文件名称：安全层协议说明

文件编号：15-Q04-000071

项目编号：SF-RD-1501

项目名称：安全控制系统开发项目一期

物料编号：--

版本号/修改码：A

文件密级：内部公开

文件状态：CFC

受控标识：受控

|  |  |
| --- | --- |
| 拟制：王东 | 2015年 07月10日 |
| 审核：朱耿华 | 2015年 07月10日 |
| 会签： | 2015年 07月10日 |
|  |  |
| 批准：温宜明 | 2015年 07月10日 |

**修订页**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 编  号 | 章节  名称 | 修订内容简述 | 修订  日期 | 订前  版本 | 订后  版本 | 拟制 | 审核 | 批准 |
|  | 全部 | 创建 | 2015．07．10 |  |  | 王东 | 朱耿华 | 温宜明 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**本版本与旧文件（版本）的关系：**

**无**

**目录**

[1 概述 1](#_Toc439331387)

[1.1 安全通信功能说明 1](#_Toc439331388)

[1.1.1 主处理器与I/O模块 1](#_Toc439331389)

[1.1.2 主处理器与主处理器 1](#_Toc439331390)

[1.1.3 控制站与控制站 1](#_Toc439331391)

[1.2 黑通道 1](#_Toc439331392)

[1.3 职责 1](#_Toc439331393)

[1.4 缩略语 1](#_Toc439331394)

[2 控制站间安全通信 1](#_Toc439331395)

[2.1 通信模型 1](#_Toc439331396)

[2.1.1 PM工作机制 2](#_Toc439331397)

[2.1.2 CM工作机制 2](#_Toc439331398)

[2.2 安全层数据帧结构 3](#_Toc439331399)

[2.2.1 请求帧 3](#_Toc439331400)

[2.2.2 应答帧 5](#_Toc439331401)

[2.3 安全措施 6](#_Toc439331402)

[2.3.1 时间预期-看门狗 6](#_Toc439331403)

[2.3.2 交叉冗余校验 6](#_Toc439331404)

[2.3.3 CRC 6](#_Toc439331405)

[2.3.4 连接验证 7](#_Toc439331406)

[2.3.5 序号 7](#_Toc439331407)

[2.3.6 Feedback Message 8](#_Toc439331408)

[2.4 安全措施与通信错误的对应关系 8](#_Toc439331409)

[2.5 错误处理与恢复机制 8](#_Toc439331410)

[2.5.1 发送站PM错误处理与恢复机制 8](#_Toc439331411)

[2.5.2 接收站PM错误处理与恢复机制 8](#_Toc439331412)

[2.6 状态图 9](#_Toc439331413)

[2.6.1 发送站PM状态图 9](#_Toc439331414)

[2.6.2 接收站PM状态图 9](#_Toc439331415)

[2.7 序列图 10](#_Toc439331416)

[2.7.1 正常通信 10](#_Toc439331417)

[2.7.2 序号错误与恢复 11](#_Toc439331418)

[3 主处理器间安全通信 13](#_Toc439331419)

[3.1 通信模型 13](#_Toc439331420)

[3.2 数据帧结构 13](#_Toc439331421)

[3.2.1 帧头 13](#_Toc439331422)

[3.2.2 安全数据 13](#_Toc439331423)

[3.2.3 CRC-32 14](#_Toc439331424)

[3.3 安全措施 14](#_Toc439331425)

[3.3.1 时间预期-看门狗 14](#_Toc439331426)

[3.3.2 CRC 14](#_Toc439331427)

[3.3.3 连接验证 14](#_Toc439331428)

[3.3.4 序号 14](#_Toc439331429)

[3.4 安全措施与通信错误的对应关系 14](#_Toc439331430)

[3.5 错误处理与恢复机制 15](#_Toc439331431)

[3.6 状态图 15](#_Toc439331432)

[3.6.1 发送方状态图 15](#_Toc439331433)

[3.6.2 接收方状态图 16](#_Toc439331434)

[3.7 序列图 16](#_Toc439331435)

[3.7.1 正常通信 16](#_Toc439331436)

[3.7.2 序号恢复 17](#_Toc439331437)

[4 主处理器与I/O模块间安全通信 18](#_Toc439331438)

[4.1 通信模型 18](#_Toc439331439)

[4.2 安全数据帧结构 19](#_Toc439331440)

[4.2.1 帧头 19](#_Toc439331441)

[4.2.2 安全数据 20](#_Toc439331442)

[4.2.3 CRC-32 20](#_Toc439331443)

[4.3 安全措施 20](#_Toc439331444)

[4.3.1 时间预期 20](#_Toc439331445)

[4.3.2 交叉冗余校验 20](#_Toc439331446)

[4.3.3 CRC 21](#_Toc439331447)

[4.3.4 连接验证 21](#_Toc439331448)

[4.3.5 序号 21](#_Toc439331449)

[4.3.6 Feedback Message 21](#_Toc439331450)

[4.4 安全措施与通信错误的对应关系 22](#_Toc439331451)

[4.5 错误处理与恢复机制 22](#_Toc439331452)

[4.5.1 主站 22](#_Toc439331453)

[4.5.2 从站 23](#_Toc439331454)

[4.6 状态图 23](#_Toc439331455)

[4.6.1 主站状态图 23](#_Toc439331456)

[4.6.2 从站状态图 24](#_Toc439331457)

[4.7 序列图 25](#_Toc439331458)

[4.7.1 正常通信 25](#_Toc439331459)

[4.7.2 序号恢复 26](#_Toc439331460)

[4.8 I/O模块参数化 28](#_Toc439331461)

[4.8.1 参数数据包结构 28](#_Toc439331462)

[4.8.2 安全措施 28](#_Toc439331463)

[4.8.3 参数化序列图 29](#_Toc439331464)

[5 残余错误率 29](#_Toc439331465)

[5.1 计算公式 29](#_Toc439331466)

[5.2 CRC生成多项式及其汉明距 30](#_Toc439331467)

[5.3 残余错误率计算 30](#_Toc439331468)

[5.3.1 控制站间安全通信 30](#_Toc439331469)

[~~5.3.2~~ ~~主处理器间安全通信~~ 30](#_Toc439331470)

[5.3.3 主处理器与IO模块间安全通信 30](#_Toc439331471)

