Design and Analysis of Functional Safety Controller Based on Domestic Chip*

XIAN Guangquan*, LI Xiang
(NR Electric Co., Ltd., Nanjing Jiangsu 211102, China)

Abstract: Targeting at the safety problems of large-scale industrial production caused by the stranglehold of imported chips in the safety instrumented system, a functional safety controller based on domestic chips is designed and developed. The key technical difficulties of using domestic chips to implement functional safety controller are first analyzed. Then, a systematic diagnostic security architecture using CPU+FPGA is proposed, and detailed design is carried out for CPU power, clock, and internal resource diagnosis methods. Thirdly, the safety performance of the controller is evaluated by using failure mode and impact analysis, calculation and verification of safety indicators, etc. Finally, the safety performance of the controller is verified by fault injection test. The results show that the controller design fully complies with functional safety integrity level 3 (SIL3), which can provide reference for the independent and controllable design of other safety equipment in the field of industrial automation.

Key words: domestic chip; safety instrument system; functional safety; reliability; fault failure mode and effects analysis; fault injection test
EEACC: 7210; 7220 **doi**: 10.3969/j.issn.1005-9490.2026.03.007

基于国产芯片的功能安全控制器设计与分析*

咸光全*, 李 响
(南京南瑞继保电气有限公司, 江苏 南京 211102)

摘 要: 针对安全仪表系统被进口芯片“卡脖子”造成的大型工业生产安全问题, 设计研制了一种基于国产芯片的功能安全控制器。首先分析了使用国产芯片实现功能安全控制器的关键技术难点; 然后, 提出了采用 CPU+FPGA 的系统性诊断安全架构, 并对 CPU 电源、时钟以及内部资源诊断方法进行了详细设计; 再次, 通过失效模式与影响分析、安全指标的计算验证等方法对该控制器的安全性能做了评估; 最后, 通过故障注入测试对该控制器的安全性能进行了验证。结果表明, 该控制器设计完全符合功能安全完整性 3 级 (SIL3), 能够为工业自动化领域其他安全设备的自主可控设计提供借鉴。

关键词: 国产芯片; 安全仪表系统; 功能安全; 可靠性; 故障失效模式及影响分析; 故障注入测试
中图分类号: TM273 **文献标识码**: A **文章编号**: 1005-9490(2026)03-0527-07

安全仪表系统 (Safety Instrumented System, SIS) 是工厂自动控制的重要安全保障措施, 可以有效降低发生事故的风险。安全仪表系统能够在生产过程发生危险的时候, 采取紧急措施并准确地执行安全功能, 使生产设备进入设定的安全状态, 从而使损失降低到最低程度, 保证生产设备和人员安全[1]。

由于具有优异的安全性能, 安全仪表系统被广泛应用于核电、石油化工、航空航天、轨道交通等重要工业领域。然而长期以来, 安全仪表系统的技术主要掌握在国外厂商手中, 国内的安全仪表系统市场被国外的厂商所垄断, 国外厂商开展功能安全的研究较早, 主导了多项国际标准, 对核心技术有着深入的研究, 行业现场应用经验比较丰富[2]。近年来, 国内厂家陆续突破技术壁垒, 开发出面向工业自动化的安全仪表系统, 但是其系统元器件使用的依然是进口芯片, 随时存在因为芯片断供等原因导致的“卡脖子”问题, 对国内大型工业系统的安全、稳定运行造成不利影响。

本文根据 IEC 61508 功能安全标准的要求, 采用功能安全标准开发流程[3-4], 研制了基于国产芯片的 PCS-9150S 安全仪表系统功能安全控制器, 并通过安全性能分析和测试证明该控制器满足功能安全 SIL3 级。

项目来源: 南瑞集团科技项目 (JS2201448)
收稿日期: 2023-10-08 **修改日期**: 2024-04-15

1 关键技术难点分析

1.1 国产功能安全芯片选型困难

国外芯片厂商对功能安全标准研究较早,NXP、TI、XILINX 等公司的处理器安全等级可达 SIL3,且可以提供完善的配套诊断芯片和软件诊断库,极大简化了功能安全产品的开发。国产芯片在功能安全方面尚处于起步阶段,取得功能安全认证的产品屈指可数,且最高安全等级仅为 SIL2。而安全仪表系统控制器要求的安全等级为 SIL3,这为产品开发带来了不小的挑战。

