第 35 卷 第 6 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.6 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)06—0176—02 文献标识码：A 中图分类号：TP309

EPA 功能安全协议的研究与实现

王 静[1,2]，徐皑冬[1]，宋 岩[1]
(1. 中国科学院沈阳自动化研究所，沈阳 110016；2. 中国科学院研究生院，北京 100039)

摘 要：现场总线在通信传输过程中，会受到各种通信故障的影响，而现场总线与功能安全的结合可降低这种影响。该文描述 EPA 功能安全通信模型，针对通信传输过程中可能出现的通信错误，采用时间戳、序列号、CRC 校验等功能安全通信技术。给出 EPA 功能安全协议层的报文结构，阐述功能安全协议层的具体实现过程。

关键词：现场总线；功能安全；EPA 标准

Research and Realization of EPA Functional Safety Protocol

WANG Jing[1,2], XU Ai-dong[1], SONG Yan[1]
(1. Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016;
2. Graduate University of Chinese Academy of Sciences, Beijing 100039)

【Abstract】 Some kinds of communication errors occur during the communication process of fieldbus. Applying functional safety on the fieldbus technology can eliminate some of these errors. This paper describes Ethernet for Plant Automation(EPA) functional safety communication model. Several measures are used to detect different communication errors, such as time stamp, sequence number and CRC. The message structure of EPA functional safety protocol layer is presented. The realization process of functional safety protocol layer is depicted.

【Key words】 fieldbus; functional safety; Ethernet for Plant Automation(EPA) standard

1 概述

由工业生产造成的事故给社会带来了很大的经济损失及人身伤害。2000 年 IEC 61508 标准的出台为工业的安全生产指明了方向。IEC61508 提出了功能安全的概念，当功能出现问题引发危险时，可避免危险，保证工作能安全可靠地进行。IEC 61508 虽然以电气、电子、可编程电子的安全相关系统命名，但它的思想适用于所有用于保证安全的系统[1]。对于现场总线来说，电磁干扰、高误码率等各种通信故障，可能会对现场总线系统造成很大影响。功能安全的提出对于现场总线同样意义重大，使其在功能出现问题引发危险时能降低风险，保证现场总线在运行中的可靠性、有效性。

EPA(Ethernet for Plant Automation)是我国第一个拥有自主知识产权的现场总线标准，2007 年被国际电工委员会正式接收为国际标准。目前，EPA 工作组正在进行包括 EPA 功能安全在内的工作。

2 EPA 功能安全

2.1 EPA 功能安全通信模型

图 1 为 EPA 通信层体系结构。

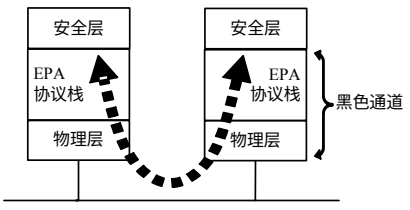

图 1 EPA 通信层体系结构

安全应用和标准应用可以共享同一条现场总线通信链路。黑色通道包括线缆、安全栅、电源、ASIC、通信栈、网线、交换机和集线器等，它不提供任何附加的技术措施来保证数据的的完整性[2]。

2.2 功能安全通信技术

对于现场总线系统，数据在进行数据传输的过程中可能会遇到电磁干扰等情况，从而对数据传输造成传输错误等影响，进而导致安全风险。数据传输中可能出现的错误有数据破坏、数据重传、数据丢失、插入、乱序、伪装、延时、寻址出错等。针对传输过程中出现的通信错误，可以采用相对应的功能安全通信技术，如：序列号，CRC 校验，时间戳，时间期望，关系密钥，回传等技术。本文采用关系密钥、序列号、时间戳和 CRC 校验等功能安全通信技术来保证 EPA 通信的数据完整性和时间有效性。

通信错误与功能安全技术之间的对应关系如表 1 所示。

表 1 通信错误与功能安全技术

错误类型	功能安全技术			
	序列号	关系密钥	CRC 校验	时间戳
数据破坏			√	
数据重传	√			
丢失	√			
插入	√	√		
乱序	√			√
伪装		√	√	
延时				√
寻址出错		√	√	

基金项目：国家“863”计划基金资助项目(2007AA04Z175)
作者简介：王 静(1982－)，女，硕士研究生，主研方向：现场总线技术；徐皑冬，研究员；宋 岩，助理研究员
收稿日期：2008-08-23 **E-mail：**hyfx569@163.com

一种功能安全技术可解决一种或多种通信错误，而对于某种确定的通信错误，可采用一种或多种功能安全技术相结合的方式来确保数据的安全传输。

3 EPA 功能安全协议层

3.1 EPA 功能安全通信报文结构

图 2 是 EPA 功能安全通信报文结构，它包含了 EPA 协议类型、IP 报文头、UDP 报文头、EPA 应用层服务报文头和 EPA 安全通信数据单元。

TYPE	IP 报文头	UDP 报文头	EPA APP 报文头	EPA FSPDU

图 2 EPA 功能安全通信报文结构

3.2 FSPDU 结构

EPA 功能安全通信数据单元(FSPDU)报文结构见图 3。

序列号 (2 Byte)	时间戳 (8 Byte)	EPA 用户数据 (*N* Byte)	CRC (4 Byte)

