文章编号：1005-8451（2017）08-0001-05

基于故障注入的安全计算机通信总线测试方法研究

邱泽宇[1]，曹　源[1,2]，马连川[2]
（1. 北京交通大学　电子信息工程学院，北京　100044；
2. 北京交通大学　轨道交通控制系统国家工程研究中心，北京　100044）

摘　要：随着我国高速铁路的飞速发展，对列车安全性的要求日益提高。由于实际环境与测试环境有区别，某些特定场景靠故障注入的方式能够有效地发现设计上的缺陷。文章使用故障注入的测试方法对安全计算机内部通信总线进行故障注入测试，对通信总线内部的故障进行分析，提出了对通信总线物理层、链路层的软件故障注入方法，并实现了对通信总线的故障注入。

关键词：故障注入；安全计算机；通信总线；物理层；链路层
中图分类号：U29：TP39　**文献标识码：**A

Test method of safety computer communication bus based on fault injection

QIU Zeyu[1], CAO Yuan[1,2], MA Lianchuan[2]
(1. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing　100044, China;
2. National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing　100044, China)

Abstract: With the rapid development of high speed railway in our country, the requirement of train safety is increasing day by day. Because the actual environment is different from the testing environment, the design flaws of some particular scenes can be effectively identified by means of fault injection. This article used the fault injection test to test the internal communication bus of the security computer, proposed a software fault injection method for communication bus physical layer and link layer, implemented the fault injection of communication bus.

Keywords: fault injection; safety computer; communication bus; physical layer; data link layer

安全计算机作为铁路系统中核心的安全设备，主要保证和实现信号系统的安全性、可靠性，并在系统发生故障时导向安全，避免造成人员伤亡[1]。传统的安全计算机的测试方法只是对安全计算机进行功能测试[2-3]，无法测量现实中在特殊环境下设备的反应。故障注入测试通过人为的方式将故障注入到目标系统中，可以模拟实际环境中的突发故障，加速软硬件失效[4]。

本文针对安全计算机内部的通信总线进行故障注入，注入层次可以分为物理层和链路层。分析总线开发中出现过和可能出现的错误，提出对应的故障注入测试方案，在实验室的安全计算机平台上进行故障注入实验，对测试方案进行验证。

收稿日期：2017-03-06
基金项目：国家自然科学基金（U1534208）；国家重大研发计划（2016YFB1200600）。
作者简介：邱泽宇，在读硕士研究生；曹　源，副教授。

1　通信总线故障类型

根据以往安全计算机通信总线测试的经验[5]，对通信总线出现的故障进行分析，总线故障主要分为通信故障、时钟故障、寄存器故障等。文章从故障类型、故障位置、故障持续时间和故障注入时刻等方面进行分析，针对不同故障，设计不同的故障方案。

1.1　通信故障

通信故障主要指总线数据传输时出现的故障。通信故障包括消息丢失、消息延迟、数据帧错误等，故障的发生可以是单个故障或多个故障的集合，发生的位置主要在总线的数据信号线。通信故障可以分为瞬时、间歇、永久性故障，瞬时故障是指测试中只注入一次的故障；间歇性故障是在一定的周期内重复注入，重复性可以制定注入间隔，如正态分布、平均分布、指数分布、二项式分布等；永久性故障也

是周期性注入，故障在每个传输周期都会出现，如注入故障的周期与正常发送的周期相同时，即发送端向总线发送数据时，故障注入器同时向总线注入故障，就会造成总线永久性故障。注入故障后观察通信总线的反应可以判断总线是否满足安全性设计，再根据撤除故障后通信总线能否恢复正常工作来判断通信总线的稳定性。

1.2 时钟故障

时钟信号是通信总线正常运行的基础，由于通信总线连接多台设备，每个设备都有各自的时钟，为了保证多台设备之间的通信，需要保证设备之间的时钟一致。时钟故障包括同步故障、占空比故障、以及幅值的变化等，其中同步故障是通信总线最主要的故障，是保障各个设备正常通信的基础。在注入故障时，可以直接对总线物理层时钟线注入故障，干扰总线上的时钟信号；或对主设备注入故障，干扰主设备发送的时钟信号，使从设备接收到错误的同步信号，达到故障注入的目的。

