ICS 91.140.90
CCS Q 78

中　国　电　梯　协　会　标　准

T/CEA 0060—2025

电梯和自动扶梯、自动人行道功能安全现场总线技术基本要求

Basic requirements of functional safety fieldbuses technology for elevators, escalators and moving walks

2025-08-28 发布　　2026-03-01 实施

中国电梯协会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件所要求达到的性能指标，应由采用本标准的制造企业在设计制造过程中自行进行验证测试（型式检验），并对销售的产品作产品符合性声明。

本文件由中国电梯协会提出并归口。

本标准负责起草单位：苏州汇川技术有限公司

本标准参加起草单位：日立电梯（中国）有限公司、上海吉盛网络技术有限公司、上海新时达电气股份有限公司、上海三菱电梯有限公司、广东菱电电梯有限公司、机械工业仪器仪表综合技术经济研究所、巨人通力电梯有限公司、上海交通大学电梯检测中心、奥的斯机电电梯有限公司、康力电梯股份有限公司、苏州帝奥电梯有限公司、建研机械建研检测（北京）有限公司（国家电梯质量检验检测中心）、通力电梯有限公司、江南嘉捷电梯有限公司、恒达富士电梯有限公司、日立楼宇技术（广州）有限公司、东芝电梯（中国）有限公司、辛格林电梯有限公司、广州广日电梯工业有限公司、浙江省特种设备科学研究院、迅达（中国）电梯有限公司、沈阳蓝光新一代技术有限公司、普拉内特（上海）传动技术有限公司、深圳海浦蒙特科技有限公司、杭州西子电梯科技有限公司、杭州新马电梯有限公司、华升富士达电梯有限公司、巨龙电梯有限公司、温州市特种设备检测科学研究院、奥的斯科技发展(上海)有限公司、日立电梯(广州)自动扶梯有限公司。

本标准主要起草人：王蕊、刘宇、赖志鹏、周耀华、李楚平、莫泽坤、温有文、熊文泽、杨香香、冯宏景、仲海忠、陈羽波、唐林钟、李新龙、李志钢、凌晨昱、严红星、陈晓东、冷涛、张建雨、黄棣华、李科、张亚刚、法乃光、祁兴、钟玉涛、卢曦、周晟、张蕾、朱中华、方学宠、潘国平、李淼、徐伟华、孙兴中、陈涛、陈雄伟、黄志恒、郑伟、陈向俊、王力虎。

引　言

安全总线是在可编程电子系统（PES）中用于传递安全功能相关数据的现场总线，本文件所述的设计方法均需要采用 PES 实现，其中 PES 的设计要求，需要满足功能安全相关的标准，例如 GB/T 35850.1、GB/T 35850.2 等，同时电梯和自动扶梯、自动人行道相关的功能应符合相关标准和安全技术规范，例如 GB/T 7588.1、GB/T 7588.2、GB 16899、TSG T7007 等，本文件规定的是安全总线的设计要求和检验、验证要求。

根据 GB/T 20438 系列标准所实现的安全通信层作为安全相关系统的组成部分，为安全相关系统中现场总线上两个或多个参与方之间传输报文（信息）提供必要的可信度，或在现场总线发生错误或失效情况下为安全行为提供足够可信度。

本文件规定的安全通信层，使现场总线可用于要求功能安全达到安全完整性等级（SIL）的应用，该 SIL 等级由其相应的功能安全通信行规来规定。

本文件基于 IEC 61784-3:2021，结合电梯、自动扶梯和自动人行道使用场景，定义了电梯、自动扶梯和自动人行道使用该项技术的具体要求。主要差异点如下：

- 修改残余错误率λ_{SCL}与 SIL 的典型关系，要求计算λ_{SCL}，而不是λ_{SC}；
- 提供了残余错误概率RP_I计算的建议公式；
- 明确了当每个逻辑连接的λ_{SC}不相等时λ_{SCL}的计算；
- 定义了安全总线故障对电梯、自动扶梯和自动人行道系统的影响评估。

电梯和自动扶梯、自动人行道功能安全现场总线技术基本要求

1 范围

本文件适用于使用了安全总线技术的乘客电梯、载货电梯以及自动扶梯和自动人行道（以下简称“电梯”）的可编程电子安全系统，其他类型电梯的可编程电子安全系统可参照本文件要求进行设计。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 7588.1 电梯制造与安装安全规范 第 1 部分：乘客电梯和载货电梯

GB 16899 自动扶梯和自动人行道制造与安装安全规范

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

GB/T 24808 电磁兼容 电梯、自动扶梯和自动人行道的产品系列标准 抗扰度

GB/T 34040 工业通信网络 功能安全现场总线行规 通用规则和行规定义

GB/T 35850（所有部分） 电梯、自动扶梯和自动人行道安全相关的可编程电子系统的应用

IEC 61784-3:2021 工业通信网络-行规-第3部分：功能安全现场总线-通用规则和行规定义（Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions）

3 术语和定义

3.1 术语和定义

GB/T 7588.1、GB 16899 GB/T 20438.4、GB/T 34040界定的以及下列术语和定义适用于本文件。

3.1.1

功能安全通信行规 functional safety communication profile

FSCP

实现安全通信层的技术规格书。

3.1.2

现场总线 fieldbus

基于串行数据传输并应用在工业自动化或过程控制中的通信系统。

3.1.3

现场总线系统 fieldbus system

使用现场总线连接设备的系统。

3.1.4

功能安全现场总线 functional safety fieldbuses

本文件重点关注基于现场总线的功能安全通信系统的使用。图 1 给出了一个功能安全现场总线示例。

当使用基于 IEC 61158 的现场总线结构而不改变每个通信层定义时，按照 GB/T 20438 要求实现安全数据传输的所有必要措施，都应由一个附加的“安全通信层（SCL）”执行。安全通信层位置见图 1。

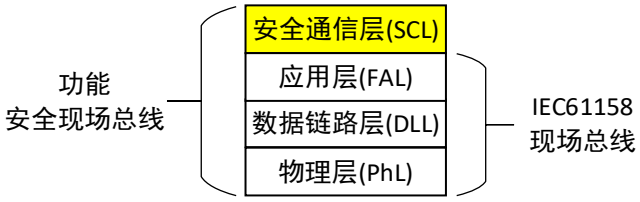


图 1 功能安全现场总线

3.1.5

时间戳 time stamp

包含在报文中的时间信息。

3.1.6

绝对时间戳 absolute time stamp

参照一个全局时间的时间戳。该全局时间对于使用现场总线的一组设备是共用的。

[来源：IEC 62280:2014，3.1.1，有修改]

3.1.7

相对时间戳 relative time stamp

参照一个实体本地时间的时间戳。

注：通常，与其他实体的时钟无关系。

[来源：IEC 62280:2014，3.1.43]

3.1.8

有源网络元件 active network element

包含允许网络扩展的电有源和/或光有源组件的网络元件。

示例：中继器和交换机。

[来源：IEC 61918:2013，3.1.2]

3.1.9

可用性 availability

自动系统在给定时间内未出现任何令人不满意的系统工况(如停产)的概率。

3.1.10

比特错误概率 bit error probability

P_e

一个给定比特接收不正确值的概率。

3.1.11

黑色通道 black channel

包含一个或多个元件的确定的通信系统，这些元件无需证据证明其依据 GB/T 20438 进行设计或验证。

注：本定义将通道的通常含义扩展为包括了含有通道的系统。

3.1.12

白色通道 white channel

确定的通信系统，其中所有相关硬件和软件元件都依据 GB/T 20438 进行设计、实现和验证。

注：该定义将通道的通常含义扩展为包括了含有通道的系统。

3.1.13

网桥 bridge

在数据链路层连接多个网段的抽象设备。

3.1.14

通信通道 communication channel

一个通信系统内两个终端之间的逻辑连接。

3.1.15

通信系统 communication system

由硬件、软件和传输介质组成，以允许将报文(GB/T 9387.1 应用层)从一个应用传输到另一个应用。

3.1.16

连接 connection

在同一或不同设备内的两个应用对象间的逻辑绑定。

3.1.17

循环冗余校验 cyclic Redundancy Check

CRC

<值>从一个数据块导出的并与数据块一起存储或传送的冗余数据，用以检测数据讹误。

<方法>用于计算该冗余数据的过程。

注1:本文件还使用术语“CRC 代码”“CRC 签名”，以及符号(如 CRC1 和CRC2)来意指冗余数据。

注2：见参考文献[3]和[4]。

3.1.18

错误 error

计算、观测或测量的值或条件与真实、规定或理论上正确的值或条件间的差异。

[来源：IEC 61508-4:2010，3.6.11]

注1:错误可能是由于硬件/软件设计失误，和/或由于电磁干扰和/或其他影响导致信息被破坏而引起的。

注2:错误并非一定导致失效或故障。

3.1.19

显式代码 explicit code

在 SPDU 中实际传输的用于安全措施的代码，该代码对于发送方和接收方已知。

3.1.20

隐式代码 implicit code

用于安全措施的代码，不在 SPDU 内传输但是发送方和接受方均已知。

3.1.21

失效 failure

功能单元执行一个要求功能的能力的终止，或功能单元在任何非要求方式下的运行。

[来源：IEC 61508-4:2010，3.6.4，有修改]

注：失效可能是由一个错误(例如：硬件/软件设计问题或报文被破坏)引起的。

3.1.22

故障 fault

可引起功能单元执行要求功能的能力降低或失去其能力的异常状况。

注：IEC 60050-191:1991，191-05-01定义“故障”是一种以无能力执行要求功能为特征的状态，不包括预防性维护或其他按计划行动期间的无能力或由于外部资源缺少而导致的无能力。

[来源：IEC 61508-4:2010，3.6.1，有修改]

3.1.23

哈希函数 hash function

一个(数学)函数，将一大组(可能非常大)的数值映射为(通常)一个较小组的数值。

注1:哈希函数用于检测数据讹误。

注2:通用哈希函数包括奇偶校验位、校验和或CRC。

[来源：IEC/TR 62210:2003，4.1.12，有修改]。

3.1.24

危险 hazard

系统的一种状态或一组条件。它与其他相关条件一起，将不可避免地对人身、财产或环境造成伤害。

3.1.25

报文 message

用于传送信息的有序八位位组序列。

[来源：ISO/IEC 2382-16:1996，16.02.01，有修改]

3.1.26

报文汇点 message sink

通信系统的一部分，被认为在此接收报文。

[来源：ISO/IEC 2382-16:1996，16.02.03]

3.1.27

报文源点 message source

通信系统的一部分，被认为在此产生报文。

[来源：ISO/IEC 2382-16:1996，16.02.02]

3.1.28

假脱扣 spurious trip

无过程要求而由安全系统引起的脱扣。

3.1.29

误脱扣 nuisance trip

无有害影响的假脱扣。

注：在通信系统(如无线传输)内可能出现内部非正常错误。例如：由干扰导致过多次重试而引起的内部非正常错误。

3.1.30

性能等级 performance level

PL

离散等级，用于规定控制系统安全相关部分在可预见条件下执行安全功能的能力。

[来源：ISO 13849-1:2006，3.1.23]

3.1.31

冗余 redundancy

存在一个以上的方法来执行要求的功能或表达信息。

[来源：IEC 61508-4:2010，3.4.6，有修改]

3.1.32

可靠性 reliability

在给定条件下，对于给定时间间隔(t_1，t_2)，自动系统能够执行要求功能的概率。

注1:一般假设自动化系统在时间间隔开始时处于执行该要求功能的状态。

注2:术语“可靠性”也用于表示由该概率来量化的可靠性性能。

注3:在 MTBF 或 MTTF 时间段内，自动系统在给定条件下执行要求功能的概率是下降的。

注4:可靠性与可用性不同。

[来源：IEC TR 62059-11:2002，3.17，有修改]

3.1.33

残余错误概率 residual error probability

RP

一个错误未被 SCL 安全措施检测出的概率。

3.1.34

残余错误率 residual error rate

SCL 安全措施未成功检测出若干错误的统计率。

3.1.35

风险 risk

出现伤害的概率与该伤害严重性的组合。

注：更多讨论参见IEC 61508-5:2010的附录A。

[来源：IEC 61508-4:2010，3.1.6；ISO/IEC导则 51:2014，3.9，有修改]

3.1.36

安全通信层 safety communication layer

SCL

在现场总线应用层(FAL)之上的通信层，包括根据GB/T 20438 要求确保数据安全传输的所有要的附加措施。

3.1.37

安全连接 safety connection

使用安全协议进行通信事务处理的连接。

3.1.38

安全数据 safety data

使用安全协议在安全网络上传输的数据。

注：安全通信层不能保证数据本身的安全性，只能保证数据被安全传输。

3.1.39

安全设备 safety device

依据GB/T 20438 设计并实现功能安全通信行规的设备。

3.1.40

安全功能 safety function

由E/E/PE 安全相关系统或其他风险降低措施所实现的功能，其目的在于当发生特定危险事件时，达到或保持 EUC 的安全状态。

[来源：IEC 61508-4:2010，定义 3.5.1，有修改]

3.1.41

安全完整性等级 safety integrity level

SIL

与安全完整性值的范围相对应的离散等级(4 种可能等级中的 1 种)。其中，安全完整性等级 4 为安全完整性最高等级，安全完整性等级 1 为最低等级。

注1:在IEC61508-1:2010的表2和表3中规定了4种安全完整性等级的目标失效措施(见IEC61508-4:2010中3.5.17)。

注2:安全完整性等级用于规定分配给E/E/PE安全相关系统的安全功能的安全完整性要求。

注3:SIL不是系统、子系统、元件或组件的属性。“SILn安全相关系统”(n为1、2、3或4)的正确解释是系统具有支持安全完整性等级达到n的安全功能的潜在能力。

[来源：IEC 61508-4:2010，定义 3.5.8]

