ICS 35.240.50
J 09

中华人民共和国国家标准

GB/T 34934—2017/IEC/TS 62513:2008

机械电气安全　安全相关设备中的通信系统使用指南

Electrical safety of machinery—Guidelines for the use of communication systems in safety-related applications

(IEC/TS 62513:2008, Safety of machinery—Guidelines for the use of communication systems in safety-related applications, IDT)

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

学兔兔 www.bzfxw.com

学兔兔 www.bzfxw.com

前　言

本标准按照 GB/T 1.1—2009 和 GB/T 20000.2—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC 62513:2008《机械安全　安全相关设备中的通信系统使用指南》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

GB 5226.1—2008　机械电气安全　机械电气设备　第 1 部分：通用技术条件(IEC 60204-1:2005，IDT)

GB/T 20438(所有部分)　电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分)]

GB 28526—2012　机械电气安全　安全相关电气、电子和可编程电子控制系统的功能安全(IEC 62061:2005，IDT)

本标准做了下列编辑性修改：

——为了与其他相应的标准名称相协调，标准名称改为《机械电气安全　安全相关设备中的通信系统使用指南》。

本标准由中国机械工业联合会提出。

本标准由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本标准起草单位：中国科学院沈阳计算技术研究所有限公司、国家机床质量监督检验中心、山东大学。

本标准主要起草人：尹震宇、黄祖广、薛瑞娟、于东、蒋峥、胡天亮、王芹。

学兔兔 www.bzfxw.com

引　言

本标准的制定用来确定通信系统的完整性。本标准为机械电气安全相关控制系统的设计与使用提供指导。

学兔兔 www.bzfxw.com

机械电气安全　安全相关设备中的通信系统使用指南

1　范围

本标准用于解决机械电气设备安全功能设计实现过程中，用于传输安全相关数据的串行数字通信系统（通常称为现场总线）的问题。它为相关应用在系统设计、安装、调试、修改和维护过程中提供指导。

注：一个串行数字通信系统支持的最大从站数量是确定的，并且其未经授权访问的风险是可以忽略不计的。

本标准假设已经开发了 SRECS 安全要求规范（SRS），并且 SRECS 的设计包含安全相关通信系统。本标准需要与 IEC 62061 一起使用。

本标准不解决安全相关的通信系统本身的设计问题。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

IEC 60204-1　机械安全　机械电气设备　第 1 部分：通用技术条件

IEC 61508（所有部分）　电气/电子/可编程电子安全相关系统的功能安全

IEC 62061　机械电气安全　安全相关电气、电子和可编程电子控制系统的功能安全

3　术语和定义

下列术语和定义适用于本文件。

3.1

类别　category

控制系统有关安全部件在防止故障能力以及故障条件下后续行为方面的分类，他通过部件的结构布置、故障检测和（或）部件可靠性来达到。

[ISO 13849-1，定义 3.1.2]

3.2

通信系统　communication system

设备（如传感器，执行器，机械控制装置等）间消息传输的硬件，软件及传播媒体的安排。

3.3

配置（参数设置）　configuration（parameter setting）

系统操作需要的任何数据的设置和/或修改。

3.4

电磁干扰　electromagnetic interference；EMI

干扰造成的电气电子设备，仪器和/或系统的性能下降，故障或失效。

注：一个典型的干扰为无线电频干扰。

学兔兔 www.bzfxw.com

3.5

容错 fault tolerance

在出现故障或失效时,SRECS、子系统或子系统元素继续执行要求功能的能力。

[IEC 62061,定义 3.2.31]

3.6

节点 Node

通信系统中由一个或多个功能单元互联的数据通道或者数据电路点。

3.7

操作模式 operation mode

操作的方法或方式。

3.8

保护特低电压 protected extra-low-voltage;PELV

由双重绝缘或其他更好绝缘方法保证的与危险电压绝缘的接地电路,无论在正常情况下或者单一故障情况下电压值都不允许超过 GB/T 17045—2008 中的规定。

[GB/T 17045—2008,定义 3.26]

3.9

验证测试 proof test

在 SRECS 系统及其子系统中,该试验可以检测其故障和降级,如必要,以便 SRECS 及其子系统可以回复到"新"状况或尽量接近该状况。

[IEC 62061,定义 3.2.37]

注:验证测试是为了确认 SRECS 处在指定的安全完整性条件下。

3.10

保护措施 protective measure

用于达到风险减小的措施。

——通过设计者实现:本质安全设计、安全防护和附加保护措施、使用信息。

——通过用户实现:组织(安全工作程序、监督、工作许可制度)、附加安全防护装置的提供和使用;个人防护装置的使用;培训。

[ISO 13849-1,定义 3.1.27]

3.11

合理的可预见的误用 reasonably foreseeable misuse

不是按设计者预定的方法而是按照容易预见的人的习惯来使用机器。

[ISO 13849-1,定义 3.1.19]

3.12

安全功能 safety function

其失效会立即造成风险增加的机器功能。

[IEC 62061,定义 3.2.15 及 GB/T 15706—2012,定义 3.28]

注:这里的定义与 IEC 61508-4 和 ISO 13849-1 中给出的不同。

3.13

安全功能要求规范 safety functions requirements specification

一种技术规定,包括安全相关系统必须要执行的安全功能要求。

[IEC 61508-4,定义 3.5.9]

学兔兔 www.bzfxw.com

3.14

安全完整性 safety integrity

在所有规定情况下,SRECS 或其子系统执行所要求的安全相关控制功能的概率。

[IEC 62061,定义 3.2.19]

注 1:安全完整性等级越高则项目执行所需安全相关控制功能失败的概率就越低。

注 2:安全完整性包括硬件安全完整性和系统安全完整性(见 IEC 62061 中 3.2.20 及 IEC 62061 中 3.2.22)。

3.15

安全完整性等级 safety integrity level (SIL)

