故障安全通信系统的研究与设计 *

王海凤，何之栋，黄文君
（浙江大学 智能系统与控制研究所 工业控制技术国家重点实验室，浙江 杭州 310027）

摘 要：针对工业通信中可能出现的各种故障，研究并设计一种故障-安全通信协议。首先基于黑色通道的通信结构，设计序列号、CRC 校验、时间监视和 SIL 等级监视等安全措施；其次提出故障安全通信协议的软件实现方案；最终在验证平台上进行测试。实验结果表明，安全通信层可以有效地监测通信状态，保证系统在出现故障时的安全性，满足 SIL3 等级要求。

关键词：故障-安全通信；通信协议；SIL 等级
中图分类号：TP27　　**文献标识码**：B　　**文章编号**：0258-7998(2014)01-0115-04

Research and design of a fail-safe communication system

Wang Haifeng, He Zhidong, Huang Wenjun
(State Key Lab of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou 310027, China)

Abstract: A fail-safe communication protocol is presented for fieldbus systems to guarantee the safety of industrial control systems confronting failures. A safety layer is proposed based on 'black-channel' communication structure, in which secure measures including sequence number, CRC checksum, watchdog-timer, and SIL monitor are taken to detect corresponding communication errors. Experiment results show that error rate is reduced to an acceptable level and the SIL3 level requirement is met.

Key words: fail-safe communication; communication protocol; SIL

工业现场中经常存在电磁干扰、高误码率等现象，对现场总线系统的通信造成很大的影响。随着用户对安全的认识不断提高和国家对工业现场安全要求的不断提高，现场总线故障安全通信的研究具有重要的意义[1]。

对于安全关键系统，一方面对于高速列车、核能核电系统等，系统的可靠与安全是生命安全的基本保证，因此受到很多的关注[2]；另一方面，现有的现场总线系统由于布线多、改造困难，如果直接对现有现场总线协议进行修改、增加安全机制，将产生很大的投资。因此，如何在尽量维持现有总线的基础上实现系统的安全可靠成为关键[3-4]。

现场通信协议易受环境、人为破坏等影响，出现各种通信故障。参考文献[5]总结了现场总线中的常见故障。为提高通信可靠性，保障系统的安全稳定运行，需要采取一定的措施避免通信故障。一种常见的规避风险的方式是增加冗余[6]。参考文献[7]利用三模同步表决总线、冗余控制器局域网总线和冗余以太网总线实现各模块间的数据通信。但是在规模很大的网络情况下，增加冗余会产生较大的额外成本开销，并不是一种理想的解决方案。

参考文献[5-6]针对常见现场总线的安全措施作了较为详细的阐述。针对 CAN 总线、EPA 总线等也已有相应研究[8-9]。基本思想是在现有总线之上增加安全通信层，通过安全通信层实现安全机制。但上述文献只分析了安全层的功能，并未提出具体设计方案。

功能安全标准 IEC61508 中提出了安全完整性等级，即 SIL 等级(Safety Integrity Level)的概念。SIL 等级是功能安全等级的一种划分，分为 4 级。本文的故障安全协议通过增加安全通信层，以达到所要求的 SIL 等级。

1 故障安全通信协议的设计

1.1 通信结构设计

在不改变现有总线网络结构的基础上，采用增设安全通信层的方式扩展标准协议，以满足安全通信的要求。如图 1 所示，现有总线网络的通信部件(如连接线缆和通信栈)均被划入“黑色通道”，对它们的传输可靠性不作假定。在安全通信层中设计并实现多种安全措施，“黑色通道”中可能出现的所有故障均由安全通信层查出。