3.1.42

安全措施 safety measure

用于控制可能的通信错误的措施，该措施的设计和实现符合 GB/T 20438 要求。

注1:在实践中，组合若干安全措施以达到所要求的安全完整性等级。

注2:通信错误和相关安全措施在5.3和5.4中详细介绍。

3.1.43

安全 PDU safety PDU

SPDU

通过安全通信通道传输的 PDU。

注1:SPDU可能包含一个以上使用不同编码结构和哈希函数的安全数据的副本，以及附加的保护部分，如密钥、序 列计数或时间戳机制。

注2:冗余SCL可能提供2种不同的 SPDU 版本以插入现场总线帧的各个字段。

3.1.44

安全相关应用 safety-related application

为满足应用的 SIL 要求，根据 GB/T 20438 设计的程序。

3.1.45

安全相关系统 safety-related system

根据 GB/T 20438 执行安全功能的系统。

3.2 符号和缩略语

下列符号和缩略语适用于本文件。

BSC: 二进制对称通道(Binary Symmetric Channel)

CP: 通信行规(Communication Profile)[IEC 61784-1]

CPF: 通信行规族(Communication Profile Family)[IEC 61784-1]

CRC: 循环冗余校验(Cyclic Redundancy Check)

DLL: 数据链路层(Data Link Layer)[GB/T 9387.1]

EMC: 电磁兼容性(Electromagnetic Compatibility)

EMI: 电磁干扰(Electromagnetic Interference)

EUC: 受控设备(Equipment Under Control)[IEC 61508-4:2010]

E/E/PE: 电气/电子/可编程电子(Electrical/Electronic/Programmable Electronic)[IEC 61508-4:2010]

FAL: 现场总线应用层(Fieldbus Application Layer)[IEC 61158-5]

FIT: 失效时间(等于每小时 10^{-9} 次失效)(Failure In Time(equals 10^{-8} failure per hour))

FS: 功能安全(Functional Safety)

FSCP: 功能安全通信行规(Functional Safety Communication Profile)

IACS: 工业自动化和控制系统(Industrial Automation and Control System)

MTBF: 平均失效间隔时间(Mean Time Between Failures)

MTTF: 平均失效时间(Mean Time To Failure)

NSR: 非安全相关(Non Safety Related)

PDU: 协议数据单元(Protocol Data Unit)[GB/T 9387.1]

P_e: 比特错误概率(Bit error probability)

PES: 可编程电子系统(Programmable Electronic System)[1EC 61508-4:2010]

PFD: 要求时平均危险失效概率(Average Probability of dangerous Failure on Demand) [IEC 61508-4:2010]

PFH: 每小时平均危险失效频率(Average frequency of dangerous failure [h^{-1}]per hour) [IEC 61508-4:2010]

PhL: 物理层(Physical Layer)[ISO 13849-1]

PL: 性能等级(Performance Level)

PLC: 可编程逻辑控制器(Programmable Logic Controller)

RP: 残余错误概率(Residual Error Probability)

SCL:安全通信层(Safety Communication Layer)

SIL: 安全完整性等级(Safety Integrity Level)[IEC 61508-4:2010]

SIS: 安全仪表系统(Safety Instrumented Systems)

SL: 信息安全等级(Security Level)[IEC 62443]

SMS: 信息安全管理系统(Security Management System)

SPDU: 安全 PDU(Safety PDU)

SR: 安全相关(Safety Related)

4 基本要求

4.1 基本概念

4.1.1 安全功能分解

根据 GB/T 20438，风险分析要定义安全功能。这些安全功能可以分解到对整个安全功能有影响的部件(例如：传感器-安全通信通道-PES-安全通信通道-执行器)。

本文件中的通信系统本身执行安全数据的传输。为简化系统计算，推荐安全功能的安全通信通道的一个逻辑连接占用目标 SIL 的最大 PFH 比例不超过 1%，为此，设计功能安全通信行规(见图 2)。

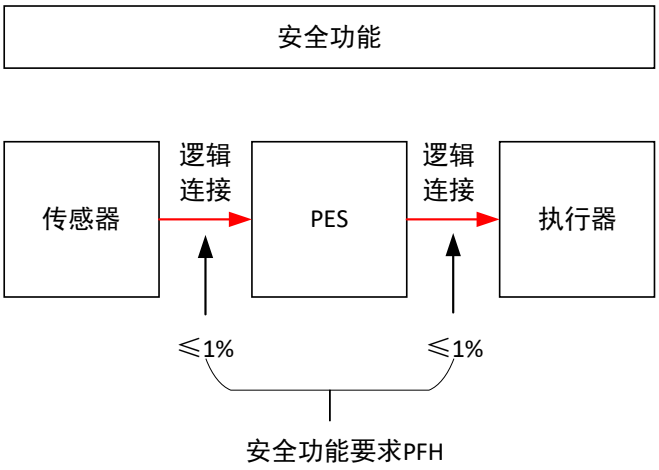


图 2 安全通信作为安全功能的一部分

4.1.2 通信通道类型

本文件使用被称为“黑色通道”或“白色通道”的概念，来定义用来传输安全数据的基础现场总线的要求。本文件规定使用黑色通道方法的功能安全通信行规。附录 A 给出黑色通道和白色通道的概念。

在本文件中，安全通信通道被定义为从源点的安全通信层顶部开始，在汇点的安全通信层顶部结束(见图 A.1)。黑色通道包括安全通信层之间的所有部分。

4.1.3 安全功能响应时间

安全功能响应时间是指：当安全功能通道中存在错误或失效时，从与现场总线连接的一个安全传感器（例如：电气安全装置）感知后，到安全执行器（例如：制动器）进入相应安全状态之前，最坏情况下经过的时间。

安全功能响应时间的计算在功能安全通信行规中规定。

经验测量只能作为对最坏情况下计算的参考性检查。

对安全功能的要求（执行）是由模拟信号超过一个阈值或者数字信号发生状态变化而引起的。

图 3 给出了一个典型的构成安全功能响应时间的示例。

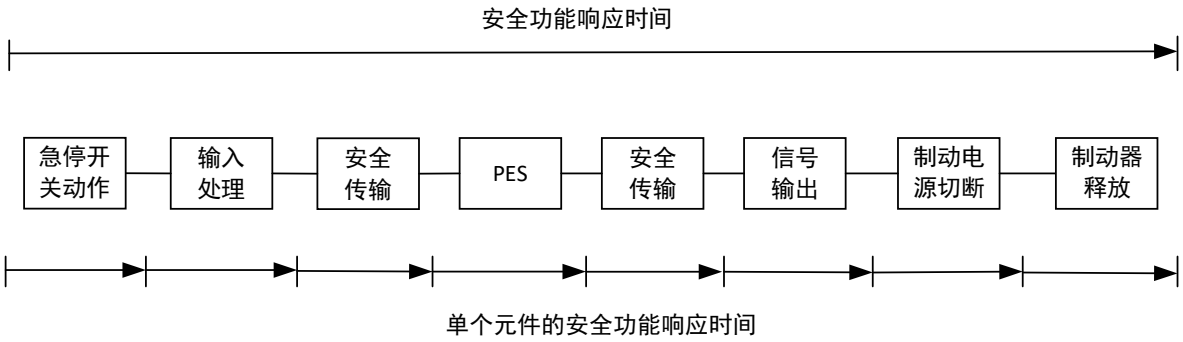


图 3 安全功能响应时间组成部分示例

4.2 总残余错误率与 SIL

依据本文件，功能安全通信系统应提供残余错误率。表 1 给出了残余错误率与 SIL 之间的典型关系，该关系基于假设：在功能安全通信系统中，安全功能的每个逻辑连接的贡献不超过 1%。

高需求模式系统都应具有一个确定的安全功能响应时间，因此，应保证必要的 SPDU 采样率。所有情况下都应提供特定 SIL 的 PFH。

表 1　SCL 的每小时残余错误率λ_{SCL}与 SIL 的典型关系

适用于安全功能的SIL	安全功能危险失效的平均频率	SCL的最大允许每小时残余错误率
	(PFH)	(λ_{SCL}(Pe))
4	$< 10^{-8}$/h	$< 10^{-10}$/h
3	$< 10^{-7}$/h	$< 10^{-9}$/h
2	$< 10^{-6}$/h	$< 10^{-8}$/h
1	$< 10^{-5}$/h	$< 10^{-7}$/h

4.3　通信模型定义

4.3.1　一般信息

以下内容考虑了针对安全现场总线设备的多种实现结构模型。这些模型提供了不同的故障诊断机制。下面所展示的模型仅为了描述可能的实现结构。应在整个系统设计过程中一直使用GB/T 20438。

4.3.2 至 4.3.5 列举了一些示例，也可使用其他的模型。

注：这些示例中的实现结构是基于冗余安全通信层，与GB/T 20438所举示例保持一致。

4.3.2　模型 A(单个报文、通道和现场总线应用层，冗余安全通信层)

图 4 所示的模型 A 作为其他模型的基本参考模型。仅有一个现场总线被用作通信通道。

两个安全通信层独立运行，基于相同的安全数据产生两个安全 PDU。在利用单一现场总线报文传送其中一个安全 PDU 之前，这些安全PDU 进行交叉校验。两个接收安全通信层对接收到的安全PDU 进行独立解码和安全检测，并进行交叉校验。两个安全通信层都产生报文。

注：这可以通过硬件和/或软件多样性来实现。

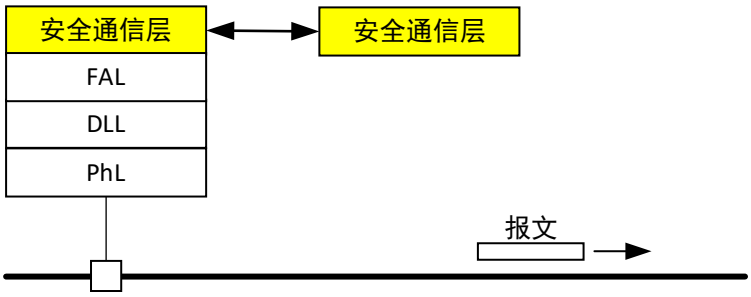


图 4　模型 A

4.3.3　模型 B（全冗余）

图 5 所示的模型 B 表示一个所有的安全通信层、传输层以及传输介质都是双份(冗余)的系统。

每个安全通信层基于相同的安全数据产生一个安全 PDU，并将其发送到相连的现场总线。来自于两个安全通信通道的报文要分别经过安全检测并进行交叉校验。

传输层和传输介质可以是不同的类型。

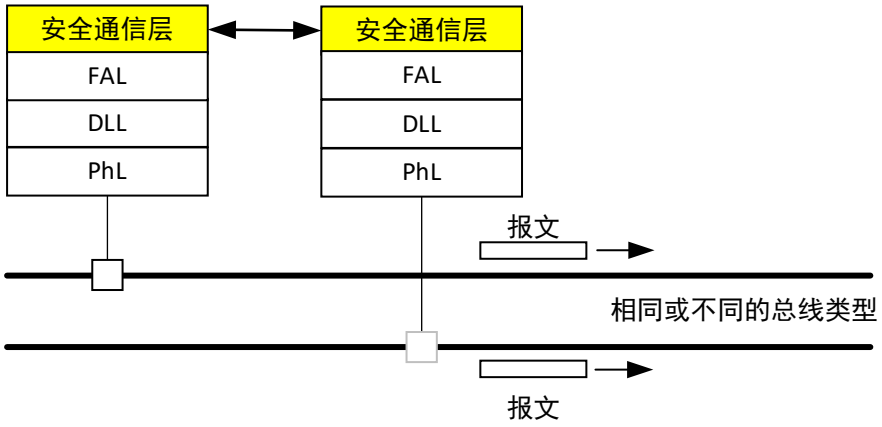


图 5 模型 B

4.3.4 模型 C(冗余报文、现场总线应用层和安全通信层，单通道)

图 6 所示的模型 C 表示一个现场设备组件全冗余而通信介质单一的系统。

两个安全通信层基于相同的安全数据产生 2 个安全 PDU。在不同的时间利用不同的报文将安全 PDU 发送到相同的现场总线上。来自于两个安全通信通道的报文要分别经过安全检测并进行交叉校验。

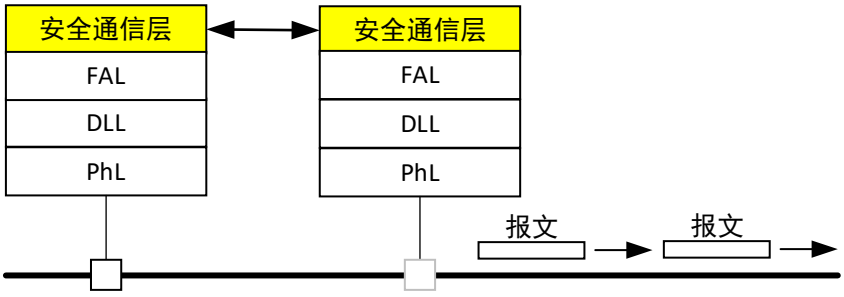


图 6 模型 C

4.3.5 模型 D(冗余报文和安全通信层，单个通道和现场总线应用层)

图 7 所示的模型 D 表示一个双安全通信层而单传输层的系统。

两个安全通信层基于相同的安全数据产生 2 个安全 PDU。在不同的时间利用不同的报文将安全 PDU 发送到相同的现场总线上。或者，可以把两个安全 PDU 放在一个报文内的不同字段进行发送。