一种离散的等级(三种可能的等级之一),用于规定分配给 SRECS 安全相关控制功能的安全完整性要求。在这里,安全完整性等级 3 是最高的,安全完整性等级 1 是最低的。

[IEC 62061,定义 3.2.23]

注:本标准不考虑安全完整性等级 4,因为该等级与降低机械相关风险的要求无关。安全完整性等级 4 的相关要求参考 IEC 61508-1 和 IEC 61508-2。

3.16

安全相关的控制功能 safety-related control function;SRCF

由具有规定的完整性等级的 SRECS 执行的控制功能,预期用于保持及其的安全状况或防止风险立即增加。

[IEC 62061,定义 3.2.16]

3.17

安全相关电气控制系统 safety-related electrical control system;SRECS

其失效可能导致风险立即增加的机械电气控制系统。

[IEC 62061,定义 3.2.4]

3.18

安全要求规范 safety requirments specification

一种技术规定,包括安全相关系统必须要执行安全功能的所有要求。

注:规范分为安全功能要求规范和安全完整性等级要求规范。

[IEC 61508-4,定义 3.5.8]

3.19

安全特低电压 safety extra-low-voltage (SELV)

由双重绝缘或其他更好绝缘方法保证的与危险电压绝缘的接地电路,无论在正常情况下或者单一错误情况下电压都不允许超过 GB/T 17045—2008 中规定的过低电压。

[GB/T 17045—2008,定义 3.16]

3.20

安全失效分数 safe failure fraction;SFF

不会导致危险失效的子系统整体失效率系数。

[IEC 62061,定义 3.2.42]

3.21

安全完整性等级要求限度(子系统) SIL claim limit (for a subsystem);SILCL

可被称作 SRECS 子系统关于结构限制和系统安全完整性的最大 SIL。

[IEC 62061,定义 3.2.24]

学兔兔 www.bzfxw.com

3.22

子系统 subsystem

SRECS 高层结构设计的实体，其中任何子系统的失效将导致安全相关控制功能失效。

注 1：完整的子系统可能由许多可识别的及单独的子系统单元构成，一起分配到子系统执行功能块的作用。

注 2：该定义局限于 IEC 61508-4 的一般定义：按照设计相互作用的一组元素，可能包括相互作用的硬件、软件和人。系统中的某一元素可以自成另外的系统，成为子系统。

注 3：这里的定义与通常表述的子系统（实体的任何细分部分）不同，本标准中使用的术语“子系统”具有强烈的术语定义层次结构：“子系统”是系统子部分的第一层次。从子系统中进一步划分出来的子部分为“子系统单元”。

[IEC 62061，定义 3.2.5]

3.23

验证 validation

通过检查（如测试，分析）确认特定应用程序的功能安全要求得到满足。

[IEC 62061，定义 3.2.52，修订]

4 功能安全管理

4.1 IEC 62061 的要求

IEC 62061 要求每一个 SRECS 设计工程都应制定一个功能安全计划，形成文档，并在需要的时候进行升级。计划应包括 IEC 62061 的第 5 章到第 9 章中指定的活动控制程序。