图 3 FSPDU 结构

代码如下：

```
typedef    unsigned char    USIGN8;
typedef    unsigned short    USIGN16;
typedef    unsigned long    USIGN32;
typedef struct
{
 USIGN16          uSequenceNO;
 USIGN8           aucReserved[2];
 long long        llTimeStamp;
 USIGN8           oEPASafeDATA[MAX_DATA_LENGTH];
 USIGN32          ulCRC;
}EPA_FSPDU;
```

EPA 功能安全通信报文不改变原有的 EPA 报文格式。EPA 功能安全通信数据单元通过采用关系密钥、序列号、时间戳和 CRC 校验等措施来保证 EPA 通信的数据完整性和时间有效性等。

(1)关系密钥：对于每一对通信关系，通信源和通信目的方具有唯一的通信标识(关系密钥)。用来防止寻址错，即安全相关报文发往错误的安全相关参与者。关系密钥用来构成 CRC，但不用于通信。

(2)序列号：用来标识通信发起方发送数据的顺序，范围为 0~255。初始时为 0，每成功发送一个 EPA 功能安全通信数据报文，就将序列号增加 1。当达到 255 时，重新返回 1。每一项服务对应一个序列号。

(3)时间戳：记录 EPA 功能安全层数据发送的时刻。接收方接收到报文时，须检测接收到报文的时间戳与接收时的时间之差是否超过了最大允许时间，若超过则判定为延时故障。

(4)CRC 校验：CRC 计算与普通除法不同，普通除法是借位相减，而 CRC 计算则是异或运算[3]。本文采用 32 位 CRC 循环冗余校验，使用查表法。

CRC32 生成多项式为

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

32 位 CRC 生成表如下：

```
const unsigned long CRC32Table[256] =
{
0x00000000, 0x77073096, 0xEE0E612C, 0x990951BA,
0x076DC419, 0x706AF48F, 0xE963A535, 0x9E6495A3, 0x0EDB8832,
0x79DCB8A4, …, 0xB3667A2E, 0xC4614AB8, 0x5D681B02, 0x2A
6F2B94, 0xB40BBE37, 0xC30C8EA1, 0x5A05DF1B, 0x2D02EF8D
};
```

使用 CRC 时，黑色通道不能使用与功能安全层相同的 CRC 多项式(除非考虑到其他特殊情况)。通过关系密钥、序列号、时间戳、EPA 用户数据来计算 CRC 的值。用于计算 CRC 的功能安全校验报文 SCM 结构如图 4 所示。

关系密钥 (4 Byte)	序列号 (2 Byte)	时间戳 (8 Byte)	EPA 用户数据 (*N* Byte)

图 4 功能安全校验报文结构

代码如下：

```
typedef struct
{
 USIGN32          ulRelationKey;
 USIGN16          uSequenceNO;
 USIGN8           aucReserved[2];
 long long        llTimeStamp;
 OCT_STRING       oEPASafeDATA[MAX_DATA_LENGTH];
}EPA_SCM;
```

4 系统实现

4.1 软硬件环境

EPA 网络节点使用 ATMEL AT91R40008 MCU，40008 是基于 RISC 指令集的 ARM7TDMI 内核的 MCU，片上整合 32 bit 单时钟周期访问的 256 Kb SRAM，支持 8 优先级的中断向量控制器，3 通道 16 位定时器/计数器，2 个 UART 和可编程的看门狗定时器，功能满足本系统需要且价格相对便宜。Flash 使用 AM 29LV800B 芯片，容量 512 K×16 bit 主要用于存储程序代码和数据。EEPROM 使用 SST 公司的 SST 29LE010 芯片，容量为 128 K×8 bit，用来存储用户程序需要保存的配置或其他数据。SRAM 使用 CYPRESS 公司的 CY7C1061AV33 芯片，主要作为程序运行时刻的存储器。以太网控制器使用 CS8900 芯片，用于网络通信。

开发环境：GreenHill 的 Multi2000 IDE 交叉编译开发环境，Nucleus 嵌入式实时多任务操作系统，Xnet TCP/IP 协议栈。

4.2 功能安全协议层的实现

功能安全协议层分别对发送(接收上层发来的用户数据，并发送给协议栈)与接收(接收协议栈发来的数据)2 个过程进行处理。处理情况如下：

(1)发送过程

功能安全协议层接收到来自上层(用户层)的用户数据之后，并不直接交给 EPA 协议栈，而是将关系密钥、时间戳、序列号以及用户数据一起(即构造 SCM)执行 CRC 校验算法，然后将得到的 CRC 码附于用户数据后，序列号、时间戳附于用户数据前(即构造 FSPDU)，一起发送给 EPA 协议栈。发送过程如图 5 所示。

(2)接收过程

功能安全协议层接收到来自协议栈的数据后，首先构造功能安全校验报文结构，执行 CRC 校验算法，得出 CRC 码。将此 CRC 码与接收到的协议栈发来的 CRC 码相比较，同时检测接收到的序列号、时间戳是否符合要求，以此来判断是否发生了数据破坏、丢失、延时等故障。若不符合要求，则说明发生了故障，丢弃此错误报文，并将故障信息发往上层用户；若符合要求，则获得用户数据，并将其发往上层用户。接收过程如图 6 所示。

(下转第 180 页)