来自于两个安全通信层的报文要分别经过安全检测并进行交叉校验。

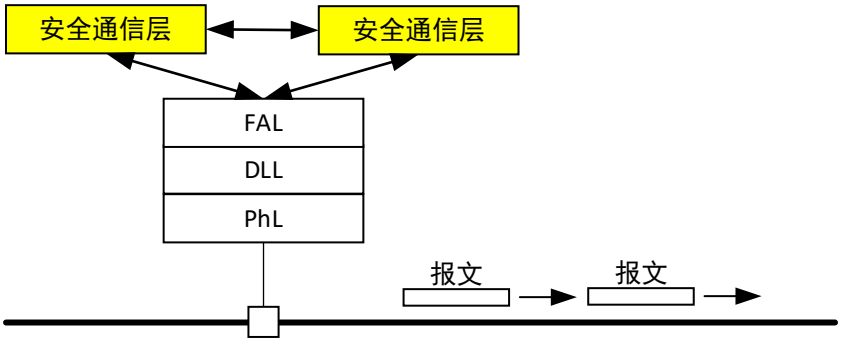


图 7 模型 D

4.4 通信错误

4.4.1 一般信息

第4.4.2至4.4.9节规定了可能的通信错误，还提供了额外的注解来说明黑色通道的典型行为。

4.4.2 讹误

由于总线通信参与方内的错误、传输介质上的错误或报文干扰，可能引起报文被破坏。

注1：传输期间的报文错误对于任何标准的通信系统都是一个正常事件，这样的事件可在接收方利用哈希函数以高概率被检测出，并且有错误的报文被忽略。

注2：大多数通信系统都包含用以从错误报文中恢复的协议，因此，在恢复或重复规程失败或未被应用之前，不能将这些报文归类为“丢失”。

注3：如果恢复或重复规程占用时间比规定的截止期限长，则该报文被归类为“不可接受的延时”。

注4：如果由于多个错误导致一个具有正确报文结构（例如：寻址、长度、哈希函数值如CRC等）的新报文，在这样很低概率的事件中，该报文将被接受并进一步处理。基于报文序列号或时间戳的评估可能导致如意外重复、错序、不可接受的延时、插入等故障分类。

4.4.3 意外重复

由于错误、故障或干扰，使得旧的未更新的报文在不正确的时间点被重复。

注1：当期望的确认/响应没有从目标站收到时，或接收站检测到报文丢失并要求重新发送时，发送方的重复是一个正常的规程。

注2：有些现场总线使用冗余多次发送相同的报文，或通过多个可选路径来提高良好接收的概率。

4.4.4 错序

由于错误、故障或干扰，使得预定的与特定源点报文相关联的序列（例如自然数、时间参考）出现错误。

注1：“错序”也被称为“失序”。

注2：现场总线系统可包含存储报文的单元（例如交换机、网桥、路由器中的FIFO），或使用可改变序列的协议（例如允许高优先级报文优先于低优先级报文）。

注3：当多个序列有效时，如来自不同源点实体的报文或与不同对象类型相关的报告，这些序列被分别监视，并可为每个序列报告错误。

4.4.5 丢失

由于错误、故障或干扰，使得一个报文或者确认未被接收到。

4.4.6 不可接受的延时

报文可能被延时超出其允许的到达时窗，例如：由于传输介质上的错误、拥挤的传输线路、干扰，或由于发送报文的总线通信参与方处于服务被延时或拒绝的模式下（例如交换机、网桥、路由器中的FIFO）。

4.4.7 插入

由于故障或干扰，接收了一个非预期或未知的源点实体相关的报文。

注：这些报文对于预期的报文流而言是额外的，且因其无期望的源点，所以不能被归类为正确的、意外重复或错序。

4.4.8 伪装

由于故障或干扰，来自非安全相关源点的报文被误认为来自有效的安全相关源点实体。因此，非安全相关的报文可能被安全相关的通信参与方接收，并将其作为安全相关报文处理。

注：用于安全相关应用的通信系统可使用其他检查方法来检测伪装，例如：被授权的源点身份和通行口令或密码。

4.4.9 寻址

由于故障或干扰，安全相关报文被传递至错误的安全相关通信参与方，通信参与方将其当作正确报文处理。这包括被称为回环的错误情况，该情况下发送方接收到自己发送的报文。

4.5 确定性的补救措施

4.5.1 一般信息

第 4.5.2 至 4.5.9 节列出了用来检测通信系统的确定性错误和失效的通用措施。确定性是相对于如电磁干扰导致报文被破坏的偶然性错误而言的。

4.5.2 序列号

序列号被集成到报文源点和汇点之间交换的报文中。它可以用一个数字作为附加数据字段来实现，以预定方式在相邻报文间变化。

4.5.3 时间戳

在大多数情况下，报文内容仅在特定时间点有效。时间戳可以是时间或时间与日期，由发送方将其包含在报文中。

注：可使用相对时间戳和绝对时间戳。

“打”时间戳要求时基同步。对于安全应用，应定期监视同步情况，并且该机制的失败率应包含在整个安全功能的评估中。

4.5.4 时间期望

报文传输期间，报文汇点检查两个连续接收报文之间的延时是否超过预定值。在这种情况下，必须假定一个错误。

示例：

面向时隙的访问方法：

— 每个通信参与方的报文交换以固定周期且在预先确定的时隙内发生；
— 可选地，即使值未变化，每个通信参与方都在其时隙内发送数据（这是周期性通信的一个例子）；
— 添加了一个源点标识，以识别出在其相关时隙内未传输数据的通信参与方。

4.5.5 连接鉴别

报文可能具有唯一的源和/或目的标识符，用于描述安全相关通信参与方的逻辑地址。

4.5.6 反馈报文

报文汇点向源点返回一个反馈报文，以证实原始报文的接收。该反馈报文必须由安全通信层处理。

注1：有些现场总线规范使用术语“回声”或“收条”作为同义词。

注2：这个返回的反馈报文可包含：例如仅有一个短确认，或者也可包含原始数据，或者促使源点检查是否正确接收的其他信息。

4.5.7 数据完整性保证

如果数据完整性保证方法的设计未从功能安全角度出发，则安全相关应用过程不应信任它。因此，在报文中包含冗余数据，使得可通过冗余检查来检测到数据讹误。

注：用于安全相关应用的通信系统可使用如密码方法确保数据完整性，作为典型方法如CRC的备选方法。

如果使用了哈希函数，则不应包含错误校正机制。

4.5.8 带交叉校验的冗余

在安全相关现场总线应用中，安全数据可在一个报文内或通过两个单独报文发送 2 次，使用相同或不同的完整性方法，独立于底层现场总线。

注：附加冗余功能安全通信模型的描述参见4.3。

此外，在现场总线上或单独源点/汇点连接上对所传输安全数据的有效性进行交叉校验。如果检测到差异，则在传输期间在源点或汇点的处理单元中应已发生了错误。

使用冗余介质时，应考虑采取适当措施（例如多样性、偏时传输）进行共模保护。

4.5.9 不同数据完整性保证系统

如果通过同一总线传输安全相关(SR)和非安全相关(NSR)数据，则可使用不同的数据完整性保证系统或编码规则（不同的哈希函数，例如不同的 CRC 生成多项式和算法），以确保 NSR 报文不会影响 SR 接收者中的任何安全功能。

为 SR 报文提供额外的数据完整性保证系统，而不为 NSR 报文提供是可接受的。

4.6 错误与安全措施间的典型关系

4.5 列出的安全措施与 4.4 中定义的可能错误集相关。二者之间的典型关系如表 2 所示，实际关系应由每个 FSCP 规定。每个安全措施可提供保护以防止传输中出现一个或多个错误。根据表 2 应说明，对于已定义的可能错误，至少有一种相应的安全措施或安全措施组合。

防止错误的措施的实际保护效果取决于该措施的具体实施。

如果安全措施在有保证的现场总线的安全响应时间之前生效，则应将该安全措施列在给定 FSCP 的

相应表中。

表 2 各种措施对可能错误的有效性概览

通信错误	安全措施							
	序列号（见4.5.2）	时间戳（见4.5.3）	时间期望（见4.5.4）	连接鉴别（见4.5.5）	反馈报文（见4.5.6）	数据完整性保证（见4.5.7）	带交叉校验的冗余（见4.5.8）	不同数据完整性保证系统（见4.5.9）
讹误（见4.4.2）					○[d]	○	仅用于串行总线[c]	
意外重复（见4.4.3）	○	○					○	
错序（见4.4.4）	○	○					○	
丢失（见4.4.5）	○				○		○	
不可接受的延时（见4.4.6）		○	○[b]					
插入（见4.4.7）	○[e]	○[e]		○[a]	○		○	
伪装（见4.4.8）				○	○[d]			○
寻址（见4.4.9）				○				

注：表格改编自IEC 62280:2014的表1。

a. 仅用于发送方标识。仅检测无效源点的插入。
b. 所有情况中都要求。
c. 两条报文通过独立收发器发送时，仅当计算能表明残余错误率λ符合4.5.9中要求的值时，该措施才可与高质量数据保证机制相比较。
d. 仅当反馈报文包含原始数据或有关原始数据的信息，且接收方仅在确认反馈报文后才处理数据时有效。
e. 仅在各源点实体的序列号或时间戳不同时才有效。

4.7 总残余错误率计算

4.7.1 适用性

第 4.7 节介绍了用于估算 FSCP 总残余错误率的模型，以评估该 FSCP。

4.7.2 黑色通道通用模型

所有 FSCP 都做一个基本假定：所有功能安全通信均通过黑色通道进行（见 3.1.11）。

为了适当量化安全措施的残余错误，首先约束关于 FSCP SCL 的黑色通道的模型是很重要的。这就允许适当定义报文类型以及错误类型和错误率，连同安全措施一起，这些都是 FSCP SCL 设计者应考虑的内容。

图 8 示出了包含不同通信类型的黑色通道：带安全 PDU 和不带安全 PDU 的现场总线报文。

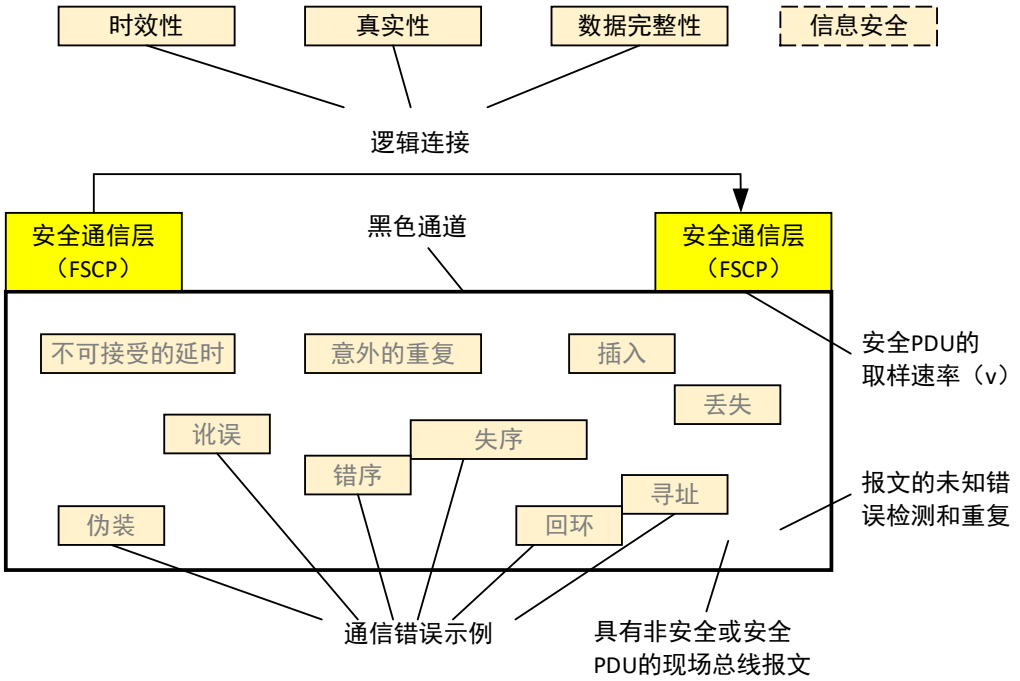


图 8 从 FSCP 角度看的黑色通道

黑色通道包括在一个设备内 SCL 之下的底层现场总线通信层，以及在 FAL 和 SCL 之间的任何附加通信。在黑色通道内的错误可能从以下来源产生：

- 在传输介质中报文的比特损坏；
- 在黑色通道内的随机硬件故障和电子装置及软件的系统故障。

黑色通道内的报文交换频率可能与 SCL 采样和处理安全 PDU 的频率不同。

4.7.3 通用安全特性的识别

表 2 列出了可能的离散安全措施，它们单独或组合为报文贡献以下通用安全特性（见图 8）：

- 数据完整性；
- 身份认证（包括伪装拒绝）；
- 时效性。

报文内容从报文源点到所组态报文汇点的正确传送是数据完整性的特性。报文从一个正确的报文源点到所组态的相关报文汇点的传送是身份验证的特性。报文汇点拒绝一个看似正确的随机比特是伪装拒绝的特性。报文在所组态的时间帧内及时在报文源点和报文汇点之间传送是时效性的特性。

另一个应考虑的通用安全方面是 FSCP 的组态和/或参数化（见 4.10）。

这些通用安全措施中的任何一项发生故障，都可能导致危险的状态或非故意的启动。

FSCP 供应商应提供整体残余错误率的充分证据，残余错误率考虑第 4.7.6.6 节中规定的三种通用安全特性。

4.7.4 残余错误率计算的假设

第 4.7.6 节规定了残余错误率计算中采用的公式类型的示例，这是基于黑色通道和 SCL 的假设。在这些假设不能适合给定的 SCL 类型的情况下，则应采用替代公式。

以下通用假设对于 4.7.6 中定义的所有公式是有效的：

a) 假设普通黑色通道设备的失效率为10^{-7}/h(100 FIT)，则SCL应假定黑色通道失效率为该值的 10，000倍。因此，对于每个有源网络元件或安全设备的现场总线部分，电子装置的失效率好于10^{-3}/h(10^{6} FIT)；

注1：一旦任意设备失效，该失效可一直持续到被检测出或被纠正。这包括永久的、间歇的和临时的错误。

注2：ISO 13849-1:2015表7指出，非安全设备的错误率为10-3。与最弱的性能水平相比，该表采用了保守裕度。

注3：当检测到一个或多个危险的黑色通道失效，如果该FSCP能驱动安全功能达到安全状态（故障状态见图15），如果当被修复时仅返回至运行状态，且如果能证明10^{-3}/h 的失效率因此会导致安全通信不可运行，则可假设，FSCP 的失效率比10^{-3}/h保守。

b) 当与FSCP相关时，考虑存在存储转发设备；
c) 安全PDU的哈希函数不同于底层现场总线DLL所用的哈希函数（可通过设计或管理规程保证）；
d) 安全PDU的哈希函数为不含错误校正机制的CRC；
e) 黑色通道的PDU的哈希函数可能包含错误校正机制；
f) 每个逻辑连接被分配一个唯一认证码，在传输SPDU之前，发送方和接收方都已获知该认证码；
g) 无论何时在错误或事件发生概率或发生率的公式中要使用固定的最坏情况值（当前技术水平），如果提供了足够的证据，FSCP可以规定自己的值来替代；
h) 无论何时使用单一机制检测多种错误类型，则在计算残余错误概率时，应既考虑单个错误类型又考虑这些错误类型的组合；
i) 针对整个SPDU进行CRC计算，包括A代码和T代码。