本标准加上 IEC 62061 中规定的功能安全管理要求都已经实施，应注意尤其是适用于与安全相关的通信系统的项目。

特别适用于安全相关通信系统的相关活动主要包括：

a) 选择管理

——见 6.2；

b) 安装管理

——见 7.1；

c) 配置和参数管理

——见 7.2；

d) 验证管理

——见第 8 章；

e) 操作、维护和定期检查管理

——见第 9 章；

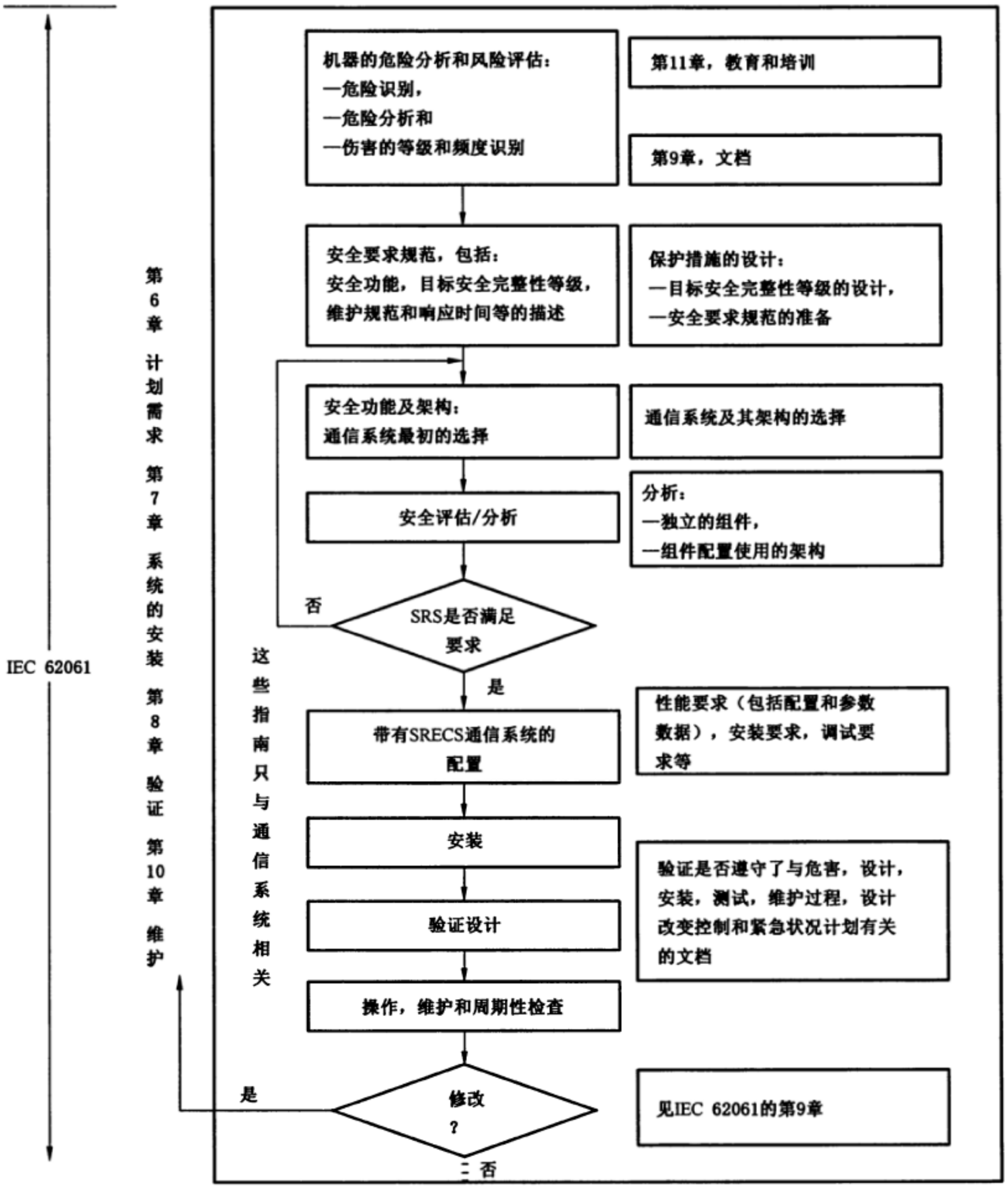
f) 修改管理

——见 IEC 62061 的第 9 章。

5 使用安全相关通信系统的安全相关电气控制系统的实现

图 1 给出了满足安全要求规范中要求的安全功能和安全完整性的 SRECS 的选择，设计和制造过程。

注：安全要求规范（SRS）的细节参考 IEC 62061 的 5.2。



注：参考本标准的参考文献，除非另有说明。

图 1 SRECS 的设计开发流程

6 安全相关通信系统的规划

6.1 系统设计

6.1.1 分配到 SRCF(S)和安全相关通信系统的安全完整性等级(SIL)

本标准假设 SRECS 安全要求规范已按照 IEC 62061 完成，同时安全相关的通信系统中的每一个安全功能的安全完整性等级都已经确定。

安全相关通信系统的安全完整性等级限制应能满足安全相关控制功能的安全完整性等级要求。

注：附录 A 提供了基于功能模块概念的使用了安全相关通信系统的 SRECS 设计的概述。

6.1.2 安全相关通信系统的配置和参数

该部分技术内容在考虑中。

6.1.3 响应时间和保护措施

包含安全相关通信系统的 SRECS 从输入到输出的最坏响应时间应该足够短，并能保证特定应用的所有安全功能可以在 SRS 要求的时间内完成。在最坏响应时间内无法完成独立的安全功能（例如，机械限制造成）的情况下，应采取其他措施（例如，附加的保护措施，选择能够提高可变响应时间的安全相关通信系统）来满足 SRS 的相关要求。

图 2 给出了应考虑的可变系统响应时间的组成部分，他们应该考虑远程安全相关输入和远程安全相关输出控制通信。

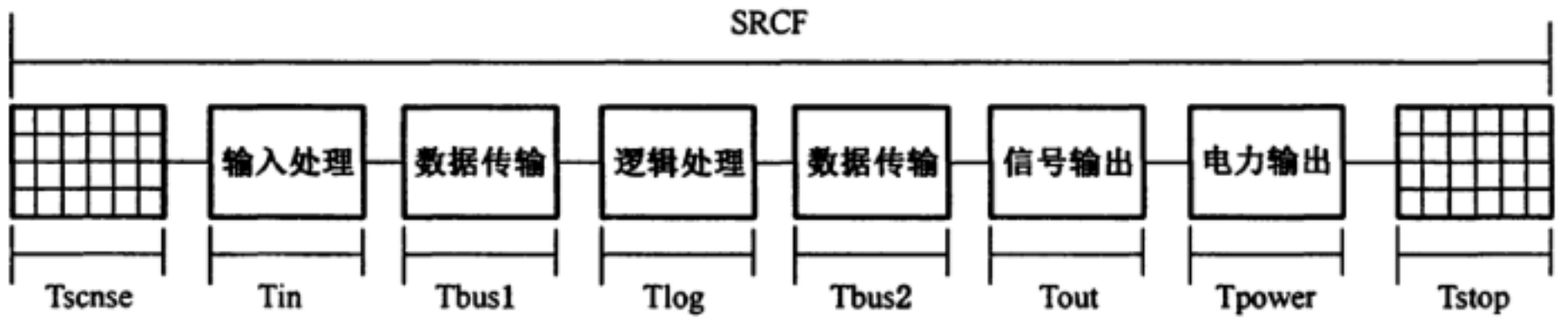


图 2 系统响应时间组成部分

安全相关通信系统的响应时间定义为：

通信系统响应时间＝Tbus1＋Tbus2；

值得注意的是 Tbus1 和 Tbus2 不独立于总线周期或一则消息时间，它们还包含重复，错误处理和同步延时等，处理细节参考安全相关通信系统规范。

注：由于 SRCF 中的非同步过程也可能出现其他延时，在计算最差响应时间的时候应予以考虑。

同样需要注意的是 Tbus1 与 Tbus2 没有直接关联。这两个参数的值可以相等也可以不同，它们依赖于上行或下行设备，以及影响响应时间的通信设置。

符合响应时间的要求是必要的。它应该被检查。在设计中应该考虑一个足够的差额以便允许指定响应时间内的可预见的变化，主要包括可预见的修改造成的变化。

6.1.4 故障检测和报警指示

SRECS 的错误信息应能够通过通信系统进行传输。建议进行集中故障监测，以便在更短的时间内排除故障。

故障的集中监测：

——任何与故障相关的信息都要发送到主站；

——主站要处理这些信息；

——故障信息要以易于定位和分析的方式表达。

也可以采用其他形式的故障监测（例如，分布式）。

报警指示要比其他指示拥有更高的优先级，并应在设计中注重人体工程学原理。报警指示应不影响安全功能的执行。

6.1.5 SRECS 失效情况下的功能安全保证

包含安全相关通信系统的 SRECS 应考虑出现故障的情况。处理这类错误的策略应在设计阶段考虑。

SRECS 中安全相关通信系统的选择与集成应考虑以下步骤：

——应用范围应包括可预见的错误；
——故障，和
——在机器按要求操作条件下可预见的人为错误。
故障实例如下：
——各种开关和传感器的错误输入；
——各种开关和传感器的错误输入；
——网络输出错误情况下的驱动器操作；
——网络失效情况下节点的输入输出；
——主站故障情况下的输入输出，等。