* 基金项目：国家 863 计划项目(2012BAF05B00)资助

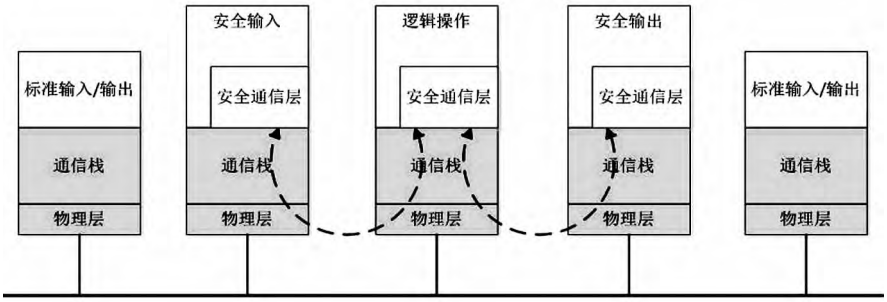

图 1 安全通信层的通信结构

1.2 安全报文设计

安全通信层的报文与原先的现场通信报文结构一致，只是将从用户程序接收到的用户数据增加了序列号、CRC 校验码和控制/状态字节，扩展成安全数据单元。序列号用于防止报文重复或丢失等故障，CRC 校验码用于保证数据的完整性，控制字节和状态字节则为安全通信协议状态机的同步化服务。

如图 2 所示，安全数据单元主要由数据区、控制/状态字节、CRC2 校验码三部分组成。当主机向从机发送报文时，安全数据单元附带控制字节，用于对从机进行控制；相反地，当从机向主机发送报文时，安全数据单元附带状态字节，用于向主机报告从机运行状态。

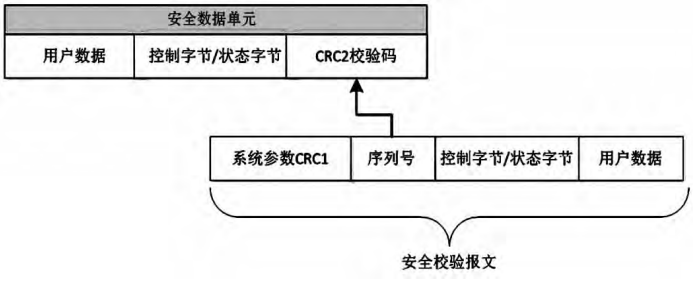

图 2 安全数据单元报文结构

1.3 安全通信协议软件设计

安全通信层的软件实现由主机和从机协议栈两部分构成。如图 3 所示，软件模块主要包括状态机模块、报文发送、报文接收、安全事件监视模块、错误检测模块和 SIL 监视器模块。

(1)主从状态机设计。状态机规定了主机和从机的所有状态以及在这些状态之间的转移和动作。主机和从机根据状态机调用相应的模块，以实现通信功能。主机和从机的状态转移条件主要体现在数据报文中的状态字节和控制字节，如图 3 所示。

(2)报文发送与接收模块。如图 4 所示，报文发送模块需要对来自上层的用户数据添加安全信息，处理过程如下：首先更新当前状态机的状态，根据第 1.2 节中的方式构造安全报文并发送至下层协议栈。安全通信层接收到来自协议栈的数据后，首先根据接收方所持有的系统参数、本地序列号以及接收到的数据中的用户数据和控制字节或状态字节，构造功能安全校验报文 SCM；再对功能安全校验报文执行 CRC 校验，得到 CRC 码。然后比较计算所得 CRC 码与接收数据中的 CRC 码，判断是否发生了数据破坏、丢失、延时等故障。

