last edit date		
Inspector		Siemens, Industry			
Description					
Consideration of safety integrity acc. to ISO 13849-1					
Required PL		PL e	<input type="button" value="Evaluate"/>	Achieved PL: PL e	
				Achieved PFHD: 5.34 E-08	
Safetyfunction		PFHD: PL a PL b, PL c PL d PL e			
		E-04	E-05	E-06	E-07
					E-08
Further functions					

安全系统评估 Safety Evaluation

输出评估报告

The screenshot displays the Siemens Safety Evaluation Tool interface. At the top, there is a menu bar with options: File, Project, Copy selection, Paste selection, Delete selection, and Create report. Below the menu bar, a sidebar on the left shows a tree view of projects, including 'User projects', 'Project', and 'Safety area 1'. The main area shows a form for 'Safety function - General description' with fields for Name (ESTOP conveyer), Project name (Project), Operation mode (automatic mode), and Industry (s, Industry). A 'Show the report' button is highlighted with a yellow box. A blue arrow points from this button to a preview window of the report.

Report Date: 5/15/10

Safety Evaluation Tool

Name: Project
Safety standard: ISO 13849-1, Safety of machinery - Safety-related parts of control systems
Manager:
Inspector:
System type:
Document risk analysis :
Description:
SET version:
Product data version:

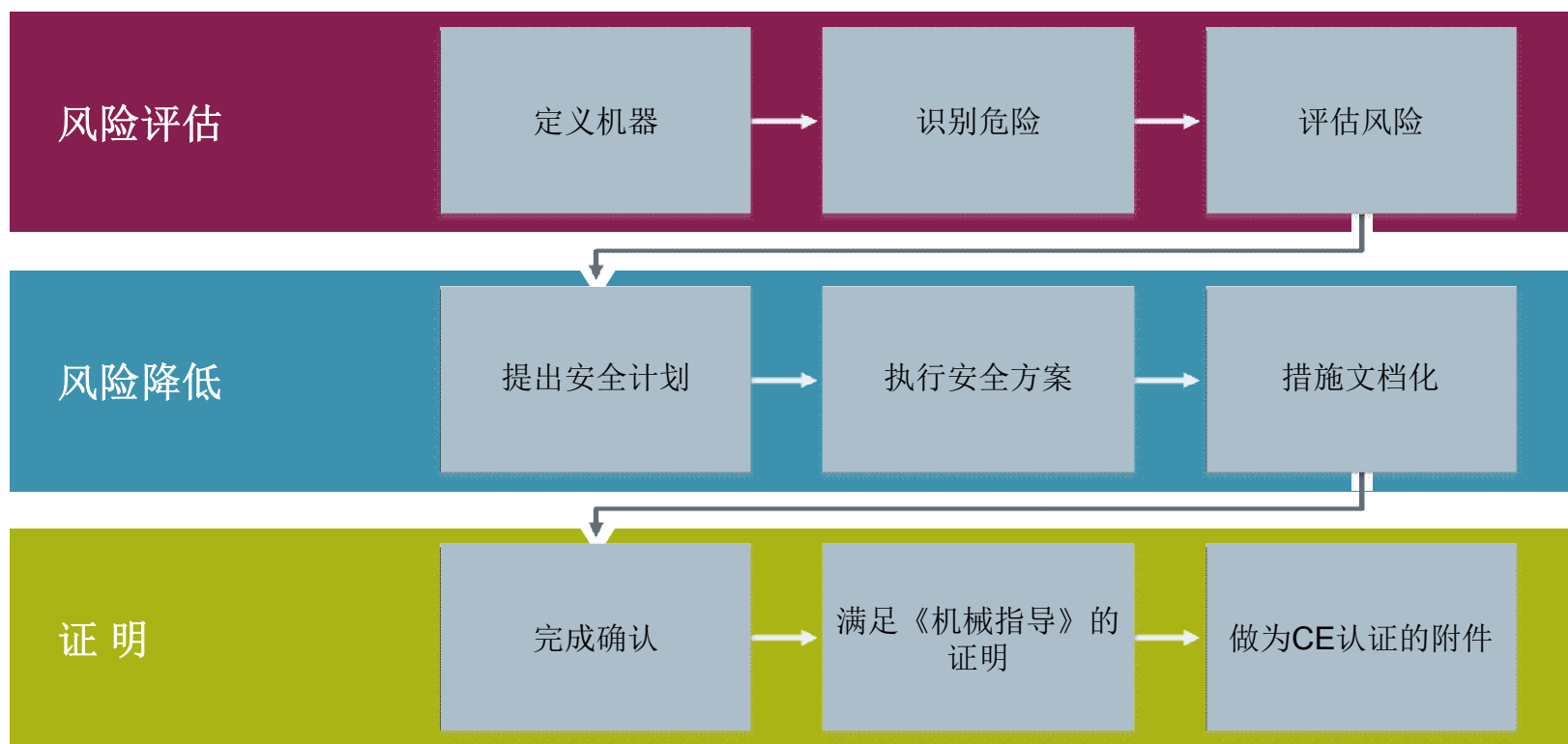
Table of contents

1. Safety functions	(page 3)
2. Approval	(page 4)
3. Annex functions	(page 5)
4. Annex SRP/CS	(page 6)
5. Annex order lists	(page 9)

安全系统评估 Safety Evaluation



机械设备安全评估



SIEMENS
Ingenuity for life

谢谢!

Restricted © Siemens AG 20XX

[siemens.tld/keyword](https://www.siemens.tld/keyword)