# 概述

主处理器与I/O模块、主处理器间和控制站间可能需要交换安全关键数据，本文档描述用于交换安全关键数据的协议，即安全层协议。

主处理器与I/O模块间的安全通信基于主从模式，主处理器为主，I/O模块为从。主处理器间和控制站间的安全通信基于点对点模式，某一方固定向其目标方发送数据。

## 安全通信功能说明

### 主处理器与I/O模块

主处理器周期性读取I模块的输入数据，周期性向O模块发送输出数据。

### 主处理器与主处理器

主处理器间周期性交换各自的IO数据，用于输入/输出表决和IEC运算等操作。

### 控制站与控制站

某一控制站可能需要其他控制站（一个或多个）的数据参与自身的安全控制，因此控制站间可能需要周期性交换安全关键数据。

## 黑通道

安全通信基于黑通道，使用端到端检查可能出现的通信错误并进行相应的处理，对网络拓扑或硬件等底层不做任何假设。

说明：黑通道是指无设计或确认的可用性证据的通信通道。

## 职责

确定性发现所有可能的通信故障/危险或使残余错误概率限定在一定范围内，满足安全等级SIL3的要求。

单通道通信系统能够满足安全要求，冗余只为增加可用性。

## 缩略语

PM：主处理器模块；

CM：通讯模块。

# 控制站间安全通信

## 通信模型

控制站间安全通信的模型如图2-1所示，发送控制站周期性向接收控制站发送安全数据，接收控制站接收数据并应答。控制站的PM模块负责生成/解析安全层数据，PM之间的通信链路为安全通信对应的黑通道。



图2-1 控制站间安全通信的模型

控制站的PM模块通过独立的通讯总线与CM模块进行连接，发送控制站的CM模块通过以太网与接收控制站的CM模块进行连接。

### PM工作机制

#### 2.1.1.1发送站PM

发送站PM均构造安全帧，然后发送给配置指定的CM模块。

只有一个发送站PM可能接收到应答帧，然后同步给其他PM模块。

#### 2.1.1.2接收站PM

只有一个接收站PM可能接收到总数据帧，接收到后，将总数据帧同步给其他PM模块。各个PM模块采用相同的处理机制，判断得知哪系通信状态正常，然后对通信状态正常的安全数据进行表决，最终得到一份安全数据。

只有接收到总数据帧的PM模块负责进行应答，将应答帧发送给配置指定的CM模块。

### CM工作机制

#### 2.1.2.1发送站CM

发送站CM将来自本站所有PM的同一控制周期的安全帧打包，打包后的格式如表2-1所示。由于CM与PM是异步工作的，所以在一个CM周期内，可能不能收到所有PM发送的安全帧。若发生上述情况，则CM需在下个周期继续接收相应的安全帧，如果还未收到，则CM认为超时，只将接收到的安全帧打包并发送。

表2-1 CM打包后的请求帧

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Additional Info. | PMA Safety Frame | PMB Safety Frame | PMC Safety Frame | FCS |
| 8 bytes | variable | variable | variable | 4 bytes |

说明：

1) Additional Info.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Data Type | Length | Desc |
| SrcStaID | unsigned char | 1 byte | 源控制站ID |
| DstStaID | unsigned char | 1 byte | 目的控制站ID |
| FrameType | unsigned char | 1 byte | 0-请求帧；1-应答帧 |
| LinkID | unsigned char | 1 byte | 冗余链路ID: 1-链路1；2-链路2  注：只对冗余通讯有效 |
| Total Length | unsigned short | 2 bytes | 打包后的数据帧的总长度-字节，包括附加信息和FCS |
| PM Info. | unsigned char | 1 byte | PM信息- Bit 0: PMA; Bit 1: PMB; Bit 2: PMC  当此数据帧包含相应PM的安全帧时，相应的位置1 |
| Reserve | unsigned char | 1 byte | 预留 |

2) FCS负责校验此完整数据帧，可根据需要采用CRC或校验和等方法。

发送站CM模块收到应答帧后，挑选一个PM模块，然后向其发送应答帧。挑选PM的机制：选取与CM通讯正常的，编号最小的PM模块。

#### 2.1.2.2接收站CM

接收站CM模块接收到总数据帧后，挑选一个PM模块，然后向其发送总数据帧。挑选PM的机制：选取与CM通讯正常的，编号最小的PM模块。

接收站CM模块收到本站PM模块发送的应答帧后，将应答帧打包，然后发往目的控制站，格式如表2-2所示。

表2-2 CM打包后的应答帧

|  |  |  |
| --- | --- | --- |
| Additional Info. | Safety Response Frame | FCS |
| 8 bytes | 24 bytes | 4 bytes |

说明：

1) Additional Info.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Data Type | Length | Desc |
| SrcStaID | unsigned char | 1 byte | 源控制站ID |
| DstStaID | unsigned char | 1 byte | 目的控制站ID |
| FrameType | unsigned char | 1 byte | 0-请求帧；1-应答帧 |
| Reserve | unsigned char | 1 byte | 预留 |
| Total Length | unsigned short | 2 bytes | 打包后的数据帧的总长度（字节），包括附加信息和FCS |
| Reserve | unsigned char[2] | 2 bytes | 预留 |

2) FCS负责校验此完整数据帧，可根据需要采用CRC或校验和等方法。

## 安全层数据帧结构

### 请求帧

PM生成的请求帧结构如表2-3所示，由附加信息和安全帧组成，其中附加信息如表2-4所示，帧头如表2-5所示，Frame Header Reverse，Safety Data Reverse和CRC-32-Reverse分别是相应域的按位翻转。下面分别进行详细说明：

表2-3请求帧

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Additional Info. | Frame Header | Safety Data | CRC-32 | Frame Header Reverse | Safety Data Reverse | CRC-32-Reverse | FCS |
| 20 bytes | 8 bytes | variable | 4 bytes | 8 bytes | variable | 4 bytes | 4 bytes |

说明：数据采用大字节序传输，即高字节在前，低字节在后。

表2-4 Additional Info.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Data Type | Length | Desc |
| SrcCMSlotID | unsigned char | 1 byte | 源控制站CM模块的槽位号 |
| SrcNETID | unsigned char | 1 byte | 源控制站CM模块的网口编号：  NET1-0；NET2-1；All NET -2 |
| Timeout Flag | unsigned char | 1 byte | 应答超时标志位：0-未超时；1-超时 |
| Link1 NetID | unsigned char | 1 byte | 链路1的网口ID: 0-Net1；1-Net2  注：只同CM双网口冗余有效 |
| DstIP1 Address | unsigned char | 4 bytes | 目的控制站的IP1地址 |
| DstIP2 Address | unsigned char | 4 bytes | 目的控制站的IP2地址，0代表未使用 |
| SrcStaID | unsigned char | 1 byte | 源控制站ID：1-64 |
| DstStaID | unsigned char | 1 byte | 目的控制站ID：1-64 |
| FrameType | unsigned char | 1 byte | 0-请求帧；1-应答帧 |
| LinkID | unsigned char | 1 byte | 冗余链路ID: 1-链路1；2-链路2  注：只对冗余通讯有效 |
| Total Length | unsigned int | 4 bytes | 数据帧的总长度（字节），包括附加信息和FCS |