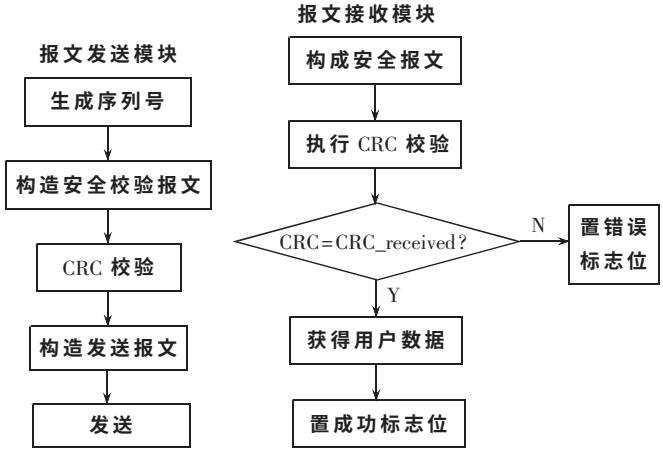

图 4 报文发送流程与报文接收流程

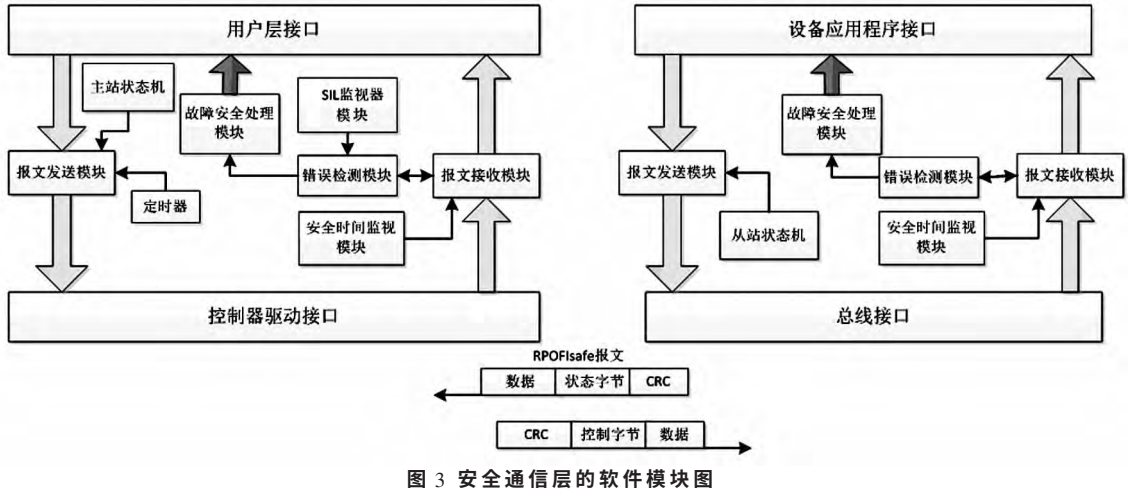

图 3 安全通信层的软件模块图

(3)安全时间监视模块。在主机和从机中分别设置一个看门狗定时器,对接收模块进行时间监控,以保证报文在安全时间内到达。看门狗定时器的周期根据报文从发送方到接收方的过程时间设置,取 3 个时间周期。发送方发出报文后,如果在定时器时间内没有收到响应报文,则重新发送该报文。

(4)错误检测模块。通信过程中,接收方发现报文出现错误,则将在响应报文中将报文中的错误标志位设置为对应值。错误检测模块通过查询错误标志位,可以确定是否发生 CRC 错误或超时错误。一旦有错误发生,将错误产生的时间报告给 SIL 监视器。错误检测模块与 SIL 监视器模块相结合,以保证系统满足一定的 SIL 等级。

(5)SIL 监视器模块。在一个 SIL 监视器时间周期内,对安全控制回路中被破坏的报文进行计数,当受干扰报文的频率超越规定的界限时,向系统报告故障状态,并采取相应措施(如停机等),以保证系统始终维持一定的 SIL 等级。由于 CRC 校验的准确度与 CRC 校验式长度和数据报文的长度有关,因此,监视器时间周期 T 取决于 SIL 等级、CRC 长度和过程数据长度。在 IEC 61508 中定义的 SIL3 要求(PFH):$10^{-8} \leqslant PFH < 10^{-7}$。

按照安全系统通信周期为 10 ms 计算,10 h 内要求通信过程出现的错误报文次数不能大于 $10\times3\,600\times100\times10^{-7}=0.36$(次)。为了方便实现,折算成相邻两次出现错误的时间间隔即:$T_d=2\div0.36\times10\approx55$ h。因此 SIL 监视器模块的周期设定为 55 h。

2 安全通信层的性能验证

2.1 软硬件环境

测试平台由一个支持以太网通信的主机站和两个 I/O 设备从站构成。标准通信层使用基于以太网的 UCP 协议,主机站和设备从机站采用本文所述软件设计,在 UCP 协议的基础上实现故障安全通信层。

通信卡使用 TI 公司生产的 AT91SAM9X,该处理器是基于 ARM Cortex 内核支持 RISC 指令集的 32 位 CPU,同时处理器还带支持 10/100 Mb/s 高速数据通信的以太网控制器,3 个 CAN 控制器等其他常用通信接口。

2.2 测试与验证

测试场景设定为主机采用以轮询方式向两个 I/O 设备发送报文。共发送报文总数 100 万条,预先设定报文中错误报文的比例,其中正常报文 20%、数据破坏报文占 40%、序列号错误报文占 20%、延时错误报文占 20%。实验结果表明,故障安全层可以检测出所有报文错误,错误漏检率接近于零。通信故障检测测试结果如表 1 所示。