1.2 处理器电源、时钟等外部电路诊断

根据 IEC 61508 功能安全标准要求,需要在设备上电过程及运行过程中,对安全相关电路进行诊断,诊断覆盖率需要达到 90%以上,以确保安全仪表系统满足 SIL3 的安全等级。

处理器的各级电源均需要做过压及欠压诊断,当电源发生过压或欠压故障时,系统应自动进入安全状态,过压等故障不能影响诊断电路及冗余控制器的正常工作。在整个温度范围内,电源芯片输出幅值加上电源输出误差和诊断电路的误差总和,不应超过芯片的推荐工作电压。进口功能安全处理器会配套开发 SBC 芯片,可以很方便地实现上述功能,但是目前尚无国产 SBC 芯片可选。

处理器的时钟和任务信号需要有独立时基的带时间窗的看门狗对其进行诊断,无论信号迟到或者提前都要被识别到,这和传统设备的看门狗电路有较大的区别,目前尚无国产元器件能够实现。

1.3 处理器内部资源诊断

IEC 61508 标准要求,需要在规定时间内,对安全功能使用所有资源完成全面诊断,包括处理器内核、Cache、BUS、运算单元、寄存器等,这需要对处理器内部架构、原理及内部指令系统非常熟悉,实现起来尤为困难。进口处理器认证级别高,可以当作“黑盒”直接用在 SIL3 系统中,可以极大地简化硬件电路和软件诊断设计。而国产处理器功能安全认证级别低,诊断库需要定制开发和适配,需要通过系统性设计实现处理器内部资源诊断,增加了系统设计的难度。

综上所述,基于国产芯片的功能安全控制器开发面临着国产功能安全芯片选型困难、处理器相关资源诊断实施复杂以及诊断监控等一系列困难。为此,文章提出了一种基于 CPU+FPGA 的安全架构,实现了基于国产芯片的安全仪表系统控制器设计,满足功能安全 SIL3 等级要求。

2 基于 CPU+FPGA 的功能安全控制器设计

2.1 总体架构

如图 1 所示,采用 CPU+FPGA 的系统级诊断安全架构。选用了一款通过了 SIL2 功能安全认证等级的国产芯片作为安全处理器,该处理器包含两对双核锁步的高可靠 Cortex-R5 内核,能满足高功能安全级别和可靠性的要求,用于实现任务调度、数据同步、表决以及自检等安全相关功能。选用了一款国产 FPGA 芯片作为诊断处理器,实现对 CPU 的电源、时钟、任务等资源的诊断[5]。

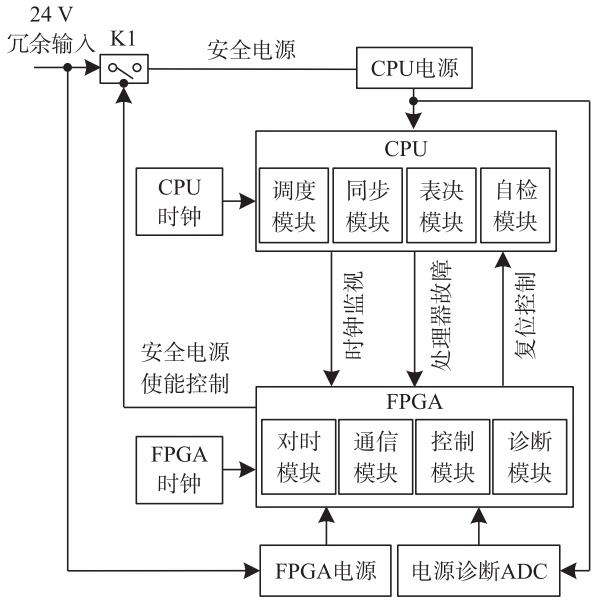

图 1 控制器架构框图

CPU 和 FPGA 各司其职,互不影响。当 FPGA 发现 CPU 相关安全电路异常时,通过控制安全电源使能控制信号和复位控制信号,来切断安全电源或者将 CPU 复位,从而使控制器进入安全状态。二者的相关电源和时钟均为独立提供,避免了共因失效,保证了控制器的安全性和可靠性。