除了同步故障外，时钟故障还包括对设备系统时钟注入故障，使设备自身时钟出现差错，由于时钟错乱而导致自身逻辑瘫痪，如将时钟线接地。时钟故障也可以根据故障的重复性划分为注入一次性故障，注入特定的分布函数的故障，及注入永久性故障等。

1.3 寄存器故障

寄存器故障是故障注入常用的故障类型，根据寄存器的重要性划分，某些寄存器直接关系到通信总线数据的收发，修改寄存器内的值会使总线通信直接出现错误，影响系统工作。通信总线中的寄存器包括板卡模块中的寄存器，存放数据或地址的寄存器，以及现场可编程门阵列（FPGA）中设置的先进先出（FIFO）、随机存取（RAM）等寄存器。寄存器故障包括读写故障及数据故障，故障注入主要使寄存器产生数据故障，即将寄存器中 1 位、多位、单字节或多字节通过故障注入器修改，对寄存器内部数据进行部分或全部数位的插入、翻转、置 0/1、替换、重新设置等。

1.4 其他故障

通信总线的故障除了以上 3 种，还存在电磁干扰、硬件失效、开路短路等故障，这些故障主要是硬件故障，发生故障可能会导致设备永久性失效，注入故障时也需要用到硬件故障注入器如电容耦合夹、群脉冲发生器等。由于条件有限，本文只进行软件故障注入，对这部分故障不做详细分析。

2 故障注入方案设计

在通信总线的物理层和链路层进行故障注入。通过在 FPGA 内部加入故障注入模块，将从用户与总线之间的发送 / 接收通道通过故障注入模块隔开，形成故障注入器，故障注入器具有负载生成、故障注入、数据收集等功能，能根据相应的故障生成对应的负载并完成注入。

2.1 物理层故障注入设计

时钟故障和通信故障可以在总线物理层进行故障注入，总线的物理层包括电气信号、数据信号、时钟信号等。通信故障注入可以采用对总线物理层直接注入故障的方式，故障注入器模拟正常设备向总线发送的电信号，并将信号直接发送到通信总线，对总线的数据信号造成干扰。如图 1 所示，故障注入器结构与板卡通信设备相似，向总线注入一定格式的数据，与正常工作的主设备形成“双主”模式干扰总线信号。由于总线采用半双工的形式，总线数据信号将会耦合干扰信号形成错误的数据信号，接收设备会因此接收到错误的波形造成通信故障。

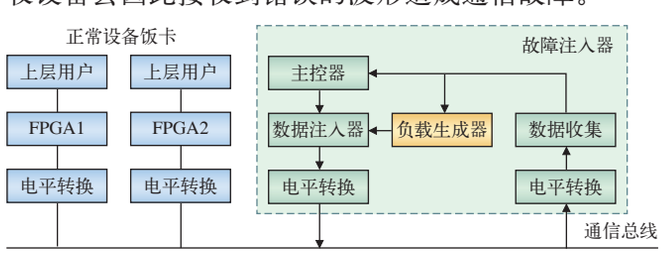

图1 总线物理层故障注入原理

时钟故障可以使用类似的模式，故障注入器向总线的时钟线注入干扰信号，干扰设备的时钟信号。当主从设备之间进行时钟同步时，总线的时钟线被注入故障会导致设备之间时钟无法同步，进而影响时间触发。根据晶振误差和时间片周期可以算出在一定周期后设备之间会失去同步，进而产生通信故障。

对时钟同步的故障注入原理如图 2 所示，故障注入器监听各个设备的时钟，当检测到从设备升级为主设备时，故障注入器同时向时钟线注入时钟信

号，造成通信总线时钟线上存在多个时钟信号，达到对总线时钟同步进行干扰，造成系统故障。

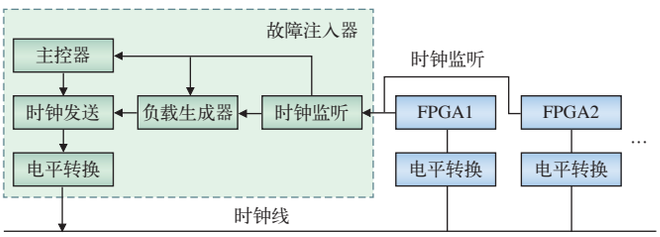

图2　监听时钟注入故障

2.2　链路层故障注入设计

寄存器故障通过对链路层通信协议的破坏达到故障注入的目的。故障注入器劫持设备与总线之间的存放数据帧的寄存器，并对寄存器内部数据进行修改。故障注入截取原理如图 3 所示，用户数据会放在寄存器中等待总线发送 / 接收。故障注入器拦截了用户与总线的通信通道，即截取了寄存器数据，寄存器数据被截取后，故障注入器可以将寄存器中的 1 位、多位或全部数据进行翻转、修改、丢失或置 0/1 修改，这些修改可能会破坏数据帧，使数据的实际校验与原有校验位不同，数据发送端 / 接受端会因为校验错误丢弃该数据帧，达到故障注入的目的。