为了保证通信总线满足 SIL3 等级要求,对总线上的通信残余误差率进行计算。现场总线通信中包含实时数据报文、广播报文及令牌帧,单个通信报文

表 1 通信故障检测测试

错误类型	错误报文数	检验率/(%)
数据破坏	400 000	99.999 7
报文重复	50 000	99.998 1
报文插入	35 000	99.998 6
报文丢失	18 000	99.999 2
报文错序	97 000	99.999 5
延时报文	200 000	99.999 8

的残余失效率按下式计算:

$$R_{CRC}(P_e)\approx 2^{-r}\times\sum_{k=d_{min}}^{n} C_n^k\times P_e^k\times(1-P_e)^{n-k} \tag{1}$$

其中,P_e 为位误码率,r 为 CRC 多项式冗余位,n 为报文长度,d_{min} 为海明距离[10]。

在实现方案中,采用 32 bit 冗余 CRC 多项式,总线上的位误差率为 10^{-4},由式(1)计算得到三种不同报文类型的单个通信报文的失效率如表 2 所示。

表 2 不同类型报文残余失效率

报文类型	报文长度/bit	报文失效率/s
实时报文	1 024	$3.367\,22\times10^{-19}$
广播报文	144	$8.654\,02\times10^{-30}$
令牌报文	64	$1.025\,43\times10^{-32}$

总线通信每小时的残余差错率由下面的公式计算得:

$$\wedge_{CRC}=3\,600\times((R(p)_{brd}\times\nu_{brd})+(R(p)_{data}\times\nu_{data})+(R(p)_{token}\times\nu_{token})) \tag{2}$$

其中,$R(p)_{data}$、$R(p)_{brd}$、$R(p)_{token}$ 分别为实时报文、广播报文和令牌的报文差错率,如表 3 所示。ν_{data}、ν_{brd}、ν_{token} 分别为实时报文、广播报文数、令牌报文的数据包产生速率。在不同通信周期下,总线通信的残余失效率计算结果如表 3 所示。

由表 3 可知,PFH(每小时平均故障率)小于 5×10^{-11},PFD(平均期望故障率)小于 5×10^{-7},因此本文设计的安全通信层可以满足 SIL3 等级中的 PFH 要求和 PFD 要求。

从实验结果可知,安全通信层可以检测不同类型的通信故障,提供可靠的通信协议。此外,结合软件方案中的多种安全监测技术,总线通信的残余失效率满足 SIL3 等级要求。因此,安全通信层可以完成系统的故障安全功能。

本文通过在现有现场总线的基础上增加安全通信

表 3 总线通信残余失效率

通信周期/ms	报文类型	最大报文速率	总线通信 $\wedge_{CRC}$	PFH	PFD
20	实时报文	6 600	8.00×10^{-12}	8.00×10^{-12}	3.50×10^{-8}
	广播报文	5 400	1.68×10^{-22}		
	令牌报文	4 000	1.48×10^{-25}		
100	实时报文	4 680	5.67×10^{-12}	5.67×10^{-12}	2.48×10^{-8}
	广播报文	4 440	1.38×10^{-22}		
	令牌报文	1 640	6.05×10^{-26}		

层实现系统的故障安全功能。采用黑色通道模型和独立的功能安全层，其故障安全性建立在单信道通信系统之上，安全通信不需要通过冗余电缆来实现。本文首先设计了一种安全通信协议，并给出了故障安全通信协议的软件实现方案。该方案目前已通过前期的性能测试，达到了安全标准的要求，可以有效地实现对系统通信的监控，保证系统在故障状态下的安全性。

参考文献

[1] IEC61508-part5: Examples of methods for the determination of safety integrity levels[Z].1998,12:15-41

[2] 杨仕平，熊光泽，桑楠.安全关键系统高可信保障技术的研究[J]. 计算机科学，2003,30(5):97-101.

[3] ALANEN J, HIETIKKO M, MALM T. Safety of digital communications in machines[C]. Finland:Research Notes 2265, VTT Industrial Systems, 2004:14-29

[4] REICHENBACH, FRANK, et al. A pragmatic approach on combined safety and security risk analysis[C]. 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW), Dallas, TX, USA, 2012: 239-244.