#### 2.2.1.1帧头

表2-5 Frame Header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| Sequence Number | unsigned short | 2 bytes |  | 序号 |
| SrcAddr | unsigned char | 1 byte |  | 源地址：PM编号+控制站节点号 |
| DstAddr | unsigned char | 1 byte |  | 目的地址：控制站节点号 |
| Reserve | unsigned char | 1 byte | 0 | 预留 |
| Control Byte | unsigned char | 1 byte |  | 控制字节 |
| Safety Data Len | unsigned short | 2 bytes |  | 安全数据的长度（字节） |

说明：

1. 源地址：由PM编号和控制站的节点号组成，具体如表2-6所示：

表2-6 地址

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| PM编号：0：PMA；1：PMB；2：PMC | | 控制站节点号：0 - 63 | | | | | |

2) 控制字节：发送站PM通过控制字节将控制信息发送给接收站的PM，具体内容如表2-7所示：

表2-7控制字节

|  |  |  |
| --- | --- | --- |
| Bit | Value | Description |
| 0 | Failure flag | 倒向安全状态标志位：PM模块倒向安全时，置1，此时发送站PM应发送安全值或正常数据，接收站PM应采用发送站下发的或自身内置的安全值 |
| 1-7 | res | 预留 |

#### 2.2.1.2安全数据

安全数据如表2-8所示，发送站PM根据目的控制站对应的数据表顺序排列相关变量的实时数值。

表2-8 Safety Data

|  |  |  |  |
| --- | --- | --- | --- |
|  | Data Type | Length | Desc |
| Data Values | - | - | 相关变量的实时数值 |

#### 2.2.1.3 CRC-32

利用CRC方法校验相应的数据，其多项式的选取主要取决于校验域的长度、通信频率（每小时安全消息的最大数目），安全消息接收者的数目和SIL3安全等级要求，最终选取的多项式为0x1 F4AC FB13，相关计算见第五章。

### 应答帧

PM生成的应答帧结构如表2-9所示，由附加信息和安全帧组成，其中附加信息如表2-10所示，帧头如表2-11所示，Frame Header Reverse和CRC-32-Reverse分别是相应域的按位翻转。下面分别进行详细说明：

表2-9应答帧

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Additional Info. | Frame Header | CRC-32 | Frame Header Reverse | CRC-32-Reverse | FCS |
| 20 bytes | 8 bytes | 4 bytes | 8 bytes | 4 bytes | 4 bytes |

说明：数据采用大字节序传输，即高字节在前，低字节在后。

表2-10 Additional Info.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Data Type | Length | Desc |
| SrcCMSlotID | unsigned char | 1 byte | 源控制站CM模块的槽位号 |
| SrcNETID | unsigned char | 1 byte | 源控制站CM模块的网口编号：  NET1-0；NET2-1；All NET -2 |
| Reserve | unsigned char | 1 byte | 预留 |
| Reserve | unsigned char | 1 byte | 预留 |
| DstIP1 Address | unsigned char | 4 bytes | 目的控制站的IP1地址 |
| DstIP2 Address | unsigned char | 4 bytes | 目的控制站的IP2地址，0代表未使用 |
| SrcStaID | unsigned char | 1 byte | 源控制站ID：1-64 |
| DstStaID | unsigned char | 1 byte | 目的控制站ID：1-64 |
| FrameType | unsigned char | 1 byte | 0-请求帧；1-应答帧 |
| Reserve | unsigned char | 1 byte | 预留 |
| Total Length | unsigned int | 4 bytes | 数据帧的总长度（字节），包括附加信息和FCS |

#### 2.2.2.1帧头

表2-11 Frame Header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| Sequence Number | unsigned short | 2 bytes |  | 序号 |
| SrcAddr | unsigned char | 1 byte |  | 源地址：PM编号+控制站节点号 |
| DstAddr | unsigned char | 1 byte |  | 目的地址：控制站节点号 |
| Status Info. | unsigned short | 2 bytes |  | 状态信息 |
| Safety Data Len | unsigned short | 2 bytes | 0 | 安全数据的长度（字节） |

说明：

1. 源地址：见表2-6；
2. 状态信息：接收站PM通过状态信息将通信状态应答给发送站PM，具体内容如表2-12所示：

**表2-12 Status Info.**

|  |  |  |
| --- | --- | --- |
| Bit | Value | Description |
| 0 | Communication failure: WD-timeout | 通信错误：看门狗超时时，置1 |
| 1 | Communication failure: PMA CRC | 通信错误：PMA CRC错误时，置1 |
| 2 | Communication failure: PMB CRC | 通信错误：PMB CRC错误时，置1 |
| 3 | Communication failure: PMC CRC | 通信错误：PMC CRC错误时，置1 |
| 4 | Communication failure: PMA Addr | 通信错误：PMA源地址或目的地址出错时，置1 |
| 5 | Communication failure: PMB Addr | 通信错误：PMB源地址或目的地址出错时，置1 |
| 6 | Communication failure: PMC Addr | 通信错误：PMC源地址或目的地址出错时，置1 |
| 7 | Communication failure: PMA SQ | 通信错误：PMA 序号错误时，置1 |
| 8 | Communication failure: PMB SQ | 通信错误：PMB 序号错误时，置1 |
| 9 | Communication failure: PMC SQ | 通信错误：PMC 序号错误时，置1 |
| 10 | Communication failure:  PMA Redundant Data Different | 通信错误：PMA 冗余数据不一致时，置1 |
| 11 | Communication failure:  PMB Redundant Data Different | 通信错误：PMB 冗余数据不一致时，置1 |
| 12 | Communication failure:  PMC Redundant Data Different | 通信错误：PMC 冗余数据不一致时，置1 |
| 13 | Alarm | 附加信息中的PM Info. 与 安全帧中的PM信息不一致 |
| 14 | Multiple PMP2P Request | 多PM请求帧标志 |
| 15 | Reserve | 预留 |