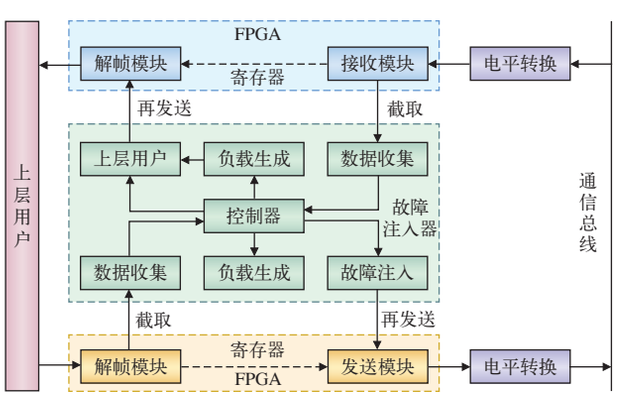

图3　寄存器故障注入原理

3　故障注入实现与验证

对实验室安全计算机测试平台的通信总线进行故障注入测试，该总线参考了高可靠性汽车安全通信总线 FlexRay[4-5]，通过时间触发（TT，Time-Triggered）保障总线设计的安全性。故障注入测试环境如图 4 所示，铁箱内包含电源板、背板及 4 块逻辑板卡，逻辑板卡通过 FPGA 连接到通信总线相互通信，背板将总线电路连接在一起。

故障注入通过修改板卡内部的程序，将一块 FPGA 变成一个故障注入系统，以下简称注入故障的 FPGA 板为 A 板，其余 B、C、D 板卡正常运行。总线数据的观察通过联合测试工作组（JTAG）接口连接到电脑，由电脑上的 SignalTapII 软件逻辑分析仪测量，测量被注入故障设备及总线实际的信号数据。

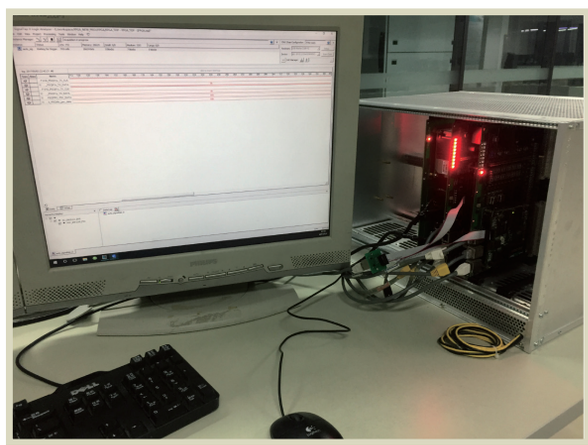

图4　故障注入测试环境

3.1　时钟同步故障注入

根据总线周期，当一个设备升为主设备时，时间片之间会有一段时间间隙进行时钟同步。图 5 表示故障未注入前，C 板接收到总线上从 A 板发出的同步信号，时钟 RX_CLK 会保持一段时间的高电平，用来进行各个设备板之间的时钟同步。

图5　正常情况下的时钟同步

当 A 板发送周期过完后会降级为从设备，同时其他板升为主设备，并在时间片间隙将进行时钟同步。故障注入器控制 A 板在其他板时钟同步信号时向总线发送干扰信息，干扰时钟同步。注入结果如图 6 所示，故障注入开始阶段，总线时间片之间的间隙内不再有时钟同步数据，但数据发送正常，在经过一段时间后（如图 7 显示帧序号 0xa8 即 168），总线停止运行运行，逻辑分析仪显示停止前总线收到最后一次的数据如图 7 所示。