在这些通信故障条件下，与 SRS 相关的 SRECS 的行为应该在早先阶段进行评估，同时系统应设计有应对这些故障的策略(故障响应功能)。

6.2 安全相关通信系统的选择标准

6.2.1 架构与应用领域

为特定应用选择合适的安全相关通信系统，因为不同的安全相关通信系统拥有不同的数据传输能力。

选择安全相关通信系统时，应至少考虑以下：
——最大响应时间；
——实现安全相关控制功能所需要的节点数量，和
——应用领域；
——传输速度；
——传输距离；
——供将来使用的备用节点。

注：上述因素没有按照优先级顺序罗列。

6.2.2 最大响应时间

在任何情况下，设计中都不能超过 SRCF 要求的响应时间(例如，包括传输错误和电磁干扰对安全相关通信系统的影响)。安全相关通信系统的最大响应时间与系统设计和应用特点相关。

注：安全相关通信系统的最大响应时间等同于 IEC 61784-3 中给出的现场总线安全响应时间。

影响最大响应时间的因素主要包括(不限于)以下因素：
——安全输入设备的延时(包含输入延时)；
——安全通信的时间延时；
——安全控制的处理时间；
——安全输出设备的延时；
——通信系统在故障情况下的行为。

另外，以下因素也应予以考虑：
——网络上连接的节点数量；
——主机控制器的逻辑处理时间；
——从站控制器的处理时间(开/关时间，等)；
——网络设置，例如重试次数；
——中继器延时(如果适用的话)；
——非同步/同步通信；

——设备的响应时间。

为确保选择能够满足 SRS 要求的最大响应时间的安全相关通信系统，最大响应时间应在安装前按照安全相关通信系统的说明书进行计算。

系统(包括网络或节点)的任何修改都要重新对系统响应时间的影响做评估。

6.2.3 传输距离，传输速度和节点个数

传输距离和传输速度应按照供应商提供的系统使用的线缆的型号和长度的说明进行设置。依据系统节点数检查特定安全相关通信系统最大响应时间的变化。需要考虑满足安全相关控制功能的节点数的前提下，设计合适的响应时间。

在提供多种传输速度的安全相关通信系统中，最大传输距离取决于设定的传输速度。要注意的是高传输速度对应较短的传输距离。

6.2.4 环境条件

安全相关通信系统的选择应考虑环境条件影响，如，环境温度，振动，冲击和电磁干扰。为了避免发生故障(如输出信号的衰退)，对布线的抗干扰的一般原则为：分离通信电缆和电力电缆(见 IEC 60204-1)。

对于环境需求，要考虑制造商提供的要求。

注 1：见 IEC 60204-1，IEC 62061 和 IEC 61131-2。

注 2：由于安全总线系统相关性能表现的多样性，设计者在设计中宜参考制造手册和环境条件以确保足够的安全性能等级。

6.2.5 设置和配置工具

应对相关通信系统的安全管理设置进行检查，如多级密码。这些安全设置的管理应该有明确的要求。

安全设置应按照制造商提供的安全相关通信系统的使用方法操作。

7 系统的安装与设置(配置)

7.1 系统的安装

7.1.1 系统的配置

首先，系统的安装中要确保子系统以及子系统单元适用于安全相关通信系统。

注：见 IEC 62061 的 6.12。

7.1.2 安全相关通信系统的布线

7.1.2.1 通信线缆规范

选择线缆时应遵循以下几点：

——只有制造商建议的或者设计使用规定的线缆可以被使用；

——如果通信系统中包含安全相关和非安全相关的设备，则选用安全相关设备要求使用的电缆；

——使用的电缆类型应兼容该传输速度。安全相关通信系统需根据传输速度的不同要求使用不同类型的电缆；

——使用的电缆类型应兼容该传输距离。安全相关通信系统需根据最大传输距离或者节点间距离的不同要求使用不同类型的电缆；

——应检查不同电缆对应的不同传输数据错误率。

7.1.2.2 布线

布线时应遵循以下各点：

——电缆长度应该有足够的余量，以避免连接端子或/和连接器间的电缆无法承受拉力；

——检查布线屏蔽是否连接。在很多情况下，为降低外部干扰应采用屏蔽端接，处理过程需遵循指导手册；

——布线不允许超过线缆制造商所允许的弧度。尤其是光纤应特别注意，因为当电缆超过了允许的弧度就有可能导致通信失效；

——光纤的端头应按照线缆制造商的指导手册使用专用的工具进行；

——如果需要同时安装通信线缆，电力线缆以及交流 I/O 电缆，应使用独立的布线线路。各布线之间的距离应遵循安全相关通信系统供应商的要求。这些处理是必要的降低外部干扰的手段；