2.2 电源诊断设计

如图 2 所示,S0V8、S1V8、S1V1 等 CPU 电源,经过调理电路处理后,送给电源诊断 ADC,FPGA 通过读取 ADC 采样值实现对 CPU 电源的过压和欠压诊断。由于 FPGA 的电源和 CPU 电源分别从冗余 24 V 输入通过独立的电源芯片转换而来,所以二者可以独立工作。当 CPU 电源发生欠压故障时,FPGA 将复位控制信号拉低,使 CPU 保持复位状态;当 CPU 电源发生过压故障时,FPGA 将复位控制信号拉低的同时,通过安全电源使能控制信号关闭 K1 开关,避免过压故障扩散。从调理电路、ADC 芯片到数据总线,都是冗余的,任意一路监视到异常时,FPGA 均将

CPU 复位,此设计诊断覆盖率可达 99%[6]。

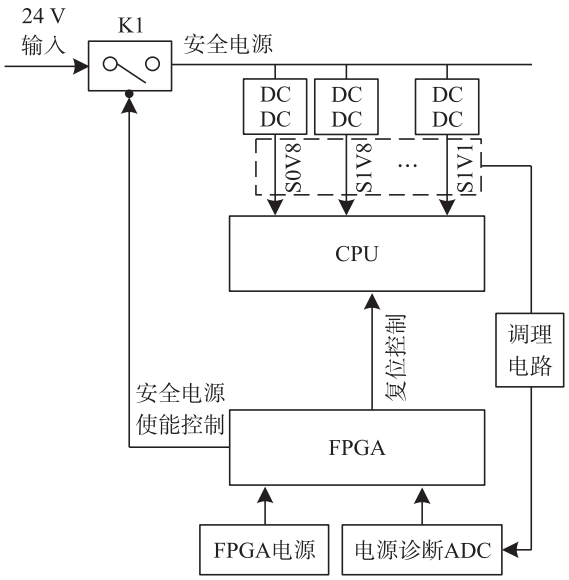

图 2　控制器电源诊断设计框图

2.3　时钟诊断设计

如图 3 所示,CPU 外部 24 MHz 的时钟信号经过 CPU 内部锁相环倍频后,通过定时器分频输出时钟监视信号,提供给 FPGA 做时钟诊断。FPGA 内部冗余的带时间窗口的看门狗模块对时钟监视信号的频率进行实时监控,当发现其偏差超过阈值时,FPGA 将复位控制信号拉低,使 CPU 保持复位状态,控制器进入安全状态。

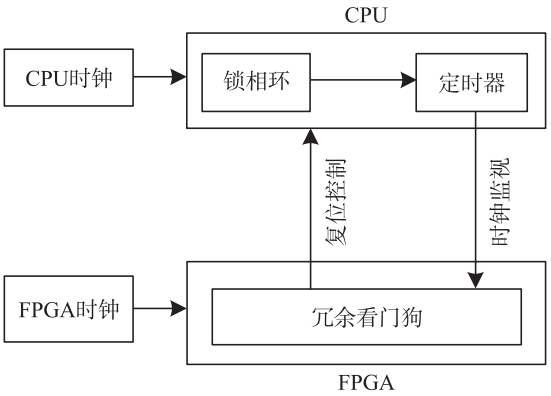

图 3　CPU 时钟诊断框图

2.4　CPU 内部资源诊断设计

如图 4 所示,通过诊断软件实现对内核、Cache、BUS 以及 DDR 等资源的监视,当任意一个功能被诊断出异常时,CPU 发给 FPGA 的处理器故障信号异常,FPGA 判定 CPU 故障,进而将复位控制信号拉低,使 CPU 保持复位状态,控制器进入安全状态。