4.7.5 显式机制和隐式机制

显式机制包括 FSCP 安全措施相对应的数据，比如安全 PDU 中的序列号、时间戳和连接认证。基于接收方具有相等知识的假设，隐式机制并不实际传输与安全措施相对应的所有数据，但是使用这些数据来计算整体 CRC 签名。

注1：隐式机制典型地应用于带有固定的黑色通道报文长度、低传输速率或实施成本较低的受限系统。

本文件规定的 FSCP 可分类为：显式、隐式和部分显式/隐式三种类型（见附录 B 中的示例）。由于存在各种可能的方法，不能为隐式类型提供通用公式。由各 FSCP 来证明足够的残余错误概率。因此，第 4.7.6 节只处理显式类型。

注2：IEC 61784-3:2021的附录G提供了特殊情况下的公式示例，以便为使用隐式数据安全机制来开发FSCP残余错误概率的附加公式提供指导。

4.7.6 残余错误率计算

4.7.6.1 一般信息

第 4.7.6.2 至 4.7.6.5 节给出了对于显式 FSCP，基于序列号长度、时间戳和连接认证数据来计算残余错误率的示例公式。特定 FSCP 可以提供适用于自己的公式。

4.7.6.2 数据完整性与计算数据完整性残余错误率（RR_I）

4.7.6.2.1 概率相关考虑

通用的安全特性数据完整性要求根据表 2 检测以下通信错误：

- 讹误（见 4.4.2）。

数据完整性保证是安全通信层达到所需安全完整性等级的基本组成部分。应采用合适的哈希函数，比如奇偶校验位、循环冗余校验(CRC)、报文和/或数据重复以及类似的冗余形式。

如果数据完整性措施的残余错误概率取决于安全数据值，则应考虑最差情况的值。

使用循环冗余校验(CRC)作为哈希函数时，FSCP 设计人员应避免或考虑“黑色通道”使用相同的多项式的可能性。可采用多种方法实现该目标。

示例

可能的方法包括：

— 仅允许FSCP和CP的特定组合的措施；
— 设计SCL时的适当措施；
— 采取措施，确保由黑色通道CRC校验的各SPDU也由SCL CRC校验，因为在黑色通道中进行相同校验的额外试验会增加残余错误率。

4.7.6.2.2 确定性的考虑

除随机比特模式外，还应评估以下特定错误模式：完全反转的数据、全"0"或全"1"数据集、同步滑动错误和突发错误。

4.7.6.2.3 数据完整性残余错误概率（RP_I）

RP_I是数据完整性的残余错误概率。

示例：见附录C中的R_{crc}。

附录 C 提供了基于 CRC 进行错误校验以解决数据完整性问题的相关信息。

4.7.6.2.4 计算数据完整性残余错误率（RR_I）

计算数据完整性残余错误率RR_I的示例如公式(1)所示。

$$RR_I = RP_I \times v \times RP_{FSCP\_I} \quad (1)$$

其中：

RR_I 数据完整性的残余错误率；

RP_I 数据完整性的残余错误概率；

v 每小时 SCL 对 SPDU 采样的最大数量（“采样率”）；

RP_{FSCP_I} FSCP 特有数据完整性的其他措施的残余错误概率。RP_{FSCP_I}所用措施应独立于数据完整性措施。

4.7.6.3 真实性与计算真实性残余错误率（RR_A）

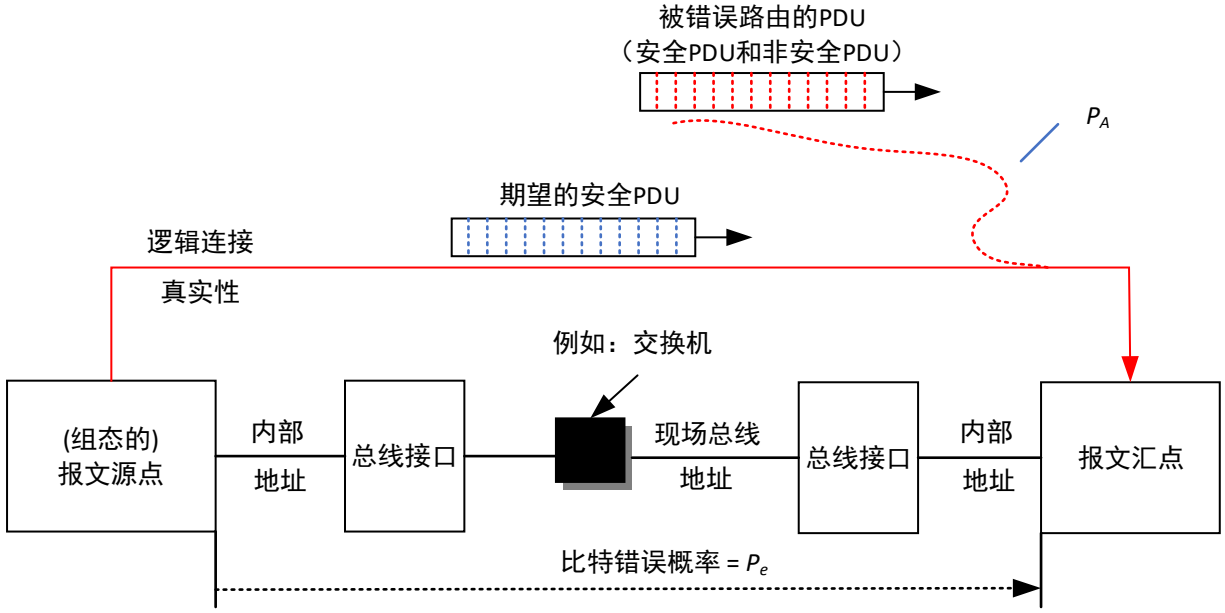
4.7.6.3.1 一般信息

通用的安全特性真实性要求根据表 2 检测以下通信错误：

- 寻址（见 4.4.9）；
- 插入（见 4.4.7）。

FSCP 应满足以下要求（见图 9）：

- 报文汇点仅应处理从已认证的报文源点接收到的正确寻址的报文中的安全数据。



说明：

PA：逻辑连接的真实性错误概率

图 9 认证考虑的模型

在 4.8 节所述的与连接认证相关的（FSCP 相关的）所有通信阶段期间，都应满足这些要求。如有例外，应在安全手册中说明。

认证可防止对通过所有其他检查但对于接收者是无效报文中的安全数据进行处理。

注：导致错误的真实性的可能随机原因包括但不限于：

— 报文内的虚假地址或内部通信链路中的错误（见图10），无论其是否与非安全或安全地址机制有关；
— 在黑色通道中被干扰或错误操作的协议栈/层；
— 被干扰的或错误操作的路由设备，例如：交换机或路由器；
— 被干扰或错误操作的网关，例如：总线耦合器；
— 被干扰或者错误操作的黑色通道设备，这些设备镜像报文（“回环错误”）或通过其他手段改变报文方向；
— 报文汇点内的验证机制不足以区分来自不同报文源点的报文。

图 10 显示了由于现场总线通信系统内地址被破坏而导致的可能的寻址错误，或者可能的内部寻址错误（例如，由于模块化远程 I/O 设备内指针被破坏）。

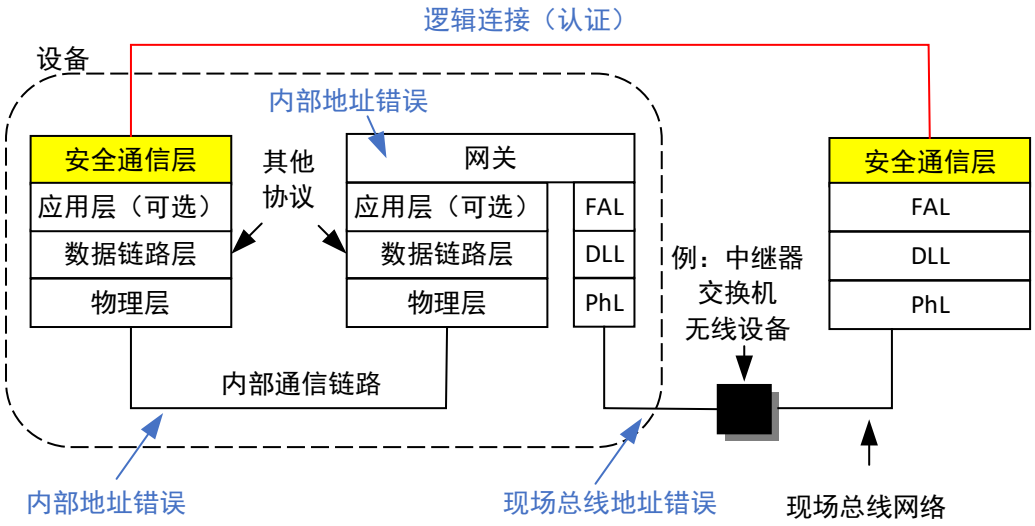


图 10 现场总线地址错误和内部地址错误

其他导致不正确真实性的系统原因可在组态和参数化过程中识别出来，如 4.10 所示。为了控制这些系统错误原因，可能要求其他组织上的措施。

连接认证可用于唯一且明确识别下列内容：

- 单个报文源点或报文汇点；
- 一个报文源点与报文汇点之间的单个连接；
- 在多播情况下，单个报文源点与多个报文汇点之间的多个连接；
- 多个报文源点与多个报文汇点之间的一组连接。

多种方法均可避免认证错误。

示例：

— 随各 FSCP 报文传输的唯一连接认证（例如“连接 ID”）。

— 本地存储的唯一连接认证（例如“连接 ID”），通过哈希函数（如CRC签名）来加密并传输至报文汇点。这种加密通常是 FSCP 整体数据完整性措施的一部分。

4.7.6.3.2 方向错误安全 PDU 的发生率（R_A）

根据第 4.7.4 节中的第 a)条，应假设每台设备的方向错误的安全 PDU 的发生率(R_A)为 10^{-3}/h，另有规定的除外。

进一步假设，在第一次发生方向错误的安全 PDU 之后直到系统被修复，R_A 应具有的值为 v（SPDU 采样率）。

认证技术措施可通过组织措施进行补充，这些措施对用户执行应是可实现的（见 4.10）。

4.7.6.3.3 计算真实性残余错误率（RR_A）

有3种因素导致该残余错误率：

a) 方向错误的 PDU；

b) 在接收到的认证码中与预期认证码相匹配的比特错误；

c) CRC 未检测到这些比特错误。

由于 A 代码为显式传输，因此，计算RP_I时已考虑了所接收认证码中的比特错误。

v 是最大报文采样率，因此 R_A（方向错误的安全 PDU 的发生率，见 4.7.6.3.2）包含在 v 中。因此，在所有包含该项的公式中，RR_A 的值均为 0。

4.7.6.4 时效性与计算时效性残余错误率（RR_T）

4.7.6.4.1 一般信息

通用的安全特性时效性要求根据表 2 检测以下通信错误：

- 不可接受的延时（见 4.4.6）；
- 意外重复（见 4.4.3）；
- 错序（见 4.4.4）；

- 丢失（见 4.4.5）。

FSCP 应满足以下要求：

- 报文汇点处理最新报文；
- 报文汇点监视报文源点安全层的操作状态。

注1：一个设备在同一时间可能提供一个报文源点和一个报文汇点，取决于是单向通信还是双向通信。

时效性的技术措施可通过组织措施进行补充。

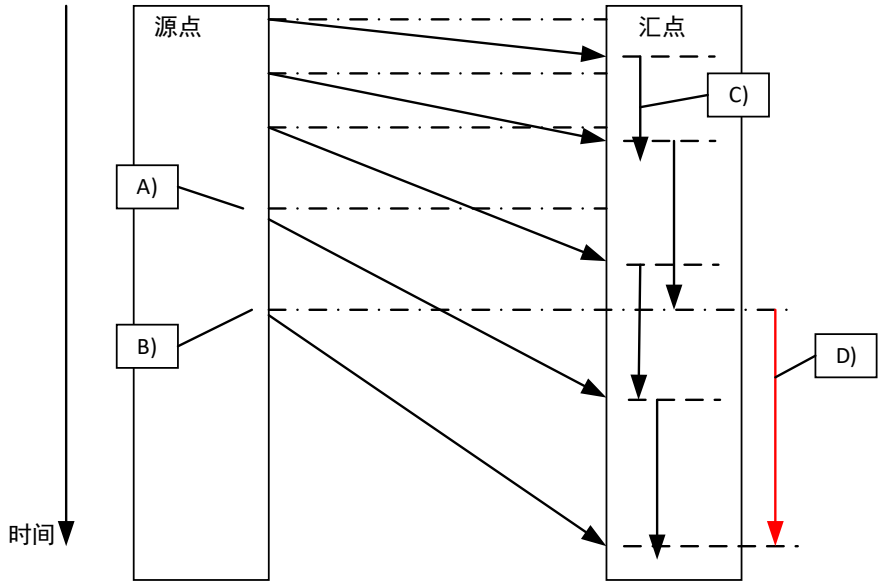
设计 FSCP 时应考虑导致非及时通信的典型原因，这些原因引起黑色通道的性能波动。

示例：

黑色通道性能变化可能源于：

— 吞吐量不足（例如带宽、通信量）；
— 通信丢失（暂时或全部的）；
— 延迟变化；
— 缓慢增长的延迟（见图11）；
— 各报文源点/汇点的不同延迟；
— 报文源点或报文汇点的同步时钟时间变化；
— 所有这些情况的组合。

