doi:10.11959/j.issn.1000-436x.2016237

安全计算机通信管理机制的形式化验证与实现

梁靓[1]，曹源[2]，马连川[2]，张玉琢[2]，李恒奎[3]

（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运行控制系统国家工程研究中心，北京 100044；
3. 中车青岛四方机车车辆股份有限公司，山东 青岛 266111）

摘 要：为提高下一代列车运行控制（简称列控）系统安全计算机的系统兼容性，首先对其结构进行简要分析，并对管理机制进行设计，建立了管理单元状态转移模型，同时以形式化验证工具对模型的正确性进行了验证。在此基础上对基于微控制单元(MCU, micro controller unit)的管理单元进行了软硬件的设计实现与测试。验证和测试结果表明，所设计的管理机制符合设计规范的要求，管理单元能够实现预期的状态转移功能。

关键词：列控系统；安全计算机；通信管理机制；形式化验证
中图分类号：U285.41 **文献标识码**：A

Formal verification and implementation of safety computer communication management mechanism

LIANG Liang[1], CAO Yuan[2], MA Lian-chuan[2], ZHANG Yu-zhuo[2], LI Heng-kui[3]

(1. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
2. National Engineering Research Center of Rail Traffic Control System, Beijing Jiaotong University, Beijing 100044, China;
3. CRCC Qingdao Sifang Co., Ltd., Qingdao 266111, China)

Abstract: In order to improve the system compatibility of the safety computer of the next generation train operation control system, first of all, the structure was analyzed and the management mechanism was designed, the state transition model of management unit was established, and the correctness of the model was verified by formal verification tools at the same time. Then the software and hardware which based on micro controller unit (MCU) were designed and implemented. The verification and test results show that the management mechanism design meets the design requirements, the management unit can achieve the expected state transfer function.

Key words: train control system, safety computer, communication management mechanism, formal verification

1 引言

在出行需求日益增长的今天，基于传统设计思想的叠加式列控系统逐渐显露出不足，各种功能子系统的叠加导致结构复杂化、可靠性降低，系统的高度集中引发能耗、散热、占用空间过大等问题，并且在受到外力冲击时极易造成设备整体瘫痪，这些问题在车载设备方面表现得尤为突出。因此，在下一代列控系统的设计中，希望建立统一的安全计算机平台，对系统整体结构进行优化，以硬件、软件模块化来降低设备的复杂程度，实现灵活配置，同时缩短开发周期，减少重复开发[1,2]。由于系统整体结构的调整，系统状态也随着单系内各单元间及两系间的复杂交互过程而增加，建模难度也随之增加。对于关键领域中应用的安全苛求系统，需要达到安全完整性等级 SIL-4 级标准，确保其在实际应用中能够稳定可靠地运行。

收稿日期：2016-05-19；**修回日期**：2016-10-10
通信作者：曹源，ycao@bjtu.edu.cn
基金项目：国家自然科学基金资助项目（No.U1534208）
Foundation Item: The National Natural Science Foundation of China (No.U1534208)

在列车安全高效运行的过程中，安全计算机因其在系统中的重要安全职能而成为深入研究的对象[3~5]。以往设计中采用可编程逻辑阵列（FPGA）进行的相同结构的冗余设计会引起共因失效，以及丰富软硬件添加导致系统中隐藏细微错误成为系统的潜在安全隐患[6]。郑升等[1]从硬件和软件这 2 个方面对现有安全计算机平台进行了简化，并通过实验进行验证；郭志良等[7]利用时间自动机理论建立了现有安全计算机平台的自动机网络模型，并对系统特性进行了验证。但是这些研究都没有对下一代列控安全计算机进行形式化建模验证。传统的测试、模拟等验证方式，不能完全覆盖系统的所有执行路径，难以检测系统中存在的并发错误，而形式化验证方法能够很大程度上降低主观设计缺陷，减少不必要的时间消耗和降低成本。模型检测作为形式化方法之一，通常基于穷尽式搜索的方式运行，可以保证 100%的覆盖率对系统进行验证。而且检测过程完全自动化，成功地实现了快速、高效的系统模型需求验证。

针对以往的 FPGA 同构冗余设计而产生的共因失效问题，本文通过 FPGA 与 MCU 对安全计算机进行差异性结构设计，在物理、功能、及流程这 3 个方面，保证各通道、模块之间或系统功能之间存在充分独立性，并对其中基于 MCU 的管理单元进行管理机制及硬件的设计实现，采用形式化方法对管理机制进行验证。在此基础上对管理单元进行软硬件实现，进行了测试和分析。

2　安全计算机通信管理机制设计

2.1　下一代列控安全计算机简介

安全计算机平台的结构主要包含通用计算域（GCD, general computational domain）、安全管理域（SCMD, safety computer management domain）以及安全输入输出域（SIOD, safety input and output domain）3 部分，单系计算机所包含的 3 个功能域分别由 2 个异构单元组成，逻辑上构成二取二关系，两系计算机之间构成二乘关系，并采用以太网的方式进行数据的传送。安全计算机平台的功能结构如图 1 所示。因两系的结构完全相同，本文以单系为主进行详细说明。

SCMD 主要实现对系统内部各个模块控制功能。首先，SCMD 向 SIOD 发送命令，由其内部输入输出单元（SIOU）完成数据获取。而后，2 个 SIOU 将数据分别传送至异构的安全管理单元（SCMU）中进行检验，2 个 SCMU 通过通信的方式对数据进行表决，在表决一致的前提下，SCMD 需通过 GCD 完成逻辑运算协处理功能以及特定的校验逻辑运