表 1 为 CPU 内部主要资源的诊断方法,对照 IEC 61508 标准的第二部分附录 A,列出了各诊断方法可以达到的诊断覆盖率。

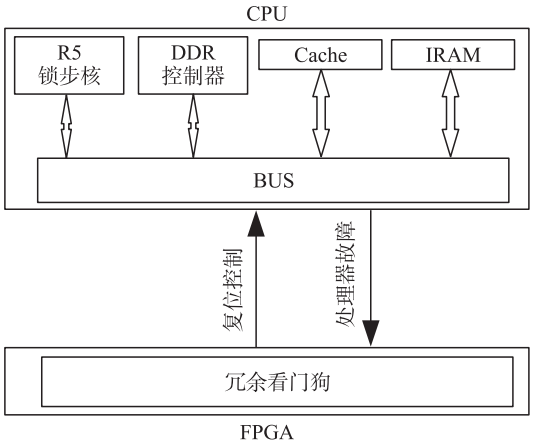

图 4　CPU 内部资源诊断框图

表 1　CPU 内部主要资源诊断方法及覆盖率

CPU 内部资源	诊断方法	诊断覆盖率/%
内核	双核锁步	99
Cache	Cache ECC	90
BUS	BUS ECC	90
DDR	DDR ECC	90
寄存器	回读	90

3　安全性能分析

3.1　功能安全等级评估参数及指标

在 IEC 61508 功能安全标准中,使用功能安全完整性等级 SIL 来衡量系统的安全性能[7]。

SIL 等级评估的一个重要参数是 PFD_{avg},即系统被要求时的平均危险失效概率,表 2 为不同 SIL 等级要求的 PFD_{avg} 对照表,文中所述 SIS 控制器要求 SIL3 等级,对应的 PFD_{avg} 要求为 10^{-4} 到 10^{-3}。

表 2　SIL 与 PFD_{avg} 对照表

SIL 等级	PFD_{avg}	SIL 等级	PFD_{avg}
4	$10^{-5}\sim10^{-4}$	2	$10^{-3}\sim10^{-2}$
3	$10^{-4}\sim10^{-3}$	1	$10^{-2}\sim10^{-1}$

SIL 等级评估的另外一个参数是安全失效分数 SFF,及硬件故障裕度,这两个指标可以统称为硬件结构约束,SIL 等级与硬件结构约束关系如表 3 所示。

表 3　功能安全硬件结构约束

安全失效分数 SFF	硬件故障裕度		
	0	1	2
≦ 60%	SIL1	SIL2	SIL3
60%~<90%	SIL2	SIL3	SIL4
90%~<99%	SIL3	SIL4	SIL4
≧ 99%	SIL3	SIL4	SIL4

文中所述 SIS 控制器卡件,采用三重化冗余 2oo3 架构,即硬件故障裕度为 1,查表可知 SIL3 等级要求对应安全失效分数为 60%~<90%;文中所述 SIS 控制器底座,采用不冗余的 1oo1 架构,即硬件故障裕度为 0,查表可知 SIL3 等级要求对应安全失效分数为 90%~<99%。

3.2 功能安全评估模型

根据硬件失效对系统的影响,如图 5 所示,将控制器可靠性框图划分为三个部分:控制器底座、控制器卡件以及共因失效。其中,控制器底座不冗余,即工作在 1oo1 模式;控制器卡件三重化冗余,工作在 2oo3 模式;三重化冗余卡件可能由于某种共同原因同时失效即共因失效,计算失效率的时候需要考虑共因失效因子的影响。

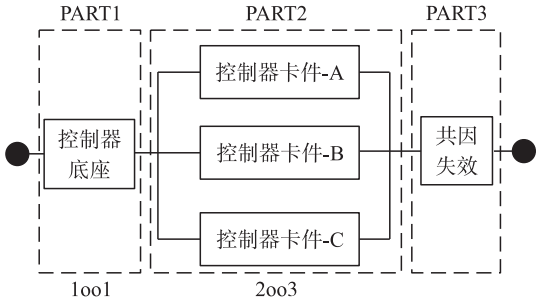

图 5 控制器可靠性框图

3.3 失效模式影响分析

失效模式影响分析(Failure Mode and Effects Analysis,FMEA)是以表格的形式对设备中所有元器件逐一进行详细的失效和影响分析,通过 FMEA 分析可以得到设备的失效率数据,通过各种失效模式下的失效率数据,可以进一步计算出设备的安全失效分数 SFF 和平均失效概率 PFD_{avg},最终评估出设备的安全完整性等级[8-9]。