——每个设备应检查它对分支和多头电缆接线的兼容性；

——如果安全相关通信系统需要端接处理，那么端接处理应遵循供应商指导手册的要求。

7.1.2.3 布线距离

以下各项应予以验证：

——节点之间的电缆长度和/或电缆的总长度要符合安全相关通信系统提供商提供的规范；

——任何两节点间的电缆应小于规定所允许的最大连接长度。应该在布线工作完成以后对电缆长度进行检查；

——电缆长度应该按照相应型号线缆的使用规范进行检查。

7.1.3 电源的选择

供电单元应由安全相关通信系统供应商指定。在为安全相关通信系统选择供电单元时应考虑到电压抖动的影响：

——应检查 I/O 电源是否需要跟安全相关通信系统分开；

——在适用的情况下应遵循 SELV 或 SELV 的电源选择要求，包括永久或暂时连接到诊断和监测设备上的电源。

7.1.4 环境条件

确保安装的环境条件符合规范值。如果有任何超过规范的情况，应在系统运行之前采取相应的应对措施。

下列各项需要检查：

——如果温度或湿度超过了规范的限定值，应增加加热器或风扇等设备确保它们在规定值的范围内；

——如果振动和冲击超过了网络部件的限定值，使用减震器等将它们降低至限定值范围内；

——如果设备安装在有灰尘的环境中，封闭式的控制面板外壳等保护措施应被采用；

注：如果加热器，风扇，减震器，防尘机箱等在实现安全完整性等级设计过程中是必须的，那么它应该被考虑成为符合要求的 SRCF 的一部分。

——如果适用，应采取电磁干扰防护措施，并通过检查确认电磁环境符合安全相关通信系统的限制要求。

7.2 设置

7.2.1 系统设置

配置数据的设置和修改必须由负责系统的并具有足够培训和经验的人员操作。

系统配置可使用硬件和/或软件进行。需遵循安全相关通信系统制造商的操作手册操作。在安全相关通信系统中,大部分的设置都是使用特定工具进行的。应特别注意配置数据的管理工作。为了防止非授权人员对系统设置进行修改,系统配置的修改要通过密码进行保护。

责任人员应至少控制以下几项:

——密码;

——最新的配置数据。

使用特定的工具时,使用的数据(准备参数集)与安全相关的参数信息,如,识别参数设置的操作信息,设置时间以及其他相关信息应被记录。

7.2.2 操作设置

在供电之前,应确保以下各项已经为安全相关通信进行了设置。

——操作模式:

通过参考制造商的指导规范对模式进行修改。

——传输速度。

——节点数量。

有两种设置方法:使用安全相关通信系统的内置开关,使用特定的设置工具。每种方法都要在遵循制造商提供的指导规范的前提下使用。

7.2.3 配置数据的设置与修改

——有两种系统配置设置方法:硬件设置和软件设置。操作前,需事先查阅制造商提供的操作指导规范手册并确保对功能模块的配置方法充分理解。

——存储在机器中的设置数据应对照制造商提供的操作指导规范手册对比验证。

——配置改变以后应进行功能测试。

这些是安全系统管理员的职责。

确保系统修改期间的设置改变一定不会引起危险。

8 验证

8.1 供电前的必要检查

以下各项为供电前需要进行的检查:

——应该使用适当的检测设备,检查安全相关通信系统的布线,例如,极性错误,短路以及由于使用测试设备引发的接地故障;

——检查所有设备的接地线是否良好;

——在给安全相关通信系统供电前应检查负载(机器驱动器)跟电源是独立的。

注:见 IEC 62061 的第 9 章。

8.2 供电后的验证

以下是供电后应该检查的基本项:

——如果可能,应该监测安全相关通信系统的信号波形,以验证信号的干扰足够低;

——检查所有供电电压是否在允许的范围内;

——当通信系统的电源与控制系统的电源是独立的,上面提到的检查应该在两套电源上均分别进行;

——参照指导手册检查各项指标以验证每个系统部件都可以供电启动。在该阶段,由于参数已经完成设置,不需要其他额外的检查工作。

注:见 IEC 62061 的第 9 章。

8.3 功能测试

在系统调试阶段,任何时候进行修改,都要对每个安全功能进行测试以验证它符合安全要求规范的要求。

通信系统的行为应该在以下情况下按照安全要求规范进行检查:

——供电中断和恢复;

——布线中断;

——输入/输出故障;

——从站的替换;

——响应时间。

注:见 IEC 62061 的第 9 章。

8.4 基线

验证过程中,设置参数、测试结果、版本信息以及其他相关信息都应该以基线的形式记录。当安全相关通信系统修改时基线也应该进行升级。

注:见 IEC 62061 的第 9 章。

9 文档

文档应该:

——准确,简明;

——使用人员容易理解;

——适用于文档的应用目的;

——可得到,可维护。

作为 SRECS 子系统的安全相关通信系统验证使用的文档应包括:

a) 安全要求规范;

b) 系统规范(包括:系统配置,应用标准等);

c) 系统管理计划;

d) 硬件规范;

e) 软件规范;

f) 布线图;

g) 硬件故障率和导致危险的硬件故障率估计;

h) 测试计划和测试报告;

i) 安装和操作指南;

j) 基线。

如果安全相关设备、功能模块或软件工具在安全相关通信系统的使用符合 IEC 61508 的认证,那么

文档应包括认证信息。这点同样适用于系统的应用软件。配置工具的相关信息也应包含在文档中。

10 操作、维护和维修

10.1 责任人的任命

必须明确责任人负责的安全相关通信系统的维护工作。责任人需要负责安全相关通信系统的操作、维护和维修。

10.2 维护计划的制定

安全相关通信系统的维护需要按照维护计划进行。维护计划应包含需要远程进行的安全相关通信系统功能维护操作(如:定期检查和测试)。维护程序需要被记录。

用于维护工作或故障分析的测试程序应提前得到验证。

应注意系统修改计划和维护计划应该是独立的,因为它们的目标完全不同。

10.3 实施定期维护

只要安全相关通信系统工作,周期性维护工作就应该执行。系统应该定期维护,以确保在系统工作期间内保持安全要求规范规定的安全完整性级别。本章给出需要维护的一般项目。周期性维护工作应该在不大于安全要求规范、维护计划或制造商提供的操作手册所给定的验证测试间隔时间内进行。