图 11 给出了缓慢增长的黑色通道报文延迟的示例。



说明：

A):报文离开时间与报文接收时间不相关。
B):报文离开时间早于前一条报文的报文接收时间。
C):汇点中超时检查。
D):报文汇点不能根据报文接收时间和间隔来确定报文离开时间。报文延时可能大于超时时间，但却未检测出。

图 11 缓慢增长的报文延迟的示例

另一个需要考虑的问题是从报文或部分报文内存处的意外传输。

示例：

— 有源网络元件，例如交换机、路由器（见图12）。
— 已定义通信系统之外的通信设备（例如通过无线通信链路接入互联网）。
— 多路径通信（例如互联网）。

图 12 显示了有源网络元件故障导致的内存处意外传输示例，如下所示：当发送指针超越接收指针时引起循环存储器中“插队”，这将导致清空/发送交换机的整个队列。

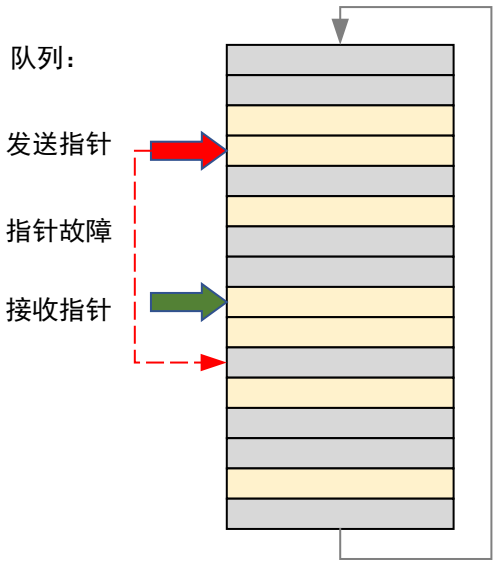


图 12 有源网络元件错误的示例

注2：黑色通道可包括除交换机外的其他类型存储元件。

有几种方法可以避免内存处的意外传输。

示例：

— 带有延迟监视的周期性通信。

— 在所有设备内同步时钟和为SPDU打时间戳。

— 足够范围的SPDU序列编号。

在每种情况下，时间精度和范围都应满足以下事项引起的要求：

- 安全应用定时问题；
- 系统内外报文的潜在存储量。

在设计和实施评估期间，应依据GB/T 20438确定时基超出规定安全限制的错误率。

注3：在整个安全网络中使用一个同步的时基是实现方面的一部分。

4.7.6.4.2 失序安全 PDU 的发生率（R_T）

在具有报文存储元件的安全相关网络（见图 12）中，根据 4.7.4 a)，应假设每个存储元件的时效性错误发生率(R_T)值为 10^{-3}/h，另有规定的除外。

如果 SCL 在检测到首个通信错误之后进入安全状态，则 R_T 应乘以 1。否则，R_T 应乘以所采样 SPDU 的最大数量（由接收 SCL 检查）直到 SCL 进入安全状态。

注：必须乘以相关系数，因为如图12所示，有源网络元件发生故障时，将接收到多个错误SPDU，所有这些SPDU都可能具有不同的时效性代码。

4.7.6.4.3 计算时效性残余错误率（RR_T）

计算时效性残余错误率RR_T的示例如公式(2)所示。

$$RR_T = 2^{-LT} \times w \times R_T \times RP_{FSCP\_T} \quad (2)$$

其中：

RR_T 时效性的残余错误率；

LT 顺序号的比特长度；

w 接收安全 PDU 中所接受的时间戳或序列号的值（窗口）的范围；

R_T 失序的安全 PDU 的发生率（见 4.7.6.4.2）（其值不能超过 4.7.6.2.4 中规定的 v 值）；

RP_{FSCP_T} 是 FSCP 特有的其他措施的残余错误概率。

RP_{FSCP_T}所用的措施应独立于时效性措施。

不同于 A 代码，T 代码值随时间变化，因此，数据完整性措施虽必不可少，但不足以检测时效性错误。

4.7.6.5 伪装与计算伪装残余错误率（RR_M）

4.7.6.5.1 一般信息

安全属性伪装要求根据表 2 检测以下通信错误：

- 伪装（见 4.4.8）。

通常，非安全（伪装的）PDU 更可能由 SCL 检测出，因为它们应满足所有前提条件（时效性、真实性和数据完整性）。

4.7.6.5.2 伪装安全 PDU 的发生率（R_M）

应依据 4.7.4 a)，假定每个设备的伪装安全 PDU 发生率(R_M)为 10^{-3}/h，另有规定的除外。

4.7.6.5.3 计算伪装残余错误率（RR_M）

SCL 可将某些特定字段限制为特定值。这由被限制字段的唯一性系数(RP_U) 表示，该系数适用时被包含在残余错误率计算中。其表达式为公式(3)。

$$RP_U = \frac{V_{A1}}{V_{R1}} \times \frac{V_{A2}}{V_{R2}} \times \ldots \times \frac{V_{AN}}{V_{RN}} \quad (3)$$

其中：

RP_U 其他唯一性字段的残余错误概率，唯一性用于区分正确格式的安全 PDU；

V_{Ai} 数据字段 N 中由汇点接受的值的数量；

V_{Ri} 代表数据字段 N 的总范围的值的数量。

计算伪装残余错误率 RR_M 的示例如公式(4)所示。

$$RR_M = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_U \times 2^{-LR} \times R_M \quad (4)$$

其中：

RR_M 伪装的残余错误率；

LA 连接认证的比特长度；

LT 序列号的比特长度；

w 接收安全 PDU 中所接受的时间戳或序列号的值的（窗口）范围；

r CRC 签名的比特长度（如果两个 CRC 使用独立的多项式，则r为两个相应比特长度之和）；

RP_U 其他唯一性字段的残余错误概率，唯一性用来区分正确格式的安全 PDU；

LR 安全 PDU 中重复部分的比特长度（带有交叉校验的冗余，否则$LR = 0$）；

R_M 伪装安全 PDU 的发生率（见 4.7.6.5.2）。

4.7.6.6 计算总残余错误率

4.7.6.6.1 基于残余错误率的总和

安全通信通道的总残余错误率 λ_{SC}为各单个残余错误率（RR_I、RR_A、RR_T和RR_M）的总和，如公式(5)所示。

$$\lambda_{SC} = RR_I + RR_A + RR_T + RR_M \quad (5)$$

SCL的残余错误率由安全通信通道总残余错误率λ_{SC}和单项安全功能所允许的最大逻辑连接的个数(m)计算得出，如公式(6) 和图13 及图 14所示。

$$\lambda_{SCL} = \lambda_{SC} \times m \quad (6)$$

注：公式（6）仅在每个逻辑连接的λ_{SC}相等时生效。当λ_{SC}不相等时，应将λ_{SC}相加计算λ_{SCL}。

其中：

λ_{SCL} SCL 的每小时残余错误率；

λ_{SC} 一个逻辑连接的安全通信通道的每小时总残余错误率（见公式(5)）；

m　　单项安全功能所允许的逻辑连接的最大个数。

逻辑连接的个数 m 取决于具体的安全功能应用。图 13 和图 14 说明了如何确定该个数。

两图所示为具有可能的网络组件（例如中继器、交换机或无线链路）的物理连接，以及安全功能相关子系统之间的逻辑连接。

逻辑连接可基于单播或多播通信。

图 13 所示为 $m = 4$ 的应用示例 1。在该应用中，根据风险分析，认为所有三个驱动器在单一时间点上都是危险的。

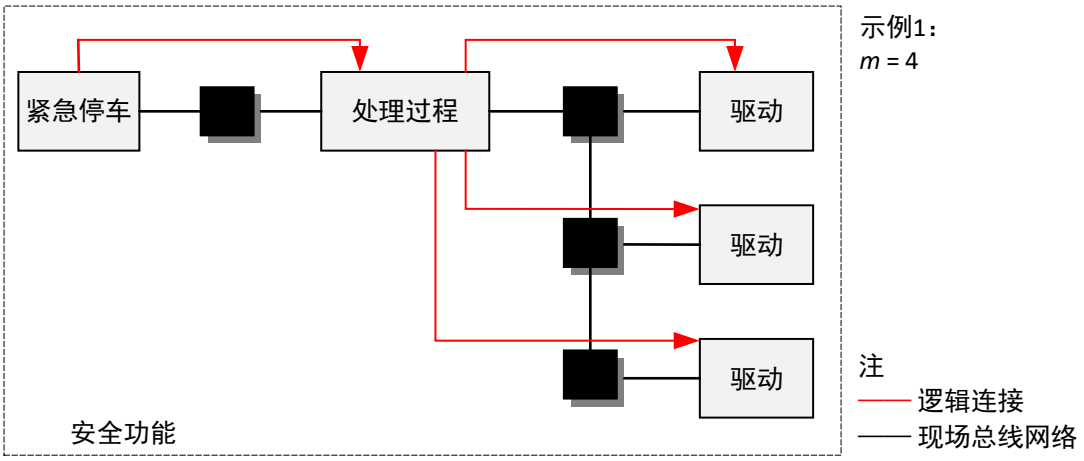


图 13 应用示例 1（$m = 4$）

图 14 所示为 $m = 2$ 时的应用示例 2。在该应用中，根据风险分析，认为仅一个驱动器在单个时间点上存在危险。

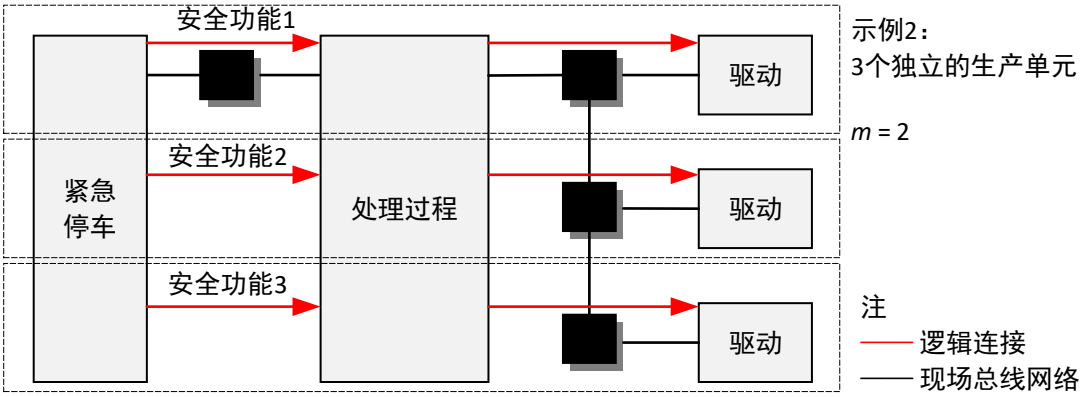


图 14 应用示例 2（m = 2）

4.7.6.6.2 基于其他定量的证据

如 4.7.6.6.1 中所示，对通用安全特性的残余错误率求和，是计算给定 FSCP 的总残余错误率的一个可接受的方法。

可以使用组合的数学方法进行计算，这些计算考虑各个安全措施的交叉影响以获得更好的残余错误率。

也可以直接使用 GB/T 20438 中的方法并确定 FSCP 的安全失效分数和诊断覆盖率。

4.8 安全总线不同通信阶段的要求

FSCP 应设计为：接收方在安全网络的每个通信阶段都可达到安全状态或残余错误率足够低，通信阶段包括：

- 建立或改变安全网络（组态和参数化）；
- 初始化启动（例如，连接建立）；
- 运行（安全数据交换）；

- 从故障转换后的热启动；
- 关闭。

图 15 所示为概念性的 FSCP 协议模型。发生故障之后，FSCP 不应直接返回至正确的 FSCP 通信状态，而是首先进行热启动阶段或新的初始化阶段，这取决于 FSCP。

注：在故障情况下，FSCP可以关注应用要求，例如在机器启动前的操作员确认。

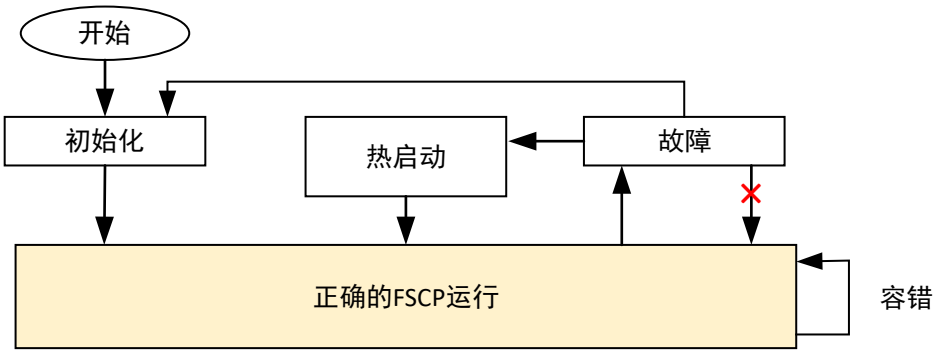


图 15 概念性的 FSCP 协议模型

4.9 FSCP 实现方面

所有 FSCP 技术措施应在按照 GB/T 20438 设计的设备的 SCL 内实现，并应满足目标 SIL。

部分协议措施依赖于其在特定安全设备中实现的方式。图 16 所示为 FSCP 实现方面与其确定性和概率方面之间的划分。

实现方面的一个示例是实时时钟、看门狗或微控制器的失效率之间的依赖关系。这些方面要求依据 GB/T 20438 进行定量安全评估，以确定其与各个通用安全特性的相关性。

本文件不考虑实现方面，除非 FSCP 具有实现方面要求，且该方面可能会影响 FSCP 的残余错误率。基于 SCL 端点之间的逻辑连接来考虑通用的安全特性（仅使用关于黑色通道性能的基本假设，这些基本假设在各 FSCP 安全手册中说明）。