## 安全措施

### 时间预期-看门狗

发送站PM利用看门狗监视两次连续发送的时间间隔，看门狗时间等于发送周期加容忍余量，容忍余量可配。此外，PM还利用看门狗监视应答是否超时-请求发出后，在一定时间内未收到应答，看门狗超时时间可配，应答超时时，发送序号增加1。错误处理与恢复机制详见2.5.1节。

接收站PM利用看门狗监视两次连续接收的时间间隔是否超时，看门狗超时时间可配，其值主要取决于相应安全回路的过程安全时间。错误处理与恢复机制详见2.5.2节。

说明：发送间隔及发送超时时间均取决于接收超时时间。

### 交叉冗余校验

接收站PM接收到总数据帧后，首先恢复翻转信息，然后与相应信息进行比较，如果不同，则进行错误处理，详见2.5.2节；如果相同，则进行后续检查。

发送站PM接收到应答帧后，首先恢复翻转信息，然后与相应信息进行比较，如果不同，则进行错误处理，详见2.5.1节；如果相同，则进行后续检查。

### CRC

接收站PM分别检查各个安全帧中的CRC是否正确，并根据检查结果设置状态信息，当某一安全帧的CRC错误时，直接丢弃此安全帧。错误处理与恢复机制详见2.5.2节。

发送站PM检查安全帧中的CRC是否正确，如果正确，则认为数据未被损坏；如果错误，则认为数据已被损坏，直接丢弃此安全帧。错误处理与恢复机制详见2.5.1节。

### 连接验证

接收站PM分别检查各个安全帧中的源地址和目的地址是否正确：源地址中的PM信息是否与附加信息中的PM Info.一致以及源地址和目的地址中的控制站节点号是否正确，并根据检查结果设置状态信息，其中当PM信息不一致时，只通过状态信息上报即可；当控制站节点号不正确时，直接丢弃此安全帧。错误处理与恢复机制详见2.5.2节。

发送站PM检查安全帧中的源地址和目的地址是否正确，当地址不正确时，直接丢弃此安全帧。错误处理与恢复机制详见2.5.1节。

### 序号

发送站PM与接收站PM各自维护一个序号，发送站各个PM的序号保持一致，初始值为0，每发送一帧数据，数值增加1，直至0xFFFF，下次发送后，数值变回为0。

接收站PM的序号初始值为0xFFFF，接收站PM分别检查各个安全帧中的序号是否符合预期 - 序号等于本地序号加1，并根据检查结果设置状态信息。如果存在完全正确的安全帧，则将本地序号更新为正确安全帧中的序号；如果不存在完全正确的安全帧，则处理机制与链路是否冗余有关：

* 链路冗余：当序号均不符合预期时，如果序号均与接收序号相等，则认为数据重复，直接丢弃，不进行错误处理和应答；如果序号均相等且不等于接收序号，则将本地序号更新为请求帧中的序号，并进行错误处理；否则将本地序号复位为初始值0xFFFF，并进行错误处理。错误处理与恢复机制详见2.5.2节；
* 链路非冗余：当序号均不符合预期时，如果序号均相等，则将本地序号更新为请求帧中的序号，并进行错误处理；否则将本地序号复位为初始值0xFFFF，并进行错误处理。错误处理与恢复机制详见2.5.2节。

发送站PM检查应答帧中的序号是否符合预期 - 序号不重复且与请求帧一致。如果序号错误，则处理机制与链路是否冗余有关：

* 链路冗余：如果应答帧重复，则直接丢弃，不进行错误处理；否则检查状态信息，当状态信息显示本PM的序号错误，其他PM（全部或部分）的序号正确，则将发送序号更新为应答帧中的序号加1；当状态信息显示所有PM的序号均错误时，清零本地序号。错误处理与恢复机制详见2.5.1节；
* 链路非冗余：检查状态信息，当状态信息显示本PM的序号错误，其他PM（全部或部分）的序号正确，则将发送序号更新为应答帧中的序号加1；当状态信息显示所有PM的序号均错误时，清零本地序号。错误处理与恢复机制详见2.5.1节。

### Feedback Message

接收站PM接收到打包后的请求帧后，进行相应的处理并应答。

## 安全措施与通信错误的对应关系

接收站PM采用2.3节中的安全措施检测可能的通信错误，安全措施以及其能够检测的通信错误类型如表2-13所示：

表2-13 安全措施与通信错误关系

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 通信错误 | 安全措施 | | | | | |
| 序号 | 接收时间预期 | CRC | 带请求超时的Feedback Message | 连接验证 | 交叉冗余校验 |
| 数据损坏(Data Corruption) |  |  | X |  |  |  |
| 重复(Repetition) | X |  |  |  |  | X |
| 不正确的序列(Incorrect sequence) | X |  |  |  |  | X |
| 丢失(Loss) | X |  |  | X |  | X |
| 不可接受的延迟(Unacceptable delay) |  | X |  | X |  |  |
| 插入(Insertion) | X |  |  | X | X | X |
| 伪装(Masquerade) |  |  |  |  | X |  |
| 寻址异常(Addressing) |  |  |  |  | X |  |

## 错误处理与恢复机制

### 发送站PM错误处理与恢复机制

发送站PM针对每一个接收站均维护一组独立的数据：一个错误计数、一个容忍标志位和一个错误标志位，初始值为0。

当检测发现应答帧错误时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位，继续发送正常的数据；否则，置错误标志位，复位容忍标志位，置控制字节的Failure flag（bit 0）为1，应用程序应发送安全值或正常的数据。

当检测发现应答帧正确时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则应用程序应继续发送安全值或正常的数据，否则，复位错误标志位和控制字节的Failure flag（bit 0），应用程序应发送正常的数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位；如果错误和容忍标志位均为0，则相应的错误计数减1。

### 接收站PM错误处理与恢复机制

接收站PM针对每一个发送站均维护一组独立的数据：一个错误计数、一个容忍标志位和一个错误标志位，初始值为0。

当检测发现发送站无正确的安全帧时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位，应用程序应采用最后一次接收到的正确数据；否则，置错误标志位，复位容忍标志位，应用程序应采用安全值。

当检测发现发送站存在正确的安全帧时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则应用程序应继续采用安全值，否则，复位错误标志位，应用程序应采用本周期接收到的正确数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位，应用程序应采用本周期接收到的正确数据；如果错误和容忍标志位均为0，则相应的错误计数减1，应用程序应采用本周期接收到的正确数据。