文章对 SIS 控制器底座及控制器卡件进行了 FMEA 分析,分析当中元器件的失效率来源于国军标 GJB/Z299C-2006《电子设备可靠性预计手册》[10]。由于 FMEA 分析过程非常复杂,篇幅限制,以电源芯片为例,对 FMEA 分析过程做了示例。如表 4 所示,电源芯片的失效模式分为开路、短路和参数变化,这三种失效模式对于控制器来说均为危险失效,即失效会导致安全功能丧失;通过《电子设备可靠性预计手册》可以查找到电源芯片各种模式下的失效率 λ,最终根据采取的诊断措施覆盖率做进一步的失效率细分计算[11-12]。

表中 λ 表示元器件总失效率,λ_S 和 λ_D 分别表示元器件的安全失效概率和危险失效概率,其中 λ_D 又细分为 λ_{DD}、λ_{DU},分别表示能够检测到的危险失效概率以及不能检测到的危险失效概率。

表 4 元器件 FMEA 分析示例

元器件	失效模式	λ/fit	失效影响	λ_S/fit	λ_{DD}/fit	λ_{DU}/fit
电源芯片	开路	10	危险	0	9.9	0.1
	短路	10	危险	0	9.9	0.1
	参数变化	10	危险	0	9.9	0.1

将控制器所有元器件按上述方法进行分析汇总,控制器最终 FMEA 分析结果[13]如表 5 所示。

表 5 控制器 FMEA 分析结果汇总

模块	失效率(fit:10^{-9}/h)			
	λ_S	λ_{DD}	λ_{DU}	λ_D
控制器底座	0.56	0.54	0.04	0.58
控制器卡件	2896	1162	27	1189

3.4 安全失效分数及平均失效概率计算

3.4.1 安全失效分数计算

安全失效分数 SFF 体现的是系统自诊断的能力,SFF 越高,表示系统自诊断能力越强[14]。

SFF 计算公式如下:

$$SFF=\frac{\sum\lambda_S+\sum\lambda_{DD}}{\sum\lambda_S+\sum\lambda_{DD}+\sum\lambda_{DU}} \tag{1}$$

代入表 5 中失效率数据,可得控制器底座的 SFF 为 96.53%,控制器卡件的诊断覆盖率为 99.35%,满足 SIL3 要求。

3.4.2 控制器底座 PFD_{avg} 计算

PFD_{avg} 体现的是需要时的平均失效概率[15],对于工作在 1oo1 模式的控制器底座,其在要求时失效概率 PFD_{avg} 的计算公式为:

$$PFD_{avg}=\lambda_D\times\left(\frac{\lambda_{DU}}{\lambda_D}\times\frac{PTI}{2}+MTTR\right) \tag{2}$$

式中:MTTR 为故障平均维修时间,计算中按 8 h 经验值考虑;PTI 为控制器测试周期,即现场设备定期检修时间,计算中按 43 800 h(5 年)经验值考虑。

代入表 5 中失效率数据,可得控制器底座的 PFD_{avg} 为 8.8×10^{-7}(fit)。

3.4.3 控制器卡件 PFD_{avg} 计算

对于工作在 2oo3 模式的控制器卡件,其在要求时失效概率 PFD_{avg} 的计算公式为:

$$PFD_{avg}=[6\times(1-\beta)\times\lambda_D]^2\times\left(\frac{\lambda_{DU}}{\lambda_D}\times\frac{PTI}{2}+MTTR\right)\times\left(\frac{\lambda_{DU}}{\lambda_D}\times\frac{PTI}{3}+MTTR\right)+\beta\times\lambda_D\times MTTR+\beta\times\lambda_{DU}\times\frac{PTI}{2} \tag{3}$$