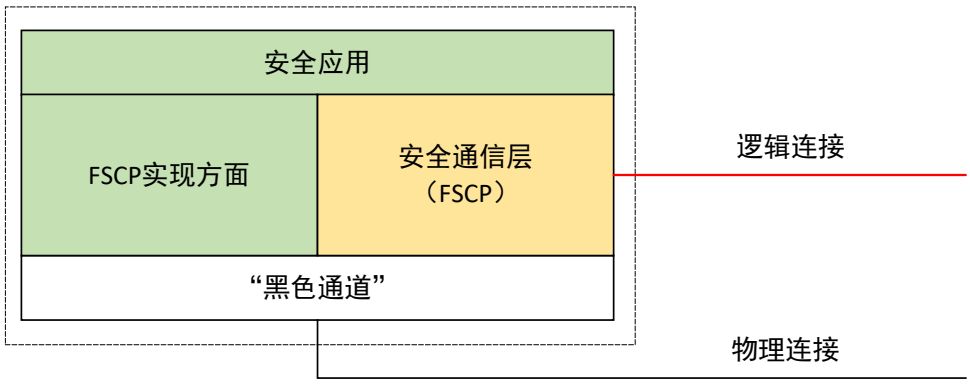


图 16 FSCP 实现方面

4.10 FSCP 的组态和参数化

4.10.1 一般信息

在不同阶段，对安全设备及其 SCL 进行正确的组态和参数化对功能安全至关重要。使用 FSCP 的安全功能的工程化通常包括组态、参数化和编程活动，如图 17 中示例所示。

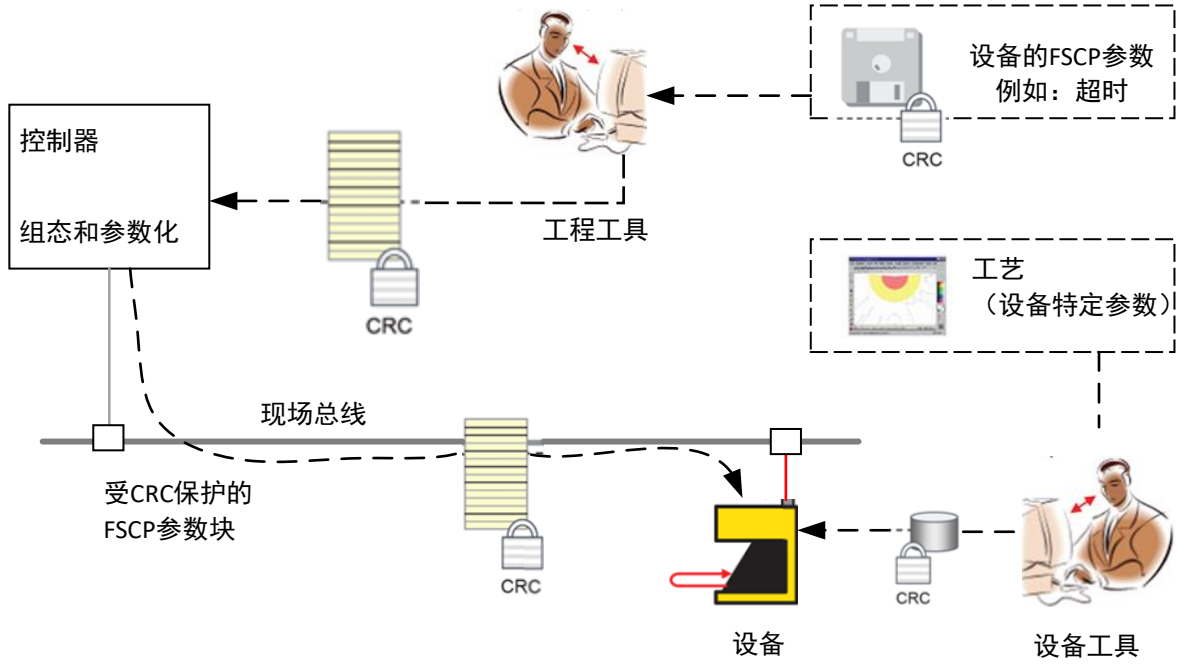


图 17 FSCP 的组态和参数化过程示例

组态要求工程工具建立现场总线网络结构、连接现场设备并对黑色通道层参数进行赋值，以及对FSCP 参数（比如连接认证、超时、SIL 声明等参数）赋值。通常，现场设备提供一个保存在文件中的电子形式的数据单，该文件可被导入工程工具中。

在组态完成后，包含若干参数值的组态数据被下载到现场总线控制器以建立通信。在周期性过程数据交换之前，组态和参数数据的现场设备相关部分被下载到特定的现场设备。

更复杂的安全设备可能需要一个专用工具来对工艺特定的安全设备应用进行组态和参数化。

注1：相关信息见IEC 62061:2005的6.11.2.3节和ISO 13849-1:2015的4.6.4节。

注2：不正确的组态和参数化包括但不限于以下方面：

— 人为错误导致错误的初始化和参数值；
— 存储期间的数据损坏；
— 下载期间的寻址错误；
— 下载期间的数据损坏；
— 安全设备更新不一致；
— 相同“安全岛”的连接（串行机器）；
— 使用工程工具时由于特定的计算机配置产生的系统错误（例如显示值和存储值之间的差异）；
— 随机的或故意的对安全设备中工艺特定的安全参数进行未能识别的改变；
— 使用此前已安装在其他安全功能中的安全设备。

FSCP 应规定防止安全组态和参数中发生随机错误的方法。

示例：

— 不正确的寻址。
— 数据损坏。
— 未能识别的更改。

FSCP 设计者应在所有相关的通信阶段考虑上述要求（见 4.8）。

可采用多种方法避免不正确的组态和参数化。

示例：

— 覆盖组态和参数数据的 CRC 签名。
— 检测安全技术限值与 FSCP 参数之间的冲突（例如安全技术循环时间超过 FSCP 看门狗时间）。

操作过程中随机的组态和参数化的错误可以通过通用安全措施来避免。

系统性组态和参数化错误只有通过验证和确认来安全地避免。安全手册应提供必要说明。

注3：相关信息见IEC 62061:2005的6.11.2.3节和ISO 13849-1:2015的4.6.4节。

FSCP 中应明确安全通信组态和参数化使用的工程工具、安全通信的配置组合、规定安全通信的参数范围，所有配置和参数的变更，应在 FSCP 允许的范围内。

配置数据如果通过远程操作的方式实现，应考虑信息安全性。工程工具要求应与 GB/T 35850 保持

一致。

4.10.2 组态和参数化的变化率

除非另有规定，用于计算的组态和参数化的变化率应假定为每天一次。

4.10.3 组态和参数化的残余错误率

在下载等一次性操作过程中，随机的组态和参数化错误的残余错误率 RR_{CP} 可由所选 CRC 签名的残余错误概率（见附录 C）与 4.10.2 中规定的变化率进行相乘计算得到。

4.11 安全总线故障对电梯系统的影响评估

4.11.1 一般信息

使用安全总线技术的电梯，除满足本文件外，应符合电梯安全功能的要求，同时宜考虑电梯安全功能的稳定性和故障率。

4.11.2 安全总线故障设计

安全总线故障，定义如下：

安全总线根据表 2，通过检测 4.4 规定的失效模式，当检测到通信错误时，认为安全总线异常，当安全总线异常达到设计的容错率时，认为安全总线故障。

安全总线故障设计时应考虑到通信的容错率、通信延时对安全功能的响应时间的影响，故障率要在合理范围。

注：

— 如果容错率设计的不合理，如要求的失效时间过短，可能导致PES系统过于频繁的进入安全状态，这将会对实际乘梯以及部分机械部件造成损伤，这是没有必要的。如要求的失效时间过长，可能导致安全功能响应时间超时，影响安全功能，这是不被允许的。

— 经由安全总线传递给控制子系统的数据会带有一定的通信延迟，当这些信号被整个电梯系统采纳时，应考虑通信延迟的影响，不应导致安全功能的异常。可对安全总线的传输延时做针对性的补偿。

4.11.3 安全总线故障处理

安全总线发生故障后，PES应进入安全状态。同时宜记录故障，在总线恢复正常时，允许安全总线故障自动复位。

4.11.4 安全总线接入设备的约束

安全总线设计时，FSCP 应明确设备类型、数量、组合方式，通信协议，总线负载率等。

安全总线系统上接入设备的变更导致设备类型和数量变更、通信协议变更、总线负载率变更时，应按照本文件对安全总线重新分析计算、测试和评估。

安全总线只能接入本台电梯本地网络内的设备，禁止 FSCP 中未明确的设备接入，如果接入未明确的设备导致安全总线故障时，PES 应能够检测出并进入安全状态。

4.11.5 非安全数据的传输

如果通过同一总线传输安全相关(SR)和非安全相关(NSR)数据，见图18，则应按照4.5.9的要求设计不同数据完整性保证系统，确保NSR数据不影响SR数据的传输。

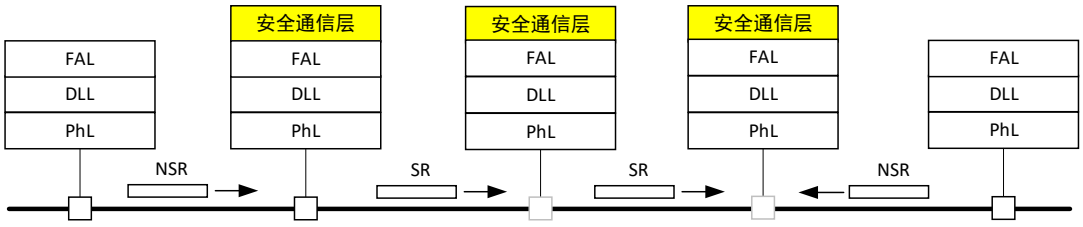


图 18 SR 和 NSR 用同一总线传输

4.12 边界条件和约束条件

4.12.1 传输介质和布线的要求

使用有线传输时，宜考虑传输介质保证信号完整性，减少外部干扰因素。

为了减少干扰，宜将强弱电分开布线，动力线和信号线分开布线，信号线远离开关电源、控制柜电源等干扰源。

4.12.2 电磁兼容性（EMC）

可编程系统应当进行符合 GB/T 24808 规定的安全电路的电磁兼容(性)抗扰度测试，且均应当达到性能标准 D，即 PESSRAL 或者 PESSRAE 按照设计连续运行，除非因故障进入安全模式，不允许有任何性能降低和功能损失。

4.12.3 电气安全

电气安全是功能安全通信系统的前提条件。因此，所有连接到此系统的设备都应符合电梯相关电气安全规范。

4.13 安全手册

设备供应商应提供安全手册。行规要求的包含在安全手册中的最小信息描述，在相关行规特定部分中提供。

4.14 安全策略

本文件的使用者应考虑以下限制，以避免对安全相关的开发和应用工作产生误解、错误预期或法律诉讼。

注1：这包括诸如培训、研讨会、讲习班和咨询等用途。

本文件中规定的通信技术，仅应在按照 GB/T 20438 要求设计的设备中实现。

在设备中使用本文件规定的通信技术，并不能确保设备满足 GB/T 20438 的中所有必要的安全相关的应用要求，包括技术上、组织上和法律上的要求。

基于本文件并适用于安全相关应用的设备，应遵循符合安全相关标准和相关法律/法规的适当的功能安全管理生命周期过程。对此应按照 GB/T 20438.1 的独立性和能力要求进行评估。

在硬件安全完整性上下关系中，一个安全功能所能声称的最高安全完整性级别受限于硬件安全完整性限制，应通过实现 GB/T 20438.2 的路线 1H 来获得，基于硬件容错和安全失效分数概念（在系统或子系统级实现）。采用本文件所规定的通信技术的设备，由制造商负责保证标准的正确实现、以及设备文档和信息的正确性和完整性。

强烈建议特定行规的实现者遵从相关技术特定组织提供的适当的一致性测试和确认。

注2：因为不正确的实现会导致严重损害或生命丧失，因此包含这些要求和建议。

5 使用安全总线技术电梯的型式试验、检验与检测

使用安全总线技术电梯的型式试验、检验与检测应符合 PES 相关的要求。同时应按照附录 D 验证安全措施。

附 录 A
（资料性）
黑色通道和白色通道概念

A.1 概要

此部分定义两种通用类型的安全通信概念，黑色通道和白色通道。本文件覆盖这两种安全通信概念。

A.2 黑色通道

当使用基于 IEC 61158 的现场总线结构而不改变每个通信层定义时，按照 GB/T 20438 要求实现安全数据传输的所有必要措施，都应由一个附加的“安全通信层”执行。安全通信层位置见图 A.1。

安全通信层包括适当的服务和协议，旨在将安全数据编码为安全 PDU 并将其传递到黑色通道上，以及从黑色通道上接收安全 PDU 并解码，从而提取安全数据。

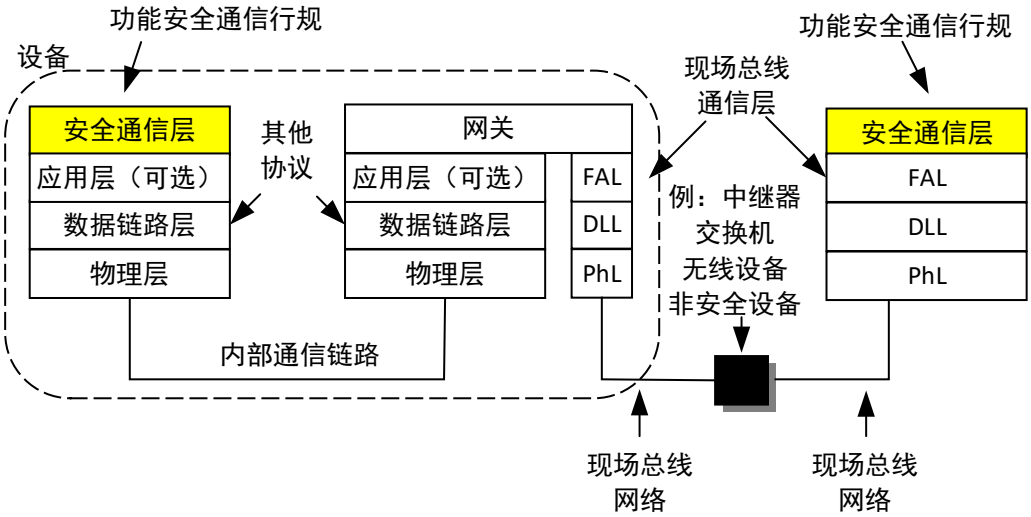


图 A.1 功能安全通信系统模型示例

当依据本文件实现功能安全通信系统要求的现场总线应用层（FAL)时，可以省略设备内部通信链路（例如：网关）的应用层。

与安全无关的用户层功能可以不通过 SCL 而直接访问 FAL。

注：依据定义3.1.11，黑色通道类型的安全通信仅要求对符合GB/T 20438的设计证据或安全通信层(SCL)确认。安全设备设计者可以使用某个经预评估并被核准的提供特定SCL功能的硬件/软件组件。如果设计者按该组件特定的方式实现此组件，则依据GB/T20438对该组件自身的安全评估可以被省略。这样，可以减少对设备安全相关技术评估的工作量，并能正确实现SCL组件。

