ICS 25.040
CCS N10

中华人民共和国国家标准

GB/T XXXXX—XXXX
代替GB/Z 37085-2018

工业通信网络 行规 第3-8部分:CC-Link系列功能安全通信行规

Industrial communication network - Profile - Part3-8: Functional safety communication profile of CC-Link family

(IEC 61784-3-8:2021, Industrial communication network - Profile - Part3-8: Functional safety communication profile of CC-Link family，IDT)

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件等同采用IEC 61784-3-8:2021《工业通信网络 行规 第3-8部分：功能安全现场总线 用于CPF8的附加规范》。

本文件作了如下编辑性修改:

——删除了标准的前言;

——“本部分”改为“本文件”;

——对全文范围内列项的标点符号进行规范。

本文件代替GB/Z 37085-2018《工业通信网络 行规 第3-8部分：CC-LINK系列功能安全通信行规》,与GB/Z 37085-2018相比，除结构调整和编辑性改动外，主要技术变化如下:

a）更改了帧格式，除复制安全数据，还采取一些措施如增加时间戳的存储数位的有关规定，新增匹配比较过程（见12.5.3，2018年版的11.5.3）；

b）更改了残差率的变化模型，以及残差率计算方式（见附录A，2018年版11.9.5.2）；

c）更改了完整性保证中有关使用安全PDU中包含的CRC以保证数据完整性的相关描述（见11.5.3.6，2018年版10.2.3.6）；

d）增加了有关交叉校验冗余的有关内容（见11.5.3.7）；

e）增加了过程数据SAR ASEs有关M1 安全循环传输类规范和S1 安全循环传输类规范表格（见11.6.4）；

f）更改了抽象语法中有关M1和S1安全循环传输有关语法内容（见11.7.1.2，2018版11.7.1.2）；

g）更改了传输语法中有关M1和S1安全设备管理器属性编码有关内容（见11.7.1.3，2018版11.7.1.3）；

h）删除了系统特征计算的约束中有关残差率的描述（见2018版11.9.5）；

i）更改了FSCP 8/2中所有TS为T_code（见第12章，2018版第12章）；

j）更改了FSCP 8/2安全措施中有关讹误交叉检验，以及意外重复出现时的处理方法等有关内容（见12.4.2，2018版12.4.2）；

k）更改了FSCP 8/2安全措施中有关伪装交叉检验的有关内容（见12.4.2.8，2018版12.4.2.8）；

l）增加了FSCP 8/2安全通信层协议，CTRL结构元素中，有关Application bit, Sub CID active bit以及Sub CID的有关描述（见12.7.1.2）；

m）增加了S-Data的结构中，有关安全刷新数据Safety_data的要求与描述（见12.7.1.6.1）；

n）更改了FSCP 8/2安全通信层协议的行为中，有关安全初始化的有关要求（见12.1.6.1.7.1，2018版12.1.6.1.7.1）；

o）更改了FSCP 8/2的系统要求中有关系统特性计算约束的相关要求，移除了有关站的数量、概率考虑部分条款（见12.9.5，2018版12.9.5）；

p）增加了附录A中有关FSCP 8/1的CRC残余误差概率的对照表（见附录A，2018版见附录A）。

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专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会（SAC/TC 124）归口。

本文件起草单位:

本文件主要起草人:

引　　言

IEC 61158 现场总线标准与其配套标准 IEC 61784-1 和 IEC 61784-2 共同定义了一组通信协议以实现自动化应用的分布式控制。现场总线技术目前已被普遍接受并证明可行。因此，很多现场总线技术不断提升，覆盖了尚未标准化的领域，如实时、功能安全相关和信息安全相关的应用。

IEC 61784-3 系列标准依据 IEC 61508 系列标准，说明了功能安全通信相关原理，规范了基于 IEC 61784-1，IEC 61784-2 和 IEC 61158 系列标准的通信行规和协议层的若干安全通信层（行规和对应协议），但不包括电气安全和本质安全方面内容，也不包括信息安全方面内容，且不提供信息安全的任何要求。

图 1 给出了 IEC 61784-3 系列标准与机械环境中相关安全和现场总线标准之间的关系。

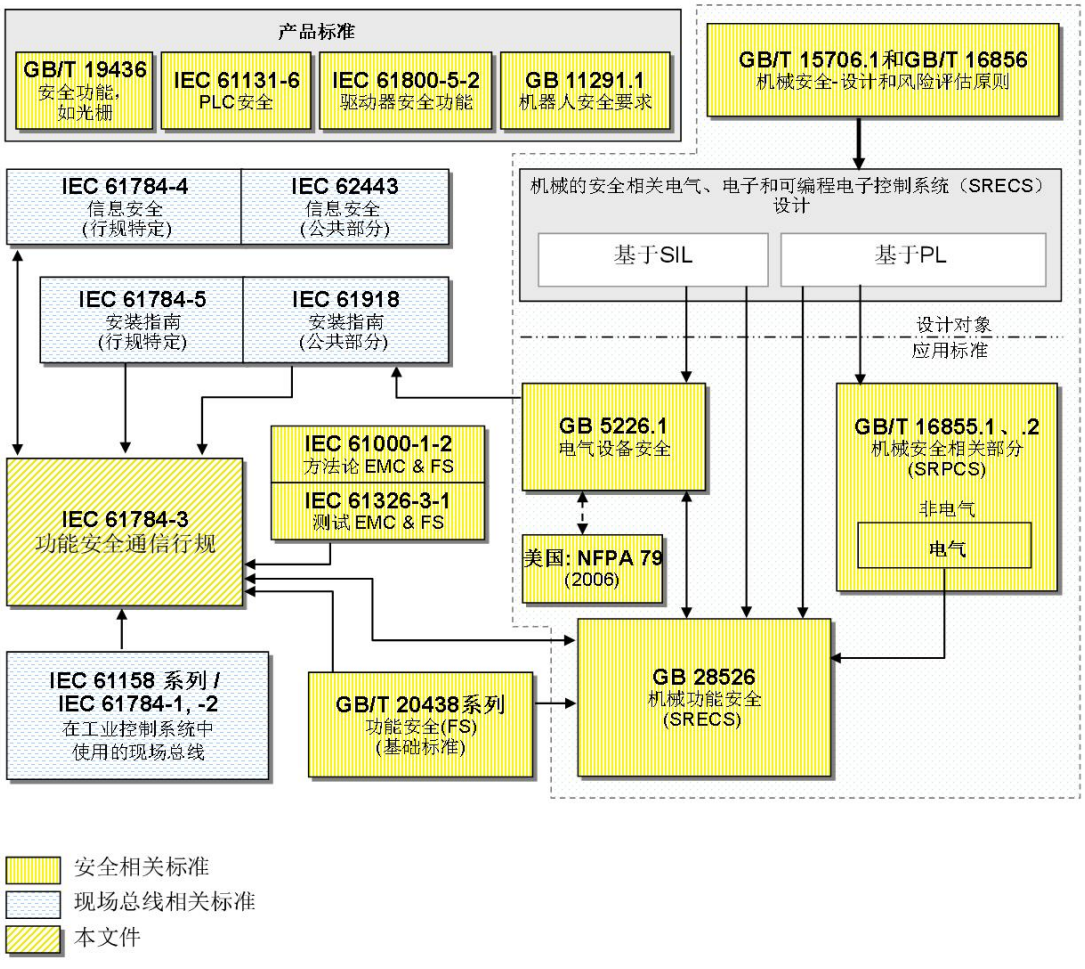

图 1　IEC 61784-3 与其他标准（机械）的关系

注:GB 28526 中 6.7.6.4（高复杂性）和 6.7.8.1.6（低复杂性）规定了 PL（类别）和 SIL 的关系

图 2 给出了 IEC 61784-3 系列标准与过程环境中相关安全与现场总线标准间的关系。

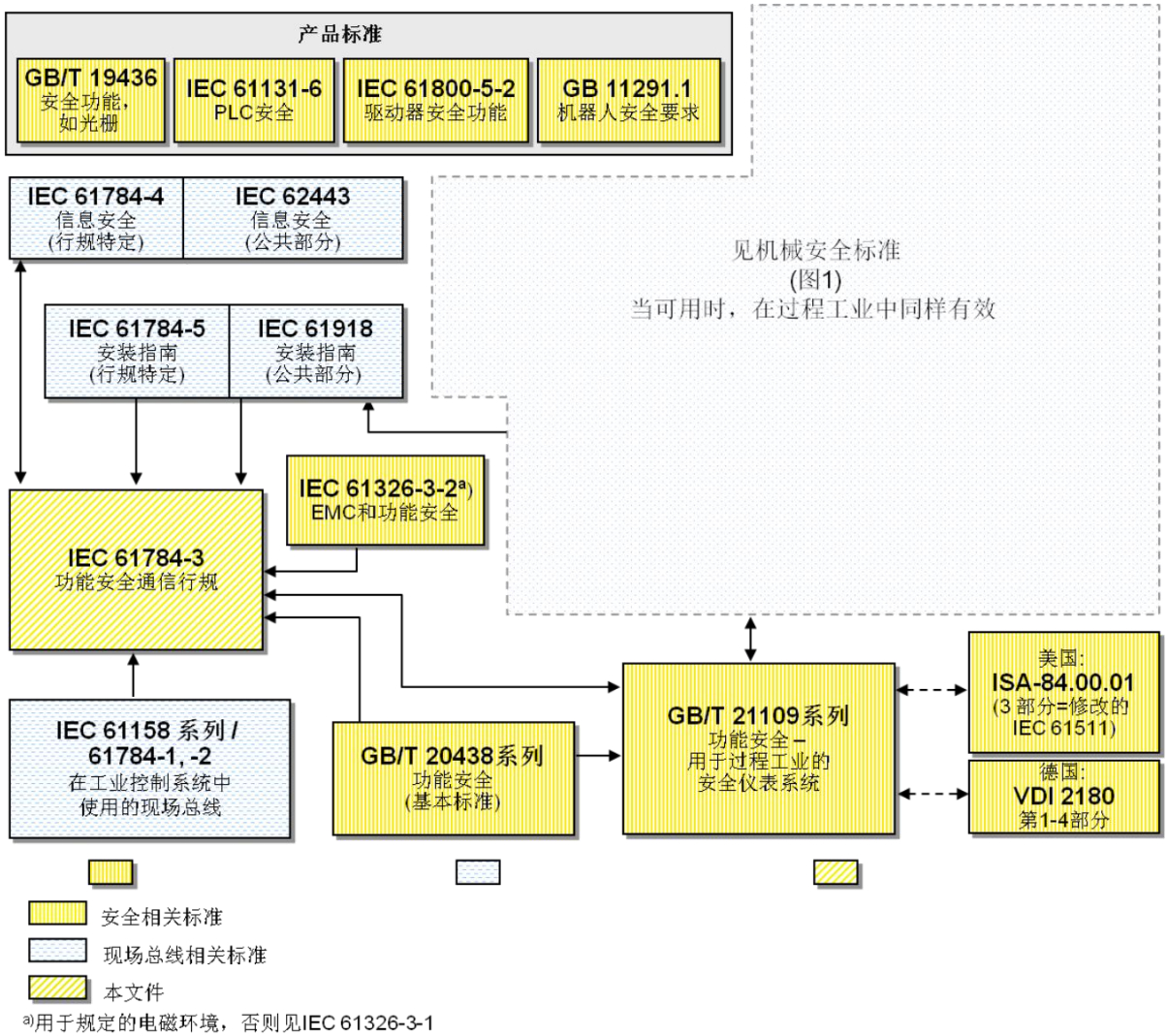

图 2　IEC 61784-3 与其他标准（过程）的关系

根据 IEC 61508 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者之间传输报文（信息）提供了必要的可信度，或为现场总线错误或失效事件中的安全行为提供了足够可信度。

IEC 61784-3 系列标准规定的安全通信层，使现场总线可以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。

一个系统最终的 SIL 声明取决于该系统内所选择的功能安全通信行规的实现——在标准设备中实现的功能安全通信行规不足以证明该设备是安全设备。

IEC 61784-3 系列标准描述了：

——实现 IEC 61508 系列标准对安全相关数据通信要求的基本原则，包括可能的传输故障、补救措施和对影响数据完整性的考虑；

——IEC 61784-1 和 IEC 61784-2 中多个通信行规族的功能安全通信行规，包括对 IEC 61158 系列标准中通信服务和协议部分的安全层扩展。

工业通信网络 行规 第3-8部分:CC-Link系列功能安全通信行规

1 范围

本文件规定了基于IEC 61784-1、IEC 61784-2以及IEC 61158类型18与类型23的CPF 8的安全通信层（服务和协议），并标识出在IEC 61784-3中定义的功能安全通信原理与本文件中的安全通信层是相关的。该安全通信层仅在安全设备中实现。

注1：不包括电气安全和本质安全方面内容。电气安全涉及如电击的危险。本质安全涉及潜在爆炸性环境相关的危险。

本文件定义了在使用现场总线技术的分布式网络内的参与者之间传输安全相关报文的机制，该机制符合IEC 61508系列标准对于功能安全的要求。这些机制可用于各种工业应用，如过程控制、制造自动化和机械。

本文件为遵循本文件的设备和系统的开发者和评估者提供指导。

注2：一个系统最终的SIL声明取决于该系统内所选择的功能安全通信行规的实现——在标准设备中依据本文件实现功能安全通信行规不足以证明该设备具有安全设备的资格。

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 61131-2 工业过程测量和控制 - 可编程控制器 - 第2部分：设备要求和测试（Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests）

IEC 60204-1 机械电气安全 机械电气设备 第1部分:通用技术条件（Safety of machinery - Electrical equipment of machines - Part 1: General requirements）

IEC 61131-3 可编程序控制器 第3部分:编程语言（Programmable controllers - Part 3: Programming languages）

IEC 61158（所有部分） 工业通信网络 现场总线规范（Industrial communication networks - Fieldbus specifications）

IEC 61158-2 工业通信网络 现场总线规范 第2部分:物理层规范和服务定义（Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition）

IEC 61158-3-18 工业通信网络 现场总线规范 第3-18部分:数据链路层服务定义 类型18元素（Industrial communication networks - Fieldbus specifications - Part 3-18: Data-link layer service definition - Type 18 elements）

IEC 61158-4-18 工业通信网络 现场总线规范 第4-18部分:数据链路层协议规范 类型18元素（Industrial communication networks - Fieldbus specifications - Part 4-18: Data-link layer protocol specification - Type 18 elements）

IEC 61158-5-18 工业通信网络 现场总线规范 第5-18部分:应用层服务定义 类型18元素（Industrial communication networks - Fieldbus specifications - Part 5-18: Application layer service definition - Type 18 elements）

IEC 61158-5-23 工业通信网络 现场总线规范 第5-23部分:应用层层服务定义 类型23元素

（Industrial communication networks - Fieldbus specifications - Part 5-23: Application layer service definition - Type 23 elements）

IEC 61158-6-18　工业通信网络 现场总线规范 第6-18部分:应用层协议规范 类型18元素（Industrial communication networks - Fieldbus specifications - Part 6-18: Application layer protocol specification - Type 18 elements）

IEC 61158-6-23　工业通信网络 现场总线规范 第6-23部分:应用层协议规范 类型23元素（Industrial communication networks - Fieldbus specifications - Part 6-23: Application layer protocol specification - Type 23 elements）

IEC 61326-3-1　测量、控制和实验室用电气设备- EMC要求-第3-1部分:安全相关系统和执行安全相关功能（功能安全）设备的抗扰要求-一般工业应用(Electrical equipment for measurement, control and laboratory use -EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) - General industrial applications)

IEC 61326-3-2　测量、控制和实验室用电气设备- EMC要求-第3-2部分:安全相关系统和执行安全相关功能(功能安全)设备的抗扰要求-具有特定电磁环境的工业应用(Electrical equipment for measurement, control and laboratory use -EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) - Industrial applications with specified electromagnetic environment)

IEC 61508(所有部分)　电气/电子/可编程控制电子安全相关系统的功能安全（Functional safety of electrical/electronic/programmable electronic safety-related systems）

IEC 61511(所有部分)　功能安全-过程工业行业安全仪表系统（Functional safety - Safety instrumented systems for the process industry sector）

IEC 61784-1　工业通信网络行规 第1部分:现场总线行规（Industrial communication networks - Profiles - Part 1: Fieldbus profiles）

IEC 61784-2　工业通信网络 行规 第2部分: 基于ISO/IEC 8802-3的实时网络的附加现场总线行规（Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3）

IEC 61784-3　工业通信网络 行规 第3部分:功能安全现场总线 一般规则和行规定义(Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions)

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（Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems）

IEEE 802.3 IEEE　信息技术标准 系统间的通信和信息交换 局域网和城域网 特定要求 第3部分:带有冲突检测的载波监听多路访问（CSMA/CD）访问方法和物理层规范（IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method And Physical Layer Specifications）

3　术语、定义、符号、缩略语和约定

3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1　通用术语和定义

3.1.1.1

绝对时间戳 absolute time stamp

参考全局时间的时间戳，该全局时间对于现场总线中的一组设备是通用的。

[来源:IEC 62280:2014，定义 3.1.1，有修改]

3.1.1.2

有源网络元件 active network element

包括电和（或）光的有源组件的网络元件，用于网络扩展。

注： 有源网络元件例如中继器和交换机。

[来源:IEC 61918:2013，定义 3.1.2]

3.1.1.3

误比特率（Pe） bit error probability（Pe）

接收到特定比特出现不正确值的概率。

3.1.1.4

黑色通道 black channel

无需依据 GB/T 20438 获得设计或验证证明的包含一个或多个元件的通信系统。

注： 该定义扩展了通道的一般含义，以包括那些包含通道的系统。

3.1.1.5

桥 bridge

在数据链路层连接多个网段的抽象设备。

3.1.1.6

封闭的通信系统 closed communication system

由固定数量或固定最大数量的参与者构成的通信系统，该通信系统具有明确的固定属性，并且不考虑未授权访问的风险。

[来源:IEC 62280:2014，定义 3.1.6]

3.1.1.7

通信通道 communication channel

一个通信系统内两个端点之间的逻辑连接。

3.1.1.8

通信系统 communication system

由硬件、软件和传输媒体组成，以允许将报文（ISO/IEC 7498-1 应用层）从一个应用传输到另一个应用。

3.1.1.9

连接 connection

在相同或不同设备内的两个应用对象间的逻辑连接。

3.1.1.10

循环冗余校验（CRC） Cyclic Redundancy Check（CRC）

值——为检测数据讹误，从某个数据块得到并与该数据块一起存储或传输的冗余数据。

方法——用于计算冗余数据的规程。

注 1：本文件中还使用术语“CRC 代码”、“CRC 签名”，以及符号（如 CRC1 和 CRC2）来指示冗余数据。

注 2：参见参考文献[26]和参考文献[27]。

3.1.1.11

确定的通信系统（确定通道） defined communication system (defined channel)

由固定数量或固定最大数量的参与者通过现场总线链接构成的通信系统，该通信系统具有明确的固定属性，如安装条件、电磁抗扰性和工业（有源）网络元件，并且根据 IEC 62443 系列标准中的全生命周期模型，如使用区域和管道技术，将未授权访问的风险减少至可容忍程度。

3.1.1.12

多样性 diversity

执行所要求功能的不同方法。

注： 多样性可通过不同物理方法或不同设计方法实现。

[来源:IEC 61508-4:2010，定义 3.3.7]

3.1.1.13

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。

注 1：错误可能是由于硬件/软件内的设计失误，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。

[来源:61508-4:2010，定义 3.6.11，有修改]

3.1.1.14

失效 failure

功能单元执行一个要求功能之能力的终止，或功能单元在任何非要求方式下的操作。

注： 失效可能是由一个错误（如硬件/软件设计或报文破坏的问题）引起的。

[来源:IEC 61508-4:2010，定义 3.6.4，有修改]

3.1.1.15

故障 fault

可能导致功能部件执行所需功能的能力下降或丧失的异常状态。

注： IEC 60050-191:1990,191-05-01 定义“故障”是一种无能力执行要求功能的特征状态，不包括预防性维护或其他按计划行动期间的无能力或外部资源缺少产生的无能力。

[来源:IEC 61508-4:2010，定义 3.6.1，有修改]

3.1.1.16

现场总线 fieldbus

基于串行数据传输并用在工业自动化或过程控制应用中的通信系统。

3.1.1.17

现场总线系统 fieldbus system

使用现场总线连接设备的系统。

3.1.1.18

帧校验序列 frame Check Sequence（FCS）

为检测数据讹误，使用哈希函数从 DLPDU（帧）内的数据块得到并与该数据块一起存储或传输的冗余数据。

注 1：FCS 可由 CRC 或其他哈希函数得到。

注 2：见参考文献[26]、参考文献[27]。

3.1.1.19

哈希函数 hash function

一个（数学）函数，将一个（可能非常）大的数值集映射成（通常）较小范围的数值集。

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 62210:2013，定义 4.1.12，有修改]

3.1.1.20

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。

注： 该术语包括在短时间内对人员产生的危险(例如火灾和爆炸), 以及那些对人的健康有长期影响的物质 (例如，有毒物质的释放）。

3.1.1.21

主站 master

能够发起和调度其他站（可能是主站或从站）通信活动的主动通信实体。

3.1.1.22

报文 message

用于传送信息的有序八位位组序列。

[来源:ISO/IEC 2382:2016，定义 16.02.01，有修改]

3.1.1.23

信宿 message sink

接收报文的那部分通信系统。

[ISO/IEC 2382-16:1996，16.02.03]

3.1.1.24

信源 message source

发起报文的那部分通信系统。

[ISO/IEC 2382-16:1996，16.02.02]

3.1.1.25

性能等级（PL）performance level（PL）

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的离散等级。

[来源:ISO 13849-1:2006，定义 3.1.23]

3.1.1.26

冗余 redundency

存在一种以上用于执行同一规定功能或表达信息的方法。

注： 改写 IEC 61508-4:2010，3.4.6，删除的示例和注释。

3.1.1.27

相对时间戳 relative time stamp

参考实体的本地时钟的时间戳。

注： 通常与其他实体的时钟无关。

3.1.1.28

残差概率（RP） residual error probability（RP）

SCL 安全措施未发现的错误的概率。

3.1.1.29

残差率 residual error rate

SCL 安全措施未能检测出错误的统计率。

3.1.1.30

风险 risk

出现伤害的概率与该伤害严重性的组合。

注 1：见 IEC 61508-5:2010 的附录 A。

注 2：改写 ISO/IEC Guide 51:2014,3.9。[IEC 61508-4:2010，3.1.6]

3.1.1.31

安全通信通道 safety communication channel

起始于信源顶部 SCL，终止于信宿顶部 SCL 的通信通道。

注：可被模型化为由一个黑色通道、一个特定通信系统或者一个特定通道所连接的两个 SCL。

3.1.1.32

安全通信层（SCL） safety communication layer （SCL）

在 FAL 之上的通信层，包括根据 IEC 61508 保证数据安全传输的所有必要措施。

3.1.1.33

安全连接 safety connection

使用安全协议进行通信事务处理的连接。

3.1.1.34

安全数据 safety data

使用安全协议在安全网络中传输的数据。

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。

3.1.1.35

安全设备 safety device

依据 IEC 61508 进行设计并实现功能安全通信行规的设备。

3.1.1.36

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，其目的是在发生特定危险事件时，达到或保持 EUC 的安全状态。

注：改写 IEC 61508-4:2010,3.5.1。

3.1.1.37

安全功能响应时间 safety function response time

当安全功能通道出现错误或故障时，从与现场总线相连的安全传感器启动，到其安全执行器达到相应的安全状态之前，最差情况持续的时间。

注：该定义在 IEC 61784-3 的 5.2.4 给出，本文件定义的功能安全通信行规进行说明。

3.1.1.38

安全完整性等级（SIL） safety integrity level（SIL）

对应于安全完整性值的范围的离散等级（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，1 为最低等级。

注 1：4 种安全完整性等级的目标失效措施（见 IEC 61508-4:2010 的 3.5.17）在 IEC 61508-1:2010 的表 2 和表 3 中规定。

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

注 3：安全完整性等级（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。[IEC 61508-4:2010，3.5.8]

3.1.1.39

安全措施 safety measure

控制可能的通信错误的措施，该措施的设计和实现符合 IEC 61508 的要求。

注 1：实际上，结合若干安全措施可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 IEC 61784-3 的 5.3 和 5.4 中详细介绍。

3.1.1.40

安全 PDU（SPDU） safety PDU(SPDU)

在安全通信通道中传输的 PDU。

注 1：SPDU 可包含多于一个的安全数据（使用不同的编码结构和哈希函数）副本和明确的附加保护部分，如密钥、序列数或时间戳。

注 2：冗余的 SCL 提供两个不同版本的 SPDU，插入现场总线帧的分离的字段中去。

3.1.1.41

安全相关应用 safety-related application

为满足应用的 SIL 要求，根据 IEC 61508 设计的程序。

3.1.1.42

安全相关系统 safety-related system

根据 IEC 61508 执行安全功能的系统。

3.1.1.43

从站 slave

能够接收报文并将报文发送给另一个通信实体(主站或从站)的通信实体，但不能发起通信。

3.1.1.44

假脱扣 spurious trip

无过程要求而由安全系统引起的脱扣。

3.1.1.45

时间戳 time stamp

包含在报文中的时间信息。

3.1.1.46

均匀分布 uniform distribution

有限集合中的所有值可能以相同概率发生的概率分布。

注：对于一个比特长度为 i 的字段，一个特定字段值的发生概率为 2-i，因为所有发生概率之和等于 1。

3.1.1.47

白色通道 white channel

特定的通信系统。在这个系统中，所有相关的硬件和软件都根据 IEC 61508 进行设计、实施和验证。

注：该定义扩展了通道的一般含义，用以包括那些包含通道的系统。

3.1.2 **附加术语和定义**

3.1.2.1

周期 cycle

重复并连续执行一系列命令或动作的时间间隔。

3.1.2.2

安全应用关系 （SAR）safety application relationship(SAR)

两个或多个安全相关应用关系端点之间的应用关系。

3.1.2.3

安全应用服务元素 （SASE）safety application service element(SASE)

安全相关的应用服务元素。

3.1.2.4

安全时钟 safety clock

记录事件（如安全通信相关报文的传输和接收）发生时间的时钟（计数器）。

3.1.2.5

安全数据监视定时器 safety data monitor timer

用于安全数据传输的时间期望值功能所使用的定时器。

3.1.2.6

安全监视定时器 safety monitor timer

用于安全连接管理的时间期望值功能所使用的定时器。

3.1.2.7

安全刷新 safety refresh

主站和从站之间安全数据的周期性传输和接收。

3.1.2.8

槽 slot

循环数据字段的位置相关映射的最小单位（粒度）。

3.1.2.9

站 station

安全数据的传输和接收相关的设备及其 SAREP。

注： 循环数据字段的位置相关映射中所使用的站号（一个站占用一个或多个槽）。

3.1.2.10

安全协议传输信息 safety protocol transmission information

区别安全相关报文的信息。

3.2 符号和缩略语

3.2.1 通用符号和缩略语

A-code	Authentication code	验证码	
CP	Communication Profile	通信行规	[IEC 61784-1]
CPF	Communication Profile Family	通信行规族	[IEC 61784-1]
CRC	Cyclic Redundancy Check	循环冗余校验	
DLL	Data Link Layer	数据链路层	[GB/T 9387.1]
DLPDU	Data Link Protocol Data Unit	数据链路协议数据单元	
EMC	Electromagnetic Compatibility	电磁兼容	
EUC	Equipment under Control	受控设备	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	电气/电子/可编程电子	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	现场总线应用层	[IEC 61158-5 (all parts)]
FS	Functional Safety	功能安全	
FSCP	Functional Safety Communication Profile	功能安全通信行规	
FSPM	FAL Service Protocol Machine	FAL 服务协议机	[IEC 61158-1]
MTBF	Mean Time Between Failures	平均失效间隔时间	
MTTF	Mean Time To Failure	平均失效时间	
PDU	Protocol Data Unit	协议数据单元	[GB/T 9387.1]
Pe	Bit error probability	误比特率	
PhL	Physical Layer	物理层	[GB/T 9387.1]
PL	Performance Level	性能等级	[ISO 13849-1]
PLC	Programmable Logic Controller	可编程逻辑控制器	
SCL	Safety Communication Layer	安全通信层	