10.4 维护工作的主要项目

安全要求规范或制造商提供的指导规范中的所有验证测试项目都应可执行。在不替换设备的情况下将安全相关通信系统重置以实现“设备更新”是不可能实现的,设计验证测试的间隔要特别注意考虑安全相关通信系统中使用的设备的设计寿命大于 20 年。

在 PFHD 高度独立于验证测试的地方(如:测试没有被诊断系统发现的故障),验证测试间隔应在安全相关通信系统预期使用范围内表现为现实可行的。

例如,一个小于 10 年的验证测试间隔对于很多机械应用都是不合理的,一般 20 年的验证测试间隔比较合理。必须承认一些子系统或者子系统单元(如具有高占空比的机电元件)在验证测试间隔内需要替换。

10.5 维护结果的记录

维护程序的结果需要被记录和保存。记录和保存应定义在维护计划中,任何基线的改动都应该被记录。

11 教育和培训

11.1 概要

应该对责任人员进行教育和培训,以确保胜任安全相关通信系统的安全操作的维护工作。需要进行的培训项目在下面的子章节给出。

11.2 范围

任何涉及安全相关通信系统操作的人员都应该加强安全教育和培训,如:操作人员,维护人员,程序安装人员,以及他们的领导和管理员。

11.3 继续教育和培训

应对所有涉及安全相关通信系统操作的人员进行周期性教育和培训。

适当的教育和培训应该被提供：

——当一个人被任命时；

——当一个安全相关通信系统被修改，和

——在由于事故导致系统要进行重启之前。

11.4 教育和培训的内容

以下项目应包含在教育和培训课程中：

——与安全工作人员相关的规范和标准；

——保护措施的原则；

——安全相关设备及其功能；

——每个设备的操作流程；

——安全工作流程(正常操作的)；

——紧急情况下的操作流程。

11.5 教育活动的规划和教育记录的存储

教育工作应该按照教育计划进行，同时记录应该在定义阶段被保存。

附 录 A
（资料性附录）
使用安全相关通信系统的 SRECS 的设计
功能块的概念

A.1 概要

安全相关通信系统只是一个具有 SRECS 的子系统。依据标准 IEC 61508 和 IEC 62061，SRECS 通常包含图 A.1 中给出的部件。为替代常规布线使用了安全相关通信系统。SILCL 通常在安全相关通信系统供应商提供的文档中指明。

图 A.1 SRECS 的组件

安全相关通信系统只是执行安全相关电气控制系统特定的部分安全功能。因此，还需要配合安装传感器（如，防护门开关），执行器（如，接触器）以及必要的应用软件等。

安全相关通信系统的主要安全功能是在特定时间内特定完整性要求下，将安全相关数据从输入端传输到输出端或执行相反过程。在这个实例中，安全相关通信系统中引入了简化的逻辑处理器示例。这个设备可以是带有 SRECS 的单独设备或者安全输入输出设备的一部分。这取决于安全相关通信系统的架构。

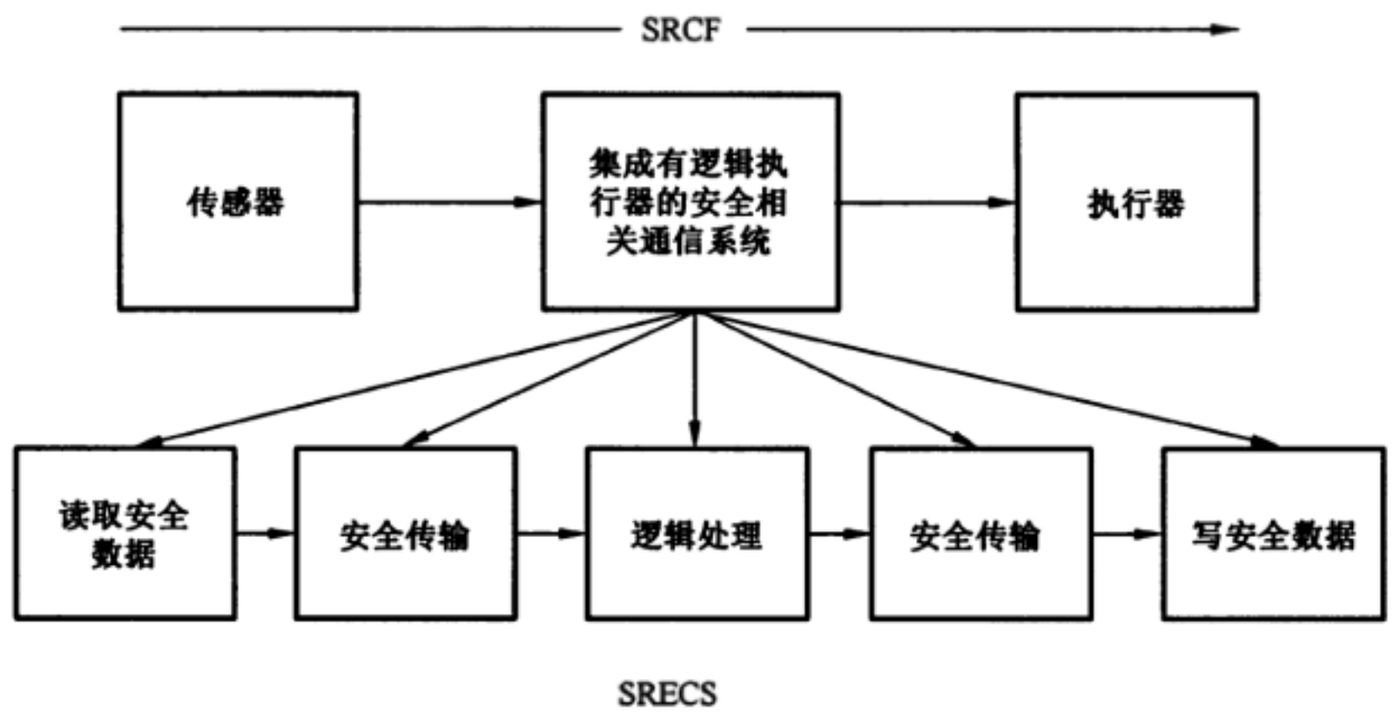


图 A.2 使用安全相关通信系统的 SRECS

注：功能模块的实现通常需要详细的安全要求规范。同样，安全要求规范对子系统的功能模块的执行是必要的。这些规范由安全相关通信系统提供商编写但是不包括这些指导范围。通常安全相关通信系统提供商会定义能够通过修正安全相关通信系统和所使用设备的配置参数而达到最大 SILCL。