A.3 白色通道

依据定义3.1.12，白色通道类型安全通信要求所有相关硬件和软件组件的设计、实现和验证都应符合GB/T 20438。由于可能的解决方案有很多，因此A.3的内容仅对如何保证数据完整性方面提供帮助。

注：进一步信息可以参考IEC 62280。

通常，单个的白色通道方法可以使用4.3中的模型之一来进行评估。

A.3.1 白色通道方法的数据完整性考虑

A.3.1.1 概要

对于数据完整性考虑，可以确定两类白色通道，见 A.3.1.2 和 A.3.1.3 中的描述。

A.3.1.2 模型 B 和模型 C

此方法认为该总线通信系统的每个通道不是安全的。协议层是冗余的，并发送两个报文。因此，该

总线通信系统的数据完整性措施(measures)被完全地使用。在两个通道中的一个失败时，充分的错误检测是不可能的。由于它们的架构，某些已知总线通信系统使能其他参与方来检查每个报文，这样就已经发现了大多数错误可能性。

注1:模型B和模型C可以被实现为白色通道解决方案或黑色通道解决方案。

注2:在A.3.1.2 中的公式也可以应用于黑色通道系统。

以下的方法基于“具有交叉校验的冗余”概念，如4.5.8 中的描述。这意味着，在安全报文的双重传输并在接收方内一个比特一个比特的进行比较情况下，未发现错误的前提条件是两个报文的损坏是相等的。残余错误概率可以通过附录 C 中方法进行计算。在这种情况下，每个报文内特定的比特错误组合的概率是相同的，因此，表达式被平方(squared) 。比特错误组合的概率与那些单个报文的相一致(二项式系数)。

FSCP 应调整个别措施，这样可假定最大的独立性。此外，有必要使用更复杂的考虑依赖性的公式。

当通过 CRC 签名获得数据完整性保证时相同的系数2^{-r}是有效的(见附录 C)， 并且公式(A.1)提供有关残余错误概率的估计：

$$R_{crc}(P_e) \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times (P_e^k \times (1-P_e)^{n-k})^2 \qquad (A.1)$$

在白色通道解决方案情况下，对于残余错误概率的完整评估必需依据 A.3.1.3 的分析以及使用公式(A.1)的计算。

注3：更多信息见IEC 62280。

根据 4.7.6.6.1 中式(6)计算$\lambda_{SCL}(P_e)$。

完整的安全评估应依据 GB/T 20438(例如：失效模式和影响分析，安全失效分数，共因错误)来完成。

A.3.1.3 模型 A 和模型 D

此方法依赖于现有总线传输通道的错误检测措施和补充措施，在分层的安全通信层中附加这些补充措施以达到所期望的 SIL。

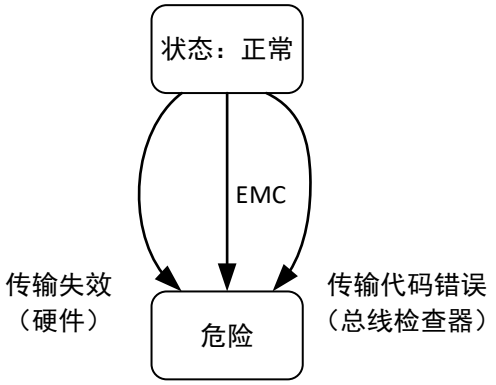


图 A.2 基本马尔科夫模型

在此方法中，安全风险是由于总线协议线路失效，因此必须考虑其硬件故障容许度，并从而考虑其期望的寿命。

在此情况下，马尔可夫分析可以得出三种基本转移的可能性(图A.2)：

- 未发现的故障报文，它是由传输层中的实际硬件失效引起从而导致损坏报文的传递(R_{HW})；
- 带有未发现比特错误的故障报文，它是由作为正常操作一个部分出现的电磁干扰(EMC)引起的(R_{EMC})；
- 未发现的故障报文，它是由传输通道的相应总线检查部件的失效引起(R_{TC})。

注1：马尔可夫分析源自IEC 62280。

注2：信道的参与错误概率RPSC及由此产生的$\lambda_{SCL}(P_e)$的相关计算详见IEC 62280。

完整的安全评估应依据GB/T 20438(例如：失效模式和影响分析，安全失效分数，共因错误)来完成。

注3：更多信息见IEC 62280。

附 录 B
（资料性）
显式和隐式 FSCP 安全措施示例

B.1 一般信息

第 B.2 至 B.7 节中的示例解释显式和隐式安全措施的概念。

B.2 含有安全PDU的现场总线报文示例

图 B.1 所示为传输时嵌入在现场总线报文中的安全 PDU。

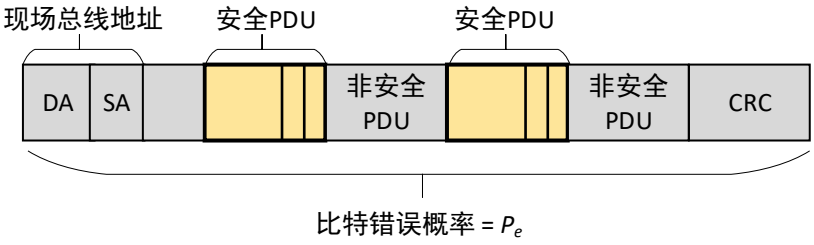


图 B.1 嵌入在现场总线报文中的安全 PDU 示例

B.3 全部显式安全措施的模型

图 B.2 示出了时效性和真实性全为显示措施的安全 PDU 的模型和安全检查。

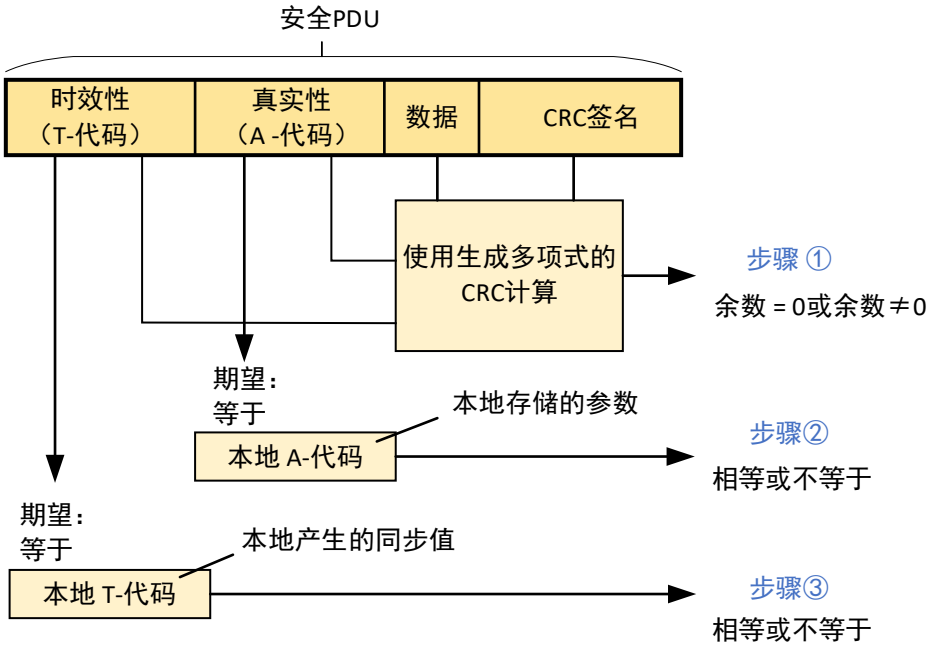


图 B.2 完全显式的安全措施的模型

依据以下步骤进行检查：

步骤 ① 余数 ≠ 0 → 检测到任何错误

余数 = 0 → 根据4.7.6.2.4的RR_I，判断数据正确或错误

步骤 ② 不相等 → 检测到任何错误

相等 → 根据4.7.6.3.3的RR_A，判断真实性正确或错误

步骤 ③ 不相等 → 检测到任何错误

相等 → 根据4.8.6.4.3的RR_T，判断时效性正确或错误

B.4 显式A-代码和隐式T-代码安全措施的模型

图 B.3 所示为真实性为显式安全措施，时效性为隐式安全措施的安全 PDU 的模型和安全检查。

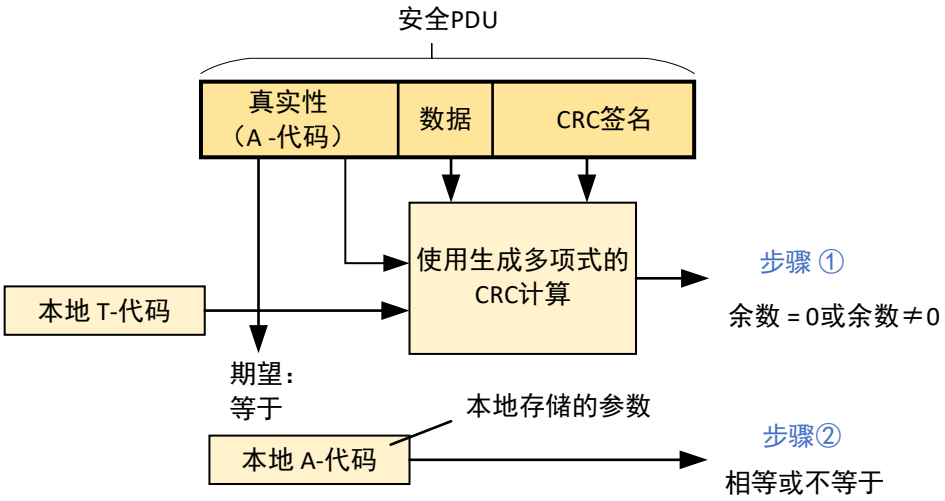


图 B.3 显式 A-代码和隐式 T-代码安全措施的模型

依据以下步骤进行检查：

步骤 ① 余数 ≠ 0 → 检测到任何错误

余数 = 0 → 根据特定RR，判断数据和时效性正确或错误

步骤 ② 不相等 → 检测到任何错误

相等 → 根据4.7.6.3.3的RR_A，判断真实性正确或错误

B.5 显式T-代码和隐式A-代码安全措施的模型

图 B.4 所示为时效性为显式安全措施，真实性为隐式安全措施的安全 PDU 的模型和安全检查。

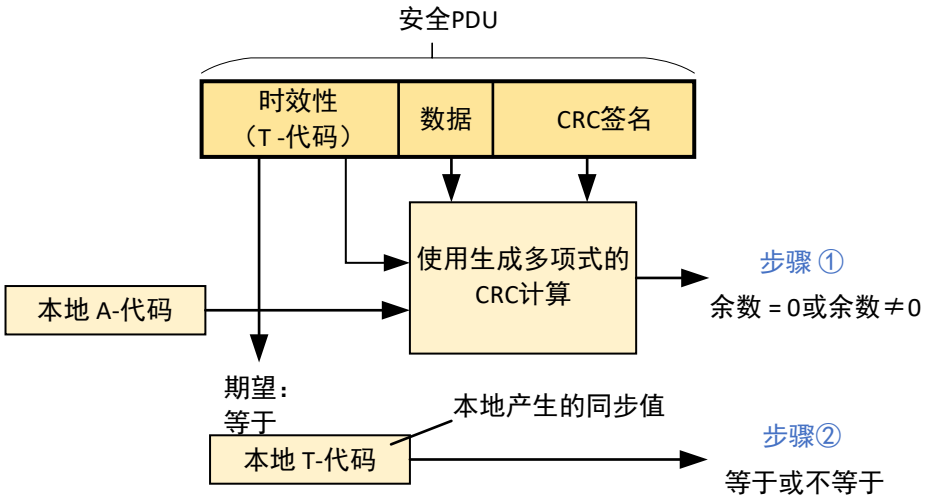


图 B.4 显式 T-代码和隐式 A-代码安全措施的模型

依据以下步骤进行检查：

步骤 ① 余数 ≠ 0 → 检测到任何错误

余数 = 0 → 根据特定*RR*，判断数据和真实性正确或错误

步骤 ② 不相等 → 检测到任何错误

相等 → 根据4.7.6.4.3的RR_7，判断时效性正确或错误

B.6 具有分离显式和隐式安全措施的模型

图 B.5 所示为时效性为分离显示和隐式安全措施，真实性为隐式安全措施的安全 PDU 的模型和安全检查，具有分离的显式和隐式时效性安全措施以及隐式真实性安全措施。