SIL	Safety Integrity Level	安全完整性等级	[IEC61508-4:2010]
SPDU	Safety PDU	安全 PDU	
T-code	Timeliness code	时效性代码	

3.2.2 附加符号和缩略语

AR	Application Relationship	应用关系
ASE	Application Service Element	应用服务元素
CC	Carry Counter	进位计数器
CID	Connection Identifier	连接标示符
CMD	Command Data	命令数据
LED	Light Emitting Diode	发光二极管
LID	Link Identifier	链接标识符
OBL	Offset Base Line	偏移基线
RNO	Running Number	运行号
SAR	Safety Application Relationship	安全应用关系
SAREP	Safety Application Relationship Endpoint	安全应用关系端点
SARPM	Safety Application Relationship Protocal State Machine	安全应用关系协议状态机
SASE	Safety Application Service Element	安全应用服务元素
SFSPM	Safety FSPM（appended with -S Slave Or -M Master)	安全 FSPM（后缀-S 标识从站或后缀-M 表示主站）
SRC	Safety Relevant Controller	安全相关控制器
SRP	Safety Relevant Peripheral	安全相关外围设备
TPI	Safety Transmission Packet Information	安全传输包信息
TPI-T	Safety Transmission Packet Information from master	主站的安全传输包信息
TPI-R	Safety Transmission Packet Information from slave	从站的安全传输包信息
TS	Time Stamp	时间戳

3.3 约定

本文件使用的约定在IEC 61158 类型18和类型23，以及IEC 61784-1 CPF8和IEC 61784-2 CPF8中定义。

为了帮助读者熟悉本文件的章条编号，并与IEC 61784-3保持一致，第4章至第10章参考FSCP 8/1的第11章至第17章，FSCP 8/2的第18章至第24章。

4 概览

对于FSCP 8/1，见11.4。对于FSCP8/2，见12.4。

5 概述

对于FSCP 8/1，见11.5。对于FSCP 8/2，见12.5。

6 安全通信层服务

对于FSCP 8/1，见11.6。对于FSCP8/2，见12.6。

7 安全通信层协议

对于FSCP 8/1，见11.7。对于FSCP8/2，见12.7。

8 安全通信层管理

对于FSCP 8/1，见11.8。对于FSCP8/2，见12.8。

9 系统要求

对于FSCP 8/1，见11.9。对于FSCP8/2，见12.9。

10 评估

对于FSCP 8/1，见11.10.对于FSCP8/2，见12.10。

11 FSCP 8/1

11.1 范围-FSCP 8/1

见第1章。

11.2 规范性引用文件-FSCP 8/1

见第2章。

11.3 术语、定义、符号、缩略语和约定-FSCP 8/1

见第3章。

11.4 FSCP 8/1 概览（CC-Link Safety）

通信行规族8（一般指CC-Link）定义了基于IEC 61158-2类型18，IEC 61158-3-18，IEC 61158-4-18，IEC 61158-5-18和IEC 61158-6-18的通信行规。

基本行规CP 8/1，CP 8/2和CP 8/3在IEC 61784-1中定义。CPF 8功能安全通信行规FSCP 8/1基于IEC 61784-1中CPF 8基本行规和本文件中定义的安全通信层规范。

FSCP 8/1是一种在使用现场总线技术的分布式网络中用于参与者之间安全相关数据（如急停信号）通信的协议，符合IEC 61508的功能安全要求。该协议可用于各种应用，如过程控制、制造自动化和机械装置。

FSCP 8/1协议使用CPF 8通过实现序列号、时间期望值、连接身份验证、报文回送、数据完整性保证和不同数据完整性保证安全措施，从而支持安全完整性等级SIL3（见IEC 61508）。

FSCP 8/1的SCL能力通过引入安全应用服务元素（SASE）来提供。这些SASE被用在如本文件所规定的其相应的ASE位置。SASE来源于CPF8中的定义，本文件用于规范CPF8的安全专用部分。

11.5 FSCP 8/1 概述

11.5.1 为行规提供规范的外部文件

鼓励FSCP 8/1安全设备的制造商查阅文献[30]、[31]和[32]，这些文献提供了有关实现本文件中定义的SCL的附加规范。

11.5.2 安全功能要求

FSCP 8/1为基于IEC 61158类型18的功能安全通信系统规定了服务和协议。在本文件中规定的通信技术仅在依据IEC 61508的要求所设计的设备中实现。

如下要求适用于实现FSCP 8/1协议的设备开发，并且也在FSCP 8/1开发中使用：

——FSCP 8/1 协议支持安全完整性等级 SIL 3（见 IEC 61508）；

——FSCP 8/1 的实现应遵循 IEC 61508；

——对开发 FSCP 8/1 协议的基本要求见 IEC 61784-3；

——离散数据的安全状态是失电状态（0）。对于模拟值，失电状态应由安全相关应用定义；

——除非具有特定的产品标准，否则，对于基本等级，环境条件应符合 IEC 61131-2；对于安全裕度测试，环境条件应符合 IEC 61326-3-1 和 IEC 61326-3-2；

——除非本文件中规定，否则对于安全性 CPF 8 的要求应保持不变。

11.5.3 安全措施

11.5.3.1 概述

在本文件中定义的安全通信层为实现其安全通信层，提供了如下确定性补救措施：

——序列号；

——时间期望值；

——连接身份验证；

——报文回送；

——数据完整性保证；

——交叉校验冗余；

——不同数据完整性保证系统。

表1列出了对可能发生错误的各种检测措施。

表 1 对可能发生错误的各种检测措施

通信错误	确定性检测措施							
	序列号	时间戳	时间期望值	连接身份验证	报文回送	数据完整性保证	交叉校验冗余	不同数据完整性保证系统
讹误						X	X	
非预期重复	X							
错序	X							
丢失	X							
不可接受的延迟			X					
插入	X			X	X			
伪装				X	X		X	X
寻址				X				

注:见IEC 62280:2014

11.5.3.2 序列号

安全报文包含一个24比特的指定顺序的序列号（RNO）（见11.7.1和11.7.2）。这个RNO由RNO-1（4比特）、RNO-2（4比特）和 RNO-3（16比特）组成。如果不按这个顺序，则所有安全相关输出信号应设置为安全状态。

11.5.3.3 时间期望值

一个集成的看门狗定时器给每个安全输出从站的每个输出通道提供时间期望值,从而保证了安全功能的响应时间,即在安全输入从站监测到事件和在安全输出从站的相应输出通道的响应之间的时间，见11.9.3。

安全功能响应时间包含从安全输入从站到主站的现场总线传输时间和从安全主站到安全输出从站的现场总线传输时间，包括由于传输错误导致的安全PDU重复、安全输出从站上的处理时间和安全相关控制器（SRC）内的处理时间。

如果安全输出从站的特定输出通道的安全功能响应时间超时,那么对应的输出通道就设定为安全状态，通常是电源断电状态。SRP的应用层应监测到这些。

11.5.3.4 连接身份验证

连接身份验证是由一组安全连接ID（Link ID）和一个站号来实现的。每个安全从站使用一个3比特Link ID来规定其安全网络系统。Link ID向SRC提供了最多8个安全网络系统。在一个功能安全通信系统内， Link ID的值是惟一的。安全报文总是包含Link ID。

11.5.3.5 报文回送

报文回送由每一个从站提供，以证实接收来自主站的报文。报文回送包含来自从站的错误状态信息以及RNO、Link ID和Command ID。

11.5.3.6 数据完整性保证

通过使用安全PDU中包含的CRC来保证数据完整性。发送节点发送包含其计算出的CRC的安全PDU。接收节点将收到的安全PDU中的CRC与接收到的安全PDU中计算出的CRC进行比较，判断是否发生讹误。

11.5.3.7 交叉校验冗余

接收节点交叉校验接收到的安全PDU的冗余部分，以验证这些部分是否逐位匹配。

11.5.3.8 不同数据完整性保证系统

安全相关报文与非安全相关报文的区别是安全相关报文包含CRC校验和（32比特）。IEC 61158类型18协议使用了不同的CRC算法（16比特CRC）。此外，每个报文包含一个8比特的Command ID、一个3比特的Link ID、一个24比特的RNO，并且这些元件每个都应符合为这些字段定义的限制。

11.5.4 安全通信层结构

FSCP 8/1的SCL能力通过引入SASE来提供。这些SASE被用在如本文件所规定的其相应的ASE位置。因为SASE来源于CPF8中的定义，本文件为CPF8定义了安全方面的附加内容。SASE的实现基于以下方面:

——设备管理器:用于 M1 和 S1 类型设备管理器的 ASE 类规范;
——连接管理器:用于 M1 和 S1 类型连接管理器的 AR 类定义;
——循环传输:用于 M1 和 S1 类型循环传输的过程数据 AR ASE 类规范。

SCL为ASE定义增加了:
——M1 和 S1 类型安全设备管理器;
——M1 和 S1 类型安全连接管理器
——M1 和 S1 类型安全循环传输。

SCL的所有管理、行为和功能都是用这些SASE来处理的。

11.5.5 与 FAL（和 DLL、PhL）的关系

11.5.5.1 概述

图3给出了SCL与IEC 61158类型18通信栈中其他层之间的关系。

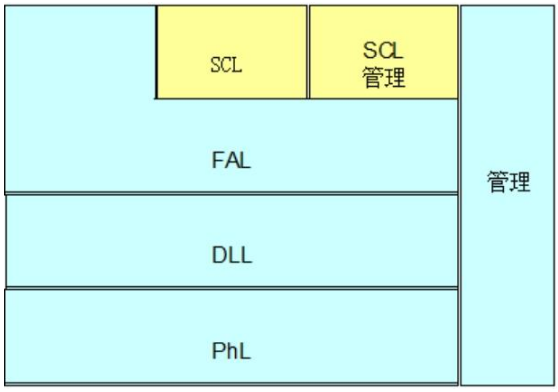

图 3 SCL 与 IEC 61158 类型 18 通信栈中其他层之间的关系

11.5.5.2 数据类型

安全数据的数据类型在IEC 61158-5-18中规定。

11.6 FSCP 8/1 的安全通信层服务

11.6.1 概述

对于过程数据输入和输出，FSCP 8/1 SAR使用缓冲的传输。所需的传输触发类型服务取决于实例化对象的配置。连接管理由安全连接管理器类来处理。安全相关应用使用SASE通过安全通信层进行通信。这些服务元素的形式模型在11.6中定义。

11.6.2 SASE

11.6.2.1 M1 安全设备管理器类规范

M1安全设备管理器类支持在轮询类型DL上实现主站类型的SCL用户。

SCL ASE:	Management SASE
类:	M1 safety device manager
类 ID:	not used
父类:	M1 device manager

属性:			
1	(m)	属性:	Management information
1.1	(m)	属性:	Link id
1.2	(o)	属性:	Software/protocol version
2	(m)	属性:	Connected slaves management information
2.1	(m)	属性:	Software/protocol version 1
…	…	…	…
2.n	(m)	属性:	Software/protocol version n
…	…	…	…
2.64	(m)	属性:	Software/protocol version 64

11.6.2.2 S1 安全设备管理器类规范

S1安全设备管理器类支持从站类型SCL用户在轮询类型DL实现。

SCL ASE:			Management SASE
类:			S1 safety device manager
类 ID:			not used
父类:			S1 device manager
属性:			
1	(m)	属性:	Management information
1.1	(m)	属性:	Link id
1.2	(m)	属性:	Software/protocol version

11.6.3 SAR

11.6.3.1 M1 安全连接管理器类

M1安全连接管理器类支持主站类型SCL用户在轮询类型DL实现。

SCL ASE:			Management SASE
类:			M1 safety connection manager
类 ID:			not used
父类:			M1 connection manager
属性:			
1	(m)	属性:	Parameter information
1.1	(m)	属性:	Safety monitor timer value
1.2	(m)	属性	Safety data monitor timer value
1.3	(m)	属性:	Safety slave specification
1.4	(m)	属性:	Safety slave specification source
1.5	(m)	属性:	Safety slave product information
2	(m)	属性:	Safety slave parameter data
3	(m)	属性	Safety slave link status

11.6.3.2 S1 安全连接管理器类

S1安全连接管理器类支持从站类型SCL用户在轮询类型DL实现。

SCL ASE:			Management SASE
类:			S1 safety connection manager
类 ID:			not used
父类:			S1 connection manager
属性:			
1	(m)	属性:	Safety product information
2	(m)	属性:	Safety slave parameter data

11.6.4 过程数据 SAR ASEs

11.6.4.1 M1 安全循环传输类规范

M1安全循环传输类支持主站类型SCL用户与M1安全连接管理器相连。

SCL ASE:			Process Data SAR ASE
类:			M1 safety cyclic transmission
类 ID:			not used
父类:			M1 cyclic transmission
属性:			
1.	(m)	属性:	Data out
1.1.	(m)	属性:	Safety RY data
1.2.	(m)	属性:	RWw data
1.2.1.	(m)	属性:	Safety RWw data
1.2.2.	(m)	属性:	Safety TPI-T
1.3	(m)	属性:	Safety RY-r data
1.4	(m)	属性:	RWw-r data
1.4.1	(m)	属性:	Safety RWw-r data
1.4.2	(m)	属性:	Safety TPI-T-r
2.	(m)	属性:	Data in
2.1.	(m)	属性:	Safety data in 1
2.1.1.	(m)	属性:	Safety RX data 1
2.1.2.	(m)	属性:	RWr data 1
2.1.2.1	(m)	属性:	Safety RWr data 1
2.1.2.2	(m)	属性:	Safety TPI-R 1
2.1.3	(m)	属性:	Safety RX-r data 1
2.1.4	(m)	属性:	RWr-r data 1
2.1.4.1	(m)	属性:	Safety RWr-r data 1
2.1.4.2	(m)	属性:	Safety TPI-R-r 1
…	…	…	…
2.n.	(m)	属性:	Safety data in n
…	…	…	…

2.64.	(m)	属性:	Safety data in 64

11.6.4.2 S1 安全循环传输类规范

S1安全循环传输类支持从站类型SCL用户与S1安全连接管理器相关联。

SCL ASE:			Process Data SAR ASE
类:			S1 safety cyclic transmission
类 ID:			not used
父类:			S1 cyclic transmission
属性:			
1.	(m)	属性:	Data out
1.1	(m)	属性:	Safety RY data
1.2	(m)	属性:	RWw data
1.2.1.	(m)	属性:	Safety RWw data
1.2.2.	(m)	属性:	Safety TPI-T
1.3	(m)	属性:	Safety RY data
1.4	(m)	属性:	RWw-r data
1.4.1	(m)	属性:	Safety RWw-r data
1.4.2	(m)	属性:	Safety TPI-T-r
2.	(m)	属性:	Data in
2.1	(m)	属性:	Safety RX data
2.2	(m)	属性:	RWr data
2.2.1	(m)	属性:	Safety RWr data
2.2.2	(m)	属性:	Safety TPI-R
2.3	(m)	属性:	Safety RX-r data
2.4	(m)	属性:	RWr-r data
2.4.1	(m)	属性:	Safety RWr-r data
2.4.2	(m)	属性:	Safety TPI-R-r

11.7 FSCP 8/1 的安全通信层协议

11.7.1 安全 PDU 格式

11.7.1.1 概述

在IEC 61158-6-18的抽象语法和传输语法的条款中，描述了安全PDU的语法和编码。

11.7.1.2 抽象语法

11.7.1.2.1 M1 安全设备管理器 PDU 的抽象语法

表2列出了该类属性的抽象语法。

表 2 M1 安全设备管理器属性格式

属性	格式	大小（比特）
Management information	2 个元素的结构:	11
Link id	Unsigned3	3
Software/protocol version	1 个八位位组,比特映射	8
Connected slave management information	64 个成员的数组:	64 个八位位组
Software/protocol version	1 个八位位组,比特映射	8

11.7.1.2.2 S1 安全设备管理器 PDU 抽象语法

表3列出了该类属性的抽象语法。

表 3 S1 安全设备管理器属性格式

属性	格式	大小（比特）
Management information	2 个元素的结构:	11
Link id	Unsigned3	3
Software/protocol version	1 个八位位组,比特映射	8

11.7.1.2.3 M1 安全连接管理器 PDU 抽象语法

表4列出了该类属性的抽象语法。

表 4 M1 安全连接器管理器属性格式

属性	格式	大小（比特）
Parameter information	5 个元素的结构:	2004 个八位位组
Safety monitor timer value	Unsigned16	16
Safety data monitor timer value	Unsigned16	16
Safety slave specification	8 个八位位组，比特映射	64
Safety slave specification source	8 个八位位组，比特映射	64
Safety slave product information	64 个成员的数组:	1984 个八位位组
Safety product information 1 ~ 64	面向字的数据结构	31 个八位位组
Safety slave parameter data	16 ~ 52224 个八位位组	16 ~ 52224 个八位位组
Safety slave link status	8 个八位位组，比特映射	64

11.7.1.2.4 S1 安全连接管理器 PDU 抽象语法

表5列出了属于该类属性的抽象语法。

表 5 S1 安全连接管理器属性格式

属性	格式	大小（比特）
Safety product information 1 ~ 64	面向字的数据结构	31 个八位位组
Safety slave parameter data	16 ~ 816 个八位位组	16 ~ 816 个八位位组

11.7.1.2.5 M1 安全循环传输 PDU 抽象语法

表6列出了该类属性的抽象语法。

表 6 M1 安全循环传输属性格式

属性	格式	大小（比特）
Data out	2 个元素的结构:	192 × n
Safety RY data	面向比特的数据结构	32 × n
RWw data	面向字的数据结构	64 × n
Safety RWw data	面向字的数据	64 × (n - m)
Safety TPI-T	安全传输包信息	64 × m
Safety RY-r data	面向比特的数据结构	32 × n
RWw-r data	面向字的数据结构	64 × n
Safety RWw-r data	面向字的数据	64 × (n - m)
Safety TPI-T-r	安全传输报信息	64 × m
Data in	n 个元素的结构	192 × m
Safety data in 1	2 个元素的结构	192
Safety RX data	面向比特的数据结构	64
RWr data	面向字的数据结构	128
Safety RWr data	面向字的数据	64
Safety TPI-R	安全传输包信息	64
Safety RX-r data	面向比特的数据结构	32
RWr-r data	面向字的数据结构	64
Safty RWr-r data	面向字的数据	64
Safty TPI-R-r	安全传输报信息	64
…	…	…
Safety data in n	2 个元素的结构	192
注:n和m的值取决于主站状态中对应配置的设定值。		

11.7.1.2.6 S1 安全循环传输 PDU 抽象语法

表7列出了该类属性的抽象语法。

表 7 S1 安全循环传输属性格式

属性	格式	大小（比特）
Data out	2 个元素的结构:	192
Safety RY data	面向比特的数据结构	32
RWw data	面向字的数据结构	64
Safety RWw data	面向字的数据	64
Safety TPI-T	安全传输包信息	64
Safety RY-r data	面向比特的数据结构	32
RWw-r data	面向字的数据结构	64
Safety RWw-r data	面向字的数据	64
Safety TPI-T-r	安全传输报信息	64

Data in	2 个元素的结构：	192
Safety RX data	面向比特的数据结构	64
RWr data	面向字的数据结构	128
Safety RWr data	面向字的数据	64
Safety TPI-R	安全传输包信息	64
Safety RX-r data	面向比特的数据结构	64
RWr-r data	面向字的数据结构	128
Safty RWr-r data	面向字的数据	64
Safty TPI-R-r	安全传输报信息	64

11.7.1.3 传输语法

11.7.1.3.1 M1 安全设备管理器 PDU 编码

表8列出了该类属性的详细PDU编码。

表 8 M1 安全设备管理器属性编码

属性	编码		
Management information	表示主设备的配置		
Link id	0～7:允许的范围		
Software/protocol version	比特	描述	值
	5～0	软件版本	1～63=允许的范围
	7～6	协议版本	0=版本 1 1=版本 2 2=版本 3 3=版本 4
Connected slave management information	表示连接的从站的配置		
Slave information 1 - 64	64 个元素的数组，每一个元素编码如下=		
Software/protocol version	比特	描述	值
	5～0	软件版本	1～63=允许的范围
	7～6	协议版本	0=版本 1 1=版本 2 2=版本 3 3=版本 4

11.7.1.3.2 S1 安全设备管理器 PDU 编码

表9列出了该类属性的详细的PDU编码。

表 9 S1 安全设备管理器属性编码

属性	编码		
Management information	表示主设备的配置		
Link id	0～7=允许的值		
Software/protocol version	比特	描述	值
	5～0	软件版本	1～63=允许的范围
	7～6	协议版本	0=版本 1 1=版本 2

			2=版本 3 3=版本 4

11.7.1.3.3 M1 安全连接管理器 PDU 编码

表10列出了该类属性的详细的PDU编码。

表 10 M1 安全连接管理器属性编码

属性	编码
Parameter information	表示连接的配置
Safety monitor timer value	1～65535=ms
Safety data monitor timer value	1～65535=ms
Safety slave specification	比特 0～63 对应槽 1～64，并且 0=不支持 SCL 1=支持 SCL
Safety slave specification source	比特 0～63 对应槽 1～64，并且 0=不支持 SCL-user 规范 1=支持 SCL-user 规范
Safety slave product information 1 - 64	64 个元素的数组，每个元素编码如下：
Safety product information	31 个八位位组的安全产品信息数据
Safety parameter data	0～52224 个八位位组的从站内存访问数据
Safety slave link status	比特 0～63 对应槽 1～64，并且 0=安全从站未运行 1=安全从站正在运行

11.7.1.3.4 S1 安全连接管理器 PDU 编码

表11列出了该类属性的详细的PDU编码。

表 11 S1 安全连接管理器属性编码

属性	编码
Safety product information	31 个八位位组安全产品信息数据
Safety parameter data	0～816 八位位组的从站内存访问数据

11.7.1.3.5 M1 安全循环传输 PDU 编码

表12列出了属于该类属性的特定PDU编码。

表 12 M1 安全循环传输属性编码

属性	编码
Data out	主站为从站输出设定的过程数据存储器
Safety RY data	按 32 比特的槽排序的所有连接从站的面向比特的输出数据的位置映射字段。
RWw data	位置映射字段，它映射所有连接的安全从站的面向字

<table>
<tr><td></td><td colspan="4">的输出数据以及传输到安全从站的安全传输包信息。</td></tr>
<tr><td>Safety RWw data</td><td colspan="4">用于所有已连接从站的面向字的输出数据的位置映射字段。每个槽包含 4 个字，从第二个槽开始，因为在非安全从站中后续字段占用了为第一个槽分配的空间。</td></tr>
<tr><td rowspan="10">Safety TPI-T</td><td>八位位组</td><td>比特</td><td>描述</td><td>值</td></tr>
<tr><td>0～1</td><td>-</td><td>RNO-3</td><td>0～65535</td></tr>
<tr><td rowspan="8">2～3</td><td>0～3</td><td>RNO-1</td><td>0～15</td></tr>
<tr><td>4～6</td><td>Link id</td><td>0～7</td></tr>
<tr><td>7</td><td>保留</td><td>0</td></tr>
<tr><td>8～11</td><td>传数据类型</td><td>0～15</td></tr>
<tr><td>12</td><td>忙标志</td><td>0=忙
1=不忙</td></tr>
<tr><td>13</td><td>保留</td><td>0</td></tr>
<tr><td>14</td><td>读请求</td><td>0=无请求
1=请求</td></tr>
<tr><td>15</td><td>SCL 用户应用模式</td><td>0=测试模式
1=安全模式</td></tr>
<tr><td>4～7</td><td>-</td><td>CRC32-A</td><td>CRC32-A</td></tr>
<tr><td>Safety RY-r data</td><td colspan="4">与 RY 相同</td></tr>
<tr><td>RWw-r data</td><td colspan="4">与 RWw 相同</td></tr>
<tr><td>Safety RWw-r data</td><td colspan="4">与安全 RWw 相同</td></tr>
<tr><td rowspan="4">Safety TPI-T-r</td><td>八位位组</td><td>比特</td><td>描述</td><td>值</td></tr>
<tr><td>0-1</td><td>-</td><td>Tx/Rx (A-code)</td><td>255/1-64</td></tr>
<tr><td rowspan="2">2-3</td><td>0-3</td><td>RNO-2</td><td>0-15</td></tr>
<tr><td>4-15</td><td colspan="2">同 Safety TPI-T</td></tr>
<tr><td>4-7</td><td>-</td><td>CRC32-B</td><td>CRC32-B</td></tr>
<tr><td>Data in</td><td colspan="4">主站读取的表示从站输入的过程数据存储器</td></tr>
<tr><td>Safety data in</td><td colspan="4">主站读取的表示安全从站输入的过程数据存储器</td></tr>
<tr><td>Safety RX data</td><td colspan="4">含有从站 n 面向比特的输入数据的字段，按 32 比特的槽的顺序排列。</td></tr>
<tr><td>RWr data</td><td colspan="4">含有从站 n 面向字的输入数据的字段，每个槽 4 个字，按槽的顺序排列。</td></tr>
<tr><td>Safety RWr data</td><td colspan="4">从站 n 的面向字的输入数据的位置映射字段，每个槽包括 4 个字，从第二个槽开始。因为在一个非安全从站中后续字段占用了为第一个槽分配的空间。</td></tr>
<tr><td rowspan="2">Safety TPI-R</td><td>比特</td><td colspan="2">描述</td><td>值</td></tr>
<tr><td>0～15</td><td colspan="2">RNO-3</td><td>0～65535</td></tr>
</table>

	比特	描述	值
	16～19	RNO-1	0～15
	20～22	Link id	0～7
	23	保留	0
	24～27	传输数据类型	0～15
	28	忙标志	0=忙 1=不忙
	29	错误通知	0=无错误 1=错误
	30	保留	0
	31	SCL-user 应用模式	0=测试模式 1=安全模式
	32～63	CRC32-A	CRC32-A
Safety RX-r data	与 Safety RX 相同		
RWw-r data	与 RWr 相同		
Safety RWw-r data	与 Safety RWr 相同		
Safety TPI-R-r	比特	描述	值
	0～15	Tx/Rx(A-code)	255/1-64
	16～19	RNO-2	0-15
	20～31	与 Safety TPI-R 相同	
	32～63	CRC32-B	CRC32-B
注 RNO 的值通过下列 RNO 的子部分组合得到： RNO-1 = RNO 比特 0-3 RNO-2 = RNO 比特 4-7 RNO-3 = RNO 比特 8-23			