图6　注入故障后的时钟同步

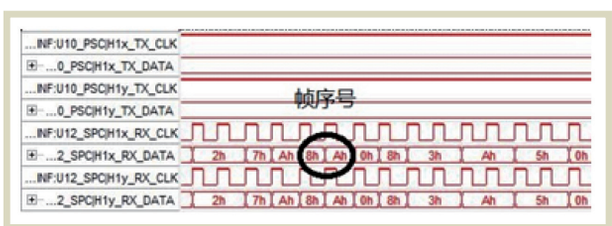

图7　通信停止时逻辑分析仪数据

这是由于设备之间时钟无法同步而出现的错误。设定所有设备之间完成接收和发送的总时间为周期T，主设备发送，某一个从设备接收的时间为t，总线设备总数为n，则存在如下关系：

$$T=n\bullet(n-1)\bullet t \quad (1)$$

每个T内时钟偏差即晶振误差设为α，N为设备可以正常运行的周期，总误差在t时间内才能保证正常通信，即：

$$N\bullet T\bullet\alpha\leqslant t \quad (2)$$

根据时间片周期t为1 ms，实验设备n为4，误差参数α为1‰，由公式（1）和公式（2）可以估算出设备最少运行周期N为83个周期。由图7可知总线在故障后运行了168个周期，大于预期。由此可见设备之间的时钟同步是十分必要的，同时证明了总线设计的合理性，出现故障时能停止运行自动导向安全态。

3.2　通信故障注入

通信故障的测试由故障注入器向总线发送干扰数据。正常的数据发送如图8所示，通过C板观测到的总线数据波形，RX_DATA表示总线接收的到的数据信号，0xA5为空闲数据帧，数据帧从帧头0x02开始，发送目的地址为0x44，源地址为0x11，表示A板作为主设备向总线发送了数据。

当A板过完发送周期，B板会升为主设备后向总线发送数据，故障注入器控制A板同时向总线发送数据，导致总线停止工作。由于逻辑分析仪工作

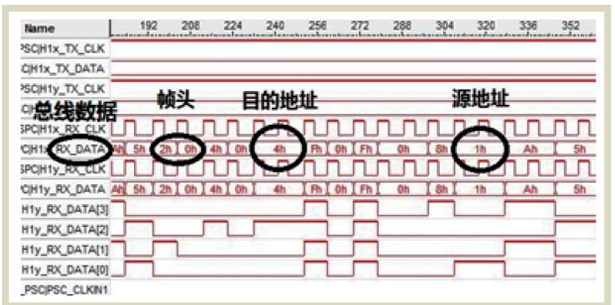

图8　正常运行时总线信号

方式是周期采样，总线停止时显示最后一次总线正常收发的数据，波形与图8相似，只是总线停止运行。

由于总线传输使用半双工的方式，同时写入数据会引起总线故障，出现“双主”的情况，造成总线数据线的干扰，系统停止工作。实验结果说明，故障注入器实现了通信总线的故障注入，在半双工的总线上设备不能同时向总线写入数据。

3.3　寄存器故障注入

测试中故障注入器向A板FPGA中寄存器注入故障，对存放组帧完成后的数据帧寄存器进行故障注入，对组帧完成后的数据进行修改。

图9、图10中FIFO_PSC_DATA表示组帧完成后送入到寄存器中的数据帧，fifo-psc-data表示将要发送数据时从寄存器拿出的数据帧。图9可以看出正常情况下进入寄存器的数据与从寄存器拿到的数据以及向总线发出的数据都是同样的数据帧，图10是对寄存器进行故障注入后的波形图，可以看出进入寄存器的数据还是完整的数据帧，但从寄存器出来的数据被修改为0xfe，修改后的数据被发送进入通信总线，即TX_DATA也变成0xfe。注入故障后，A板无法与其他设备进行通信，总线系统停止工作，逻辑分析仪停留在图10。

寄存器故障注入通过破坏数据帧使数据发送错误信息造成通信总线故障，达到了故障注入的目的。同时也证明了通信总线设计安全性，一旦发送故障，总线会将错误数据丢弃，使设备导向安全状态，证明了安全计算机设计的合理性。

4　结束语

本文研究了安全计算机通信总线软件故障注入

（下转P12）

数据库是可行的，客票系统团队秉承坚持自主创新，理论与实践相结合，先简单后复杂，先外围后核心的研究原则，通过理论研究、技术研究和应用推广3条路线，形成开源数据库研究应用的指导策略和理论依据，并在客票系统典型业务中进行试点应用。通过及时总结、完善应用研究经验，指导客票系统后续在开源技术深入应用研究。