式中:β 为共因失效概率,根据 IEC 61508 标准第六部分附录 D 中 E/E/PE 系统中与硬件相关的共因失效影响的量化方法,评估值为 1.5%,具体评估过程限于篇幅,不再展开。MTTR 为故障平均维修时间,计算中按 8 h 经验值考虑;PTI 为控制器测试周期,即现场设备定期检修时间,计算中按 43 800 h(5 年)经验值考虑。

代入表 5 中失效率数据,可得控制器卡件的 PFD_{avg} 为 7.3×10^{-6}(fit)。

3.5　分析结果

将上述分析计算所得结果汇总,如表 6 所示,通过对比分析可知,SIS 控制器的安全性能满足 IEC 61508 标准要求的 SIL3 等级要求。

表 6　控制器安全性能分析结果

	标准要求值		实际计算值	
	SFF	PFD_{avg}	SFF	PFD_{avg}
控制器底座	>90%	$10^{-5}\sim10^{-4}$	96.53%	8.8×10^{-7}
控制器卡件	>90%	$10^{-5}\sim10^{-4}$	99.35%	7.3×10^{-6}

4　安全性能验证测试

4.1　故障注入测试平台

为了进一步验证和测试安全仪表系统控制器安全机制的正确性和完整性,根据 IEC 61508 标准要求,对 PCS-9150S 控制器进行了故障注入测试[16](FIT)。

如图 6 所示,测试平台由上位机软件、控制器以及外部设备三部分组成。控制器和上位机软件通过网线和串口线连接,通过诊断软件可以查看控制器的故障注入测试结果,通过串口工具可以对控制器的 CPU 内部资源注入软件故障,通过外部设备对控制器注入电源、时钟等硬件故障。

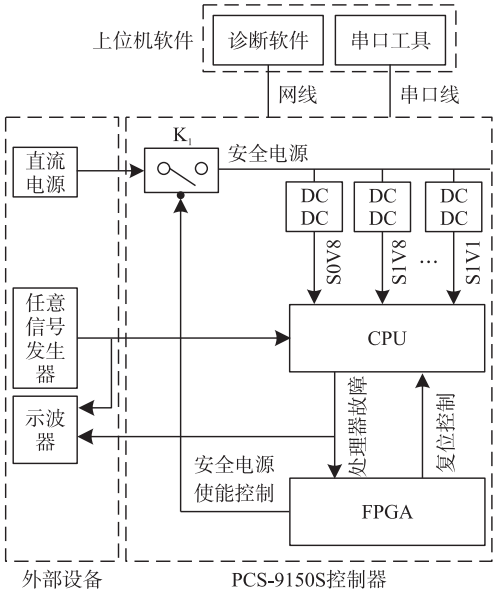

图 6　故障注入测试平台

4.2　故障注入测试结果

根据控制器设计的诊断措施,对 CPU 电源过压、电源欠压、时钟及内部资源进行了故障注入测试。测试结果表明控制器设计阶段所采取的诊断措施可以有效地识别各种故障并执行安全功能[17-18]。

①CPU 电源过压故障注入测试

以 S1V8 为例,其过压监控门槛值为 1.92 V,调节电源 S1V8 的反馈电阻使电源电压输出至 1.92 V,2 ms 后 FPGA 将安全电电源使能控制信号由 1 变 0,关闭电源回路开关 K_1,S1V8 在约 5 ms 后逐渐降为 0 V。过压故障注入测试波形如图 7 所示。