11.7.1.3.6 S1 安全循环传输 PDU 编码

表13列出了属于该类属性的特定PDU编码。

表 13 S1 安全循环传输属性编码

属性	编码
Data out	从主站收到的过程数据
Safety RY data	该字段含有按 32 比特的槽排序的面向比特的输入数据。

<table>
<tr><td>RWw data</td><td colspan="3">位置映射字段，它映射从主站收到的面向字的输出数据（可选的）和安全传输包信息。</td></tr>
<tr><td>Safety RWw data</td><td colspan="3">从站面向字的输出数据的位置映射字段。每个槽包含 4 个字，从第二个槽开始。这是因为在非安全从站中后续字段占用了为第一个槽分配的空间。</td></tr>
<tr><td rowspan="10">Safety TPI-T</td><td>比特</td><td>描述</td><td>值</td></tr>
<tr><td>0 ~ 15</td><td>RNO-3</td><td>0 ~ 65535</td></tr>
<tr><td>16 ~ 19</td><td>RNO-1</td><td>0 ~ 15</td></tr>
<tr><td>20 ~ 22</td><td>Link id</td><td>0 ~ 7</td></tr>
<tr><td>23</td><td>保留</td><td>0</td></tr>
<tr><td>24 ~ 27</td><td>传输数据类型</td><td>0 ~ 15</td></tr>
<tr><td>28</td><td>忙标志</td><td>0=忙
1=不忙</td></tr>
<tr><td>29</td><td>保留</td><td>0</td></tr>
<tr><td>30</td><td>读请求</td><td>0=无请求
1=请求</td></tr>
<tr><td>31</td><td>SCL-user 应用模式</td><td>0=测试模式
1=安全模式</td></tr>
<tr><td>32 ~ 63</td><td>CRC32-A</td><td>CRC32-B</td></tr>
<tr><td>Safety RY-r data</td><td colspan="3">与 Safety RY 相同</td></tr>
<tr><td>RWw-r data</td><td colspan="3">与 RWw 相同</td></tr>
<tr><td>Safety RWw-r data</td><td colspan="3">与 Safety RWw 相同</td></tr>
<tr><td rowspan="5">Safety TPI-T-r</td><td>比特</td><td>描述</td><td>值</td></tr>
<tr><td>0 ~ 15</td><td>Tx/Rx(A-code)</td><td>1-64/255</td></tr>
<tr><td>16 ~ 19</td><td>RNO-2</td><td>0-15</td></tr>
<tr><td>20 ~ 31</td><td>与 Safety TPI-T 相同</td><td></td></tr>
<tr><td>32 ~ 63</td><td>CRC32-B</td><td>CRC32-B</td></tr>
<tr><td>Data in</td><td colspan="3">发送给主站的过程数据</td></tr>
<tr><td>Safety RX data</td><td colspan="3">该字段含有按 32 比特的槽排序的面向比特的输入数据</td></tr>
<tr><td>RWr data</td><td colspan="3">该字段含有来自主站的面向字的输入数据。</td></tr>
<tr><td>Safety RWr data</td><td colspan="3">从站面向字的输入数据的位置映射字段。每个槽包含 4 个字，从第二个槽开始。这是因为在一个非安全从站中后续字段占用了为第一个槽分配的空间。</td></tr>
<tr><td>属性</td><td colspan="3">编码</td></tr>
<tr><td rowspan="4">Safety TPI-R</td><td>比特</td><td>描述</td><td>值</td></tr>
<tr><td>0 ~ 15</td><td>RNO-3</td><td>0 ~ 65535</td></tr>
<tr><td>16 ~ 19</td><td>RNO-1</td><td>0 ~ 15</td></tr>
<tr><td>20 ~ 22</td><td>Link id</td><td>0 ~ 7</td></tr>
</table>

	23	保留	0
	24～27	传输数据类型	0～15
	28	忙标志	0=忙 1=不忙
	29	错误通知	0=无错误 1=错误
	30	保留	0
	31	SCL-user 应用模式	0=测试模式 1=安全模式
	32～63	CRC32-A	CRC32-A
Safety RX-r data	与 Safety RX 相同		
RWw-r data	与 RWr 相同		
Safety RWw-r data	与 Safety RWr 相同		
Safety TPI-R-r	比特	描述	值
	0～15	Tx/Rx(A-code)	1-64/255
	16～19	RNO-2	0-15
	20～31	与 Safety TPI-R 相同	
	32～63	CRC32-B	CRC32-B
注:RNO 的值通过下列 RNO 的子部分组合得到: RNO-1 = RNO 比特 0-3 RNO-2 = RNO 比特 4-7 RNO-3 = RNO 比特 8-23			

11.7.2 状态描述

11.7.2.1 概述

SCL状态模型是从IEC 61158类型18以及一个安全状态扩展而来的，如图4所示。一旦出现错误状态，就进入该安全状态，并且配置安全状态以保证所有输出都保持在安全状态：数字输出是低电平、零或者关闭，模拟输出保持在由SCL用户事先配置的安全水平。M1安全主站设备分别管理每个安全从站设备的状态。

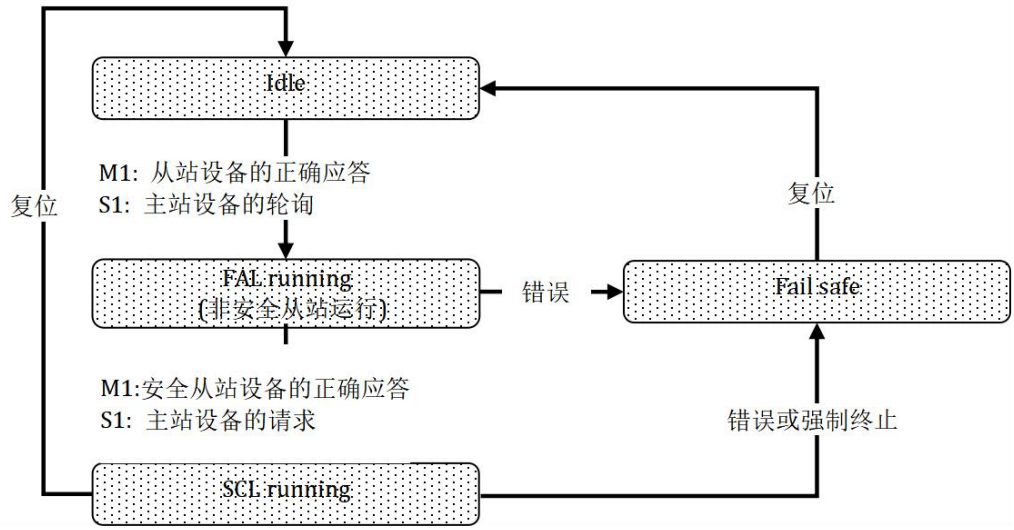

图 4　状态图

连接建立、从站验证以及数据刷新的通用方法都在IEC 61158类型18上进行了扩展，包括安全参数的传输和处理（见11.8的SCL管理）和安全数据传输以及确认监视。

11.7.2.2　Idle

11.7.2.2.1　概述

Idle状态存在于任何设备FAL通信开始之前。

11.7.2.2.2　转换

当FAL用户对M1安全主站发出一个适当请求，接收到来自S1安全从站设备的正确回答时，就产生从Idle状态到FAL running状态的转换。

当接收到来自M1安全主站的轮询通信的时候，S1安全从站设备转换到FAL running状态。

11.7.2.3　FAL running

11.7.2.3.1　概述

M1安全主站设备和S1安全从站设备已建立非安全通信。

11.7.2.3.2　转换

当接收到来自M1安全主站请求的时候，S1安全从站转换到SCL running状态。

当接收到来自S1安全从站设备适当响应的时候，M1安全主站转换到SCL running状态。

在FAL running状态中任何错误或者故障，或者转换到SCL running状态的过程失败，都会导致FSCP 8/1设备转换到Fail safe状态。

11.7.2.4　SCL running

11.7.2.4.1　概述

SCL running状态的细节见11.8。

11.7.2.4.2　转换

根据 11.7.2.6，在检测到如下任何错误类型时，FSCP 8/1 设备转换到 Fail safe 状态：
——序列号；
——时间期望值；
——连接身份验证；
——报文回送；
——数据完整性保证；
——交叉校验冗余；
——不同的数据完整性保证系统。
根据 11.7.2.7，在接收到一个强制终止请求时，FSCP8/1 设备转换到 Fail safe 状态。

11.7.2.5 Fail safe

11.7.2.5.1 概述

Fail safe状态是指所有输出都保持在其安全状态。对于数字量输出，除非另有规定，否则就是关状态闭（0或低电平）；对于模拟量输出，除非另有规定，否则就是零输出状态（即没有电压和/或没有电流）。典型地，模拟量输出将被配置一个安全值，该值是在Fail safe状态下被强加在输出上的。

11.7.2.5.2 转换

从Fail safe状态退出的惟一途径是通过从站复位。

11.7.2.6 安全数据的传输与处理

11.7.2.6.1 概述

FSCP 8/1 的 SCL 提供了如下安全措施：
——序列号；
——时间期望值；
——连接身份验证；
——报文回送；
——数据完整性保证；
——交叉校验冗余；
——不同的数据完整性保证系统；
安全主站和每一个安全从站都管理和分析安全传输，以验证其完整性。

11.7.2.6.2 序列号

安全报文包含4比特的指定顺序的序列号（RNO）。该序列号由主站来递增和传输。安全从站对收到的序列号进行回应。如果接收到的序列号出现错误，则安全从站转换到Fail safe状态。

11.7.2.6.3 时间期望值

SCL使用安全监视定时器和安全数据监视定时器来确保可靠、连续的通信。SCL管理配置定时器的值，该值的范围是1ms～65535ms。

安全监视定时器用于证实安全循环通信的正常运行，安全数据监视定时器用于证实连续的安全循环通信的正常运行。安全站通过该安全监视定时器监视循环数据的接收间隔，这些循环数据通过正常的安全数据保护信息来保护。另外，安全从站也通过该安全数据监视定时器监视循环数据的接收间隔，这些循环数据通过正常的安全数据保护信息来保护。

表14和表15列出了安全主站设备和安全从站设备的安全监视定时器的运行。表16列出了安全数据监视计时器的运行。

表 14　安全主站监视定时器运行

启动	终止	错误终止
发送安全数据 (RNO ≠ 0)	接收从站响应（刷新）数据（使用相同的 RNO 作为发送 RNO），该数据已被适当添加了安全数据保护信息。	(1)　出现了监视超时 (2)　监测到 RNO 错误

表 15　安全从站监视定时器运行

启动	复位	终止
接收安全数据 (CMD ID=01h)	接收主站轮询和刷新数据（之前的 RNO + 1），该数据已被适当添加了安全数据保护信息	(1)　出现了监视超时 (2)　监测到 RNO 错误 (3)　接收到强制终止请求

表 16　安全数据监视定时器运行

启动	复位	终止
接收安全循环 I/O 数据 (CMD ID = 0Fh)	接收主站轮询和刷新数据（之前的 RNO + 2），该数据已被适当添加了安全数据保护信息	(1)　出现了监视超时 (2)　监测到 RNO 错误 (3)　接收到强制终止请求
注:安全从站有两个安全数据监视定时器。一个安全数据监视定时器在接收到安全循环I/O数据（CMS ID=0Fh，RNO=n）时开始，并在接收到两个连续的数据（RNO=n+2）时复位。另一个安全数据监视定时器在接收到安全循环I/O数据（CMD ID=0Fh和RNO=n+1）时开始，并在接收到两个连续的数据（RNO=n+3）时复位。		

在安全监视定时器超时时，安全主站的的行为是:

1) 故障安全处理，如将递交给 SCL 用户的 S-RX 进行清零。
2) 向 SCL 用户通知错误。
3) 转换到 Idle 状态。

在安全监视定时器超时时，安全从站的行为是:

1) 故障安全处理，如终止向外部设备输出。
2) 向 SCL 用户通知错误。
3) 转换到 Fail safe 状态。

11.7.2.6.4　连接身份验证

连接身份验证是通过一组安全连接标识（Link ID）和站号来实现的。每个安全从站使用3个比特的Link ID来指示它的安全网络系统。Link ID向SRC提供了最多8个安全网络系统。在一个功能安全通信系统内，Link ID的值是惟一的。安全报文总是包含Link ID。

此外，在SPDU中添加传输的16比特逻辑连接标识，用于确认。该字段包含T_X（8比特的源标识）和R_X（8比特的目的标识），检查该字段以保证连接的正确性，并用作数据完整性措施。

11.7.2.6.5 报文回送

报文回送由每一个从站提供，以证实接收来自主站的报文。报文回送包含来自从站的错误状态信息以及RNO、Link ID和Command ID。

11.7.2.6.6 数据完整性

用于FSCP 8/1的CRC 32计算方法见附录A。用于FSCP 8/1的残差率的计算符合IEC 61784-3。

11.7.2.6.7 交叉校验冗余

冗余的数据字段对应部分进行逐位比较。

11.7.2.6.8 不同的数据完整性保证系统

区分安全相关和非安全相关报文是通过验证安全报文的惟一性来保证，包含格式正确的CRC校验和（32比特）、16比特的协议支持数据字段、8比特的Command ID、3比特的Link ID、24比特的RNO。

IEC 61158类型18协议使用不同的CRC校验（16比特CRC），不包含Command ID、Link ID和RNO。

11.7.2.7 强制终止

在安全主站请求某个安全从站终止通信时，使用强制终止处理。安全从站接收到强制终止的命令后转换为Fail safe状态（停止外部输出），然后立即终止通信。

11.8 FSCP 8/1 的安全通信层管理

11.8.1 概述

安全相关应用使用如下的服务来配置安全通信系统：

——创建连接；

——验证从站配置；

——安全从站参数传输。

11.8.2 连接建立和证实处理

一旦连接建立，通过验证安全设备中是否包含SAREP和是否支持安全循环传输来证实初始配置。表17列出了这个过程。

表 17 连接建立和证实处理的说明

SAREP 类型	处理说明
安全主站	（1）证实从站是安全从站设备（通过传输安全循环数据进行证实） （2）证实安全从站接收到建立连接命令（通过检查响应数据的 CMD 和 PSD 与发送数据是否相同来证实） （3）发送安全监视定时器的值
安全从站	（1）证实主站是安全主站设备（通过传输安全循环数据进行证实） （2）接收到安全监视定时器的值，并在内部登记该值。

安全主站发送创建连接命令时，发送RNO=0。

11.8.3 安全从站验证

11.8.3.1 概述

产品信息验证处理通过证实实际连接的安全从站与当前设置为安全主站设备网络参数的安全从站设备相匹配，来检测连接错误和配置错误。如果一个替代从站不是安全从站，将在启动阶段被检测出来并停止使用。

11.8.3.2 安全从站信息验证过程

表18列出了安全从站信息验证过程。

表 18 安全从站信息验证过程的说明

SAREP 类型	处理说明
安全主站	（1）读取安全从站的产品信息，并对照设置为网络参数的产品信息进行验证。 （2）验证之后，给安全从站设备发送产品信息。
安全从站	（1）对照从安全主站接收到的产品信息，验证该从站的产品信息。

从站信息验证处理验证了安全从站产品信息。

11.8.3.3 安全从站参数传输

安全从站配置参数传输是通过安全主站向每一个安全从站发送的，表19描述了这个过程。

表 19 安全从站参数传输处理的说明

SAREP 类型	处理说明
安全主站	（1）读取安全从站 ROM 中存储的 CRC 32，将此 CRC 32 与 SCL 用户在 ROM 中登记的 CRC 32 进行验证。 （2）发送安全从站参数给安全从站
安全从站	（1）接收来自安全主站的安全从站参数，证实这些设定值，并进行内部登记处理。

11.9 FSCP 8/1 的系统要求

11.9.1 指示灯和开关

11.9.1.1 开关

每个安全设备都应提供物理手段来进行以下设置：

——Online：设置该模式以建立数据链接；

——站号 0：安全主站；站号 1～64：安全从站（仅是对安全从站的要求）；

——Link ID：0～7；

——波特率：156 kbit/s、625 kbit/s、2,5 Mbit/s、5 Mbit/s、10 Mbit/s（仅是对安全主站的要求）；

——Reset：仅是对安全从站的要求。

并且还可以提供以下可选的物理手段：

——被占用的槽的数量：一个安全从站占用的槽的数量（1 或 2）；

——线路测试 1：验证主站能够连接所有从站；

——线路测试 2：验证主站能够连接一个特殊的从站；

——参数检查测试：验证参数内容；

——硬件测试：验证各模块是否正常运行。

11.9.1.2 指示灯

表20规定的指示灯的要求如下：：

M：必备的

O：可选的

指示灯的类型、颜色和形状没有指定。此外，若使用带屏幕的电脑或其他设备，指示灯可以通过屏幕进行指示。

表 20 监视 LED

编号	LED 名称	描述	安全主站	安全远程设备站	安全远程 I/O 站
1	RUN	亮：模块正常 灭：看门狗定时器错误	M	O	O
2	ERR	亮：与任何站通信发生错误 该指示灯在如下任何一项发生时点亮： ——开关设置错误； ——在同一线路上重复设置了两个主站； ——参数内容错误； ——数据连接监视定时器启动； ——电缆电线断路； 或者电缆在传输路径上受到噪声影响。 闪烁：通信错误	M	O	O
3	L RUN	亮：数据链路正在运行	M	O	O
4	L ERR	亮：通信错误（本站） 闪烁：上电后开关类型设置改变	M	O	O

11.9.2 安装指南

本文件规定了基于IEC 61158类型18安全通信系统的协议和服务。使用符合本文件中所规定的安全协议的安全设备需要正确的安装。

其他的安装信息见参考文献[30]和参考文献[31]。

11.9.3 安全功能响应时间

11.9.3.1 概述

如11.5.3所述，使用集成的看门狗定时器给每个安全输出从站的每个输出通道提供时间期望值，从而保证了安全功能的响应时间。

如果安全输出从站某一特定输出通道的安全功能响应时间超时，则对应的输出通道就设定为安全状态，通常是电源OFF状态。

11.9.3.2 时间计算

集成的看门狗定时器给每个安全输出从站的每个输出通道提供时间期望值，保证安全功能的响应时间，即从安全输入从站监测到事件到安全输出从站的相应输出通道的响应之间的时间，不包括安全输入的处理时间。

功能安全响应时间包括从安全输入从站到主站和从安全主站到安全输出从站的现场总线传输时间，包括由于传输错误可能导致的安全PDU重复、安全输出从站的处理时间及在SRC内的处理时间。

安全功能响应时间是通过表21中的（a）到（e）的和计算出来的，其中各项时间的定义在表22中给出。

注1：安全主站计算超时的方法：安全刷新监视时间-((WDT × n) × 2)。

注2：((WDT × n) × 2)是安全主站传输通信数据所需的时间。

表 21　安全功能响应时间计算

项	最大值
(a) 输入设备响应时间	DT1
(b) 安全从站输入处理时间	噪声去除滤波器时间+远程输入站处理时间
(c) 从安全输入到安全输出的监视时间	安全数据监视器时间
(d) 安全从站输出处理时间	远程输出站的处理时间
(e) 输出设备响应时间	DT2
总和	(a)+(b)+(c)+(d)+(e)

表 22　安全功能响应时间项的定义

项	定义
LS	由制造商指定的链接扫描时间
n	LS/WDT的向上取整值
SRRP	由制造商规定的安全刷新响应处理时间
m	SRRP/(WDT × n)的向上取整值
噪声去除滤波器时间	安全远程站设置的配置 (设定值: 1ms ~ 50ms)
DT1、DT2	由制造商规定的传感器或输出目标控制装置的响应时间
安全数据监视器时间	设置在网络参数中的时间，使用如下公式计算出的值: 监视器安全刷新时间 × 2-((WDT × n) × m)-10 (ms)
安全刷新监视器时间	在网络参数中的时间设置，使用如下公式计算出的值: 在触发模式下: (WDT × n) × 3+(WDT × n) × m × 2+(WDT × α) (ms) 在自由运行模式下: (WDT × n) × 3+LS+(WDT × n) × m × 2+(WDT × α) (ms) 其中: 当LS ≤ 1.5 ms时, α=0; 当LS > 1.5 ms时, α=1。
WDT(看门狗定时器)	配置参数中的时间设置
触发模式	序列扫描与链接扫描同步时，执行数据链路的模式。 在触发模式下，顺控扫描和链接扫描同时启动。
自由运行模式	顺控扫描和链路扫描不同步的模式。

11.9.4 要求的持续时间

安全相关应用对安全通信层的要求的持续时间应足够长，以保证在最长的安全功能响应时间内，该应用能检测到此要求。

11.9.5 系统特征计算的约束

FSCP 8/1安全系统应符合以下约束：

——IEC 61158 类型 18：无限制；

——安全槽的最大数量：64；

——最小扫描周期时间：10ms；

——对于每个安全 PDU，安全相关 I/O 比特的最大数量：从站到主站：208；

——对于每个安全 PDU，安全相关 I/O 比特的最大数量：主站到从站：7168。

11.9.6 维护

对维护没有SCL的特别要求。

设备修复和更换情况下系统的行为规范不在本文件的范围内。这些活动和责任的规范与服务和协议的规范无关。通常，这应是功能安全管理计划的一部分。然而，依据IEC 61508，修复、更换及维护、总体安全确认、总体运行、维修、改造和退役或废弃是必须予以考虑的重要议题。此方面问题，建议联系设备或系统供应商。

关于SRP编程和安全设备的参数设定，强烈建议联系设备或系统供应商。此外，建议考虑参考文献[30]和参考文献[31]。这些文件为CC-LINK Safety系统的用户提供了其他额外信息，如检查清单。

注：其他额外的维护要求及其他要求在IEC 61508、IEC 61511和/或IEC 62061中规定。

11.9.7 安全手册

纳入SCL的安全从站供应商应按照本文件给出的SCL规范依据IEC 61508准备相应的安全手册。安全手册应包含11.9.2中规定的安装要求及设备开关的配置指南。除IEC 61508类型18的开关外，该指南还应规定在同一网络上的所有安全设备应使用同一Link ID来配置。详见11.9.1.1。

针对基于IEC 61158类型18的安全通信系统，强烈推荐参照参考文献[30]、参考文献[31]和参考文献[32]。

注：在安装安全设备之前，建议联系CLPA以确定安装指南和安装要求是否有修订。

11.10 对 FSCP 8/1 的评估

制造商有责任依据安全标准（见IEC 61508、IEC 61511、IEC 62061等）和相关法律条例的适当开发流程来开发设备。相关信息在附件B中提供。

12 FSCP 8/2

12.1 范围——FSCP 8/2

见第1章。

12.2 规范性引用标准——FSCP 8/2

见第2章。

12.3 术语、定义、符号、缩略语和约定——FSCP 8/2

见第3章。

12.4 FSCP 8/2 的概述（CC-Link IE Safety 通信功能）

通信行规8/4和8/5（即CC-Link IE）定义了基于ISO/IEC/IEEE 8802.3、IEC 61158-5-23和IEC 61158-6-23的通信行规。

基本行规CP 8/4和CP 8/5在IEC 61784-2中定义。CPF 8功能安全通信行规FSCP 8/2（CC-Link IE Safety通信功能）是基于IEC 61784-2中的CP 8/4和CP 8/5基本行规及在本文件中定义的安全通信层规范。

FSCP 8/2是用于与数据相关的通信安全协议，例如分布式网络中用于功能安全、符合IEC 61508要求的现场总线技术的紧急停车信号。该协议可用于各类应用，如过程控制、制造自动化和机械装置。

FSCP 8/2协议的设计支持安全完整性等级SIL 3（IEC 61508），通过使用CP 8/4和CP 8/5的具体机制实现：时间戳、时间期望值、连接身份验证、报文回送、数据完整性保证及不同数据完整性保证安全措施。用于FSCP 8/2的SCL能力由SASE提供。这些SASE用来替代由本文件规定的与其相对应的ASE。SASE来源于CP 8/4和CP 8/5中的定义，本文件用于规范CP 8/4和CP 8/5的安全专用部分。

主从结构产生了两个SASE，分别是SASE-M和SASE-S。它们各自被安全FAL服务协议机、SFSPM-M和SFSPM-S管理。

12.5 FSCP 8/2 概述

12.5.1 为行规提供规范的外部文档

鼓励FSCP 8/2安全设备的制造商审阅CC-Link Safety规范，它提供了关于实现本文件定义的SCL的附加规范。

注：参考文献[30]和参考文献[31]包含了有关FSCP 8/2的重要信息。

12.5.2 安全功能要求

本文件规定了基于IEC 61158类型23的功能安全通信系统的服务和协议。本文件中规定的通信技术仅在依据IEC 61508要求所设计的设备中实现。

如下要求适用于实现FSCP 8/2协议的设备开发，并在FSCP 8/2开发中使用：

——FSCP 8/2 协议支持 SIL 3（见 IEC 61508）；

——FSCP 8/2 的实现应遵循 IEC 61508；

——对开发 FSCP 8/2 协议的基本要求见 IEC 61784-3；

——离散数据的安全状态是失电状态（0）。对于模拟值，失电状态应由安全相关应用定义；

——除非具有特定的产品标准，否则，对于基本等级，环境条件应符合 IEC 61131-2；对于安全裕度测试，环境条件应符合 IEC 61326-3-1 和 IEC 61326-3-2；

——除非本文件中规定，否则 CPF 8 对于安全性的要求是不变的。

12.5.3 安全措施

12.5.3.1 概述

在本文件中定义的安全通信层为实现其安全通信层，提供了如下确定性检测措施：

——时间戳；
——时间期望值；
——连接身份验证；
——报文回送；
——数据完整性保证；
——交叉校验冗余；
——不同数据完整性保证系统。

表23给出了对可能发生错误的各种检测措施。

表 23　对可能发生错误的各种检测措施

通信错误	确定性检测方法							
	序列号	时间戳	时间期望值	连接身份验证	报文回送	数据完整性保证	交叉校验冗余	不同数据完整性保证系统
讹误						×	× [c]	
非预期重复		×						
乱序		×						
丢包		× [a,c]			× [b]			
不可接受的延迟		× [c]	×					
插入				×				
伪装							× [c]	×
寻址				×				

[a] 通过接收的时间戳评估。
[b] 适用于请求/响应模式。
[C] 不用于请求/响应模式。

12.5.3.2　讹误

讹误是使用安全PDU中包含的CRC检测得到。发送节点发送包含有其计算出CRC的安全PDU。接收节点将接收到的安全PDU中包含的CRC与从接收到的安全PDU中计算出的CRC进行比较，以确定是否出现讹误。此外，接收节点交叉校验接收到的冗余的安全PDU部分，以验证这些部分的每个比特都一致。如果CRC比较或交叉校验的结果不匹配，则接收节点认为发生了讹误，并应丢弃接收到的安全PDU。当接收到的安全PDU被丢弃时，则用于不可接受延迟的定时器delay_detection_timer应不被复位。

12.5.3.3　非预期重复

非预期重复是重复地接收安全PDU，但不是在合适时机的最新的安全PDU，其原因为错误、故障或干扰。安全PDU的标识使用包含在安全PDU中的T_code（T code与CC结合形成的单一时效性代码）检测。发送节点发送包含有一个T_code的安全PDU。

接收节点接收安全PDU并保存接收到的安全PDU的T_code，以便在下次接收时检测安全PDU非预期重复。一旦收到安全PDU，接收节点即比较包含在安全PDU中的T_code与保存的上次接收的安全PDU的T_code。如果接收到的安全PDU中的T_code与上次接收的T_code相同，则接收节点认为发

生了非预期重复，并应丢弃接收到的安全PDU。当接收到一个含有相同T_code的安全PDU时，用于检测不可接受延迟的定时器delay_detection_timer应不被复位。

图5给出了安全PDU由SASE-M发送到SASE-S，并在SASE-S中检测到非预期重复的序列。同样，当一个安全PDU由SASE-S发送到SASE-M，在接收节点上的SASE-M检测出非预期重复。