## 状态图

### 发送站PM状态图

发送站PM状态图如图2-2所示：

图2-2 发送站PM状态图

说明：

x：发送站PM维护的本地序号；

T：发送时间间隔，即发送周期；

5 Handle local sq: x：详见2.3.5节中发送站PM检测发现序号错误时的处理机制；

发送请求帧的条件：到达发送间隔且收到应答帧 或者 应答超时。

### 接收站PM状态图

接收站PM状态图如图2-3所示，接收站PM监视两次连续接收的时间间隔，若超时则进行相应的错误处理。正常接收到数据帧后，检查是否存在完全正确的安全帧，若不存在，则进行相应的错误处理，最终将通信状态应答给发送站PM。



图2-3 接收站PM状态图

说明：

y：接收站PM维护的本地序号；

tolflag/ errflag/ errnum：接收站PM维护的容忍标志位/错误标志位/错误计数；

recvnum：安全帧中的序号。

## 序列图

### 正常通信

本节通过序列图说明发送站PM与接收站PM间正常通信时的交互过程，如图2-4所示：



图2-4 正常通信序列图

说明：

T：发送时间间隔；

T1：请求超时时间；

T2：两次连续接收超时时间；

T3：连续两次发送超时时间。

### 序号错误与恢复

图2-5和图2-6分别显示了序号恢复情况1和序号恢复情况2时的交互过程。

说明：

x：发送站PM维护的序号；

y：接收站PM维护的序号；

序号恢复情况1：某一周期的所有请求帧中的序号全部错误。由图2-5可知，只需1个周期，

序号错误就能够恢复；

序号恢复情况2：某一周期的状态信息显示本PM的序号错误，其他PM（全部或部分）的序号正确。图2-6以PMA发生序号错误为例，由图可知，只需1个周期，序号错误就能够恢复。



图2-5 序号恢复情况1



图2-6 序号恢复情况2

# 主处理器间安全通信

## 通信模型

主处理器间安全通信的模型如图3-1所示，PM模块间周期性交换各自的IO数据。PM模块负责生成/解析安全层数据，PM之间的通信链路为安全通信对应的黑通道。



图3-1 主处理器间安全通信的模型

## 数据帧结构

主处理器间通信的完整数据帧如表3-1所示，帧头如表3-2所示，数据帧包含安全相关数据和非安全相关数据，非安全相关数据的结构不在此描述。

表3-1完整数据帧

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Header | Safety Data | CRC-32 | Non-safety relevant data |
| 8 bytes | variable | 4 bytes | variable |

说明：数据采用大字节序传输，即高字节在前，低字节在后。

### 帧头

表3-2 Safety Header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| SrcAddr | unsigned char | 1 byte |  | 源地址：源主处理器的编号  0：PMA；1：PMB；2：PMC |
| DstAddr | unsigned char | 1 byte |  | 目的地址：目的主处理器的编号  0：PMA；1：PMB；2：PMC |
| Sequence Number | unsigned short | 2 bytes |  | 序号：每发送一次，数值增加1 |
| Safety Length | unsigned int | 4 bytes |  | 安全数据的长度（字节） |

### 安全数据

安全数据如表3-3所示，发送方按照事先约定好的规则顺序排列安全数据。

表3-3 Safety Data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| Safety Data | - | - |  | 安全数据 |

### CRC-32

利用CRC方法校验相应的区域，其多项式的选取主要取决于校验域的长度、通信频率（每小时安全消息的最大数目），安全消息接收者的数目和SIL3安全等级要求，最终选取的多项式为0x1 F4AC FB13，相关计算见第五章。

## 安全措施

### 时间预期-看门狗

发送方PM监视两次连续发送的时间间隔，超时时报警。

PM发送完自身的I/O数据后，期待在超时时间T1/T2内收到其他PM发送的I/O数据。错误处理与恢复机制详见3.5节。

说明：T1：接收其他PM发送的输入数据的超时时间，不可配；

T2：接收其他PM发送的输出数据的超时时间，不可配。

### CRC

PM接收到完整数据帧后，用与发送方相同的CRC算法计算得出CRC结果，然后与发送方计算的结果进行比较，如果两者相同，则认为数据未被损坏；如果不相同，则认为数据已被损坏，直接丢弃此安全帧。错误处理与恢复机制详见3.5节。

### 连接验证

各个PM均具备唯一的地址，PM接收到完整数据帧后，检查源地址和目的地址是否正确，当地址不正确时，直接丢弃此安全帧。错误处理与恢复机制详见3.5节。

### 序号

各个PM均维护四个独立的序号：两个发送序号和两个接收序号。发送序号用于维护相应的发送序列，其初始值为0，每发送一帧数据，数值增加1，直至0xFFFF，下次发送后，数值变回为0。

接收序号用于维护相应的接收序列，其初始值为0xFFFF，接收到完整数据帧后，检查数据帧中的序号是否符合预期 - 序号等于相应的接收序号加1，如果数据帧完全正确或除序号外，数据帧的其他部分均正确，则将接收序号更新为数据帧中的序号；否则，接收序号保持不变。错误处理与恢复机制详见3.5节。

## 安全措施与通信错误的对应关系

主处理器模块采用3.3节中的安全措施检测可能的通信错误，安全措施以及其能够检测的通信错误类型如表3-4所示：

表3-4 安全措施与通信错误关系

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 通信错误 | 安全措施 | | | |
| 序号 | 接收时间预期-看门狗 | CRC | 连接验证 |
| 数据损坏(Data Corruption) |  |  | X |  |
| 重复(Repetition) | X |  |  |  |
| 不正确的序列(Incorrect sequence) | X |  |  |  |
| 丢失(Loss) | X |  |  |  |
| 不可接受的延迟(Unacceptable delay) |  | X |  |  |
| 插入(Insertion) | X |  |  | X |
| 伪装(Masquerade) |  |  |  | X |
| 寻址异常(Addressing) |  |  |  | X |

## 错误处理与恢复机制

每个PM均维护两组独立的数据，分别用于维护接收其他两个PM的I/O数据的情况。每组数据均由一个错误计数、一个容忍标志位和一个错误标志位组成，初始值为0。

当PM检测到通信错误时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位，应用程序应采用最后一次接收到的正确数据；否则，置错误标志位，复位容忍标志位，应用程序应采用安全值。