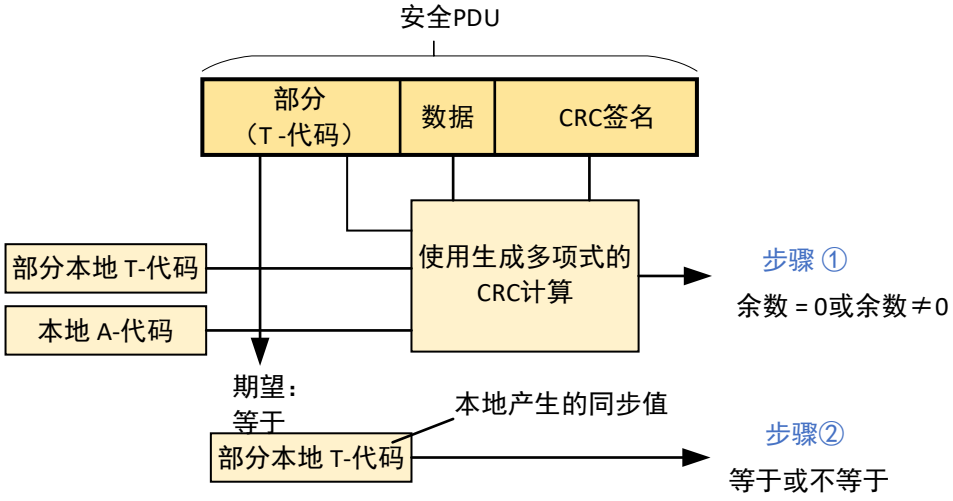


图 B.5 具有分离显式和隐式安全措施的模型

依据以下步骤进行检查：

步骤 ① 余数 ≠ 0 → 检测到任何错误

余数 = 0 → 根据特定*RR*，判断数据、真实性和时效性正确或错误

步骤 ② 不相等 → 检测到任何错误

相等 → 根据特定*RR*，判断时效性正确或错误

B.7 全部隐式安全措施的模型

图 B.6 所示为时效性和真实性全部为隐式措施的安全 PDU 的模型和安全检查。

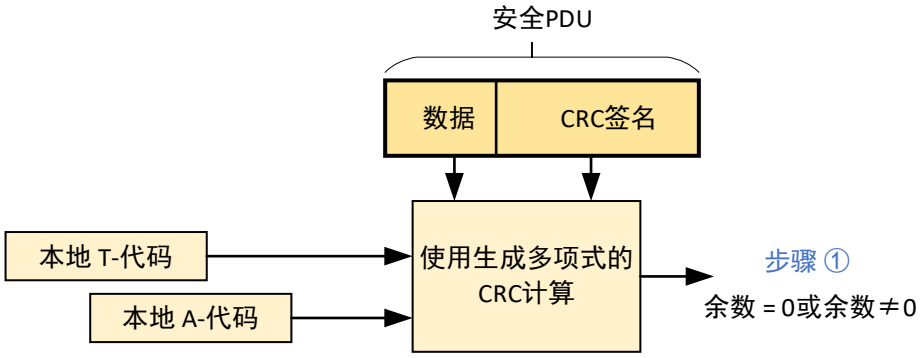


图 B.6 全部隐式的安全措施的模型

依据以下步骤进行检查：

步骤 ① 余数 ≠ 0 → 检测到任何错误

余数 = 0 → 根据特定*RR*，判断数据、真实性和时效性正确或错误

B.8 附录C的补充内容－隐式代码对适用性的影响

比特错误与不正确的隐式数据一起存在可能影响 CRC 多项式的适用性。因此，隐式措施的应用会导致额外的工作量。

由于存在各种可能的方法，所以无法提供通用公式。应由各 FSCP 来证明残余错误概率足够小。

附 录 C
（资料性）
使用基于 CRC 的错误校验的数据完整性计算

C.1 数据完整性残余错误概率RP_I

C.1.1 一般信息

RP_I是数据完整性的残余错误概率。

本文件提供了基于 CRC 进行错误校验以解决数据完整性问题的相关信息。使用基于 CRC 的错误校验时，约定 RP_I等于$R_{crc}(P_e)$。若采用其他措施计算数据完整性残余错误概率，FSCP 中应提供证明过程。

C.1.2 基于循环冗余校验的计算方法

使用循环冗余校验机制的安全总线，基于模型 B 和模型 C 的残余错误率计算推荐使用公式（C.1）。

$$R_{crc}(P_e) \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times (P_e^k \times (1-P_e)^{n-k})^2 \qquad (C.1)$$

其中：

P_e 比特错误概率（见附录 C.1.3）

d_{min} 最小海明距离（见附录 C.1.4）

n CRC 校验的数据块长度，包括 CRC 签名部分（见附录 C.1.5）

r CRC 签名长度（见附录 C.1.5）

基于模型 A 和模型 D 的残余错误率计算推荐使用公式（C.2）。

$$R_{crc}(P_e) \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times (P_e^k \times (1-P_e)^{n-k}) \qquad (C.2)$$

尚无已知保守近似公式可用于R_{crc}的通用计算。就连“保守”边界 2^{-r}也不能适用于所有多项式和所有R_{crc}值。

因此，应详细计算所选生成多项式的R_{crc}，如下所述。

- 对于使用的所有n值，都应计算R_{crc}。

注1：有时，仅计算R_{crc}还不够，比如对于最长报文长度。例如，对于部分较小的n值，多项式CCITT16（x16+x12+x5+1或0x11021）的R_{crc}值非常高。

注2：即使多项式适用于给定数据长度n，但仍可能不适用于其他数据长度（无论是更短还是更长的数据）。

- 在区间 $[2/n, 0.01]$ 内计算 Pe 所有相关值的R_{crc}。

注3：在某些情况下，R_{crc}不随P_e单调增长。

注4：有关使用2/n作为最小Pe的原因，请参见IEC 61784-3:2021的B.4.2引用文献[33]。

- 由此可见：
  - 如果 n <= 200，评估单一值 $P_e = 0.01$ 就足够了；
  - 如果 n >200，则应评估该区间内的多个值（至少 $2/n$、$4/n$、$8/n$、$16/n$，一直到 0.01）。

在选择 R_{CRC} 算法和计算过程中，应考虑数值稳定性（例如范围、精度、分辨率、误差传递），以免出现错误结果。例如，使用浮点数时，相同数量级数值求差，以及多个小数值求和，都可能出现问题。

CRC 编码对于突发型的电磁干扰具有很好的防护能力，能够检测出高达 CRC 签名比特长度数的任何突发错误。

C.1.3 比特错误概率

在持续的电磁干扰下，10^{-4} 的比特错误概率(P_e)将导致周期性数据交换的通信停止（误脱扣）（例如：经过多次尝试后看门狗时间超时）。通过正确的安装（例如屏蔽、等电位连接）这些误脱扣通常可被减少。

不推荐假设P_e为 10^{-4} 的安全层设计，因为在工业环境中常发生导致很多比特被破坏的单个突发干扰。

为检测出这些类型的干扰，错误检测机制应该足够有效以使要求的总残余错误概率是 10^{-4} 的 100 倍，即 10^{-2}。

因此，除非能够确切证明有一个更好的更低的错误概率（实际安装系统的物理测量结果和基于网络

连接可用性或长期稳定性相关讨论的理论考虑除外），否则，比特错误概率应使用最大值 10^{-2}。

对于高比特错误概率（接近 0.5），采用正确 CRC 多项式时，R_{crc}的极值为 2^{-r}（见 IEC 61784-3：2021 的 B.4.2 引用文献[73]）。

C.1.4 最小海明距离

通常，数据块比特长度n越小，CRC 机制的残余错误概率越好。因此，对于给定的合适的 CRC 多项式，数据块比特长度n与最小海明距离d_{min}有依赖关系。

FSCP 中应采用通过详细的计算或其他标准里经过证明的最小海明距离d_{min}。

示例：

表C.1所示为特定多项式（在本例中为0x1F29F）的不同d_{min}值所对应的数据块长度n的示例，多项式不同所产生的值也不同。

表 C.1 d_{min}与数据块比特长度 n 之间的依赖关系示例

d_{min}	n
12	17
8	18…22
6	23…130
4	131 … 258
2	259

C.1.5 CRC数据块长度和签名长度

值r表示增加到原始报文后面的 CRC 比特数，作为 CRC 签名以提供错误检测，如图 C.1 所示。

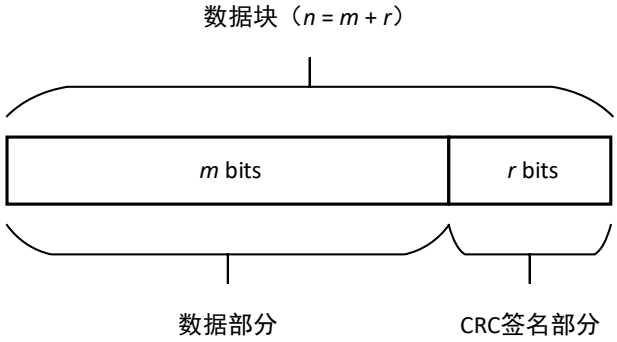


图 C.1 包含报文部分和 CRC 签名的数据块示例

附 录 D
（规范性）
安全措施的验证

D.1 一般信息

该部分规定了特定安全通信行规的验证要求。

D.2 实现

被安全传输的报文应以安全方式来产生(符合所必需的SIL) 。传输介质(例如：总线线路包含接口ASIC)本身被认为是不安全的。安全措施位于单独的负责报文源点和报文汇点的处理单元内。这涉及到白色和黑色通道解决方案。

评估：应考虑并检查GB/T 20438或其他附加标准(如：IEC61784-3)的要求。这些要求超出了此评估指南的范围，并被规范地定义。

D.3 默认安全动作

断电或未收到预期的安全报文时，SCL 及其相关设备应在规定的最长延迟时间内切换至规定安全状态。

示例1：一旦报文丢失，看门狗定时器将驱动其相关设备进入安全状态。

示例2：一旦断电，就会释放弹簧，以便实现制动或运动锁定。

评估：见 4.5.4。

D.4 安全状态

接收方应提供错误检测和反应机制，接收方在处理故障容许时间内负责建立安全相关的反应以达到安全状态。

评估：检查文件和执行；在系统的最坏情况下（例如，出现错误或发生故障）测量使用安全通信的安全设备的反应时间。

D.5 传输错误

在出现符合 4.4 的传输错误时，应启动某个确定的故障反应（比如：停止要求）。

评估：检查文件、执行，必要时进行计算，功能测试；根据 GB/T 20438 的扩展功能测试。

D.6 安全反应和响应时间

即使存在错误和故障，应不超过制造商规定的最大安全功能响应时间和完成安全相关反应所必需的时间。

注：在某些总线系统中，传输速率和反应或响应时间取决于参与方的个数。如果传输速率和反应或响应时间与安全相关，则它可能必须限制参与方的个数。

评估：检查文件和执行；在特定系统的最坏情况下，测量反应和/或响应时间。制造商或安全通信行规应提供被考虑的错误的数量定义和定时定义。

D.7 措施的组合

对于在总线系统上安全相关报文的传输，应使用这样的方法来实现 4.5 中引用的这些措施的组合，即在 4.5 中所述的每个错误在处理故障容许时间内被检测。表 2 有助于选择适当的个别措施。

评估:应根据表 2 对所使用的所有技术措施进行完整性验证。这些措施的实现应符合所要求的 SIL。

D.8 无干扰

应证明非安全相关通信参与方不会干扰安全通信参与方。

评估:应根据表 2 对所使用的所有技术措施进行完整性验证。这些措施的实现应符合所要求的 SIL。

D.9 附加的故障原因

除了已经描述的使用 BSC 模型评估残余错误概率方法外，还需考虑并控制进一步的故障原因，比

如物理层和数据链路层的“同步滑差”。

注：详细信息见 IEC 62280 或IEC 61784-3:2021的引用文献 [71]。

评估：该评估不在本文件范围内。

D.10 参考测试台和操作条件

只要切实可行，所有安全通信系统的部件应一起被测试。但是，如果分别测试安全通信系统各部件，则特定安全通信行规应定义参考系统（测试台）和/或仿真器，并且如可能，这些参考系统（测试台）和/或仿真器应由不同供应商的特定不同设备来实现。

测试台应考虑最坏情况条件，例如连接长度或设备数量。应模拟或实施安全功能所需的信号。在测试期间，应为用户定义有关操作模式，诸如，过程值的周期性数据交换或参数化数据的非周期性数据交换。

评估：根据特定 FSCP 的定义或 EUT 制造商的规范进行测试和检查。

D.11 一致性测试器

特定 FSCP 的一致性应通过行规一致性测试器来测试，该测试器由各 FSCP 定义和提供。

注：一致性测试包括正向测试和反向测试。

评估：根据特定 FSCP 的定义进行测试和检查。

参考文献

[1] GB/T 7588.2 电梯制造与安装安全规范 第 2 部分：电梯部件的设计原则、计算和检验
[2] GB/T 24807 电磁兼容 电梯、自动扶梯和自动人行道的产品系列标准 发射
[3] GB/T 26336—2010 工业通信网络 工业环境中的通信网络安装(IEC 61918:2007, IDT)
[4] IEC 60050(所有部分) International Electrotechnical Vocabulary
[5] IEC 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4:Definitions and abbreviations
[6] IEC 61508-5:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5:Examples of methods for the determination of safety integrity levels
[7] IEC 61784-3 Edition 4.0 2021 Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions
[8] IEC/TR 62059-11:2002 Electricity metering equipment – Dependability – Part 11:General concepts
[9] IEC/TR 62210:2003 Power system control and associated communications – Data and communication security
[10] IEC 62280:2014 Railway applications – Communication, signalling and processing systems –Safety related communication in transmission systems
[11] ISO/IEC 2382-16:1996 Information technology – Vocabulary – Part 16:Information theory.
[12] ISO 13849-1:2015 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
[13] TSG T7007 电梯型式试验规则
[14] ANDREW S.TANENBAUM, DAVID J.VETHERALL, Computer Networks, 5th Edition, Prentice Hall, N.J., ISBN-10:0132126958, ISBN-13:978-0132126953
[15] W.WESLEY PETERSON, EDWARD J.WELDON, Error-Correcting Codes, 2nd Edition 1972, MIT—Press, ISBN 0-262-16-039-0

中国电梯协会标准
电梯和自动扶梯、自动人行道功能安全现场总线技术基本要求
T/CEA 0060—2025

*

中国电梯协会
地址：065000 河北省廊坊市金光道 61 号
Add：61 Jin-Guang Ave.，Langfang，Hebei 065000，P.R. China
电话/Tel：（0316）2311426，2012957
传真/Fax：（0316）2311427
电子邮箱/Email：info@cea-net.org
网址/URL：http://www.elevator.org.cn