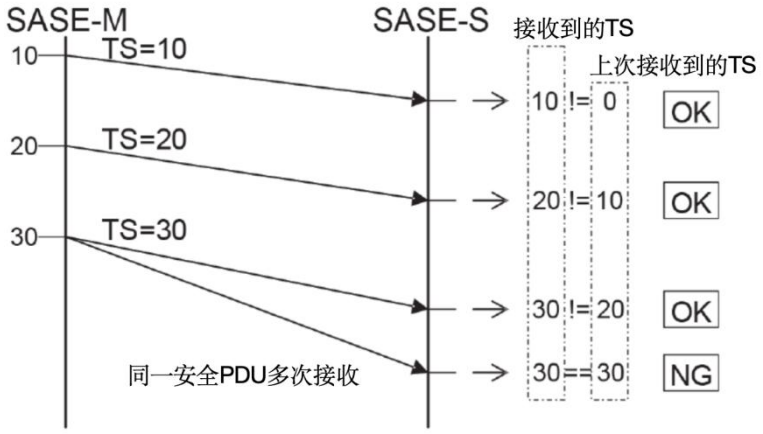

图 5　非预期重复的检测

注：此图假设 T-code 的前 32 位 (CC) 未发生变化。

12.5.3.4　错序

错序是接收节点收到安全PDU的顺序与发送节点发出安全PDU的顺序不一致。T code与CC结合形成单一时效性代码。其顺序依据包含在安全PDU中的T_code进行检测。发送节点发送的安全PDU中包含一个T_code。

接收节点接收到一个安全PDU并保留接收到的安全PDU的T_code。在接收下一个安全PDU时，接收节点将包含在安全PDU中的T_code与保留的前一个安全PDU的T_code进行比较。如果接收到的PDU中的T_code小于前一个接收到的T_code，则接收节点认为顺序不正确，并应终止安全连接。

图6给出了安全PDU由SASE-M发送到SASE-S并在SASE-S中检测到错序情况下的序列。同样，当一个安全PDU由SASE-S发送到SASE-M，在接收节点上的SASE-M检测出错序。

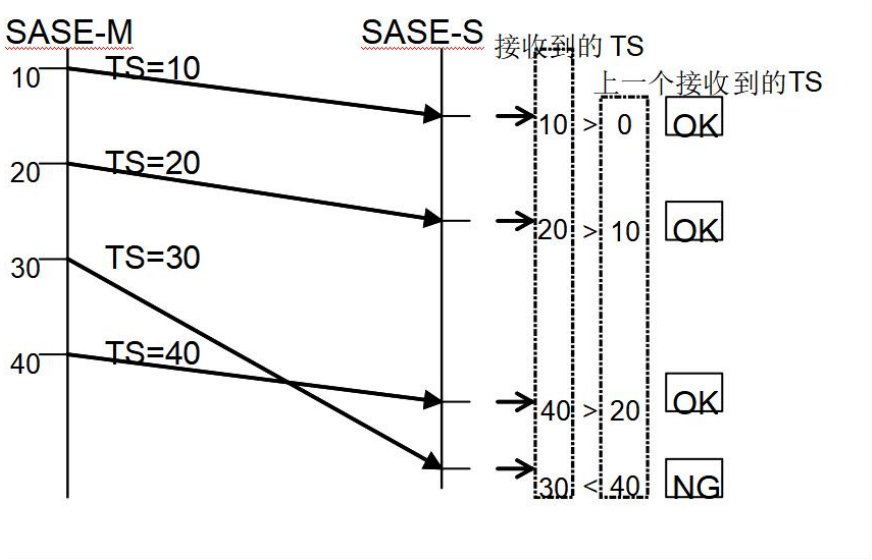

图 6　错序的检测

注：此图假设 T-code 的前 32 位 (CC) 未发生变化。

12.5.3.5　丢失

使用T_code检测丢失。

依据SASE-M的传输间隔（transmission_interval），SASE-M周期性地发送安全PDU到SASE-S。T_code包含在SASE-M发送的安全PDU中，为安全PDU发送时的安全时钟的值。依据SASE-S的传输间隔（transmission_interval），SASE-S周期性地发送安全PDU到SASE-M。T_code包含在SASE-S发送的安全PDU中，其值基于安全PDU发送时的安全时钟的值和SASE-M的偏移ts_offset计算得出。

接收节点接收安全PDU，验证接收到的安全PDU的T_code是否不大于发送节点的transmission_interval及上次接收到的安全PDU的T_code之和，如果大于，则认为发生了丢失。如果检测到丢失，接收节点应终止安全连接。

图7给出了安全PDU由SASE-M发送到SASE-S并在SASE-S中检测到丢失的序列。同样，当一个安全PDU由SASE-S发送到SASE-M，在接收节点上的SASE-M检测出丢失。

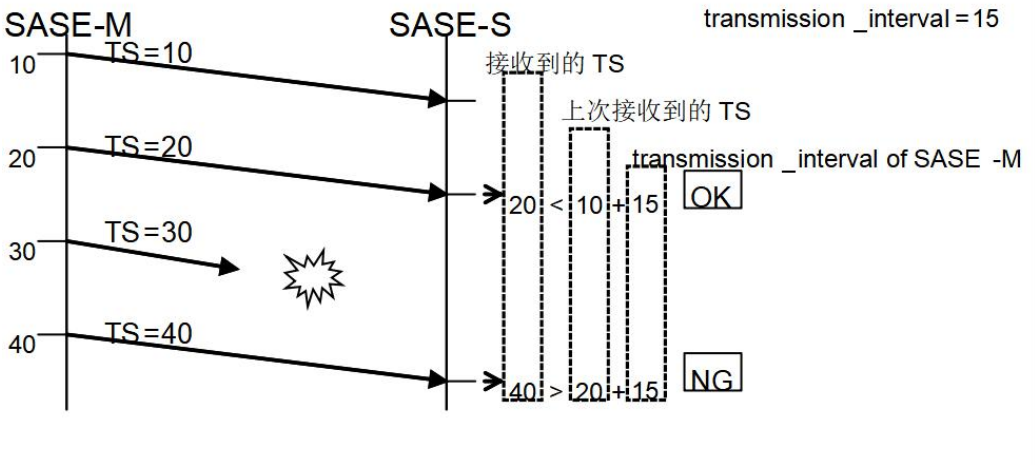

图 7　丢失的检测

注：此图假设 T-code 的前 32 位 (CC) 未发生变化。

12.5.3.6 不可接受的延迟

使用定时器和T_code检测不可接受的延迟。

SASE-M依据其传输间隔（transmission_interval）周期性地向SASE-S发送安全PDU。包含在SASE-M发送的安全PDU中的T_code是安全PDU传输时的安全时钟值。SASE-S依据其传输间隔（transmission_interval）周期性地发送安全PDU给SASE-M。包含在SASE-S发送的安全PDU中的T_code是安全PDU传输时的安全时钟值与SASE-M的偏移ts_offset之和。

在接收节点上的SASE-S接收来自SASE-M的安全PDU，在安全PDU接收的时刻记录安全时钟的值，并启动或复位定时器delay_detection_timer。SASE-S计算记录的安全时钟值与偏移ts_offset之和与接收到的T_code之间的差，并计算从SASE-M到SASE-S的延迟值。如果计算值不满足以下偏移传播（offset_dispersion）条件，则接收节点认为发生了不可接受的延迟。

offset_dispersion <Calculated value< allowable_delay + offset_dispersion

在allowable_refresh_interval期间，在delay_detection_timer溢出之前，如果没有接收到有效的安全PDU，则接收节点认为发生了不可接受的延迟。如果发生这种情况，SASE-S应终止安全连接。

接收节点上的SASE-M接收来自SASE-S的安全PDU，在安全PDU接收的时刻记录安全时钟的值，并启动或复位定时器delay_detection_timer。SASE-M计算记录的安全时钟值与接收到的T_code之间的差，并计算从SASE-S到SASE-M的延迟值。如果计算值不满足上述SASE-S评价公式，则接收节点认为发生了不可接受的延迟。另外，如果有效的安全PDU没有在delay_detection_timer溢出之前收到，则接收节点认为发生了不可接受的延迟。如果发生这种情况，SASE-M应终止安全连接。

图8给出了安全PDU由SASE-M发送到SASE-S并在SASE-S中通过SASE-S的时间戳检测到不可接受的延迟的序列。图9给出了通过SASE-S的定时器检测到不可接受的延迟的情况。同样，当一个安全PDU由SASE-S发送到SASE-M，在接收节点上的SASE-M检测到不可接受的延迟。

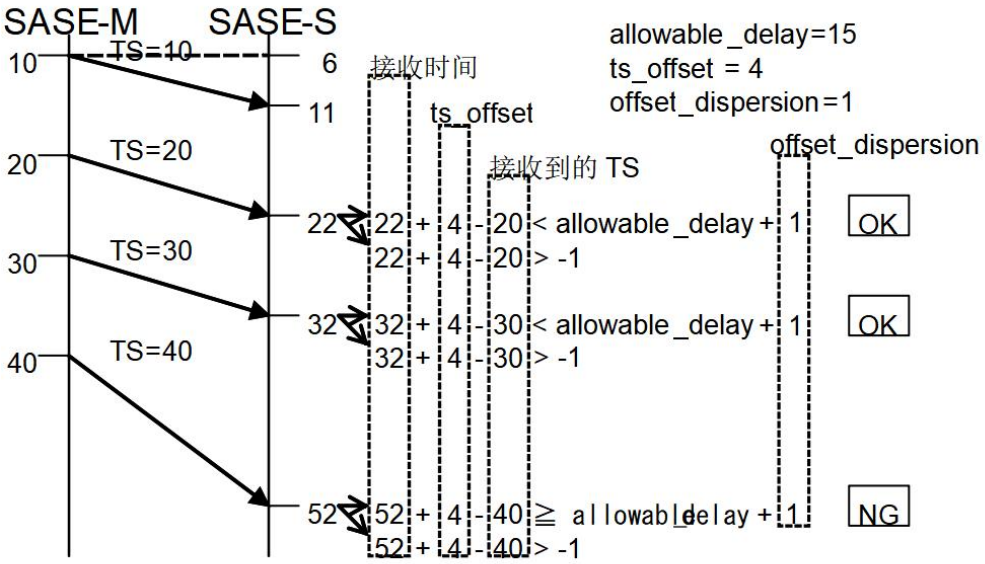

图 8　通过时间戳检测到不可接受的延迟

注：此图假设 T-code 的前 32 位 (CC) 未发生变化。

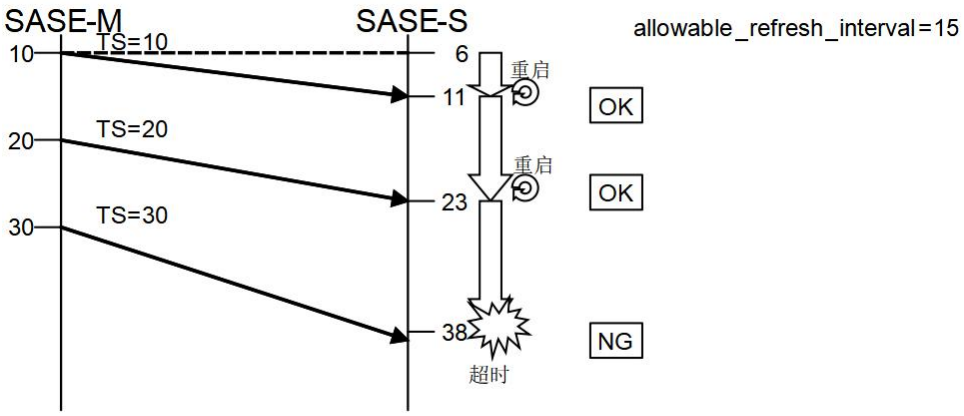

图 9　通过定时器检测到不可接受的延迟

注：此图假设 T-code 的前 32 位 (CC) 未发生变化。

12.5.3.7　插入

插入指来自非预期或未知传输源的报文插入。使用包含在安全PDU中的安全连接标识connection_id（CID）检测插入。发送节点发送一个安全PDU，在其CID中存有connection_id。

接收节点将包含在安全PDU中的CID与连接建立时约定的connection_id进行比较，确定二者是否匹配。如果二者不匹配，则接收节点应丢弃接收到的安全PDU。如果接收到的安全PDU被丢弃，则用来检测不可接受延迟的定时器delay_detection_timer应不被复位。

12.5.3.8　伪装

伪装是安全站接收到非安全报文，并且由于故障或干扰的结果，插入了来自看似有效传输源的报文。除了在接收PDU中验证SCL协议特定数据约束以外，还使用了由生成器多项式生成的CRC来检测伪装，该CRC与非安全通信的CRC不同。

发送节点发送安全PDU，该PDU包含其计算出的CRC。接收节点将包含在安全PDU中的CRC与通过接收到的安全PDU计算得出的CRC进行比较。此外，接收节点交叉校验所接收的安全PDU的冗余部分，以验证这些部分是否逐位一致。如果不一致，或者其他预期数据超出了正确定义的安全PDU的约束，则接收节点应丢弃接收到的安全PDU。如果接收到的安全PDU被丢弃，则用来检测不可接受延迟的定时器delay_detection_timer应不被复位。

12.5.3.9　寻址

寻址、或认证，是对错误的安全站进行安全报文的传输并因故障或干扰将报文视为正确报文。使用包含在安全PDU中的安全连接标识connection_id检测寻址。

发送节点发送安全PDU，在其CID中存有connection_id。接收节点将包含在安全PDU中的CID与连接建立时约定的connection_id进行比较，确定二者是否匹配。如果二者不匹配，则接收节点应丢弃接收到的安全PDU。如果接收到的安全PDU被丢弃，则用来检测不可接受延迟的定时器delay_detection_timer应不被复位。

12.5.4　安全通信层结构

安全站的协议层级结构包括:作为基础的CP 8/4和CP 8/5（ISO/IEC/IEEE 8802-3及FAL类型23）的协议层，实现安全通信的安全通信层FSCP 8/2，以及安全相关应用。图10给出了该层级结构（用于CP 8/5）。

图 10　协议层级结构

12.5.5　与 FAL（及 DLL、PhL）的关系

12.5.5.1　概述

除本文件所规定的要求外，没有其他FAL要求。

FSCP 8/2使用CP 8/4和CP 8/5 FAL的服务。安全数据传输使用瞬时传输服务。CP 8/4使用“Read memory”和“Write memory”服务。CP 8/5使用“AC Send ND”服务。这两种服务在FAL类型23中描述。

12.5.5.2　数据类型

安全数据的数据类型在IEC 61158-5-23中规定。

12.6　FSCP 8/2 的安全通信层服务

12.6.1　概述

FSCP 8/2由安全主站中的SFSPM-M和安全从站中的SFSPM-S这两个状态机组成，并经由12.6所描述的服务进行状态转换。安全相关应用使用安全应用服务经由安全通信层进行通信。

12.6.2　连接重建服务

12.6.2.1　SS-Start

SS-Start是用于请求开始一个安全通信的服务。表24给出了SS-Start的参数。

表 24　SS-Start

参数名	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		

ConnectionID

规定用于发起安全通信的安全连接的ID。长度为32比特。

12.6.2.2　SS-Restart

SS-Restart是用于请求重新开始一个安全通信的服务。表25给出了SS-Restart的参数。

表 25　SS-Restart

参数名	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		

ConnectionID
规定用于重新发起安全通信的安全连接的ID。长度为32比特。

12.6.2.3　SS-InvokeFunc

SS-InvokeFunc是一个用于请求执行安全应用命令的服务。表26给出了SS-InvokeFunc的参数。

表 26　SS-InvokeFunc

参数名	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
ConnectionID	M	M(=)		
Command	M	M(=)		
Data	C	C(=)		
Result			C	C(=)
R Data			C	C(=)

ConnectionID
规定目标安全连接的ID。长度为32比特。
Command
规定要执行的命令。
Data
规定要执行命令的相关信息。
R Data
包含来自已执行服务返回的信息。

12.6.3　数据传输服务

12.6.3.1　SS-Read

该服务用于从安全循环存储器中读取指定长度的安全数据。表27给出了该服务的参数。

表 27　SS-Read

参数名	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Address	M	M(=)		
Size	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Address
规定目标存储器首地址。
Size
规定目标存储器长度（单位：比特）。
Data
包含读存储器的内容。

12.6.3.2 SS-Write

该服务用于把指定长度的安全数据写到安全循环存储器中。表28给出了该服务的参数。

表 28 SS-Write

参数名	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Address	M	M(=)		
Size	M	M(=)		
Data	M	M(=)		

Address
规定目标存储器首地址。
Size
规定目标存储器长度（单位：比特）。
Data
规定写到目标存储器的安全数据。

12.6.4 连接终止通知服务

12.6.4.1 SS-Terminate

该服务用于发布安全连接终止的通知。表32给出了该服务的参数。

表 29 SS-Terminate

参数名	Req	Ind	Rsp	Cnf
Argument		M		
CID		M		

CID
规定已终止的安全连接CID。

12.7 FSCP 8/2 安全通信层协议

12.7.1 安全 PDU 格式

12.7.1.1 安全 PDU 结构

用于FSCP 8/2安全通信功能的安全PDU结构如图11所示。S-Data表示安全数据区域并存储安全输入数据或安全输出数据。S-Data最大长度是800比特。

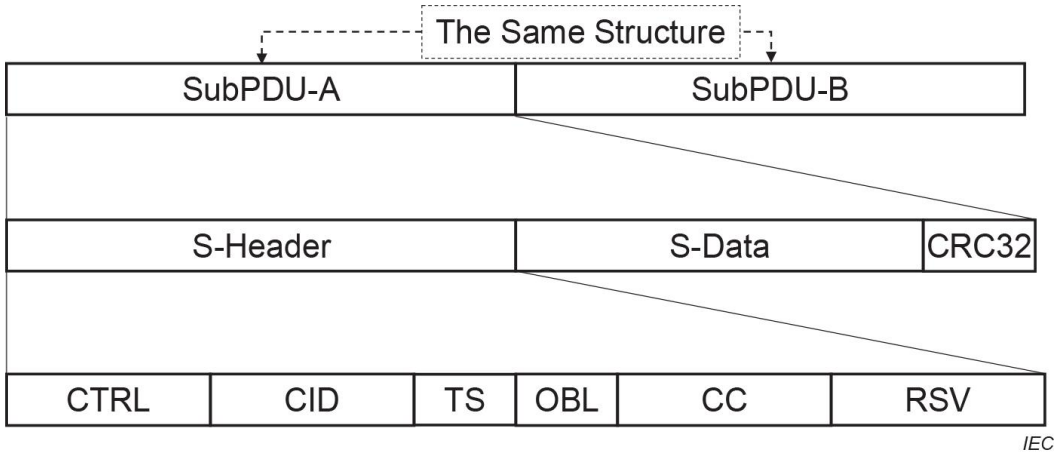

图 11　安全 PDU 结构

组成安全PDU的元素名称、长度及内容见表30。虽然SubPDU重复了两次，分别显示为SubPDU-A和SubPDU-B，但只展示一个SubPDU实例。

表 30　安全 PDU 元素

属性	描述	长度（比特）
S-Header	6 个元素组成：	160
CTRL	命令类型、状态	32
CID	安全连接标识符	32
T code	时间戳	16
OBL	偏移生成信息	16
CC	安全时钟的高 32 比特	32
RSV	留作将来使用	32
S-Data	安全数据（长度以 4 个八位位组为单位）	最小 32 最大 800
CRC32	循环冗余检查	32

12.7.1.2　CTRL

CTRL的结构如图12所示。表31给出了组成CTRL的元素内容。

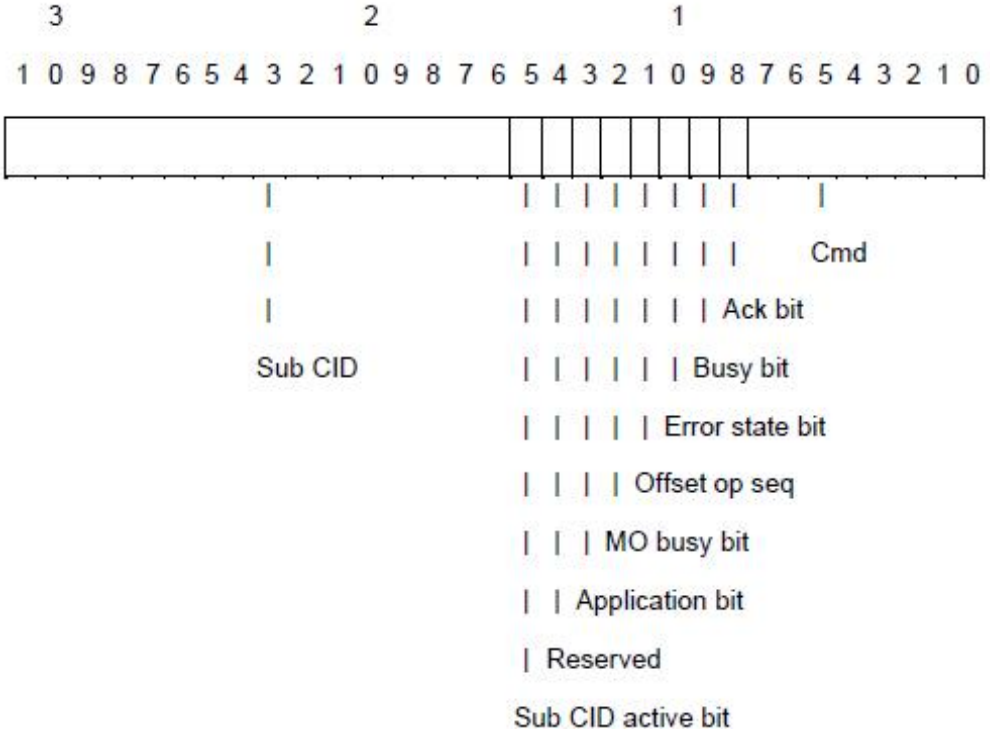

图 12　CTRL 结构

表 31　CTRL 元素

项		值	描述
Cmd	S-Connect	0x00	建立安全连接
	S-InitConfirmNetPrm	0x01	证实安全网络参数
	S-InitVerifyStnPrm	0x02	验证安全站参数
	S-InvokeFunc	0x03	安全应用命令
	Reserved	0x04 - 0xF8	用于将来扩展
	S-Disconnect	0xF9	安全连接终止
	S-ReadErrorInfo	0xFA	读错误信息
	S-WriteErrorInfo	0xFB	发布错误通知
	S-RefreshReady	0xFC	发布安全刷新就绪通知并测量偏移
	S-RefreshMO	0Xfd	安全刷新;测量偏移
	S-RefreshGO	0xFE	安全刷新;生成偏移
	S-Refresh	0xFF	安全刷新
Ack bit		0x00	请求
		0x01	响应
Busy bit		0x00	处理完成
		0x01	处理未完成

Error state bit	0x00	无错误
	0x01	错误
Offset op seq	0x00, 0x01	测量偏移、生成序列号
MO busy bit	0x00	处理完成
	0x01	处理未完成
Application bit	0x00,0x01	应用程序标识比特
Reserved	—	用于将来扩展
Sub CID active bit	0x00	子安全连接标识符未启用
	0x01	子安全连接标识符正在使用
Sub CID	0x0000 - 0xFFFF	子安全连接标识符

Cmd

表示安全PDU类型。

Ack bit

表示Cmd是请求还是响应。0表示请求，1表示响应。

Busy bit

表示除了安全刷新之外每次对传输节点Cmd的处理是否完成。0表示请求处理完成，1表示请求处理未完成。安全刷新期间Busy bit为0。

当Busy bit置1发送Cmd时，Busy bit的处理完成后，SASE-M将发送同样的Cmd，同时将Busy bit置0。当收到将Busy bit置1的安全PDU时，SASE-M丢弃接收到的安全PDU，重启roundtrip_timer并重新发送同样的Cmd。当收到将Busy bit置1的安全PDU时，SASE-S丢弃接收到的安全PDU，重启roundtrip_timer并发送将Busy bit置0的响应。

Error state bit

表示错误状态。0表示没有错误，1表示错误。在错误发生至错误清除期间，Error state bit为1。

Offset op seq

用于在偏移测量和偏移生成时，将SASE-M发出的请求与SASE-S发出的响应联系起来，当Cmd是S-RefreshReady、S-RefreshMO ,或S-RefreshGO时需使用Offset op seq。

它的初值是0，每次偏移测量时SASE-M交替指定0或1。偏移测量偏移生成完成后，用于偏移测量的值用作Offset op seq。SASE-S用从SASE-M请求接收到的Offset op seq值作为响应Offset op seq。

注：在偏移测量和偏移测量后的偏移生成期间，偏移测量和偏移生成是使用相同的Offset op seq值来关联的。

MO busy bit

表示在安全刷新期间偏移测量传输节点处理是否完成，0表示处理完成，1表示未完成。当接收到MO Busy bit置1的安全PDU时， roundtrip_timer已经启动，安全PDU将重启。当发送MO Busy bit置1的安全PDU时，传输节点不启动roundtrip_timer。

注：MO Busy bit仅用于重启roundtrip_timer。它不延长时钟偏移插入的间隔。

Application bit

用于指示设备特定的应用程序标识。

Sub CID active bit

表示子安全连接标识符Sub CID的有效性。0表示Sub CID未启用，因此是一个无效的字段。1表示Sub CID正在使用，因此Sub CID有效。

Sub CID

表示在给定CID中的子安全连接标识符。仅当Sub CID active为1时使用。

12.7.1.3 CID

CID是安全连接标识符，表示传输源与传输目的地之间的关系。CID生成时列入了SASE-M地址和SASE-S地址。

每个安全站最多有2个连接。假设n1是A站网络号，n2是站号，n3是B站网络号，n4是站号，CID为：

$CID_1 = ((n1 \times 256+n2) \times 65536) + (n3 \times 256+n4)$

$CID_2 = ((n3 \times 256+n4) \times 65536) + (n1 \times 256+n2)$

其中：

CID_1为安全连接1的CID，CID_2为安全连接2的CID。

12.7.1.4 T code 和 CC

T code是时间戳,表示48比特安全时钟的低16比特。它的单位是128μs。T code用SASE-M的安全时钟作为基准。

注：48比特的安全时钟（单位:128μs）的时间周期大约是1140年。

当SASE-M执行一个Cmd请求，在Cmd请求期间安全时钟低16比特的值应存储在T code。

当SASE-S执行一个Cmd请求，应将下式计算的值存储在T code中。Sending_time是SASE-S安全时钟低16比特的值，并且ts_offset是SASE-M安全时钟的偏移。

时间戳

$$T\ code=(sending\_time + ts\_offset) \bmod 2^{16}$$

图13给出了SASE-M和SASE-S安全时钟的关系以及Cmd请求期间的T code。

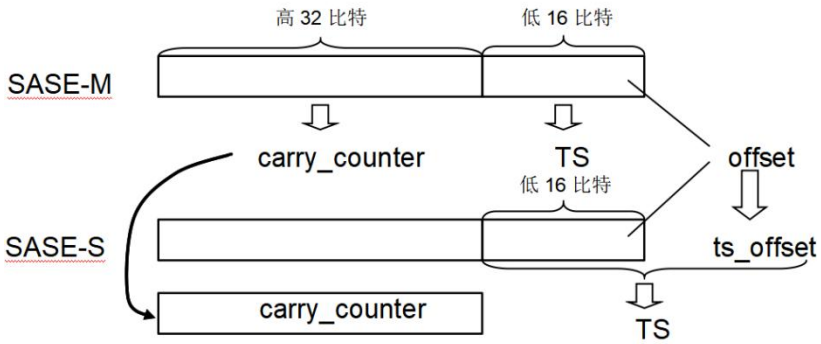

图 13 SASE-M 和 SASE-S T code

当响应发送给Cmd请求时，T code与Cmd请求节点使用的T code值应一致。

CC是48比特安全时钟的高32比特。T code和CC合并构成一个T-code。

12.7.1.5 OBL

OBL用于生成安全时钟偏移ts_offset。OBL用在SASE-M发送的请求S-RefreshGO-req以及SASE-S发送的响应S-RefreshGO-rsp中。