安全传输功能模块确保安全相关数据从源节点到下游节点(如从发送器到接收器)的安全传输:它可以分为两个附加功能模块:

——主安全传输功能模块;

——从安全传输功能模块。

注:根据 IEC 62061,一个功能模块只由单独的子系统(如,设备)执行。每个功能模块会在安全功能架构范围内分配给一个子系统。许多功能模块可能分配给同一个子系统。每一个功能模块只能由一个单独的子系统执行。

通信系统通常使用主从设备。在一些系统中,这些设备被称为服务器端和客户端。同样,多主站通信系统通常有一个安全相关消息发送单元和一个或多个安全相关消息接收单元。在本指南中假设使用单主设备(服务器端)和多从设备(客户端)。

在此前提下,安全相关通信系统建立在以下两个子系统(设备)之上:

——安全相关从设备(如,输入,输出,输入和输出);

——安全相关主设备(如,安全相关控制器)。

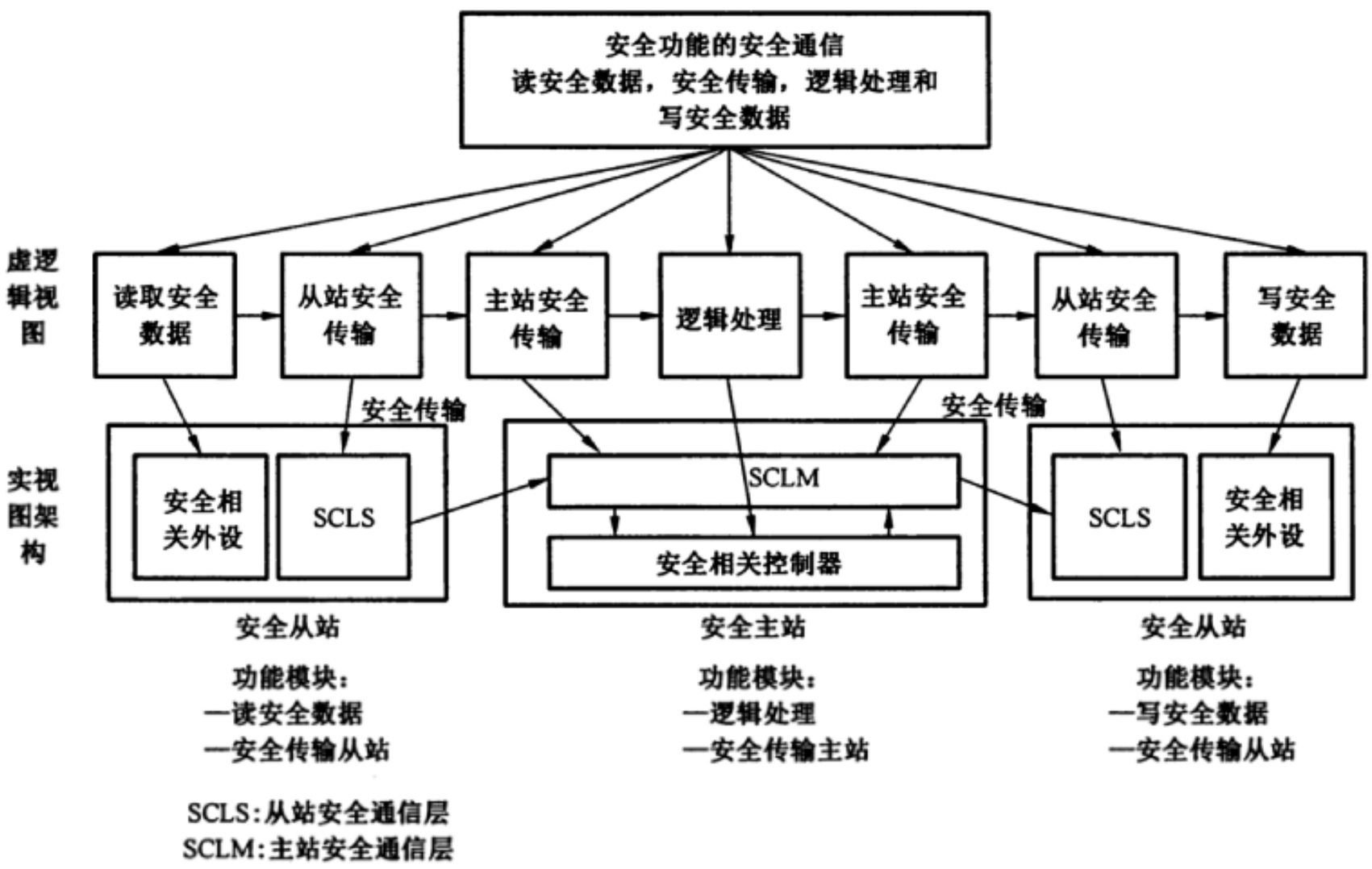


图 A.3 安全相关通信系统的不同意见

每个子系统(设备)执行一个或多个功能模块。如图 A.3 所示,子系统安全相关外部设备和 SCLS 都在一个安全相关从设备上执行。两个子系统可以是单独的设备(例如执行 SCLS 服务的芯片组和安全输入设备)。