[5] IEC61784-3: Digital data communication for measurement and control-Part 3:Profiles for functional[Z].

[6] 王志颖，马卫东，熊光泽，等. 面向安全关键系统的CAN总线应用研究综述[J].计算机应用研究，2011,28(4)：1216-1220.

[7] 黄涛，陈祥献，黄海.基于三取二冗余结构的安全计算机系统[J]. 计算机工程，2011,37(18):254-257.

[8] 马磊，王海峰.计算机联锁系统CAN总线故障安全通信研究[J]. 北京交通大学学报，2008,32(2):104-108.

[9] Fu Peng, Fan Xiaoping. Research on safety monitor system of coal mine based on EPA[J]. Advanced Materials Research, 2012,433-440(1):6128-6133.

[10] Koopman, Philip. 32-bit cyclic redundancy codes for Internet applications[C]. Dependable Systems and Networks. Proceedings. International Conference on. IEEE, 2002.

（收稿日期：2013-06-24）

作者简介：

王海凤，女，1990年生，硕士生，主要研究方向：工业网络安全系统。

何之栋，男，1989年生，硕士生，主要研究方向：工业无线网络。

黄文君，男，1972年生，研究员，主要研究方向：控制系统与现场总线，实时工业以太网现场总线技术。

（上接第114页）

比，主用户不在时，在混合模型下没有主用户的功率干扰，使频谱资源尽可能得到充分利用。当主用户的平均频谱效率 R_p 小于1.75时，混合模型下比interweave共享模式下高是因为，混合模型下主用户占用信道时，只要保证对主用户不产生干扰的前提下，次用户同时进行通信，能够更充分地利用频谱资源。

本文提出了基于主用户活跃性混合接入机制下认知链路的平均频谱效率的优化框架，主用户和次用户均采用AMC技术的传输方案，最大化认知链路的平均频谱效率。数值分析表明，本文提出的混合接入机制下认知链路的平均频谱效率相比单一接入机制下有所提高。

参考文献

[1] ASGHARI V, AISSA S. Adaptive rate and power transmission in spectrum-sharing systems[J]. IEEE Transactions on Wireless Communications, 2010,9(10):3272-3280.

[2] CHAI C C.On power and rate adaptation for cognitive radios in an interference channel: Vehicular Technology Conference(VTC 2010-Spring)[C].2010 IEEE 71st,2010:1-5.

[3] TAKI M, LAHOUTI F. Spectral efficiency optimized adaptive transmission for interfering cognitive radios:IEEE International Conference on[C].Communications Workshops,2009, ICC Workshops 2009,2009:1-6.

[4] Zhang Zhaoyang, Luo Haiyan, Zhang Jianmin, et al. Cognitive radio transmission strategies exploiting the primary-link adaptivity[J]. IEEE Transactions on Vehicular Technology, 2011,60(8):3805-3813.

[5] TAKI M, LAHOUTI F. Discrete rate interfering cognitive link adaptation design with primary link spectral efficiency provisioning[J]. IEEE Transactions on Wireless Communications,2011,10(9):2929-2939.

[6] SENTHURAN S, ANPALAGAN A, DAS O. Throughput analysis of opportunistic access strategies in hybrid underlay overlay cognitive radio networks [J]. IEEE Transactions on Wireless Communications, 2012,11(6):2024-2035.

[7] Liu Qingwen, Zhou Shengli, Georgios B G. Cross-layer combining of adaptive modulation and coding with truncated ARQ over wireless links[J]. IEEE Transactions on Wireless Communications, 2004,3(5):1746-1755.

[8] LEE W Y,AKYILDIZ I F.Optimal spectrum sensing framework for cognitive radio networks[J]. IEEE Transactions on Wireless Communications, 2008,7(10):3845-3857.

（收稿日期：2013-05-03）

作者简介：

梁晓，女，1987年生，硕士研究生，主要研究方向：认知无线电频谱感知。

赵海峰，男，1984年生，博士研究生，主要研究方向：认知无线电频谱感知。

高昊民，男，1988年生，硕士研究生，主要研究方向：认知无线电频谱感知。