在S-RefreshGO-req的OBL中存储的信息是12.7.2.5描述的offset_baseline。在S-RefreshGO-rsp中的OBL中存储的信息是计算的ts_offset与使用的ts_offset之间的差值，也在12.7.2.5中描述。

12.7.1.6 S-Data

12.7.1.6.1 结构

S-Data是存储安全数据的一个区域。安全刷新期间S-Data使用图14所示的格式，Safety_data是安全刷新数据。最小为32比特，最大为800比特。S-Data的长度是可变的，并以4个八位位组为单位（32比特增量）。

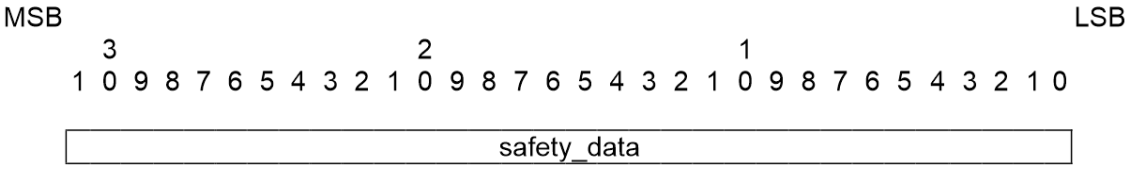

图 14 安全刷新期间的 S-Data

图15和图16给出了非安全刷新期间的S-Data格式。

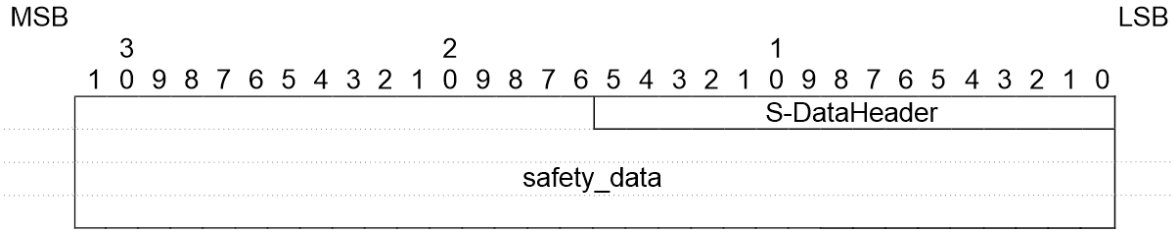

图 15 非安全刷新期间的 S-Data

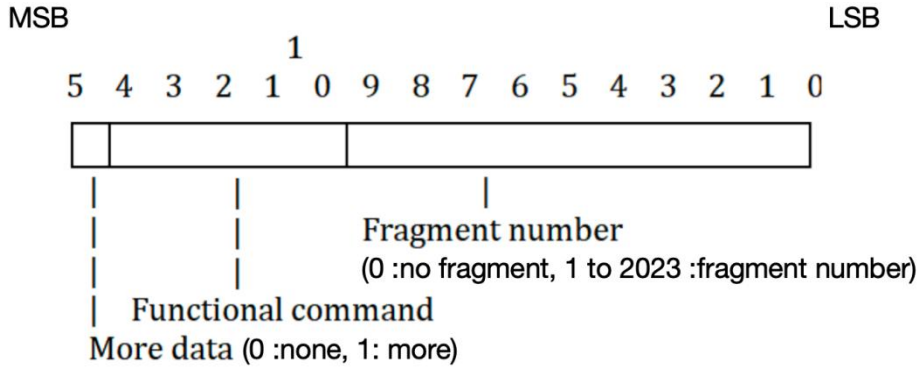

图 16 S-DataHeader 结构

S-DataHeader

当安全数据以分段的型式传输或执行功能命令时使用的首部。

Fragment number

表示分段数。0表示不分段，1～1023表示分段数。

Functional command

表示功能命令。

More data

表示当安全数据分段传输时是否有更多的数据。0表示没有更多数据，1表示有更多数据。

12.7.1.6.2 分段

当安全数据按照分段进行传输时，SASE-M将分段的安全数据的第一个S-DataHeader的分段数和More data设置为1。在第2个及后面的S-DataHeader中，SASE-M按顺序将分段数加1。只有当分段是最后一个段时，SASE-M设置More data为0。

当请求SASE-S传输安全数据时，SASE-M发送一个请求，将S-DataHeader的分段数设置为1，More data设置为0。当SASE-S分段传输安全数据时，SASE-S将第一个分段安全数据S-DataHeader和More data设置为1。当SASE-M从SASE-S接收第一个分段安全数据时，发送一个请求，将S-DataHeader的分段数设置为2（等于以前请求传输时的值加1），More data设置为0。SASE-S输入一个以1递增的值作为第二个和后面的S-DataHeader的分段数。

SASE-S仅对最后的More data输入0，其他的More data为1。SASE-M对S-DataHeader的分段数输入的值始终等于前面的值加1，More data为0。

12.7.1.7 CRC32

CRC32是安全通信的32比特CRC。下式应用于具有FSCP 8/2安全通信功能的CRC生成多项式：

$$G(x) = x^{32}+x^{31}+x^{30}+x^{29}+x^{28}+x^{24}+x^{23}+x^{20}+x^{17}+x^{13}+x^{11}+x^{4}+x^{2}+1$$

注：该CRC生成多项式在参考文献[36]中描述。当块长度（n）（信息长度与CRC长度之和）小于2046时，该式适用。当99 ≤ n ≤ 1024时，CRC生成多项式最小海明距离是8。

应使用包含在安全PDU中的CRTL、CID、T code、OBL、S-Data和 carry_counter计算CRC32，如图17所示。

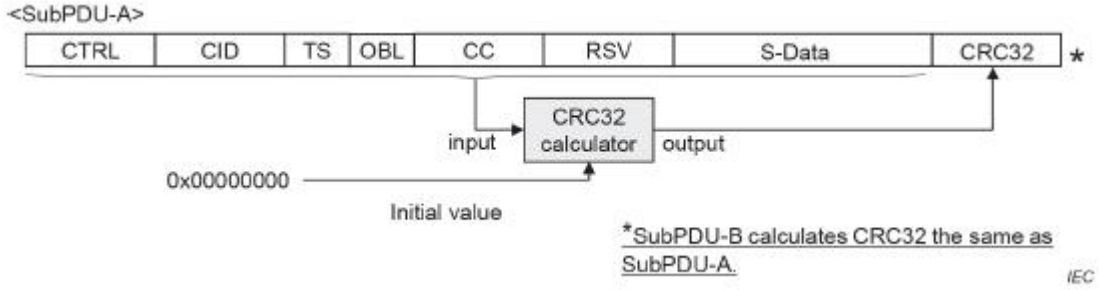

图 17 CRC 计算

12.7.2 安全 FAL 服务协议机（SFSPM）

12.7.2.1 概述

每次安全连接建立，FSCP 8/2安全通信层的行为由状态机SFSPM-M及SFSPM-S定义。当执行配置为发送和接收安全输入和输出的安全刷新操作时，以及当执行非安全刷新操作时，SFSPM-M及SFSPM-S使用图18所示的通信模型。

当执行非安全刷新操作时，SFSPM-M发送一个请求给SFSPM-S，SFSPM-S发送一个响应给SFSPM-M。当执行安全刷新操作时，SFSPM-M及SFSPM-S相互独立地发送请求给对方。

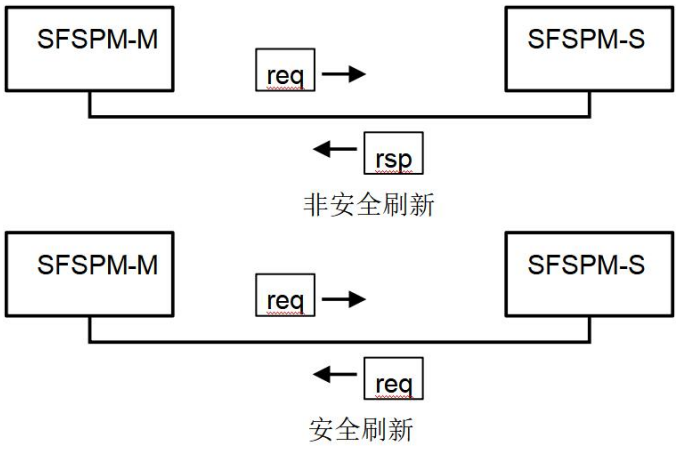

图 18　通信模型

图 19 示出了安全通信层的状态转换过程。

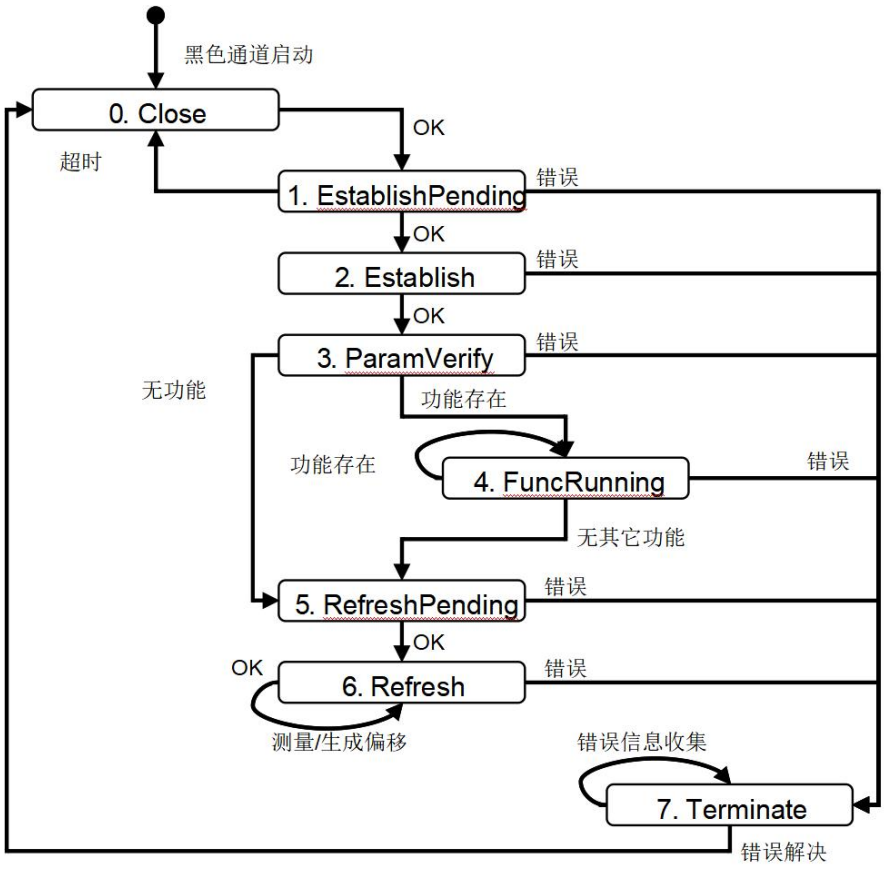

图19　SFSPM状态转换图

表32列出了图19中的状态。

表 32　状态列表

序号	状态名称	状态	描述
0	Close	安全连接没有建立	SFSPM-M 与 SFSPM-S 之间没有建立安全连接
1	EstablishPending	等待建立安全连接	正在等待建立 SFSPM-M 与 SFSPM-S 之间的安全连接
2	Establish	安全连接建立	SFSPM-M 与 SFSPM-S 之间建立了安全连接
3	ParamVerify	参数验证	正在验证 SFSPM-M 与 SFSPM-S 所持有的参数
4	FuncRunning	功能运行	正在运行 SFSPM-M 与 SFSPM-S 所支持的功能可执行的支持功能见表 35，比特 2 至 31。该状态为未来扩展用。不存在状态转换至该状态。
5	RefreshPending	安全刷新等待	正在验证 SFSPM-M 和 SFSPM-S 的安全刷新就绪状态，并测量安全时钟偏移量
6	Refresh	安全刷新进行中	SFSPM-M 和 SFSPM-S 正在交换安全输入/输出信息。同时，正在测量和生成周期安全时钟偏移。
7	Terminate	安全连接终止	在 SFSPM-M 和/或 SFSPM-S 发生错误时，安全连接终止。

12.7.2.2 行为

12.7.2.2.1 安全初始化

安全通信层在通信之前建立一个安全连接，如图20所示。遵循下面的步骤建立SFSPM-M和SFSPM-S间的安全连接:

1) SFSPM-M启动建立安全连接的过程。SFSPM-M基于预先提供的安全连接参数发送一个建立安全连接请求。

2) SFSPM-S确认接收到的协议版本和S-Data大小是正确的。

3) SFSPM-S发送建立安全连接的请求。

4) SFSPM-M确认接收到的协议版本和S-Data大小是正确的。

5) SFSPM-M基于安全连接建立时约定的支持功能信息，发送调用支持功能的请求。SFSPM-M发送一个相关支持功能的网络参数确认请求。

6) SFSPM-S存储请求中包含的网络参数，并发送网络参数确认响应。

7) SFSPM-M存储响应中包含的网络参数。

8) SFSPM-M发送一个验证安全站参数的请求。

9) SFSPM-S发送一个包含预先约定的安全站参数的响应。

10) SFSPM-M通过预先约定的安全参数验证接收到的信息，将SFSPM-S识别为正确的目标。

11) SFSPM-M发送另一个支持功能请求，直到所有支持功能请求都被执行。

12) SFSPM-S发送对请求的响应，直到所有支持功能请求都被接收。

13) SFSPM-M发送一个刷新准备和偏移量测量请求。

14) SFSPM-S发送一个刷新准备和偏移量测量响应。

15) SFSPM-M生成计算偏移的信息，并发送安全刷新和偏移生成请求。

16) SFSPM-S 基于接收到的包含在请求中的信息生成偏移并发送响应。

17) SFSPM-M 通过发送安全刷新和偏移生成请求来启动安全刷新，并以指定的时间间隔发送安全刷新请求。

18) SFSPM-S 通过发送安全刷新和偏移生成请求来启动安全刷新，并以指定的时间间隔发送安全刷新请求。

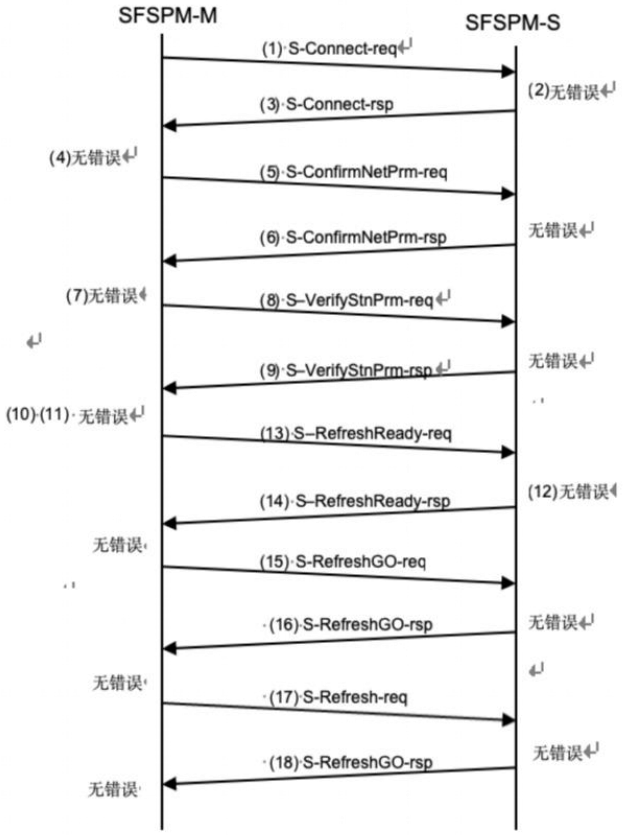

图 20　连接建立顺序

在安全连接的建立过程中，可以在安全参数验证后执行可选序列。在执行可选序列后，SFSPM-M向SFSPM-S发送一个刷新准备和偏移测量请求。

在建立安全连接期间，SFSPM-M和SFSPM-S之间商定的支持功能执行可选序列。

站特定的ID信息验证、站特定的配置信息校验码验证、站特定的配置信息写入、S-Data格式协商的可选序列图如图21所示。

19) SFSPM-M在建立安全连接时，如果同意验证站特定的ID信息，则发送站特定的ID信息验证请求。

20) SFSPM-S发送一个响应，其中包含预先给出的站特定的ID信息。

21) SFSPM-M验证接收站的特定ID信息。

22)如果在建立安全连接时同意站内配置信息校验码验证，则SFSPM-M发送站内配置信息校验码验证请求。

23) SFSPM-S发送一个响应，其中包含预先约定的站特定的配置信息检查代码。

24) SFSPM-M对接收到的站特定的配置信息校验码和存储的站特定的配置信息校验码进行校验。

25) SFSPM-M在建立安全连接时，如果同意写入站特定的配置信息，则发送一个站特定的配置信息写入请求。

26) SFSPM-S存储请求中包含的配置并发送响应。

27)如果在安全连接建立时同意S-Data格式协商，则SFSPM-M发送S-Data格式协商请求。

28) SFSPM-S发送一个包含预先约定的S-Data格式信息的S-Data格式协商响应。

29) SFSPM-M验证S-Data格式信息。

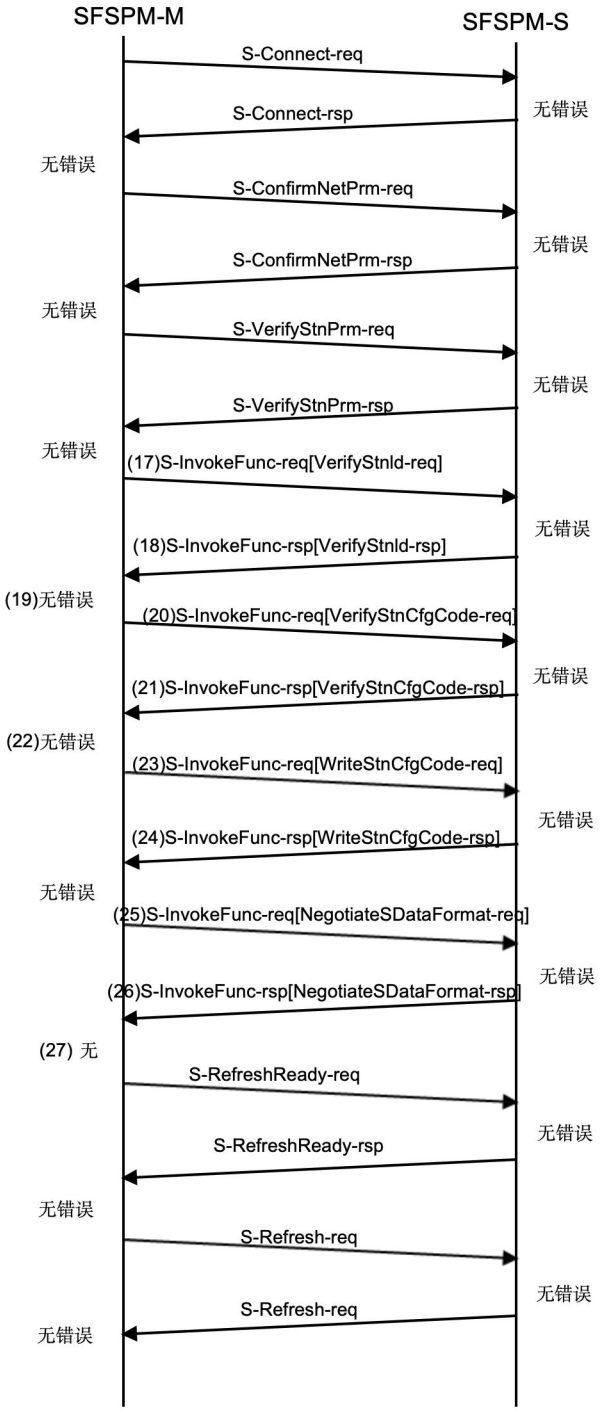

图 21　连接建立过程中的可选序列

12.7.2.2.2　安全刷新

图22示出了在安全刷新通信执行输入/输出发送和接收期间，从SFSPM-M到SFSPM-S的正常通信顺序。

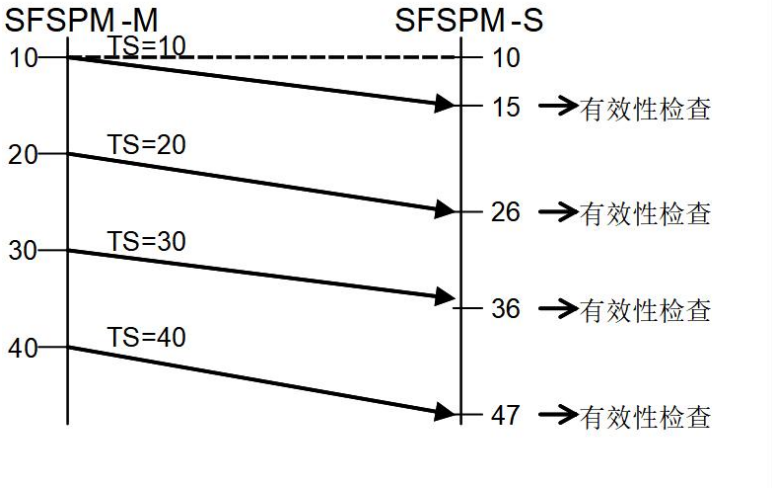

图 22　安全刷新通信期间的通信顺序

注：此图假设 T-code 的前 32 位 (CC) 未发生变化。

基于SFSPM-M传输时间间隔，SFSPM-M定期向SFSPM-S发送安全PDU。SFSPM-S验证接收的安全PDU。

基于SFSPM-S传输时间间隔，SFSPM-S定期向SFSPM-M发送安全PDU。SFSPM-M验证接收的安全PDU。

SFSPM-M和SFSPM-S应对接收的安全PDU进行安全连接标识符验证、CRC验证、时间戳验证。SFSPM-M和SFSPM-S应相互监视安全PDU的周期传输。

当接收的安全PDU验证结果表明PDU是正常时，SFSPM-M和SFSPM-S应向上层提交接收的安全数据。

在安全刷新通信期间，SFSPM-M和SFSPM-S定期执行偏移量测量和生成。图23示出了在SFSPM-M和SFSPM-S之间偏移量测量和生成时的顺序。

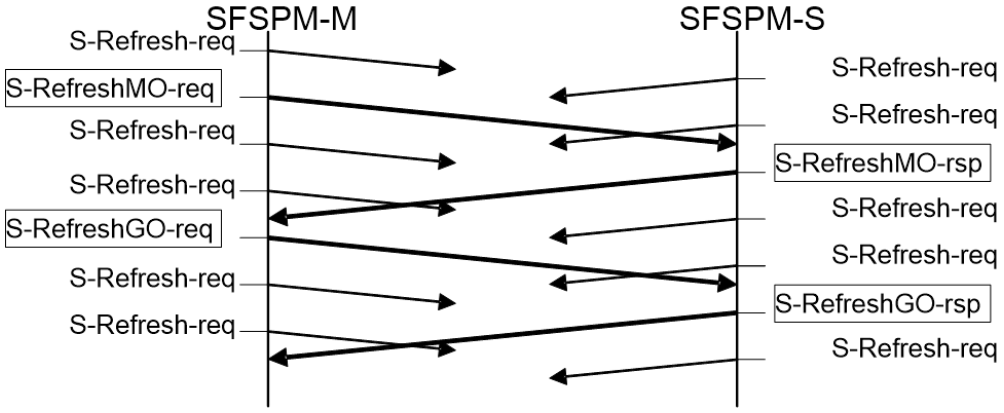

图 23　安全刷新通信期间偏移测量和生成顺序

12.7.2.2.3　安全连接终止

在安全初始化或者安全刷新期间，当检测到一个通信错误时，SFSPM-M和SFSPM-S停止安全刷新（如果错误发生在安全刷新期间）并终止安全连接。

SFSPM-M或SFSPM-S应按以下步骤终止安全连接：

1）SFSPM-M或SFSPM-S检测到需要终止安全连接的错误。

2）SFSPM-M或SFSPM-S向安全用户层发出通知，提示安全连接发生错误，需要终止安全连接，然后安全连接终止。

3）安全用户层应用将与发生错误的安全连接相关的状态和信息切换到安全状态。

4）SFSPM-M或SFSPM-S终止发生错误的安全连接。

5）一旦错误清除后，SFSPM-M重新建立安全连接。

12.7.2.3 SFSPM-M

12.7.2.3.1 状态转换

图24示出了SFSPM-M状态转换图。

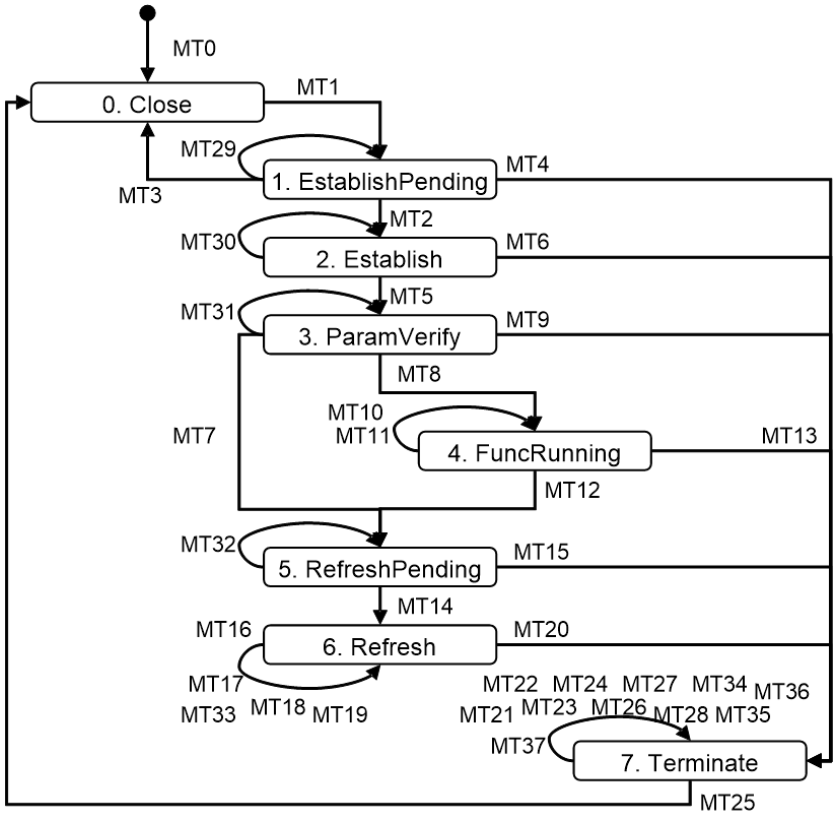

图 24 SFSPM-M 状态转换图

表33列出了SFSPM-M使用的定时器。

表 33 SFSPM-M 定时器

名称	描述
roundtrip_timer	用于检测除安全刷新期间外的不允许的延迟。 它在 allowable_roundtrip_delay 之后到期。

delay_detection_timer	用于检测不允许的延迟。它在 allowable_refresh_interval 之后到期。

表34列出了SFSPM-M状态转换表。

表 34　SFSPM-M 状态转换表

转换	状态	条件	动作	下一状态
MT0	—	Black channel ready	—	0.Close
MT1	0.Close	—	Send S-Connect-req && Start roundtrip_timer	1.EstablishPending
MT2	1.EstablishPending	Receive S-Connect-rsp　[NoError]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-req && Start roundtrip_timer	2.Establish
MT29	1.EstablishPending	Receive S-Connect-rsp　[Busy]	Stop roundtrip_timer && Send previously sent S-Connect-req && Start roundtrip_timer	1.EstablishPending
MT3	1.EstablishPending	roundtrip_timer timeout	—	0.Close
MT4	1.EstablishPending	Receive S-Connect-rsp　[Error]	Stop roundtrip_timer	7.Terminate
MT5	2.Establish	Receive S-InitConfirmNetPrm-rsp [NoError]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-req && Start roundtrip_timer	3.ParamVerify
MT30	2.Establish	Receive S-InitConfirmNetPrm-rsp　[Busy]	Stop roundtrip_timer && Send previously sent S-InitConfirmNetPrm-req && Start roundtrip_timer	2.Establish
MT6	2.Establish	roundtrip_timer timeout	—	7.Terminate
MT6	2.Establish	Receive S-InitConfirmNetPrm-rsp　[Error]	Stop roundtrip_timer	7.Terminate
MT7	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp　[NoError] && OptFuncs not exist	Stop roundtrip_timer && Send S-RefreshReady-req && Start roundtrip_timer	6.RefreshPending