在客票系统中应用开源数据库成熟、稳定后，可将开源数据库自主化、产品化，形成客票数据库产品并在铁路行业内进行市场推广，引领铁路信息系统实现国产化。

参考文献：

[1] 朱建生．新一代客票系统总体技术方案的研究 [J]. 铁路计算机应用，2012，21（6）：1-6.
[2] 大数据时代数据库混合部署方案探究 [DB/OL]. [2014-12-25]. http://blog.csdn.net/dzta831121/article/details/42147909.
[3] 梁春丽．银行信息系统国产化浪潮来袭 [J]. 金融科技时代，2015（2）：15.
[4] 周世超．数据库产品与应用场景趋势 [J]. 数字通信世界，2016（1）：75-76.
[5] 陈姗姗．数据库厂商聚会开源社区 [J]. 开发系统世界，2005（2）：12-14.
[6] 曹江华．开源数据库百花齐放 [J]. 软件和信息服务，2007（14）：45-47.
[7] 阎志远，王智为，张常顺，等．铁路客票 CTMS 架构和关键技术 [J]. 铁路技术创新，2012（4）：26-28.
[8] 崔建岷 .Sybase 复制服务器构造及其在客票系统中应用 [J]. 铁路计算机应用，2000，9（1）：34-36.

责任编辑　陈　蓉

（上接 P4）

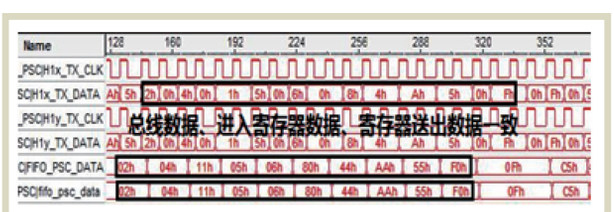

图9　正常情况下寄存器与总线数据

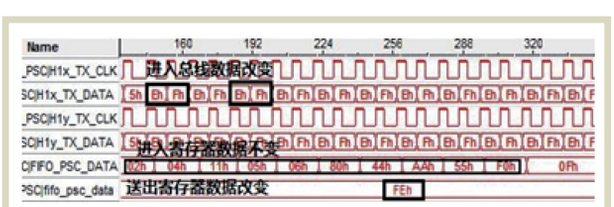

图10　注入故障后寄存器与总线数据

的测试方法，实验成功将故障注入到通信总线中，对通信总线上设备的通信造成了干扰，并且没有对总线造成破坏性故障，在故障撤除后总线又能重新恢复通信，验证了通信总线符合安全计算机安全标准，即发生故障时设备导向安全状态的设计。故障注入的方式可以弥补安全计算机测试手段的不足，进一步证明了安全计算机的通信设计的安全性，出现错误时拥有故障 - 安全的机制。

参考文献：

[1] 郭志良．基于时间自动机模型的 CBTC 系统安全计算机平台的形式化验证 [D]. 北京：北京交通大学，2010.
[2] 刘海旭，马连川，李世光．一种安全计算机板级测试系统的设计与实现 [J]. 现代电子技术，2011, 34（5）：131-134.
[3] 金　丹．安全计算机平台测试序列的生成及应用 [D]. 北京：北京交通大学，2013.
[4] Hsueh M C, Tsai T K, Iyer R K. Fault injection techniques and tools[J]. Computer, 1997, 30（4）：75-82.
[5] 何浩洋．改进的FlexRay总线实现及调度算法优化 [D]. 北京：北京交通大学，2013.
[6] Ding S, Yin X, Xu H, et al. A Hybrid GA-based Scheduling Method for Static Segment in FlexRay Systems[C]. Chinese Control and Decision Conference，2010:1548-1552.
[7] Maier R, Bauer G, Stöger G, et al. Time-triggered architecture: a consistent computing platform[J]. IEEE Micro, 2010, 22(4):36-45.
[8] 徐光侠．分布式实时系统的软件故障注入及可靠性评测方法研究 [D]. 重庆：重庆大学，2011.
[9] Du W, Mathur A P. Vulnerability Testing of Software System Using Fault Injection[J]. Purdue University, 2000.
[10] J. Arlat, Y. Crouzet, and J.C. Laprie, Fault Injection for Dependability Validation of Fault-Tolerant Computer Systems[C]. Proc. 19th Ann. Int’l Symp. Fault-Tolerant Computing, IEEE CS Press, Los Alamitos, Calif., 1989：348-355.

责任编辑　陈　蓉