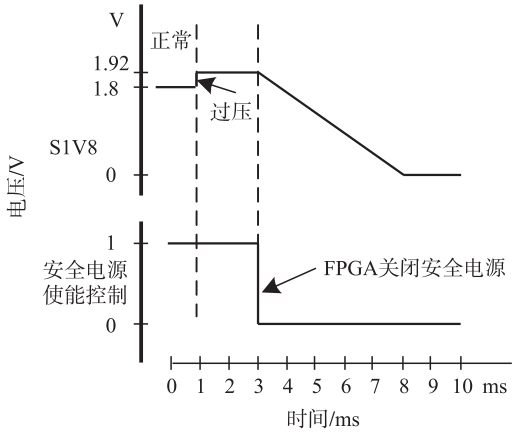

图 7　过压故障注入测试波形

②CPU 电源欠压故障注入测试

依然以 S1V8 为例,其欠压监控门槛值为 1.73 V,控制器运行后,调节电源 S1V8 的反馈电阻使电源电压输出至 1.73 V,2 ms 后 FPGA 输出的复位控制信号由 1 变 0,CPU 复位,控制器进入安全状态。欠压故障注入测试波形如图 8 所示。

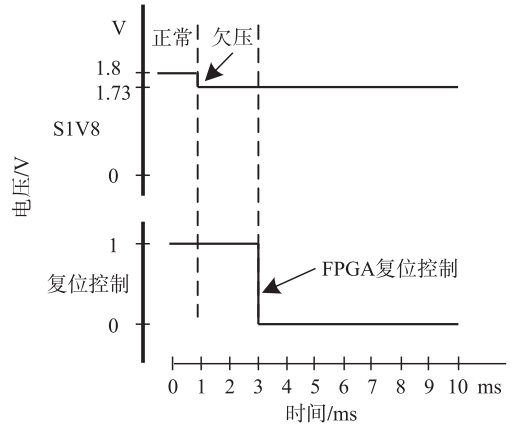

图 8　欠压故障注入测试波形

③CPU 时钟故障注入测试

如图 9 所示,断开处理器外部的晶振,接入任意信号发生器为 CPU 提供时钟信号,设置信号发生器输出频率为 24 MHz,控制器上电后运行正常;缓慢调节信号输出频率变化至偏差阈值,约 200 ns 后 FPGA 输出的复位控制信号由 1 变 0,CPU 复位,控制器进入安全状态。

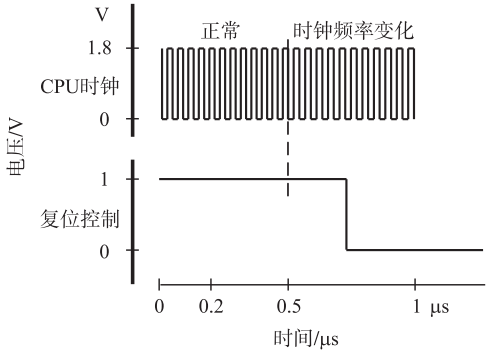

图 9 CPU 时钟故障注入测试波形

④CPU 内部资源故障注入测试

如图 10 所示,CPU 正常的时候,处理器故障信号输出低频方波信号;通过上位机软件向 CPU 内部 Dcache 选定位置注入 1 bit 错误[19],处理器故障信号输出高频方波信号,由于 Dcache 具备 ECC 功能,可纠正 1 bit 错误,所以此时控制器继续正常运行;向 Dcache 选定位置注入 2 bit 错误,处理器故障信号变为常低电平,约 10 μs 后,FPGA 输出的复位控制信号由 1 变 0,CPU 复位,控制器进入安全状态。

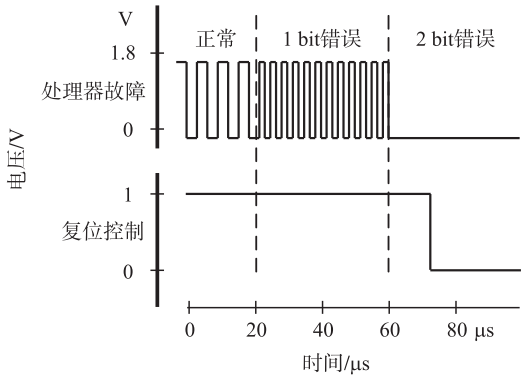

图 10 CPU 内部资源故障注入测试波形

5 结论

文章深入分析了使用国产芯片实现功能安全控制器的关键技术难点,提出了相应的设计方案并研制了 PCS-9150S 完全自主可控的功能安全控制器,通过失效模式影响分析、故障注入测试等相关验证,保证了控制器的安全性能[20]。