A.2 安全相关通信系统的架构

在安全相关通信系统中,传感器和执行器被安置到相应的输入输出设备中。这些设备可能本地或者远程的连接到逻辑处理单元。典型的安全相关通信系统包含以下实例。

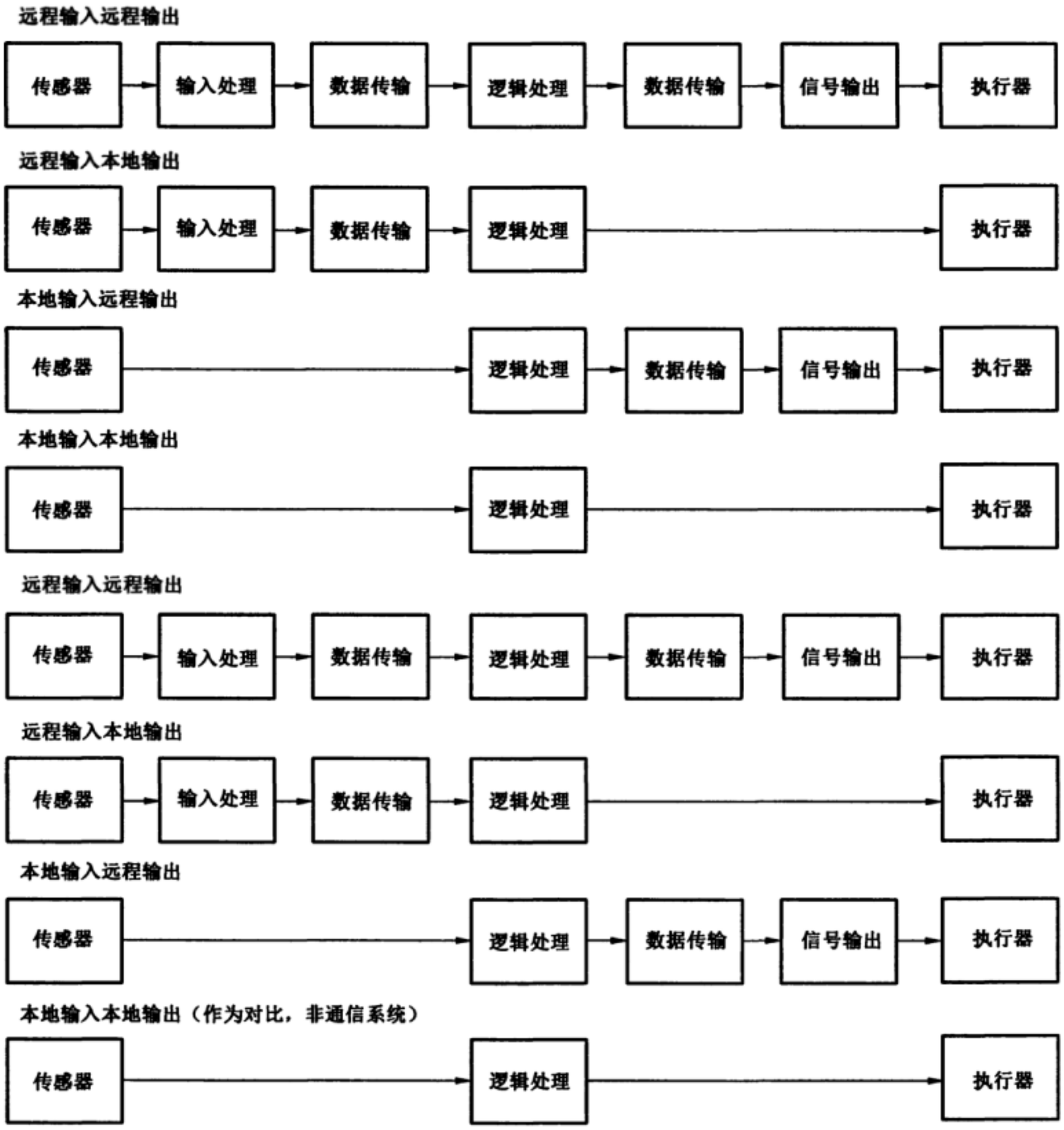


图 A.4　典型安全相关通信系统的架构实例

A.3　SRECS 中 PFHD 的计算

SRECS 中 PFHD 计算时需要考虑的到数值，通常由安全相关通信系统提供商为每个安全相关设备提供。在大多数情况下，SRECS 中 PFHD 为安全链(传感器—安全相关通信系统—逻辑处理器—执行器)中每个设备的 PFHD 之和。

传感器部分的 PFHD 取决于设备的架构和参数(单/多传感器，有/没有测试脉冲，……)。这需要在安全相关设备或通信系统提供商提供的使用手册中说明。

传感器和执行器与安全相关通信系统的连接是影响实现 SRCF 规定安全完整性等级的重要因素。一定要着重考虑提供商提供的使用手册中的信息。

参 考 文 献

[1] GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小

[2] GB/T 15969.2—2008 可编程序控制器 第2部分:设备要求和测试

[3] GB/T 16855.1—2008 机械安全 控制系统有关安全部件 第1部分:设计通则

[4] GB/T 17045—2008 电击防护 装置和设备的通用部分(IEC 61140:2001, IDT)

[5] GB/T 24339.1—2009 轨道交通 通信、信号和处理系统 第1部分:封闭式传输系统中的安全相关通信

[6] GB/T 25105.3—2014 工业通信网络 现场总线规范 类型10:PROFINET IO规范 第3部分:PROFINET IO通信行规

[7] GB/T 26336—2010 工业通信网络 工业环境中的通信网络安装

中 华 人 民 共 和 国
国 家 标 准
机械电气安全 安全相关设备中的
通信系统使用指南
GB/T 34934—2017/IEC/TS 62513:2008
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 38 千字
2017年11月第一版 2017年11月第一次印刷
*
书号:155066·1-57887 定价 24.00 元

GB/T 34934-2017