当PM未检测到通信错误时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则应用程序应继续采用安全值，否则，复位错误标志位，应用程序应采用本周期接收到的正确数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位，应用程序应采用本周期接收到的正确数据；如果错误和容忍标志位均为0，则相应的错误计数减1，应用程序应采用本周期接收到的正确数据。

## 状态图

### 发送方状态图

发送方状态图如图3-2所示，PM准备好输入/输出数据后，将数据发送给其它PM。



图3-2 发送方状态图

说明：x：本地维护的与某一PM相对应的发送序号；

### 接收方状态图

接收方状态图如图3-3所示：



图3-3 接收方状态图

说明：

y：本地维护的与某一PM相对应的接收序号；

recvnum：数据帧中的序号；

tolflag/errflag/ errnum：本地维护的与某一PM相对应的错误计数，容忍和错误标志。

## 序列图

### 正常通信

本节通过序列图说明某两个PM间正常通信时的交互过程，如图3-4所示：



图3-4 正常通信序列图

说明：

T1：接收PM1发送的输入数据的超时时间；

T2：接收PM1发送的输出数据的超时时间；

### 序号恢复

图3-5和图3-6分别显示了序号恢复情况1和序号恢复情况2时的交互过程。

说明：

m：非1的有符号整型数；

x：PM1维护的与PM2相对应的发送序号；

y：PM2维护的与PM1相对应的接收序号；

序号恢复情况1：某一安全帧除序号外，其他部分均正确，之后的安全帧序号在此帧序号基

础上正常增加。由图3-5可知，只需1个周期，序号错误就能够恢复；

序号恢复情况2：某一安全帧存在addr或crc错误，序号可能正确也可能不正确，之后的安全帧序号恢复正常。由图3-6可知，最多只需2个周期，序号错误就能够恢复。



图3-5 序号恢复情况1



图3-6 序号恢复情况2

# 主处理器与I/O模块间安全通信

## 通信模型

PM与I/O模块间安全通信的模型如图4-1所示，PM模块周期性轮询各个I/O模块，I/O模块接收到PM发送的请求帧后，进行相应的处理并应答。PM模块和I/O模块负责生成/解析安全层数据，它们之间的通信链路为安全通信对应的黑通道。



图4-1 PM与I/O模块间的安全通信的模型

## 安全数据帧结构

每种I/O模块对应的安全帧的长度是固定的，数据帧结构如表4-1所示，Frame Header Reverse，Safety Data Reverse和CRC-32-Reverse分别是相应域的按位翻转。下面分别进行详细说明：

表4-1 I/O模块对应的安全帧

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Frame Header | Safety Data | CRC-32 | Frame Header Reverse | Safety Data Reverse | CRC-32  Reverse |
| 8 bytes | variable | 4 bytes | 8 bytes | variable | 4 bytes |

说明：数据采用大字节序传输，即高字节在前，低字节在后。

### 帧头

表4-2 Frame Header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| SrcAddr | unsigned short | 2 bytes |  | 源地址 |
| DstAddr | unsigned short | 2 bytes |  | 目的地址 |
| Sequence Number | unsigned short | 2 bytes |  | 序号：主站每发送一次增加1，从站应答时序号与请求帧一致 |
| Control/Status | unsigned char | 1 byte |  | 控制/状态字节 |
| Safety Length | unsigned char | 1 byte |  | 安全数据的长度（字节） |

说明：

1. 控制/状态字节：主站负责将控制信息通过控制字节发送给从站，从站的相关状态将通过状态字节应答给主站。控制/状态字节的具体内容分别如表4-3和表4-4所示：

表4-3 控制字节

|  |  |  |
| --- | --- | --- |
| Bit | Value | Description |
| 0 | Fail-safe values (FV) to be activated  (active\_FV) | 使用故障安全值时，置1：  输入数据：I模块正常应答其输入数据，主站使用相应的故障安全值替代实际输入数据；  输出数据：O模块输出主站下发的或自身内置的故障安全值。 |
| 1 | i-parameter assignment deblocked  (iPar\_En) | 主站准备下发从站模块参数时，置1 |
| 2-7 | res | 预留 |

表4-4 状态字节

|  |  |  |
| --- | --- | --- |
| Bit | Value | Description |
| 0 | Failure exists | 存在失效时，置1 |
| 1 | Communication failure: Codename | 通信错误：Codename错误时，置1 |
| 2 | Communication failure: CRC or Sequence Number | 通信错误：CRC 或序号错误时，置1 |
| 3 | Communication failure: WD-timeout | 通信错误：看门狗超时，置1 |
| 4 | Fail-safe values (FV) activated | 从站使用故障安全值时，置1 |
| 5 | new i-Parameter OK(iPar\_OK) | 从站采用主站下发的新参数后，置1 |
| 6 | Communication failure:Redundant Data Different | 通信错误：冗余数据不一致 |
| 7 | res | 预留 |

2) 源/目的地址：主站地址：0-PMA；1-PMB；2-PMC；从站地址：IO模块的编号。

### 安全数据

安全数据如表4-5所示：

表4-5 Data Block

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| Safety Data | - | - |  | 安全数据 |

### CRC-32

利用CRC方法校验相应的区域，其多项式的选取主要取决于校验域的长度、通信频率（每小时安全消息的最大数目），安全消息接收者的数目和SIL3安全等级要求，最终选取的多项式为0x1 F4AC FB13，相关计算见第五章。

## 安全措施

### 时间预期

主站利用看门狗监视两次连续启动发送的时间间隔，看门狗时间等于控制周期加容忍余量，不可配。请求是否超时由底层的超时标志位判断得出。错误处理与恢复机制详见4.5.1节。

从站利用看门狗监视两次连续接收的时间间隔是否超时，看门狗时间与容忍机制有关，不可配。错误处理与恢复机制详见4.5.2节。

### 交叉冗余校验

主/从接收到完整数据帧后，首先恢复翻转信息，然后与相应信息进行比较，如果不同，则进行错误处理，详见4.5节；如果相同，则进行后续检查。

### CRC

主/从站用与发送方相同的CRC算法计算得出CRC结果，然后与发送方计算的结果进行比较，如果两者相同，则认为数据未损坏，如果不相同，则认为数据已被损坏，直接丢弃此安全帧。错误处理与恢复机制详见4.5节。