转换	状态	条件	动作	下一状态
MT8	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [NoError] && OptFuncs exist	Stop roundtrip_timer && Send S-InvokeFunc-req && Start roundtrip_timer	4.FuncRunning
MT31	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-InitVerifyStnPrm-req && Start roundtrip_timer	3.ParamVerify
MT9	3.ParamVerify	roundtrip_timer timeout	—	7.Terminate
MT9	3.ParamVerify	Receive S-InitVerifyStnPrm-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT10	4.FuncRunning	Receive S-InvokeFunc-rsp [NoError] && Another OptFunc exists	Stop roundtrip_timer && Send S-InvokeFunc-req && Start roundtrip_timer	4.FuncRunning
MT11	4.FuncRunning	Receive S-InvokeFunc-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-InvokeFunc-req && Start roundtrip_timer	4.FuncRunning
MT12	4.FuncRunning	Receive S-InvokeFunc-rsp [NoError] && No other OptFunc exists	Stop roundtrip_timer && Send S-RefreshReady-req && Start roundtrip_timer	6.RefreshPending
MT13	4.FuncRunning	roundtrip_timer timeout	—	7.Terminate
MT13	4.FuncRunning	Receive S-InvokeFunc-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT14	5.RefreshPending	ReceiveS-RefreshReady-rsp [NoError]	Stop roundtrip_timer && Send S-RefreshGO-req && Start roundtrip_timer	6.Refresh
MT32	5.RefreshPending	ReceiveS-RefreshReady-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-RefreshReady-req &&	6.RefreshPending

转换	状态	条件	动作	下一状态
			Start roundtrip_timer	
MT15	5.RefreshPending	roundtrip_timer timeout	—	7.Terminate
MT15	5.RefreshPending	ReceiveS-RefreshReady-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT16	6.Refresh	Time to send [NoError]	Send S-Refresh-req	6.Refresh
MT17	6.Refresh	Time to measure offset	Send S-RefreshMO-req && Start roundtrip_timer	6.Refresh
MT18	6.Refresh	ReceiveS-RefreshMO-rsp [NoError]	Stop roundtrip_timer	6.Refresh
MT18	6.Refresh	Time to send [at first after S-RefreshMO-rsp with NoMOBusy received]	Send S-RefreshGO-req && Start roundtrip_timer	6.Refresh
MT33	6.Refresh	ReceiveS-RefreshMO-rsp [MOBusy]	Stop roundtrip_timer && Start roundtrip_timer	6.Refresh
MT19	6.Refresh	ReceiveS-RefreshGO-rsp [NoError]	Stop roundtrip_timer	6.Refresh
MT20	6.Refresh	Receive S-Refresh-req [Error]	—	7.Terminate
MT20	6.Refresh	roundtrip_timer timeout	—	7.Terminate
MT20	6.Refresh	ReceiveS-RefreshMO-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT20	6.Refresh	ReceiveS-RefershGO-rsp [Error]	Stop roundtrip_timer	7.Terminate
MT21	7.Terminate	Need to collect error information	Send S-ReadErrorInfo-req && Start roundtrip_timer	7.Terminate
MT22	7.Terminate	Receive S-ReadErrorInfo-rsp [No more data]	Stop roundtrip_timer	7.Terminate
MT34	7.Terminate	Receive S-ReadErrorInfo-rsp [More data]	Stop roundtrip_timer && S-ReadErrorInfo-req && Start roundtrip_timer	7.Terminate
MT35	7.Terminate	ReceiveS-ReadErrorInfo-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-ReadErrorInfo-req && Start roundtrip_timer	7.Terminate
MT23	7.Terminate	Need to send error information	Send S-WriteErrorInfo-req && Start roundtrip_timer	7.Terminate
MT24	7.Terminate	Receive S-WriteErrorInfo-rsp [No more data]	Stop roundtrip_timer	7.Terminate
MT36	7.Terminate	Receive S-WriteErrorInfo-rsp [More	Stop roundtrip_timer	7.Terminate

转换	状态	条件	动作	下一状态
		data]	&& S-WriteErrorInfo-req && Start roundtrip_timer	
MT37	7.Terminate	ReceiveS-WriteErrorInfo-rsp [Busy]	Stop roundtrip_timer && Send previously sent S-WriteErrorInfo-req && Start roundtrip_timer	7.Terminate
MT25	7.Terminate	Error resolved	—	0.Close
MT26	7.Terminate	Need to invoke Function	Send S-InvokeFunc-req && Start roundtrip_timer	7.Terminate
MT27	7.Terminate	Receive S-InvokeFunc-rsp	Stop roundtrip_timer	7.Terminate
MT28	7.Terminate	Receive S-InvokeFunc-rsp [Busy]	Send previously sent S-InvokeFunc-req	7.Terminate
MT4，MT6，MT9，MT13 和 MT15 错误:异常 CTRL，错误状态位 = 1，异常 S-Data MT20 错误:错误顺序，遗失，非允许延时，异常 CTRL，错误状态位= 1				

12.7.2.3.2 非安全刷新期间的操作

SFSPM-M启动定时器roundtrip_timer的同时发出请求指令。SFSPM-M收到SFSPM-S所发出请求指令的响应，并停止定时器roundtrip_timer。roundtrip_timer定时器按allowable_roundtrip_delay确定的时间计时到期。如果SFSPM-M在定时器roundtrip_timer终止之前没有收到对于该请求指令的响应，会出现非允许的延时。图25示出了非安全刷新期间的状态序列。

当发送请求指令时，SFSPM-M 向安全PDU的T code中插入安全时钟的低16比特数值，并发送请求指令。当发送一个响应时，SFSPM-S向安全PDU的T code中插入对应要求指令的安全PDU中的T code值作为响应。SFSPM-M 对比响应中T code的值和T code发出的值，来验证对于请求指令的响应。如果这两个值不匹配，那么SFSPM-M应放弃所接收到的安全PDU。

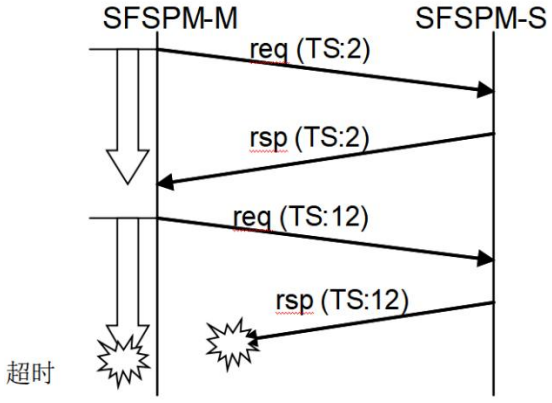

图 25 非安全刷新期间的序列

12.7.2.3.3 S-Data 语法

12.7.2.3.3.1 S-Connect-req

S-Connect-req使用图15中所示的S-Data格式。 safety_data区域中储存图26中所描述的数据。

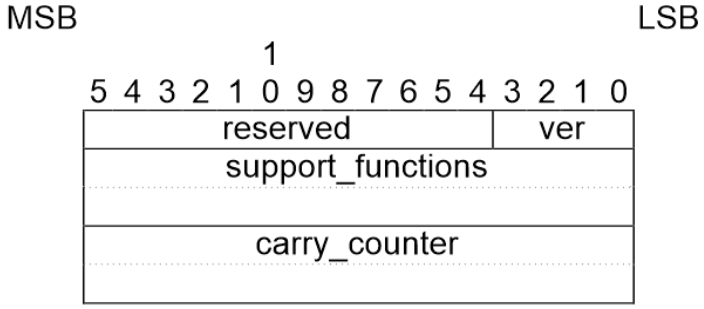

图 26 S-Connect-req

ver

指示了SFSPM-M支持的FSCP 8/2的协议版本。协议版本是 0000b。

reserved

保留用于未来扩展。

support_functions

表35列出了S-Connect-req所支持功能的详述。每一比特表示是否支持该表中的功能。1代表支持该功能，0代表不支持该功能。

表 35 support_functions

比特	功能	描述
0	安全网络参数验证	验证 SFSPM-M 和 SFSPM-S 持有的安全网络参数。
1	安全站参数验证	验证 SFSPM-M 和 SFSPM-S 持有的安全站参数。
2 ~ 31	用于未来扩展	用于未来扩展

carry_counter

S-Connect 发送/接收之后，由SFSPM-M 和SFSPM-S所使用的carry_Counter初始值。

如果安全PDU的S-Data是 S-connect-req，在CRC32生成中使用的carry_counter初始值为0。

12.7.2.3.3.2 S-InitConfirmNetPrm-req

S-InitConfirmNetPrm-req使用图15中所示的S-Data格式。 safety_data区域中储存图27中所描述的数据。

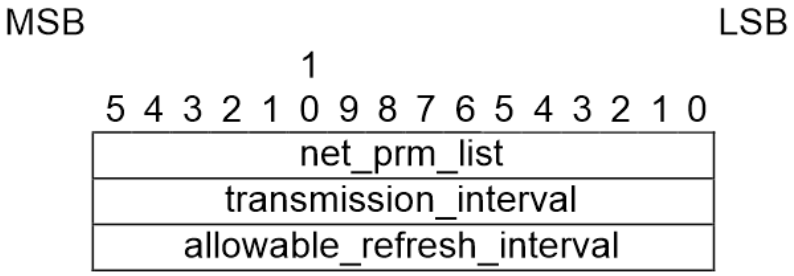

图 27　S-InitConfirmNetPrm-req

net_prm_list

需要证实的安全网络参数清单。net_prm_list的组成见图28。1表示该参数需要证实，0表示不需要。transmission_interval和allowable_refresh_interval的比特设置为1。

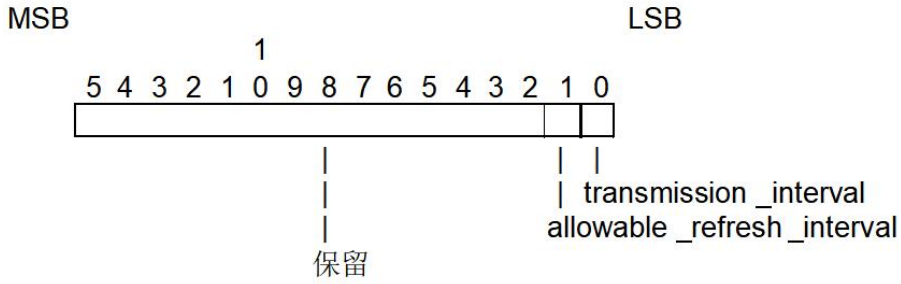

图 28　net_prm_list

transmission_interval

在安全刷新期内，SFSPM-M的安全PDU的传输间隔。单位为128μs。

allowable_refresh_interval

在安全刷新期内，被SFSPM-M和 SFSPM-S使用的允许的接收间隔。单位为128μs。

12.7.2.3.3.3　S-InitVerifyStnPrm-req

S-InitVerifyStnPrm-req使用图15中所示的S-Data格式。safety_data区域储存图29中所描述的数据。

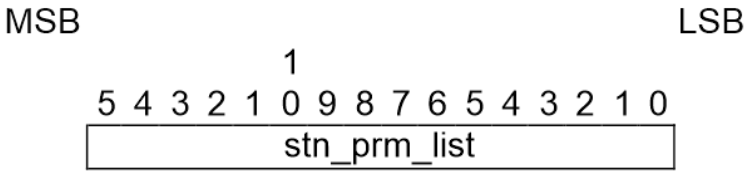

图 29　S-InitVerifyStnPrm-req

stn_prm_list

需要确认的安全站参数清单。stn_prm_list的结构见图30。1代表该参数需验证，0表示该参数不需要验证。

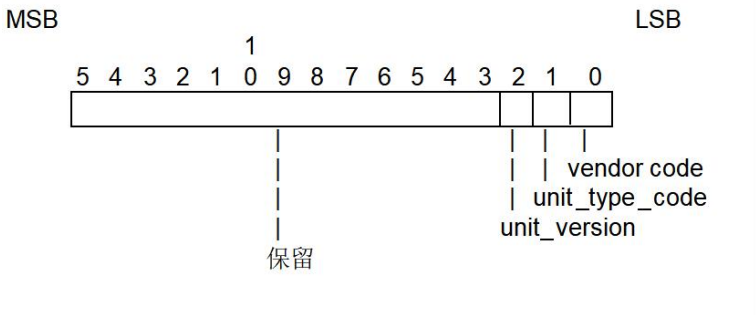

图 30　stn_prm_list

12.7.2.3.3.4　S-InvokeFunc-req

S-InvokeFunc-req使用图15中所示的S-Data格式。 safety_data区域中储存图31中所描述的数据。

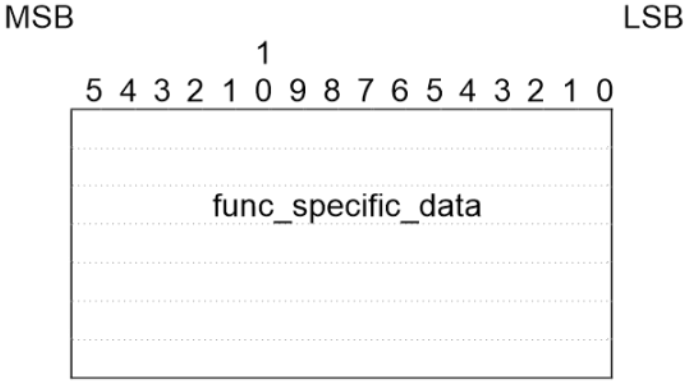

图 31　S-InvokeFunc-req

func_specific_data
与S-DataHeader功能命令所规定的功能相关的数据，funcspecific_data取决于每个功能命令。

12.7.2.3.3.5　S-RefreshReady-req

S-RefreshReady-req使用图15的所示S-Data格式。safety_data区域不存储任何信息。

12.7.2.3.3.6　S-ReadErrorInfo-req

S-ReadErrorInfo-req使用图15所示的S-Data格式. safety_data区域不存储任何信息。

12.7.2.3.3.7　S-WriteErrorInfo-req

S-WriteErrorInfo-req使用图15所示的S-Data格式。safety_data区存储图32中描述的数据。

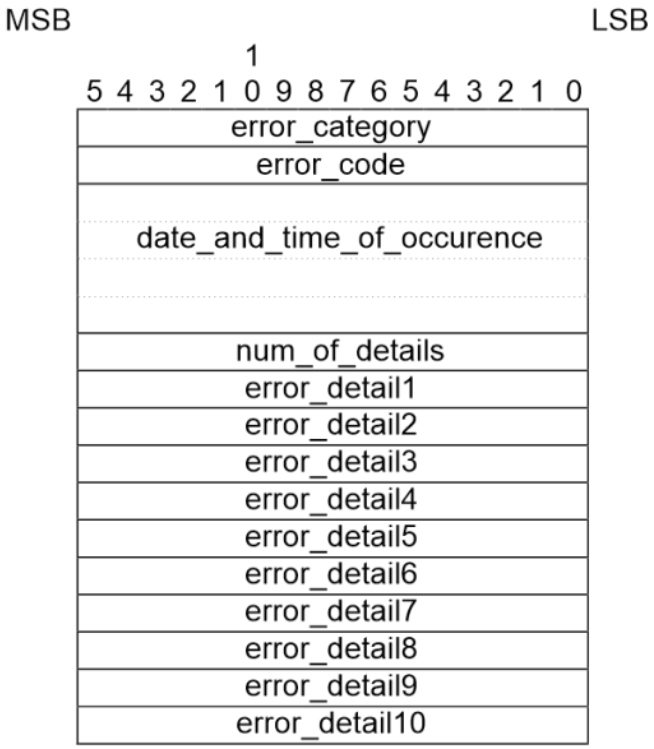

图 32　S-WriteErrorInfo-req

error_category
指示错误类别，使用表 36 和表 37 中所列出的值。

表 36　error_category

值	含义
0～299	用于未来扩展
300～349	应用层通用错误 (见表37)
350	应用层供应商定义的错误
351～399	用于未来扩展(应用层错误)
400～449	用于未来扩展(服务用户层通用错误)
450	服务用户层供应商定义的错误
451～449	用于未来扩展(服务用户层错误)
500～66535	用于未来扩展

表 37　AL 错误的 error_category

值	含义
300～309	用于未来扩展
310～314	应用层错误

error_code
指示错误编号。使用的编号如表 38 中所示。

表 38　error_code

error_category 错误类别	error_code 错误代码	含义
310	0	检测到 CRC 错误
	1	T code 错误
	2	CID 错误
311	0	delay_detection_timer 超时
	1	roundtrip_timer 超时
312	0	分段号错误
313	0	安全网络参数错误
314	0	安全站参数错误

date_and_time_of_occurence

指示错误发生的日期和时间。使用的格式如图 33 所示。year_upper (年的前两位数字)、year_lower (年的后两位数字)、月、日、小时、分、秒和 day_of_week 都用 BCD 码表示。

MSB LSB

15 14 13 12 11 10 9 8	7 6 5 4 3 2 1 0
year_lower	year_upper
天	月
分钟	小时
day_of_week	second

图 33 date_and_time_of_occurence

num_of_details

指示 error_detail1 ~ error_detail10 代表的错误详情的编号。

error_detail

指示错误详情(1 ~ 10)。

reserved

保留用于未来扩展。

12.7.2.3.3.8 S-RefreshMO-req

S-RefreshMO-req 使用图 14 所示的 S-Data 格式。safety_data 是安全更新数据。

12.7.2.3.3.9 S-RefreshGO-req

S-RefreshGO-req 使用图 14 所示的 S-Data 格式。 safety_data 是安全更新数据。

12.7.2.3.3.10 S-Refresh-req

S-Refresh-req 使用图 14 所示的 S-Data 格式。 safety_data 是安全更新数据。

12.7.2.4 SFSPM-S

12.7.2.4.1 状态转换

图 34 示出了 SFSPM-S 的状态转换图。

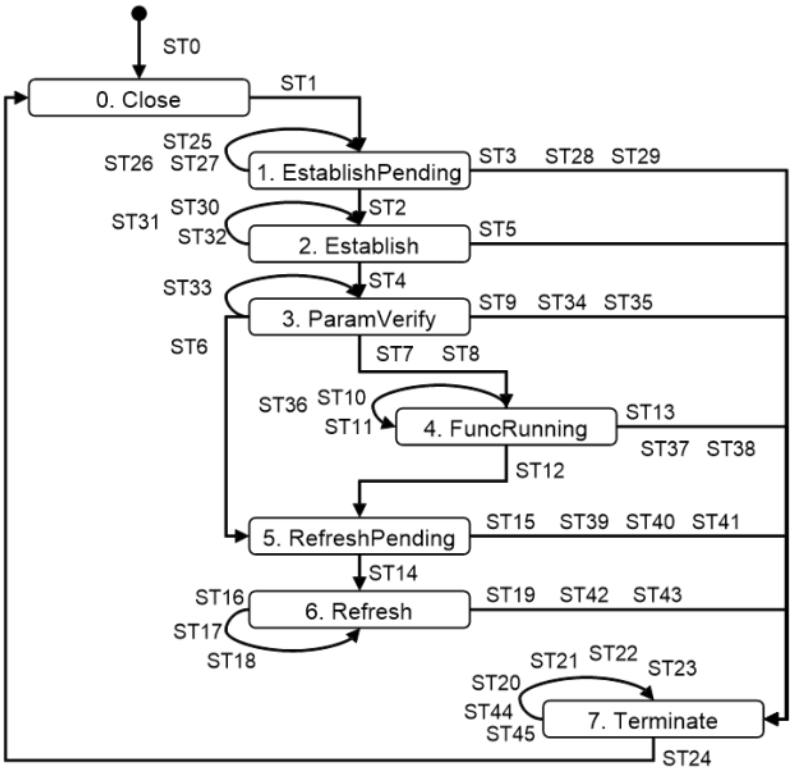

图 34　SFSPM-S 状态转换图

表39列出了SFSPM-S所用的定时器。

表 39　SFSPM-S 定时器

名称	描述
roundtrip_timer	用于检测除安全刷新期间外的不允许延迟。 它在 allowable_roundtrip_delay 之后到期。
delay_detection_timer	用于检测不允许的延迟。它在 allowable_refresh_interval 之后到期。

表40列出了SFSPM-S的状态转换表。

表 40　SFSPM-S 状态转换表

转换	状态	条件	动作	下一状态
ST0	—	Black channel ready	—	0.Close
ST1	0.Close	Receive S-Connect-req [NoError]	Send S-Connect-rsp && Start roundtrip_timer	1.EstablishPending
ST2	1.EstablishPending	Receive S-InitConfirmNetPrm-req [NoError]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-rsp && Start roundtrip_timer	2.Establish
ST25	1.EstablishPending	Receive S-Connect-req [NoError]	Stop roundtrip_timer && Send S-Connect-rsp &&	1.EstablishPending

转换	状态	条件	动作	下一状态
			Start roundtrip_timer	
ST26	1.EstablishPending	Receive S-InitConfirmNetPrm-req [Busy]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-rsp && Start roundtrip_timer	1.EstablishPending
ST27	1.EstablishPending	roundtrip_timer timeout	—	7.Terminate
ST3	1.EstablishPending	Receive S-InitConfirmNetPrm-req [Error]	Stop roundtrip_timer && Send S-InitConfirmNetPrm-rsp	7.Terminate
ST28	1.EstablishPending	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST29	1.EstablishPending	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST4	2.Establish	Receive S-InitVerifyStnPrm-req [NoError]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-rsp && Start roundtrip_timer	3.ParamVerify
ST30	2.Establish	Receive S-InitVerifyStnPrm-req [Busy]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-rsp && Start roundtrip_timer	2.Establish
ST31	2.Establish	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST32	2.Establish	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST5	2.Establish	roundtrip_timer timeout	—	7.Terminate
ST5	2.Establish	Receive S-InitVerifyStnPrm-req [Error]	Stop roundtrip_timer && Send S-InitVerifyStnPrm-rsp	7.Terminate
ST6	3.ParamVerify	Receive S-RefreshReady-req [NoError]	Stop roundtrip_timer && Send S-RefreshReady-rsp && Start roundtrip_timer	5.RefreshPending
ST33	3.ParamVerify	Receive S-RefreshReady-req [Busy]	Stop roundtrip_timer && Send S-RefreshReady-rsp && Start roundtrip_timer	3.ParamVerify
ST7	3.ParamVerify	Receive S-InvokeFunc-req [NoError] && Processing complete	Stop roundtrip_timer && Send S-InvokeFunc-rsp [NoBusy]	4.FuncRunning

转换	状态	条件	动作	下一状态
			&& Start roundtrip_timer	
ST8	3.ParamVerify	Receive S-InvokeFunc-req [NoError] && Function in progress	Stop roundtrip_timer && Send S-InvokeFunc-rsp [Busy] && Start roundtrip_timer	4.FuncRunning
ST34	3.ParamVerify	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST35	3.ParamVerify	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rspStart roundtrip_timer	7.Terminate
ST9	3.ParamVerify	roundtrip_timer timeout	—	7.Terminate
ST9	3.ParamVerify	Receive S-InvokeFunc-req [Error]	Stop roundtrip_timer	7.Terminate
ST9	3.ParamVerify	Receive S-RefreshReady-req [Error]	Stop roundtrip_timer && Send S-RefreshReady-rsp	7.Terminate
ST10	4.FuncRunning	Receive S-InvokeFunc-req [NoError] && Processing complete	Stop roundtrip_timer && Send S-InvokeFunc-rsp [NoBusy] && Start roundtrip_timer	4.FuncRunning
ST11	4.FuncRunning	Receive S-InvokeFunc-req [NoError] && Function in progress	Stop roundtrip_timer && Send S-InvokeFunc-rsp [Busy] && Start roundtrip_timer	4.FuncRunning
ST12	4.FuncRunning	Receive S-RefreshReady-req [NoError]	Stop roundtrip_timer && Send S-RefreshReady-rsp && Start roundtrip_timer	5.RefreshPending
ST36	4.FuncRunning	Receive S-InvokeFunc-req [Busy]	Stop roundtrip_timer && Send S-InvokeFunc-rsp && Start roundtrip_timer	4.FuncRunning
ST37	4.FuncRunning	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST38	4.FuncRunning	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST13	4.FuncRunning	roundtrip_timer timeout	—	7.Terminate
ST13	4.FuncRunning	Receive S-InvokeFunc-req	Stop roundtrip_timer	7.Terminate

转换	状态	条件	动作	下一状态
		[Error]	&& Send S-InvokeFunc-rsp	
ST13	4.FuncRunning	Receive S-RefreshReady-req [Error]	Stop roundtrip_timer && Send S-RefreshReady-rsp	7.Terminate
ST14	5.RefreshPending	ReceiveS-RefreshGO-req [NoError]	Stop roundtrip_timer && Send S-RefreshGO-rsp	6.Refresh
ST39	5.RefreshPending	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST40	5.RefreshPending	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST15	5.RefreshPending	roundtrip_timer timeout	—	7.Terminate
ST15	5.RefreshPending	ReceiveS-RefreshGO-req [ErrorA]	Stop roundtrip_timer	7.Terminate
ST15	5.RefreshPending	ReceiveS-RefreshGO-req [ErrorB]	Stop roundtrip_timer && Send S-RefreshGO-rsp && Start roundtrip_timer	7.Terminate
ST16	6.Refresh	Time to send[NoError]	Send S-Refresh-req	6.Refresh
ST17	6.Refresh	Receive S-RefreshMO-req [NoError]	Stop roundtrip_timer	6.Refresh
ST17	6.Refresh	Time to send [at first after S-RefreshMO-req with NoError received]	Send S-RefreshMO-rsp && Start roundtrip_timer	6.Refresh
ST18	6.Refresh	Receive S-RefreshGO-req [NoError]	—	6.Refresh
ST18	6.Refresh	Time to send [at first after S-RefreshGO-req with NoError received]	Send S-RefreshGO-rsp	6.Refresh
ST41	6.Refresh	Receive S-WriteErrorInfo-req [No more data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp	7.Terminate
ST42	6.Refresh	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST19	6.Refresh	Receive S-Refresh-req [Error]	—	7.Terminate
ST19	6.Refresh	Time to send [at first after S-Refresh-req with ErrorA received]	Send S-Refresh-req && Start roundtrip_timer	7.Terminate
ST19	6.Refresh	Receive S-RefreshMO-req [Error]	—	7.Terminate
ST19	6.Refresh	Time to send [at first after S-RefreshMO-req with ErrorA received]	Send S-RefreshMO-rsp && Startroundtrip_timer	7.Terminate