研究结果表明:使用国产芯片设计的功能安全控制器满足 SIL3 对应的指标要求,该控制器已经取得了 TUV 的 SIL3 功能安全认证。文中提出的 CPU +FPGA 系统级诊断安全架构,弥补了国产芯片功能安全等级低、选型难以及自诊断能力弱等短板;采取的电源诊断措施可以覆盖过压等故障类型,并在故障发生时快速切断安全回路总电源,有效避免故障扩散;CPU 相关其他资源的故障也可以通过 FPGA 快速诊断,能够为工业自动化领域的其他设备自主可控设计提供借鉴。

参考文献:

[1] 郑锐,刘美佳,平洋,等. 安全仪表系统 SIL 定级及 LOPA 的应用研究[J]. 化工自动化及仪表,2020,47(5):447-449.

[2] 咸光全,李响. 功能安全在继电保护装置中的应用[J]. 电气技术,2019,20(12):69-73.

[3] 郭建昇,徐伯庆. 智能型功能安全继电器的设计与实现[J]. 仪表技术与传感器,2017(1):46-49.

[4] 裘坤,刘志勇,江竹轩,等. 功能安全控制系统研发实践[J]. 工业控制计算机,2016,29(7):27-29.

[5] 刘济源,宋长骏,汤勇明. 基于国产 FPGA 的智能监测报警系统设计[J]. 电子器件,2023,46(3):585-591.

[6] 王海龙,左付山,杨柳,等. 基于 CAN 总线电池性能监测系统设计[J]. 仪表技术与传感器,2021(6):77-81.

[7] 丁龙,王宏. 安全仪表系统通信功能的可靠性评估[J]. 仪表技术与传感器,2016(5):84-88.

[8] 袁晓慧,尹震宇,黄祖广,等. 基于故障树分析的数控装置硬件平台功能安全设计与实现[J]. 组合机床与自动化加工技术,2015(8):70-73,78.

[9] 檀旋,黄波,卫玮,等. 电子液压制动系统 HARA 分析及其逆变器电路 FMEDA 分析[J]. 制造业自动化,2020,42(10):116-119.

[10] 白丹. 基于 FMEA 的安全仪表系统安全完整性研究[J]. 机电产品开发与创新,2016,29(5):32-35.

[11] 马永超,赵伟,黄松岭. 提高智能电能表可靠性技术研究综述[J]. 电测与仪表,2022,59(4):1-7.

[12] 董贤光,代燕杰,王婷婷,等. 基于现场删失数据的电能表可靠性评估方法及轮换策略研究[J]. 电测与仪表,2021,58(12):175-183.

[13] 冯晓栋,王先培,田猛,等. 基于故障树的智能电能表可靠性分析[J]. 电测与仪表,2019,56(8):148-152.

[14] 陈小全,周 婷. 双 MCU 功能安全型智能安全继电器设计[J]. 自动化仪表,2020,41(1):56-60.

[15] 巨汉基,郑蒙蒙,田海亭,等. 基于故障注入的电能表存储信息突变问题分析方法研究[J]. 电测与仪表,2016,53(z1):67-69,78.

[16] 戴玲玲,江竹轩,郑志方. 硬件故障注入测试在安全产品开发中的应用[J]. 工业控制计算机,2013,26(12):47-48.

[17] 李光明,曾永航. 基于 LVDS 总线的故障注入系统设计[J]. 电子器件,2023,46(2):337-341.
[18] 郭健忠,张举,闵锐,等. 基于功能安全的汽车全液晶仪表电源供电系统设计[J]. 电子器件,2021,44(6):1339-1345.
[19] 马书丽,孙武. 基于 FPGA 技术的核安全级系统功能安全认证应用研究[J]. 自动化仪表,2020,41(10):106-110.
[20] 秦剑华,刘洋,杨景刚,等. 电力电缆局放及温度的多维度检测方法研究[J]. 电测与仪表,2023,60(3):92-96.

咸光全(1986—),男,高级工程师,硕士,从事工业控制以及电力系统保护控制平台开发,xiangq@ nrec.com。