### 连接验证

主从存在唯一的对应关系，主/从站检查对应关系代号Codename是否正确，若不正确，则直接丢弃此安全帧。错误处理与恢复机制详见4.5节。

### 序号

主站针对每一个从站均维护一个序号，初始值为0，每发送一帧数据，数值增加1，直至0xFFFF，下次发送后，数值变回为0。

从站各自维护一个序号，检查请求帧中的序号是否符合预期 - 序号等于前一请求帧中的序号加1，如果请求帧完全正确或除序号外，请求帧的其他部分均正确，则将从站的序号更新为请求帧中的序号；否则，从站序号保持不变。应答时，序号与本地序号一致。错误处理与恢复机制详见4.5.2节。

主站检查应答帧中的序号是否符合预期 - 序号与相应的请求帧一致。错误处理与恢复机制详见4.5.1节。

### Feedback Message

从站收到请求帧后，进行相应的处理并应答。对于I模块，应答帧包含其采集到的输入数据；对于O模块，请求帧包含相应的输出数据。安全数据帧具体如下所示：

Request Message to Input Slave

|  |  |  |
| --- | --- | --- |
| Frame Header | CRC-32 | Reverse Msg |

ACK of Input Slave

|  |  |  |  |
| --- | --- | --- | --- |
| Frame Header | I Data Block | CRC-32 | Reverse Msg |

Request Message to Output Slave

|  |  |  |  |
| --- | --- | --- | --- |
| Frame Header | O Data Block | CRC-32 | Reverse Msg |

ACK of Output Slave

|  |  |  |
| --- | --- | --- |
| Frame Header | CRC-32 | Reverse Msg |

## 安全措施与通信错误的对应关系

主从采用4.3节中的安全措施检测可能的通信错误，安全措施以及其能够检测的通信错误类型如表4-6所示：

表4-6 安全措施与通信错误关系

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 通信错误 | 安全措施 | | | | | |
| 序号 | 接收时间预期 | CRC | 带请求超时的Feedback Message | 连接验证 | 交叉冗余校验 |
| 数据损坏(Data Corruption) |  |  | X |  |  |  |
| 重复(Repetition) | X |  |  |  |  | X |
| 不正确的序列(Incorrect sequence) | X |  |  |  |  | X |
| 丢失(Loss) | X |  |  | X |  | X |
| 不可接受的延迟(Unacceptable delay) |  | X |  | X |  |  |
| 插入(Insertion) | X |  |  | X | X | X |
| 伪装(Masquerade) |  |  |  |  | X |  |
| 寻址异常(Addressing) |  |  |  |  | X |  |

## 错误处理与恢复机制

### 主站

#### 4.5.1.1针对I模块从站

针对每一个I模块从站，主站均维护一个错误计数、一个容忍标志位和一个错误标志位，初始值为0。当主站检测到通信错误时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位，主站应用程序应采用最后一次接收到的正确数据；否则，置错误标志位，复位容忍标志位，置控制字节的bit0：active\_FV为1，主站应用程序应采用安全值。

当主站未检测到通信错误时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则主站应用程序应继续采用安全值，否则，复位错误标志位和控制字节的bit0：active\_FV，应用程序应采用本周期接收到的正确数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位，主站应用程序应采用本周期接收到的正确数据；如果错误和容忍标志位均为0，则相应的错误计数减1，主站应用程序应采用本周期接收到的正确数据。

#### 4.5.1.2针对O模块从站

无论是否发生通信错误，主站始终向O模块从站下发相应的输出数据。针对每一个O模块从站，主站均维护一个错误计数、一个容忍标志位和一个错误标志位，初始值为0。检测到通信错误时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位；否则，置错误标志位，复位容忍标志位，置状态字节的bit 4：FV activated为1，从站应用程序应输出安全值。

未检测到通信错误时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则从站应用程序应继续输出安全值，否则，复位错误标志位和状态字节的bit 4：FV activated，从站应用程序应输出实时输出数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位；如果错误和容忍标志位均为0，则相应的错误计数减1。

### 从站

从站检测到通信错误后，根据错误种类，置相应的状态位。

#### 4.5.2.1 I模块从站

I模块从站始终将实时输入数据和相应的状态信息应答给主站。I模块从站维护一个错误计数，一个容忍标志位和一个错误标志位，初始值为0。检测到通信错误时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位；否则，置错误标志位，复位容忍标志位，置状态字节的bit 4：FV activated为1，主站应用程序应采用安全值。

未检测到通信错误时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则主站应用程序应继续采用安全值，否则，复位错误标志位和状态字节的bit 4：FV activated，主站应用程序应采用实时输入数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位；如果错误和容忍标志位均为0，则相应的错误计数减1。

#### 4.5.2.2 O模块从站

O模块从站维护一个错误计数，一个容忍标志位和一个错误标志位，初始值为0。检测到通信错误时，相应的错误计数加8，如果更新后的错误计数小于门限值（（配置的可容忍次数+1）×8-4），则置容忍标志位，从站应用程序应采用最后一次接收到的正确数据；否则，置错误标志位，复位容忍标志位，置状态字节的bit 4：FV activated为1，从站应用程序应采用安全故障设定值。

未检测到通信错误时，如果错误标志位为1，则相应的错误计数减8，若更新后的错误计数大于0，则从站应用程序应继续采用安全故障设定值，否则，复位错误标志位和状态字节的bit 4：FV activated，应用程序应采用本周期接收到的正确数据；如果容忍标志位为1，则相应的错误计数减1，复位容忍标志位，从站应用程序应采用本周期接收到的正确数据；如果错误和容忍标志位均为0，则相应的错误计数减1，从站应用程序应采用本周期接收到的正确数据。