转换	状态	条件	动作	下一状态
ST19	6.Refresh	Receive S-RefreshGO-req [Error]	Stop roundtrip_timer	7.Terminate
ST19	6.Refresh	Time to send [at first after S-RefreshGO-req with ErrorA received]	Send S-RefreshGO-rsp && Startroundtrip_timer	7.Terminate
ST19	6.Refresh	roundtrip_timer timeout	—	7.Terminate
ST20	7.Terminate	Receive S-ReadErrorInfo-req [No more data]	Send S-ReadErrorInfo-rsp	7.Terminate
ST43	7.Terminate	Receive S-ReadErrorInfo-req [More data]	Stop roundtrip_timer && Send S-ReadErrorInfo-rsp && Startp roundtrip_timer	7.Terminate
ST21	7.Terminate	Receive S-WriteErrorInfo-req [No more data]	Send S-WriteErrorInfo-rsp	7.Terminate
ST44	7.Terminate	Receive S-WriteErrorInfo-req [More data]	Stop roundtrip_timer && Send S-WriteErrorInfo-rsp && Start roundtrip_timer	7.Terminate
ST22	7.Terminate	Receive S-InvokeFunc-req [NoError] && Processing complete	Send S-InvokeFunc-rsp [NoBusy]	7.Terminate
ST23	7.Terminate	Receive S-InvokeFunc-req [NoError] && Function in progress	Send S-InvokeFunc-rsp [Busy]	7.Terminate
ST24	7.Terminate	Error resolved	—	0.Close

注 1:ST3、ST5、ST9 和 ST13 错误：异常 CTRL，Error state bit = 1，异常 S-Data
注 2:ST15 Error A：不允许的延迟
注 3:ST15 Error B：顺序不正确，异常 CTRL，Error state bit = 1
注 4:ST19 Error：顺序不正确，丢失，不允许的延迟，异常 CTRL，Error state bit = 1
注 5:ST19 Error A：顺序不正确，异常 CTRL，Error state bit = 1

12.7.2.4.2 非安全刷新期间的操作

SFSPM-S启动定时器roundtrip_timer的同时发出响应指令。作为对来自SFSPM-M的响应的应答，SFSPM-S 将收到下一请求并停止定时器 roundtrip_timer 。 roundtrip_timer 定时器按allowable_roundtrip_delay确定的时间计时到期。如果SFSPM-S在roundtrip_timer定时器到期之前没有收到对其响应的应答的下一请求，则不允许的延迟发生。图35示出了非安全刷新期间的状态序列。

当发送响应时，SFSPM-S将包含在对应请求的安全PDU中的T code的值插入到安全PDU的T code中。

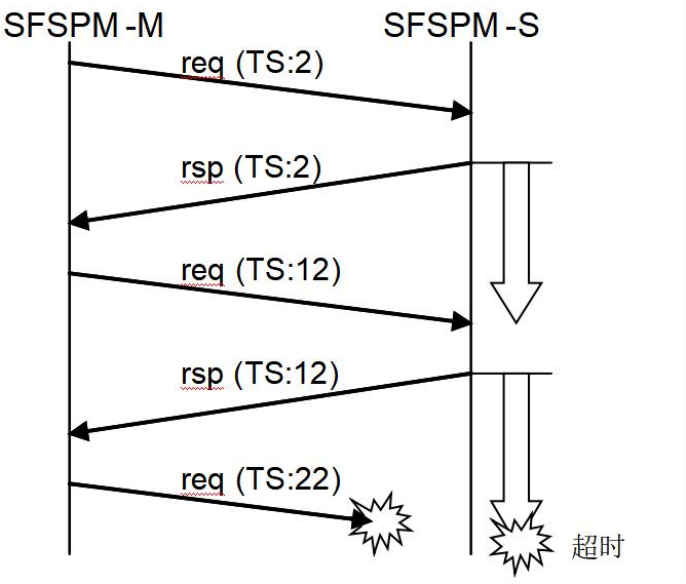

图 35　非安全刷新期间的序列

12.7.2.4.3　S-Data 语法

12.7.2.4.3.1　S-Connect-rsp

S-Connect-rsp使用图15所示的S-Data格式。safety_data区域储存图36中所描述的数据。

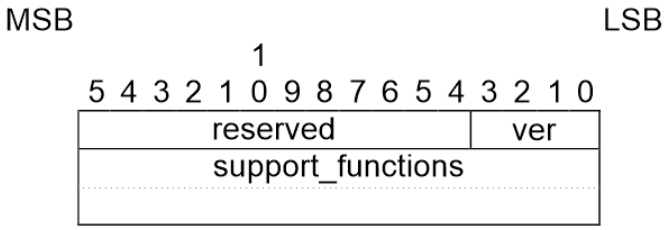

图 36　S-Connect-rsp

ver

指示了SFSPM-S支持的FSCP 8/2的协议版本。协议版本是 0000b。

reserved

保留用于未来扩展。

support_functions

在SFSPM-M报告给SFSPM-S的support_functions中，指示出SFSPM-S所支持的功能。表35列出了规定的功能详情。每一比特表示是否支持该表中的功能。1代表支持该功能，0 代表不支持该功能。SFSPM-S将SFSPM-M通知的support_functions和SFSPM-S支持的功能的逻辑值作为support_functions。

12.7.2.4.3.2　S-InitConfirmNetPrm-rsp

S-InitConfirmNetPrm-rsp使用图15所示的S-Data格式。safety_data区域储存图37中所描述的数据。

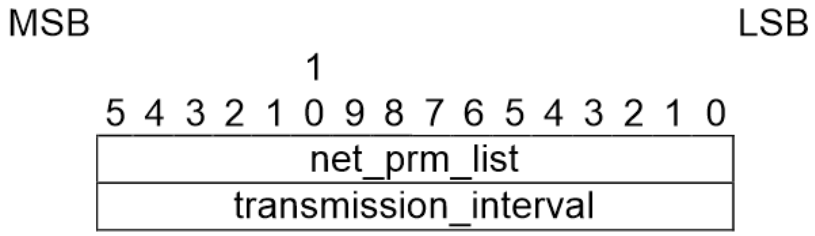

图 37　S-InitConfirmNetPrm-rsp

net_prm_list
需要证实的安全网络参数清单。1表示该参数需要证实，0表示不需要。net_prm_list的结构见图28。transmission_interval的比特设置为1。
transmission_interval
在安全刷新期间SFSPM-S的安全PDU的传输时间间隔。单位为128μs。

12.7.2.4.3.3　S-InitVerifyStnPrm-rsp

S-InitVerifyStnPrm-rsp使用图15所示的S-Data格式。safety_data区域存储图38所描述的数据。

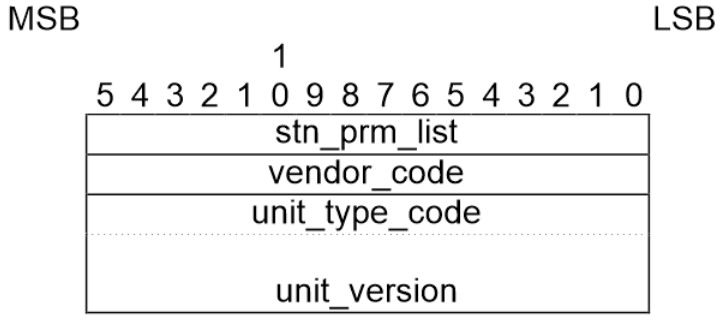

图 38　S-InitVerifyStnPrm-rsp

stn_prm_list
需要验证的安全站参数的列表。详见12.7.2.3.3.3。
vendor_code
分配给供应商的惟一编码，用来标识供应商。
unit_type_code
分配给每一产品型号的惟一编码，由供应商管理。
unit_version
由供应商管理的产品操作规范的版本。

12.7.2.4.3.4　S-InvokeFunc-rsp

S-InvokeFunc-rsp使用图15所示的S-Data格式。safety_data区域储存图39所描述的数据。

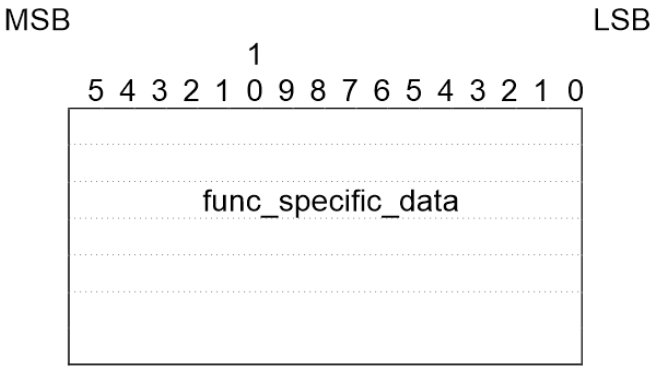

图 39　S-InvokeFunc-rsp

func_specific_data

与S-DataHeader的功能命令所指定的功能相关的数据。为每一功能命令确定Func_specific_data。

12.7.2.4.3.5　S-RefreshReady-rsp

S-RefreshReady-rsp使用图15所示的S-Data格式。safety_data区域不存储任何信息。

12.7.2.4.3.6　S-ReadErrorInfo-rsp

S-ReadErrorInfo-req使用图15所示的S-Data格式。safety_data区域存储图32所示的数据。safety_data详见12.7.1.6。

12.7.2.4.3.7　S-WriteErrorInfo-rsp

S-WriteErrorInfo-rsp使用图15所示的S-Data格式。safety_data区域不存储任何信息。

12.7.2.4.3.8　S-RefreshMO-rsp

S-RefreshMO-rsp使用图14所示的S-Data格式。safety_data是安全刷新数据。

12.7.2.4.3.9　S-RefreshGO-rsp

S-RefreshGO-rsp使用图14所示的S-Data格式。safety_data是安全刷新数据。

12.7.2.4.3.10　S-Refresh-req

S-Refresh-req使用图14所示的S-Data格式。safety_data是安全刷新数据。

12.7.2.5　时钟偏移校正

SFSPM-M和SFSPM-S安全时钟的差值是偏移量ts_offset。

SFSPM-M应使用其自身节点安全时钟低16比特的值生成时间戳。

SFSPM-S应使用其自身节点安全时钟低16比特的值current_time和偏移量ts_offset生成时间戳。SFSPM-S应使用公式（1）进行时间戳的计算：

$$T\ code=(current\_time+ts\_offset) \bmod 216$$

图40示出了安全时钟偏移量的计算过程。

注 1：该算法是 Cristian 算法的修改版。

注 2：FSCP 8/2 使用基于令牌传输的确定媒体接入控制。由于只有获得令牌才能执行传输，所以在中间节点没有冲突或多帧排队。此外，在两个节点之间只能建立一个逻辑路径。

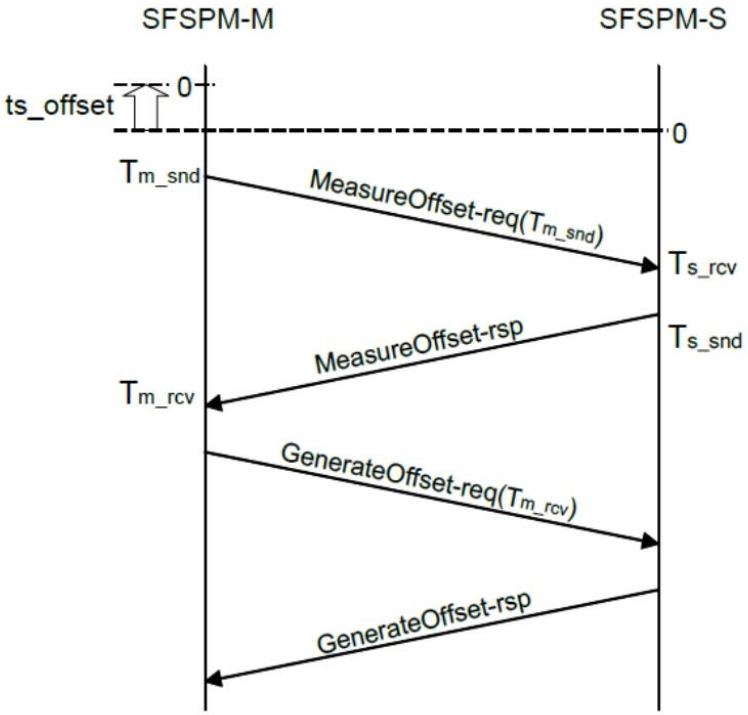

图 40　安全时钟偏移量的计算过程

SFSPM-M生成MeasureOffset-req，并向SFSPM-S发送MeasureOffset-req，该MeasureOffset-req包括MeasureOffset-req发送时的安全时钟值。

SFSPM-S接收MeasureOffset-req，并记录接收到的安全时钟值和MeasureOffset-req中包括的安全时钟值。然后，SFSPM-S生成MeasureOffset-rsp，记录MeasureOffset-rsp发送时的安全时钟值，并向SFSPM-M发送所生成的MeasureOffset-rsp。

SFSPM-M接收MeasureOffset-rsq，并记录接收到的安全时钟值。然后接收到MeasureOffset-rsq的SFSPM-M生成GenerateOffset-req，该GenerateOffset-req包括MeasureOffset-rsp接收时安全时钟值的偏移量计算信息，并向SFSPM-S发送GenerateOffset-req。

SFSPM-S接收GenerateOffset-req，计算并存储所接收安全时钟值的偏移量ts_offset和GenerateOffset-req中偏移量计算信息。然后，SFSPM-S生成GenerateOffset-rsp，该GenerateOffset-rsp存储OBL中所使用的ts_offset与计算出的ts_offset的差值，并向SFSPM-M发送GenerateOffset-rsp。

SFSPM-S验证偏移量计算时的往返传输延迟是在利用公式（2）进行ts_offset计算的范围。如果传输延迟在这个范围之外，SFSPM-S不应使用偏移量计算中收集到的信息。

$$0 < (Tm\_rcv - Tm\_snd) - (Ts\_snd - Ts\_rcv) <= 2 \times link\_transmission\_delay \quad (2)$$

link_transmission_delay是FSCP 8/2网络的传输延迟，通过allowable_refresh_interval、SFSPM-M transmission_interval以及SFSPM-S transmission_interval（见12.7.2)三个参数利用公式（3）计算获得。

$$Dlt = Iar - Imt - Ist \quad (3)$$

其中：

Dlt为链路传输延迟；

Iar为允许刷新间隔；

Imt为SFSPM-M传输间隔；

Ist为SFSPM-S传输间隔。

使用公式（4）计算偏移量ts_offset：

$$ts\_offset = 0.5 \times ((Tm\_rcv + Tm\_snd) - (Ts\_snd + Ts\_rcv)) \quad (4)$$

在计算出的偏移ts_offset中，包括利用公式（5）计算出的偏差offset_dispersion：

$$offset\_dispersion = 0.5 \times ((Tm\_rcv - Tm\_snd) + (Ts\_rcv - Ts\_snd)) \quad (5)$$

计算偏差offset_dispersion的最大值为link_transmission_delay。

当SFSPM-M接收到GenerateOffset-rsp时，SFSPM-M确认SFSPM-S计算偏移量。SFSPM-M 接收GenerateOffset-rsp，并使用可调整的T code替代GenerateOffset-rsp中的T code，以便发现不正确的命令和GenerateOffset-rsp接收的丢失，确定12.7.2中描述的传输间隔。可调整的T code是从接收到的GenerateOffset-rsp的T code中存储的值减去SFAPM-S接收到的GenerateOffset-rsp的OBL中存储的值所获得的值，即SFSPM-S计算出的ts_offset与SFSPM-S使用的ts_offset之间的差值。

注：由于安全刷新过程中进行偏移量计算，当SFSPM-S改变ts_offset，SFSPM-S的实际传输间隔不同于从GenerateOffset-rsp的T code中减去前面接收到的PDU的T code计算出的值。执行这个过程产生两个匹配值。

在安全连接建立的时候进行偏移量计算，在安全刷新过程中周期地进行偏移量计算。在安全连接建立的时候，S-RefreshReady作为 MeasureOffset，S-RefreshGO作为 GenerateOffset。SFSPM-M向SFSPM-S发送Tm_snd和Tm_rcv，分别作为S-RefreshReady的T code和S-RefreshGO的OBL。在安全刷新过程中，S-RefreshMO作为MeasureOffset，S-RefreshGO 作为GenerateOffset。SFSPM-M向SFSPM-S发送Tm_snd和Tm_rcv分别作为S-RefreshMO的T code和S-RefreshGO的OBL。

在安全刷新过程中，SFSPM-M应在下列定义的间隔校正时钟偏移。应确定resolution_factor，以便时钟漂移产生的错误低于128μs（即:安全时钟测量单位），如公式（6）所示。

$$interval= transmission\_interval \times resolution\_factor \quad (6)$$

如果安全时钟精度是100ppm，则每秒最大误差是±100μs。当SFSPM-M误差和SFSPM-S安全时钟方向相反时，时钟漂移产生的每秒最大误差是200μs。同时，可以在小于等于640ms间隔校正时钟偏移，使误差小于128μs。在这种情况下，resolution_factor计算公式（7）如下。

$$resolution\_factor < 640 / transmission\_interval \quad (7)$$

12.7.2.6 接收时间的计算

在接收的时候，SFSPM-M应使用其自身节点安全时钟低16比特的值。

SFSPM-S应使用根据receipt_time和偏移量ts_offset通过公式（8）计算出的时间值，receipt_time是接收时安全时钟低16比特的值。

$$time = (receipt\_time + ts\_offset) \bmod 2^{16} \quad (8)$$

12.7.2.7 carry_counter 操作

SFSPM-S使用公式（9），由current_time（即SFSPM-S安全时钟的低16比特）和偏移ts_offset计算出SFSPM-M_current_time。每次传输和接收一个安全PDU。

$$SFSPM\text{-}M\_current\_time = (current\_time + ts\_offset) \bmod 2^{16} \quad (9)$$

如果满足公式（10），carry_counter加1。

$$prev\_SFSPM\text{-}M\_current\_time > SFSPM\text{-}M\_current\_time \quad (10)$$

其中，prev_SFSPM-M_current_time是已计算出的SFSPM-M_current_time。

传输间隔transmission_interval和 current_time的单位和字长是相同的。current_time溢出计数是1（最大值，只要在transmission_interval之内传输）。因此，carry_counter加1。

12.8 FSCP 8/2 的安全通信层管理

12.8.1 参数定义

12.8.1.1 参数列表

表41列出了FSCP8/2使用的参数。

表 41 安全通信层使用的参数 (表序和图序需要更新)

参数名称	内容	可配置的/可生成的
connection_id	安全连接标识符	可配置的
transmission_interval	传输间隔	可配置的
allowable_refresh_interval	允许的刷新间隔	可配置的
allowable_delay	最大允许延迟	安全通信层生成的
allowable_roundtrip_delay	允许的往返延迟	安全通信层生成的

12.8.1.2 connection_id

Connection_id是可配置参数，该参数表明传输源和传输目的地之间关系的标识符，其大小为32比特。应分配connection_id为网络中的唯一值。为了保证唯一性，connection_id应是由传输源地址和传输目的地址（每个16比特）生成的值。由网络编号和站编号（每个8比特）生成传输源地址和传输目的地址。

12.8.1.3 transmission_interval

Transmission_interval是可配置参数，该参数表明安全刷新过程中传输安全PDU的最大间隔，其大小为16比特，单位是128μs。最小值是2。

安全PDU的传输间隔有时是变化的。实际传输间隔变化应在下列范围内，见公式（11）：

$$transmission\_interval / 2 < \text{实际传输间隔} \leq transmission\_interval \quad (11)$$

为了正常接收到以最大传输间隔（transmission_interval）发送的安全PDU，实际传输间隔的上限值应小于等于最大传输间隔。另一方面，连续传送3个安全PDU时，为了检测出中间的安全PDU是否丢失，要求实际传输间隔设定下限值。图41示出了这种情况的序列。如传输时间值小于最小传输间隔的两倍，则能够检测到第二个安全PDU的丢失。

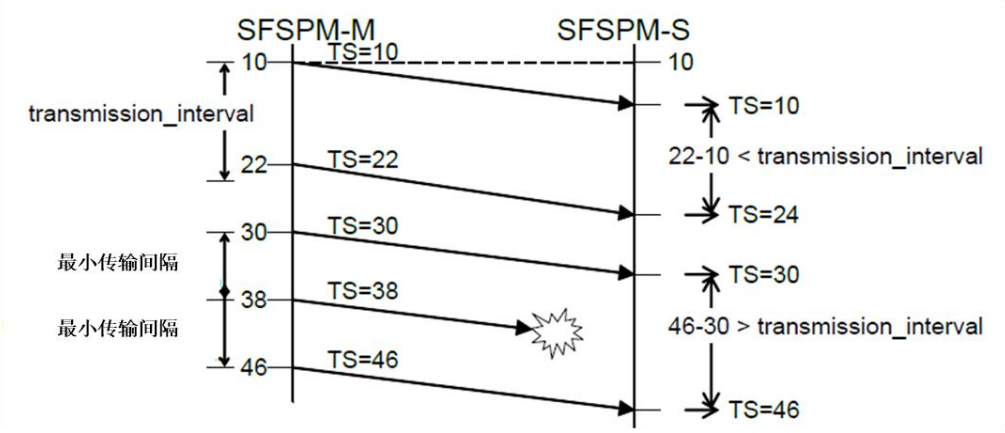

图 41 传输间隔变化与 transmission_interval 之间的关系

12.8.1.4 allowable_refresh_interval

allowable_refresh_interval是可配置参数，该参数表明接收节点允许的刷新间隔，其大小为16比特，单位是128 μs。

当SFSPM-M向SFSPM-S发送安全PDU时，使用下列公式计算SFSPM-S中的allowable_refresh_interval：

SFSPM-S允许刷新间隔I_{sar}用公式（12）计算：

$$I_{sar} = I_t + D_{lt} + T_{spc} \tag{12}$$

其中，I_{sar}为SFSPM-S允许刷新间隔；I_t为SFSPM-M传输间隔；D_{lt}为FAL23网络的链路传输延迟，T_{spc}为SFSPM-S处理周期。

当SFSPM-S是安全逻辑设备时，SFSPM-S处理周期与被处理内容相关。当SFSPM-S是安全输入/输出设备时，SFSPM-S处理周期与实现有关。

图42示出了SFSPM-S和SFSPM-M的allowable_refresh_interval确定过程。

在从SFSPM-M到SFSPM-S的通信过程中，当最大延迟时间(TS3-TS4)在最短延迟时间(TS1-TS2)之后时，按下列方式计算接收间隔，其中transmission_interval (SFSPM-M)表示SFSPM-M的transmission_interval。

SFSPM-S接收间隔I_{sr}用公式（13）和公式（14）计算：

$$I_{sr} = I_t + D_t + T_{soc} \tag{13}$$

$$I_{sr} = I_{tm} + D_{lt} + T_{spc} \tag{14}$$

其中，I_{sr}为SFSPM-S接收间隔(TS4-TS2)；I_t为传输间隔(TS3-TS1)；D_t为类型23（CC-Link IE）网络传输延迟；T_{soc}为SFSPM-S运行周期；I_{tm}为SFSPM-M传输间隔；D_{lt}为链路传输延迟；T_{spc}为SFSPM-S处理周期。

相同的过程适用于SFSPM-S，transmission_interval (SFSPM-S)表示SFSPM-S的transmission_interval。

SFSPM-S允许刷新间隔I_{sar}用公式（15）计算：

$$I_{sar} = I_t + D_{lt} + T_{mpc} \tag{15}$$

其中，I_{sar}为SFSPM-S允许刷新间隔；I_t为传输间隔；D_{lt}为链路传输延迟；T_{mpc}为SFSPM-M处理周期。

假设transmission_interval与运行周期相同，则SFSPM-M和SFSPM-S的计算公式相同。计算公式如下：

允许刷新间隔I_{ar}用公式（16）计算：

$$I_{ar} = D_{lt} + T_{mpc} + T_{spc} \tag{16}$$

其中，I_{ar}为允许刷新间隔；D_{lt}为链路传输延迟；T_{mpc}为SFSPM-M处理周期；T_{spc}为SFSPM-S处理周期。

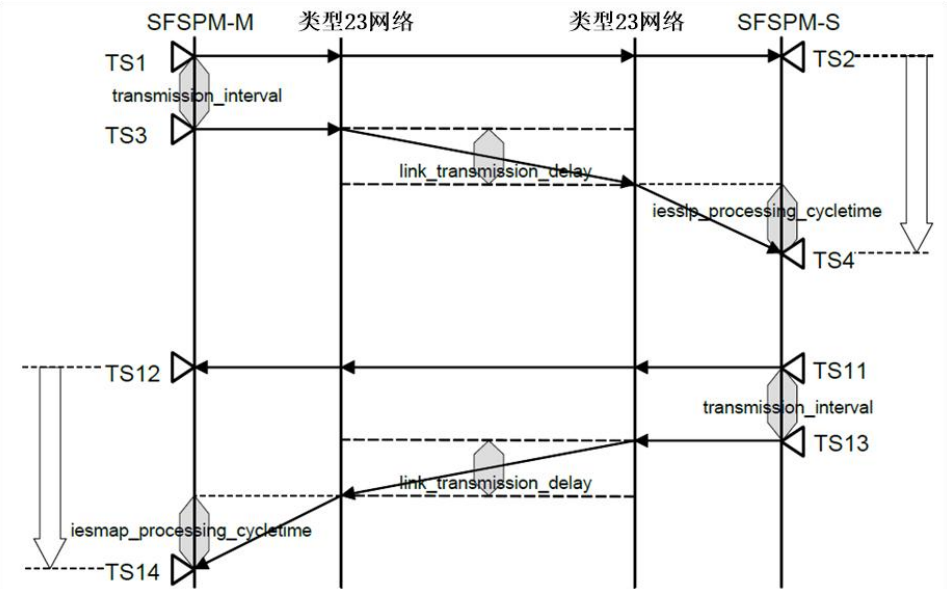

图 42　allowable_refresh_interval 的计算

12.8.1.5　allowable_delay

allowable_delay是最大允许延迟，是用于检测非允许延迟出现情况的参数，其大小为16比特，单位是128μs。

下列是计算allowable_delay的公式。Transmission_interval(SFSPM-M)和transmission_interval(SFSPM-S)分别表示SFSPM-M和SFSPM-S的传输间隔。同allowable_refresh_interval，假设transmission_interval与运行周期相同。

SFSPM-M的允许延迟D_{ma}用公式（17）和公式（18）计算：

$$D_{ma} = D_{lt} + T_{mpc} \quad (17)$$

$$D_{ma} = I_{ar} - I_{st} \quad (18)$$

SFSPM-S的允许延迟D_{sa}用公式（19）和公式（20）计算：

$$D_{sa} = D_{lt} + T_{spc} \quad (19)$$

$$D_{sa} = I_{ar} - I_{mt} \quad (20)$$

其中，D_{ma}为SFSPM-M允许延迟；D_{ms}为SFSPM-S允许延迟；D_{lt}为链路传输延迟；T_{mpc}为SFSPM-M处理周期；T_{spc}为SFSPM-S处理周期；I_{ar}为允许刷新间隔；I_{mt}为SFSPM-M传输间隔；I_{st}为SFSPM-S传输间隔。

图43示出了从SFSPM-M到SFSPM-S及从SFSPM-S到SFSPM-M传输allowable_delay的确定过程。

从SFSPM-M在TS1发送安全PDU时刻到SFSPM-S在TS2接收安全PDU时刻的时间，是FSCP 8/2网络传输延迟和接收侧SFSPM-S运行周期的总和。反之，从SFSPM-S在TS3发送安全PDU时刻到SFSPM-M在TS4接收安全PDU时刻的时间，是传输延迟和接收侧SFSPM-M运行周期的总和。