## 状态图

### 主站状态图

主站与输入从站通信时的状态图如图4-2所示：



图4-2 主站与输入从站通信时的状态图

说明：

x：与相应输入从站对应的本地序号；

tolflag/ errflag/errnum：与相应输入从站对应的容忍标志位/错误标志位/错误计数；

threshold：与相应输入从站对应的门限值 -（配置的可容忍次数+1）×8；

host timeout：主站发送完请求帧后，在一定时间内未收到从站应答的ACK；

host length error：主站发现应答帧的帧长度错误；

host addr error：主站发现应答帧中的地址(主从对应关系)错误；

host crc error：主站发现应答帧中的CRC错误；

host sq error：主站发现应答帧中的序号与相应请求帧中的序号不一致；

slave timeout：从站检测出两次连续接收的时间间隔超时；

slave length error：从站收到主站发送的请求帧后，发现请求帧的帧长度错误；

slave addr error：从站收到主站发送的请求帧后，发现请求帧中的地址(主从对应关系)错误；

slave crc error：从站收到主站发送的请求帧后，发现请求帧中的CRC错误；

slave sq error：从站收到主站发送的请求帧后，发现请求帧中的序号错误。

### 从站状态图

输出从站与主站通信时的状态图如图4-3所示：



图4-3输出从站与主站通信时的状态图

说明：

y：输出从站维护的本地序号；

recvnum：请求帧中的序号；

tolflag/ errflag/errnum：输出从站维护的容忍标志位/错误标志位/错误计数。

## 序列图

### 正常通信

本节说明正常通信过程中主站与从站的交互情况，如图4-4所示：

说明：

T1：主站两次连续发送超时时间；

T2：主站请求超时时间；

T3：从站两次连续接收超时时间。



图4-4 正常通信

### 序号恢复

图4-5和图4-6分别显示了序号恢复情况1和序号恢复情况2时的交互过程。

说明：

m：非1的有符号整型数；

x：主站维护的与某一I/O从站相对应的序号；

y：从站维护的序号；

序号恢复情况1：某一安全帧除序号外，其他部分均正确，之后的安全帧序号在此帧序号的

基础上正常增加。由图4-5可知，只需1个周期，序号错误就能够恢复；

序号恢复情况2：某一安全帧存在addr或crc错误，序号可能正确也可能不正确，之后的安全帧序号恢复正常。由图4-6可知，最多只需2个周期，序号错误就能够恢复。



图4-5 序号恢复情况1



图4-6 序号恢复情况2

## I/O模块参数化

从站参数的数据结构如图4-7所示，CRC负责校验Parameters Data，参数可能需要分多个数据包下发，每个数据包下发其中一个data set，其下发过程是非周期性操作。



图4-7 参数结构

### 参数数据包结构

参数数据包结构如表4-7所示，由包头，参数数据和CRC组成，其中包头如表4-8所示，参数数据为图4-7中的某一data set，CRC-32负责校验包头和本数据包中的参数数据，其多项式为0x1 F4AC FB13。

表4-7 参数数据包结构

|  |  |  |
| --- | --- | --- |
| Frame Header | Parameters Data | CRC-32 |
| 8 bytes | variable | 4 bytes |

表4-8 Frame Header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Data Type | Length | Value | Desc |
| Codename | unsigned int | 4 bytes |  | 代表主从唯一的对应关系：  主站地址<<16 | 从站地址 |
| Frame Number | unsigned char | 1 byte |  | 本数据包的包号：从1开始 |
| Last Flag | unsigned char | 1 byte |  | 是否最后一包：0-否；1-是 |
| Frame Length | unsigned short | 2 bytes |  | 此数据帧的总长度（字节），包括帧头 |

### 安全措施

#### 4.8.2.1 CRC

从站接收到完整数据包后，用与发送方相同的CRC算法计算得出CRC结果，然后与发送方计算的结果进行比较，如果两者相同，则认为数据未损坏，如果不相同，则认为数据已被损坏，直接丢弃此数据包。

#### 4.8.2.2连接验证

主从存在唯一的对应关系，从站接收到完整数据包后，检查对应关系代号Codename是否正确，若不正确，则直接丢弃此数据包。

#### 4.8.2.3包号

从站接收到完整数据包后，检查包号是否正确，若不正确，则直接丢弃此数据包。

### 参数化序列图

参数化过程如图4-8所示，从站采用新下发的参数后，将iPar\_OK（status byte, bit 5）清为0，主站接收到此状态信息后，置iPar\_EN（control byte, bit 1）为0，恢复周期性读写I/O数据操作。



图4-8 参数化过程

# 残余错误率

## 计算公式

残余错误率计算公式如5-1所示：

(5-1)

说明：

：传输介质位错误概率；

：安全通信层每小时的残余错误率；

：单个安全消息的残余错误概率；

v：每小时最大的安全消息个数；

m：在单个安全功能中允许的消息接收端的最大个数。

采用CRC方法时，单个安全消息的残余错误概率计算公式如5-2所示：

(5-2)

说明：

r：CRC域位的个数，项目均选取CRC-32，即r为32；

dmin：给定数据长度范围时，CRC多项式的最小汉明距；

n：安全消息的总位数（包含CRC域）。

## CRC生成多项式及其汉明距

CRC生成多项式的最小汉明距与数据长度（位数）有关，本文档中为安全通信层选取的多项式为0x1 F4AC FB13，其最小汉明距与数据长度的对应关系如表5-1所示：

表5-1 最小汉明距与数据长度

|  |  |
| --- | --- |
| 最小汉明距 | 数据长度范围 - bits：被校验域长度+CRC域长度 |
| 12 | 8 - 11 |
| 10 | 12 - 24 |
| 8 | 25 - 274 |
| **6** | **275 - 32736** |
| 4 | 32767-65502 |
| 2 | 65503+ |

## 残余错误率计算

### 控制站间安全通信

最小发送周期为200ms，相关参数及计算结果如表5-2所示，由表中结果可知能够满足SIL3安全等级要求。

表5-2相关参数及计算结果

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | m | v | dmin | 数据长度- bits：被校验域+CRC域 | | 残余错误率:  /h |
|  | 1 | 3 600 000/200=18 000 | 6 | 应答帧 | 96 （12 bytes） | 6.37E-22 |
| 请求帧 | 5216 （652 bytes） | - |
| 总残余错误率 | | | | | | - |

### ~~主处理器间安全通信~~

~~最小控制周期为5ms，每周期通信两次，相关参数及计算结果如表5-3所示，由表中结果可知能够满足SIL3安全等级要求。~~

~~表5-3相关参数及计算结果~~

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ~~m~~ | ~~v~~ | ~~dmin~~ | ~~数据长度- bits：被校验域+CRC域~~ | ~~残余错误率:~~  ~~/h~~ |
|  | ~~1~~ | ~~2×3 600 000/5=1 440 000~~ | ~~6~~ | ~~352(44bytes)~~ | ~~0.6314~~ |

### 主处理器与IO模块间安全通信

最小控制周期为5ms，相关参数及计算结果如表5-4所示，由表中结果可知能够满足SIL3安全等级要求。

表5-4相关参数及计算结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | m | v | dmin | 数据长度- bits：被校验域+CRC域 | 残余错误率:  /h |
|  | 1 | 3 600 000/5=720 000 | 6 | 96 （12 bytes） | 6.37E-22 |
| 640 （80 bytes） | 4.60E-20 |
| 总残余错误率 | 4.66 E-20 |