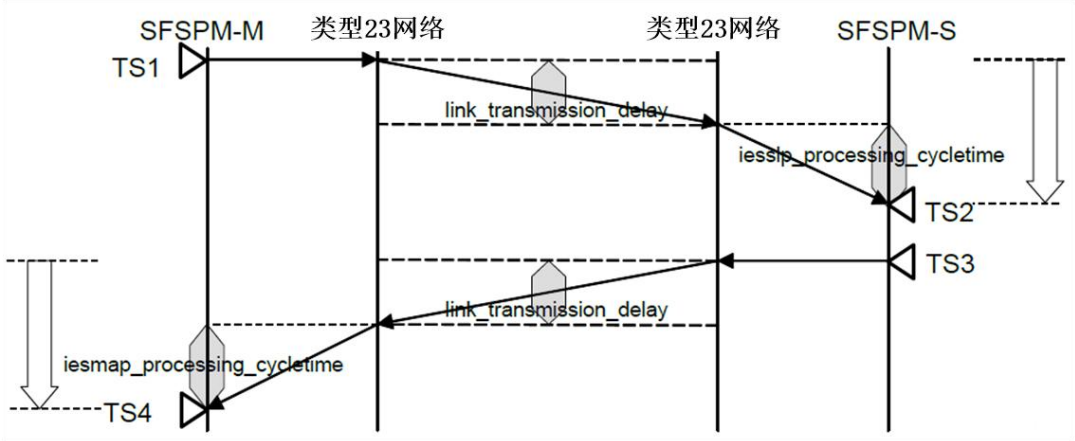

图 43　allowable_delay 的计算

12.8.1.6　allowable_roundtrip_delay

allowable_roundtrip_delay是在运行中而不是安全刷新中SFSPM-M使用的参数。其大小是allowable_refresh_interval的3倍，单位是128μs。在SFSPM-M向SFSPM-S通知allowable_refresh_interval前，SFSPM-S使用预设值。

12.8.2　参数设置

在安全通信层，使用12.6中描述的服务以设置表41中的参数。

12.8.3　管理服务

12.8.3.1　SM-SetSafetyStationInfo

SM-SetSafetyStationInfo是用于设置安全站信息的服务。表42列出了SM-SetSafetyStationInfo的参数。

表 42　SM-SetSafetyStationInfo

参数名称	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			U	U(=)
R Data			U	U(=)

Parameter
规定了安全站信息的设置参数，见表43。
R Data
包含参数设置的结果，可以是任意值。

表 43　SM-SetSafetyStationInfo 安全站信息的设置参数

序号	项	长度 (八位位组)	范围	备注
1	Network number	1	0 - 255	0 和 240-255：保留
2	Station number	1	0 - 255	121-255：保留
3	Safety station type	2	0x0000 - 0xFFFF	0x0：安全 PLC 0x1-0x3：保留 0x4：安全远程设备 0x5：安全远程 I/O 0x6-0xFFFF：保留
4	Vendor code	2	0x0000 - 0xFFFF	分配给每个供应商的编号
5	Vendor model code	4	0x00000000 - 0xFFFFFFFF	供应商为每个产品型号分配的惟一编号
6	Operationspecification version	2	0x0000 - 0xFFFF	供应商管理的产品操作规范的版本
7	Safety protocol version	2	0x00 - 0xFF	本协议版本：00

12.8.3.2　SM-SetSafetyNetworkParameter

SM-SetSafetyNetworkParameter是用于设置安全网络参数的服务。表44列出了SM-SetSafetyNetworkParameter的参数。

表 44　SM-SetSafetyNetworkParameter

参数名称	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			U	U(=)
R Data			U	U(=)

Parameter
规定了安全网络参数。见表 45。
R Data
包含参数设置的结果，其值可以任意设置。

表 45　SM-SetSafetyNetworkParameter 的安全网络参数

序号	项	长度 (八位位组)	范围	备注
1	Network number	1	0 - 255	0 和 240-255：保留
2	Station number	1	0 - 255	121-255：保留
3	Safety connection identifier	4	0x00000000 - 0xFFFFFFFF	
4	Safety connection end type	1	0x0 - 0x1	0x0:SFSPM-M 0x1:SFSPM-S
5	Maximum transmission interval	2	2 - 65535	
6	Allowable refresh interval	2	1 - 65535	
7	Safety data size	1	0-16	单位:八位位组

12.8.3.3　SM-GetSafetyStationInfo

SM-GetSafetyStationInfo是用于读取安全站信息的服务。表46列出了SM-GetSafetyStationInfo的参数。

表 46　SM-GetSafetyStationInfo

参数名称	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Parameter

规定了采集的目的站，见表47。

R Data

包含采集结果，见表48。

表 47　SM-GetSafetyStationInfo（请求）的安全站信息参数

序号	项	长度 (八位位组)	范围	备注
1	Network number	1	0 - 255	0 和 240-255：保留
2	Station number	1	0 - 255	121-255：保留

表 48　SM-GetSafetyStationInfo（响应）的安全站信息参数

序号	项	长度 (八位位组)	范围	备注
1	Safety station type	2	0x0000 - 0xFFFF	0x0：安全 PLC 0x1-0x3：保留 0x4：安全远程设备 0x5：安全远程 I/O 0x6-0xFFFF：保留
2	Vendor code	2	0x0000 - 0xFFFF	分配至每个供应商的编号
3	Vendor model code	4	0x00000000 - 0xFFFFFFFF	供应商为每个产品型号分配的惟一代码
4	Operation specification version	2	0x0000 - 0xFFFF	供应商分配的产品操作规范的版本

5	Safety protocol version	2	0x00 - 0xFF	本协议版本：00

12.8.3.4 SM-GetSafetyNetworkParameter

SM-GetSafetyNetworkParameter 是用于读取安全网络参数的服务。表 49 列出了 SM-GetSafetyNetworkParameter 的参数。

表 49 SM-GetSafetyNetworkParameter

参数名称	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Parameter	M	M(=)		
Result			M	M(=)
R Data			M	M(=)

Parameter

规定了采集的目的站，见表50。

R Data

包含采集结果，见表51。

表 50 SM-GetSafetyNetworkParameter 请求的参数

序号	项	长度 (八位位组)	范围	备注
1	Network number	1	0 - 255	0 和 240-255：保留
2	Station number	1	0 - 255	121-255：保留
3	Safety connection identifier	4	0x00000000 - 0xFFFFFFFF	

表 51 SM-GetSafetyNetworkParameter 响应的参数

序号	项	长度 (八位位组)	范围	备注
1	Safety connection end type	1	0x0 - 0x1	0x0:SFSPM-M 0x1:SFSPM-S
2	Maximum transmission interval	2	1 - 65535	
3	Allowable refresh interval	2	1 - 65535	
4	Safety data size	1	0-16	单位:八位位组

12.9 FSCP 8/2 的系统要求

12.9.1 指示灯和开关

12.9.1.1 开关

FSCP 8/2未规定开关。

12.9.1.2 指示灯

指示灯要求见表20、表52和表53。M表示必备的，O表示可选的，R表示推荐的。

指示灯的类型、颜色和外形不作规定。此外，使用带显示屏的计算机或其他设备时，可通过显示屏进行指示。对于通信端口的监视，建议能够显示标识安全主站和安全从站上每个通信端口。

表 52 监视指示灯

序号	指示灯名称	描述	安全主站	安全从站本地站	安全从站智能设备站	安全从站远程设备站	安全从站远程I/O站
1	PW	亮:电源接通 灭:电源关断	R	R	R	R	R
2	RUN	亮:运行正常 灭:站出错	M	R	R	O	O
3	ERR	亮:错误 安全主站: ▪ 站编号冲突 ▪ 获取的网络信息不一致 ▪ 站内出错 安全从站: ▪ 站出错 闪烁:数据链路出错 安全主站: ▪ 站中存在数据链路错误 灭:运行正常	M	R	R	0	O
4	MST	亮:作为主站运行 灭:未作为主站运行	O	—	—	—	—
5	D LINK	亮:执行周期性传输 灭:未连接	M	R	R	O	O
6	L.ERR	亮:接收到的数据有错误 灭:接收到的数据正常	M	R	R	R	R
7	SD	亮:数据正在发送中 灭:无数据发送	R	R	R	R	R
8	RD	亮:数据正在接收中 灭:无数据接收	R	R	R	R	R

表 1　通信端口监视指示灯

序号	指示灯名称	描述	安全主站	安全从站本地站	安全从站智能设备站	安全从站远程设备站	安全从站远程 I/O 站
1	LINK	亮:链路运行中 灭:链路未运行	O	O	O	O	O
2	L.ER	亮:接收到的数据有错误 灭:接收到的数据正常	O	O	O	O	O

12.9.2　安装指南

本文件规定了基于IEC 61158类型23的安全通信系统的协议和服务。使用符合本文件规定的安全协议的安全设备时，要求其正确安装。所有连接到本文件规定的安全通信系统的设备，都应遵循建议并符合IEC 61784-5-8中的规定。

12.9.3　安全功能响应时间

图44示出了FSCP 8/2安全站之间，安全通信期间内响应时间的概念。以两个安全PLC之间响应时间的计算为例进行说明。

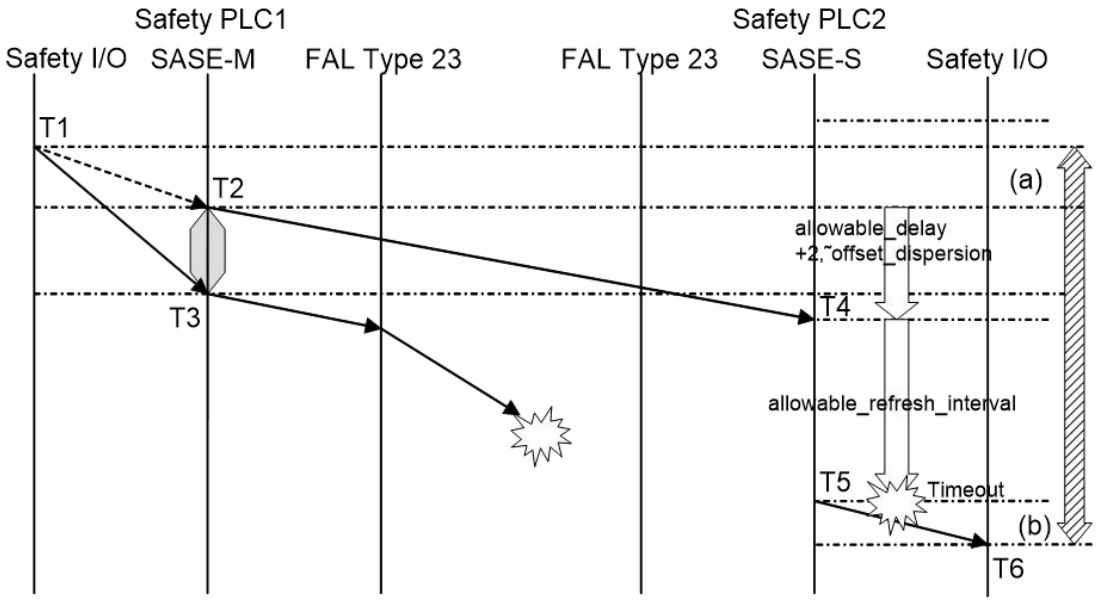

图 44　安全 PLC 之间响应时间的计算

图44中从安全PLC 1到安全PLC 2的安全通信响应时间即T1到T6时间段。T1到T2时间段是输入设备响应时间。若在T2之前进行传输，传输执行在下一个传输间隔，造成的等待时间等于一个传输间隔（SASE-M和SFSPM-M）。

最差情况是在T3时刻发送安全PDU时，值丢失。在T5时刻确认，应在T3时刻发送的安全PDU是否未在规定时间内到达。从T5到T6的时间段是输出设备的响应时间。在这种情况下，最差情况的响应时间TR用公式（21）、公式（22）和公式（23）计算：

$$TR = a + D_a + (2 \times O_d) + I_{ar} + b \tag{21}$$

$$TR = a + D_{lt} + T_{mpc} + (2 \times D_{lt}) + I_t + D_{lt} + T_{spc} + b \tag{22}$$

$$TR = a + b + T_{mpc} + (4 \times D_{lt}) + (2 \times T_{spc}) \tag{23}$$

其中，TR为响应时间；a为输入设备响应时间；D_a为允许延时；O_d为抖动偏移值；I_{ar}为允许刷新间隔；b为输出设备响应时间；D_{lt}为FSCP 8/2 链路传输延迟；T_{spc}为SASE-S 处理周期；T_{mpc}为SFSPM-M处理周期；I_t为传输间隔(SFSPM-M)。

其中，TR为响应时间；a为输入设备响应时间；D_a为允许延时；O_d为抖动偏移值；I_{ar}为允许刷新间隔；b为输出设备响应时间；D_{lt}为FSCP 8/2 网络链接传输延时；T_{spc}为SASE-S 处理周期。

注：$2 \times O_d$的抖动偏移值的详细解释，见附录A。

12.9.4　要求的持续时间

安全相关应用对安全通信层要求的持续时间应充足，以保证在最长的安全功能响应时间内，该应用能检测到此要求。安全通信层持续时间应充足，以保证安全相关应用在最长的安全功能响应时间内能检测到此要求。

12.9.5　系统特性计算的约束

FSCP 8/2是SIL3功能安全通信协议，即每小时残差率SCL（λ_{SCL}）$< 10^{-9}$。

依据IEC 61158类型23实现FSCP 8/2安全系统的唯一限制是报文储存元件(例如交换机和路由器)的最大数量（N_{SE}）。N_{SE}由各安全功能允许的最大逻辑连接数（m）和传输间隔（I_t）的函数关系决定。

FSCP 8/2安全系统应符合约束$N_{SE,}$即m和I_t的函数，见公式（24）所示。

$$N_{SE}(I_T,\mathrm{m}) < \frac{3{,}602\times10^{7}}{I_t\times\mathrm{m}} - \frac{3{,}515\times10^{3}}{I_t^{2}} \tag{24}$$

其中

N_{SE}为黑色通道的储存元件（例如交换机和路由器）的数量；

I_t为传输间隔（ms），范围为1至2000；

m为各安全功能允许的最大逻辑连接数量。

图45表示了依据公式（24）I_t不同取值时（见图中对应线）N_{SE}和m间的对应关系。

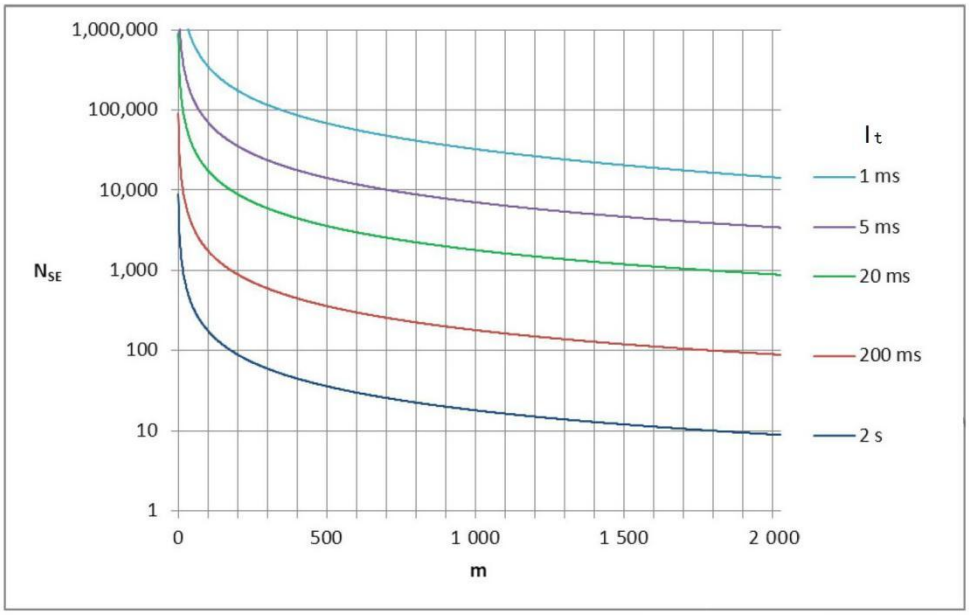

图 45　N_{SE} 和 m 之间的约束关系

图45中可看出在实现FSCP 8/2时，若$m<100$且$N_{SE}<100$，则无需考虑传输间隔。然而，对于非常复杂的安全功能（$m>500$）或具有大量黑色通道装置（$N_{SE}>500$）时，则需要考虑使用较长安全传输间隔的安全网络限制，并使用公式（24）进行计算。

12.9.6　维护

对于FSCP 8/2未规定维护方面的SCL特殊要求。

如果发生设备维修及更换，属于系统行为方面的规范，已经超出本文件的范围。这些行为的规范和责任与本文件的服务和协议无关。这些通常是功能安全管理计划的内容。但是，根据IEC 61508的规定，维修、更换以及维护，总体安全验证、总体运行、更改、改造和停运或处置是必须考虑的重要议题。同时建议联系设备或系统供应商。

关于SRP编程和安全设备参数设置的信息，强烈建议联系设备或系统供应商。此外，建议考虑CC-Link功能安全规范。这些文档包含了FSCP 8/2系统用户的其他信息。

注：[30]和[31]包含了维护相关的重要信息。

维护方面的附加要求及其他要求，在IEC 61508, IEC 61511和/或IEC 62061中规定。

12.9.7　安全手册

基于FSCP 8/2内嵌SCL的安全从站的供应商，应根据IEC 61508的要求，准备合适的安全手册。该安全手册也应包含11.9.2中规定的安全要求，以及用于设备配置开关的指南。

基于IEC 61158类型23的完整的安全通信系统应考虑CC-Link IE安全规范。

注 1：[30]和[31]包含安全手册相关的重要信息。

注 2：在安全设备启动安装运行之前，建议联系 CLPA 以确定实施指南和/或实施要求为最新版本。

12.10 FSCP 8/2 的评估

制造商有责任依据安全标准（见IEC 61508、IEC 61511、IEC 62061等）以及相关法律条例（如欧盟机械指令）规定的开发过程来开发设备。附加信息见附录B。

附 录 A
(资料性附录)
功能安全通信行规 CPF8 的附加信息

A.1 FSCP 8/1 的哈希函数计算

FSCP 8/1的CRC32的计算使用以下算法:

$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

该算法使用 0x104C11DB7由ISO/IEC/IEEE 8802-3定义。

代码长度为96字节。

残余误差概率作为误码率 (BER) 的函数, 表示了。示值如表 A.1 所示。

表 A.1 FSCP 8/1 的 CRC 残余误差概率

n(bits)	BER = 2/n	BER = 4/n	BER = 0,01	BER = 0,001	BER = 0,0001
96	8.5046432E-14	6.0272142E-12	4.3703467E-16	6.7137731E-24	6.9713053E-32

A.2 FSCP 8/2 的哈希函数计算

FSCP 8/2的CRC32的计算使用以下算法:

$G(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{24} + x^{23} + x^{20} + x^{17} + x^{13} + x^{11} + x^4 + x^2 + 1$

这个算法定义为[32]中给出的0x1F1922815。

代码长度范围从 224字节到 992 字节, 增量为 32 字节。

残余误差概率曲线作为误码率 (BER) 的功能表示行为。示值如表A.2所示。

表 A.2 FSCP 8/1 CRC 的残余误差概率

n(比特)	BER=2/n	BER=4/n	BER=0,01	BER=0,001	BER=0,0001
224	4.0322236E-13	1.6638772E-11	7.9879086E-13	5.3605698E-20	6.5083171E-28
256	4.0958621E-13	1.6802011E-11	1.7536098E-12	1.5470990E-19	1.9329636E-27
288	4.1226780E-13	1.6845400E-11	3.3658478E-12	3.8931551E-19	5.0054622E-27
320	4.1234883E-13	1.6806216E-11	5.8216501E-12	8.8020027E-19	1.1645257E-26
352	4.1362666E-13	1.6817799E-11	9.3328421E-12	1.8403714E-18	2.5054735E-26
384	4.1494272E-13	1.6836188E-11	1.4028534E-11	3.5989796E-18	5.0416342E-26
416	4.1583997E-13	1.6843934E-11	1.9967756E-11	6.6464215E-18	9.5802640E-26
448	4.1662508E-13	1.6851175E-11	2.7160147E-11	1.1697734E-17	1.7349197E-25
480	4.1738988E-13	1.6860416E-11	3.5547838E-11	1.9756122E-17	3.0147964E-25
512	4.1818700E-13	1.6873006E-11	4.5015881E-11	3.2193220E-17	5.0546386E-25
544	4.1892070E-13	1.6885164E-11	5.5390975E-11	5.0825605E-17	8.2104736E-25
576	4.1948634E-13	1.6892887E-11	6.6460435E-11	7.8003437E-17	1.2964312E-24
608	4.1998645E-13	1.6899575E-11	7.8014686E-11	1.1675705E-16	1.9964542E-24
640	4.2043580E-13	1.6905565E-11	8.9834198E-11	1.7089060E-16	3.0062514E-24
672	4.2083214E-13	1.6910621E-11	1.0170590E-10	2.4511218E-16	4.4360174E-24
704	4.2120519E-13	1.6915658E-11	1.1343936E-10	3.4519998E-16	6.4270369E-24

n(比特)	BER=2/n	BER=4/n	BER=0,01	BER=0,001	BER=0,0001
736	4.2154801E-13	1.6920328E-11	1.2486316E-10	4.7811770E-16	9.1575007E-24
768	4.2186554E-13	1.6924719E-11	1.3583561E-10	6.5219642E-16	1.2850293E-23
800	4.2217609E-13	1.6929400E-11	1.4624685E-10	8.7732699E-16	1.7781940E-23
832	4.2247640E-13	1.6934195E-11	1.5601264E-10	1.1650838E-15	2.4291166E-23
864	4.2275033E-13	1.6938486E-11	1.6507409E-10	1.5288711E-15	3.2788831E-23
896	4.2300762E-13	1.6942569E-11	1.7340149E-10	1.9842178E-15	4.3772232E-23
928	4.2324940E-13	1.6946446E-11	1.8098527E-10	2.5488862E-15	5.7836829E-23
960	4.2347661E-13	1.6950117E-11	1.8783384E-10	3.2430792E-15	7.5691417E-23
992	4.2369108E-13	1.6953615E-11	1.9397014E-10	4.0896408E-15	9.8174726E-23

A.3 FSCP 8/2 的响应时间计算公式的含义

图44中的从SFSPM-M发送的T2时刻到SFSPM-S接受的T4时刻的时间段是最大允许延时。在响应时间计算公式中，从T2到T4的时间端等于allowable_delay + 2 × offset_dispersion。图A.1示出了2 × offset_dispersion的含义。

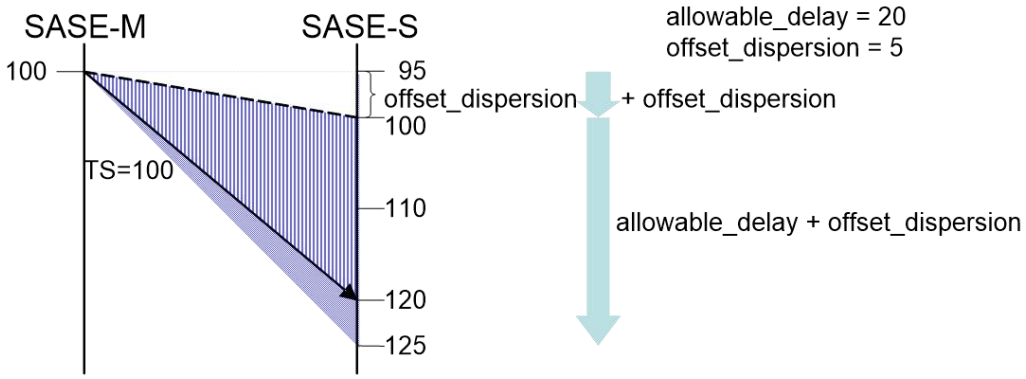

图 A.1 允许延时和抖动偏移值

由于计算偏差offset_dispersion可能发生在偏移计算中，在允许延时allowable_delay中考虑计算偏差offset_dispersion的公式用于确定12.7.2中描述的允许延时。另外，在SFSPM-M和SFSPM-S安全时钟之间offset_dispersion发生最大差异。因此，2 × offset_dispersion（组合值）是必需的。

附 录 B
（资料性附录）
CPF8 功能安全通信行规的评估信息

根据IEC规则，本文件不提供关于如何验证一致性的说明。但是，法律可能要求符合IEC 61784-3-8的FSCP 8/1和FSCP 8/2设备的合规性测试和验证。

与本文件的符合性相关和涉及测试的信息可从相关IEC国家委员会或相应的现场总线组织获得。

注：对于IEC 61784-3-8,对应的现场总线组织是CC-Link协会，见www.cc-link.org。

参 考 文 献

[1] IEC 60050 (all parts), International Electrotechnical Vocabulary (IEV) (available at <http://www.electropedia.org/)

注：见 IEC Multilingual Dictionary - Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>)

[2] IEC 60050-191:1990[5] , International Electrotechnical Vocabulary-Chapter 191: Dependability and quality of service

[3] IEC 61000-1-2, Electromagnetic compatibility (EMC)-Part 1-2: General-Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena

[4] IEC 61000-6-7, Electromagnetic compatibility (EMC)-Part 6-7: Generic standards-Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations

[5] IEC 61010-2-201, Safety requirements for electrical equipment for measurement, control and laboratory use-Part 2-201: Particular requirements for control equipment

[6] IEC 61131-6, Programmable controllers-Part 6: Functional safety

[7] IEC 61158-1, Industrial communication networks-Fieldbus specification-Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series

[8] IEC 61158-5 (all parts), Industrial communication networks-Fieldbus specifications-Part 5: Application layer service definition

[9] IEC 61496 (all parts), Safety of machinery-Electro-sensitive protective equipment

[10] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 1: General requirements

[11] IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 4: Definitions and abbreviations

[12] 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

[13] IEC 61784-3 (all parts), Industrial communication networks-Profiles- Part 3: Functional safety fieldbuses

[14] IEC 61784-5 (all parts), Industrial communication networks-Profiles - Part 5: Installation of fieldbuses-Installation profiles for CPF x

[15] IEC 61800-5-2, Adjustable speed electrical power drive systems-Part 5-2: Safety requirements-Functional

[16] IEC 61918:2018, Industrial communication networks-Installation of communication networks in industrial premises

[17] IEC 62280:2014, Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems

[18] IEC 62443 (all parts), Industrial communication networks - Network and system security

[19] ISO/IEC Guide 51:2014, Safety aspects-Guidelines for their inclusion in standards

[20] ISO/IEC 2382:2015, Information technology-Vocabulary

[21] ISO/IEC 7498-1, Information technology-Open Systems Interconnection- Basic Reference Model: The Basic Model

[22] ISO 10218-1, Robots and robotic devices-Safety requirements for industrial robots-Part 1: Robots

[23] ISO 13849 (all parts), Safety of machinery-Safety-related parts of control systems

[24] ISO 13849-1:2015, Safety of machinery-Safety-related parts of control systems-Part 1: General principles for design

[25] ISO 13849-2, Safety of machinery-Safety-related parts of control systems - Part 2: Validation

[26] ANDREW S. TANENBAUM, DAVID J. WETHERALL, Computer Networks, 5 th Edition, Prentice Hall, N.J., ISBN-10: 0132126958, ISBN-13: 978-0132126953

[27] W. WESLEY PETERSON, EDWARD J. WELDON, Error-Correcting Codes, 2 nd Edition 1972, MIT-Press, ISBN 0-262-16-039-0

[28] GUY E. CASTAGNOLI, On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[29] GUY E. CASTAGNOLI, STEFAN BRÄUER, AND MARTIN HERRMANN, Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[30] CC-Link Safety Specifications, Overview/Protocol, BAP-C1603-001, CLPA

[31] CC-Link Safety Specifications, Implementation, BAP-C1603-002, CLPA

[32] CC-Link Safety Specifications, Profiles, BAP-C1603-003, CLPA

[33] CC-Link IE Safety Specifications, Overview, BAP-C1606-001, CLPA

[34] CC-Link IE Safety Specifications, Application Layer Service and Protocol Communication profile, BAP-C1606-002, CLPA