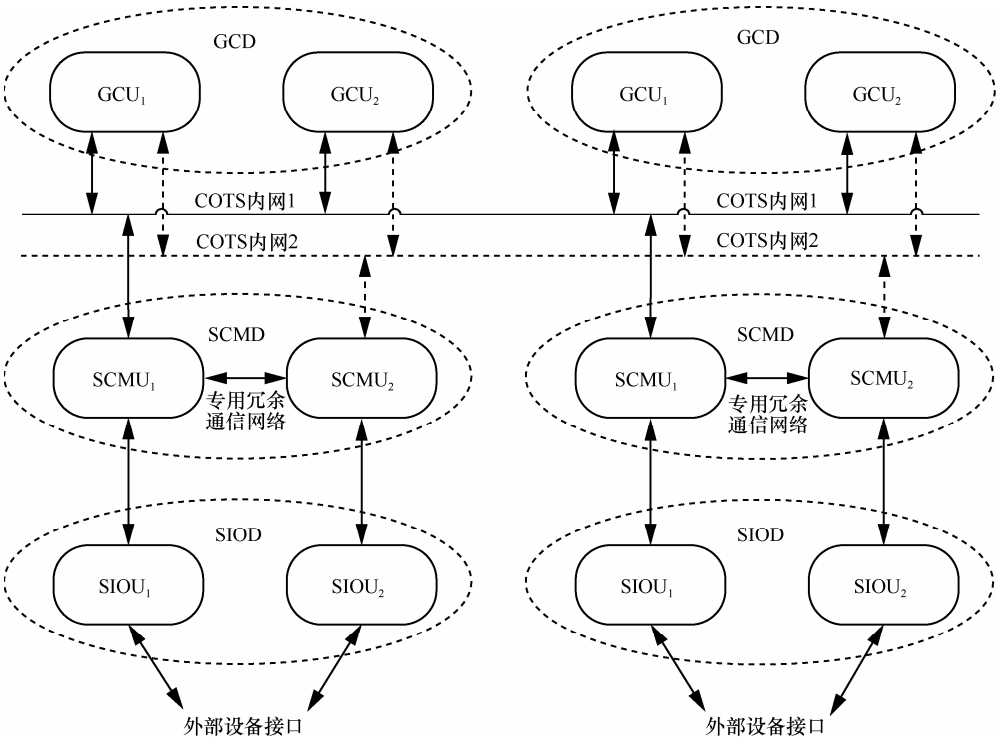

图 1　网络拓扑结构

算。首先由 SCMD 根据事先制定的安全通信协议，通过（SIOU）向 2 个通用计算单元（GCU）分别发送安全数据帧，其中包含逻辑运算的相关指令及表决一致的输入数据。2 个 GCU 为判断其是否合法，应首先对其进行安全解密或解码。若此数据帧非法，GCD 将根据安全通信协议，向 SCMD 返回带有“安全反应处理请求”的数据帧；若此数据帧合法，GCD 中的 2 个异构 GCU 将分别根据接收到的命令及数据进行逻辑运算。后由 2 个异构的 GCU 进行运算结果的交互比较，当比较结果一致时，证明所进行的逻辑运算正确，2 个 GCU 需按照安全通信协议，将各自运算结果组成安全数据帧分别返回到 SCMD 的 2 个管理单元中。同时，双系 SCMD 间进行相关通信，实现主、备系间的状态切换。

2.2 基于通信的任务级同步策略

单系中的 2 个管理单元分别采用 MCU 和 FPGA 进行软硬件差异性设计，采用基于周期的任务级同步方式。由于 FPGA 具有设计灵活、器件性能稳定、处理速度较快且没有延时的特点，采用 FPGA 向 MCU 发送同步命令，并由 MCU 进行响应的方式进行同步。

首先对管理单元进行工作周期的设置，将系统所要处理的任务通过微周期进行划分并循环操作。同步成功后，2 个 SCMU 分别开启各自内部的定时功能，在预先设定的工作周期或微周期内完成下一设定任务的处理工作。

2.3 数据比较功能

数据比较主要是对单系中 2 个 GCU 以及 2 个 SCMU 的逻辑运算结果进行相互比较。只有当 2 个 SCMU 的运算结果一致时，才认为单系内部无故障，结果安全可信。MCU 和 FPGA 这 2 个管理单元执行相同任务，因此，采用基于周期的任务级软件比较法对数据进行比较。此方法既能保证安全性又易于实现，同时软件也具有很好的适应性。

3 安全计算机通信管理机制的形式化验证

3.1 Kripke 模型及 CTL 操作符

在模型检验中，采用 Kripke 结构的迁移系统模型进行形式化描述，并通过计算树逻辑（CTL, computation tree logic）进行性质验证。

定义 1 Kripke 结构为五元组结构 $TS=(S, S_0, R, AP, L)$，其中，

1) S 是一个有限状态集合；

2) $S_0 \in S$ 是初始状态；

3) $R \subseteq S \times S$ 是转移关系，必须是完全的，即 $\forall s \in S,\ \exists s' \in S \Rightarrow (s, s') \in R$;

4) AP 是一组原子命题和它们否命题的集合；

5) $L: S \to 2^P$ 是标记函数，它把状态 $s \in S$ 映射在 s 状态下真值为真的原子命题集合，该集合是 P 的一个子集。

这些描述系统行为的状态序列又称为计算路径，通过状态序列能够实现对系统行为的完全刻画，并通过 CTL 在复杂的运行状态下对分支行结构进行推论，确定系统是否会进入死锁状态或者能够一直保持良好的性质，从而对系统的性能做出判断[8,9]。

状态机中的项根据一系列的输入事件的发生进行状态之间的变迁，这种输入事件本文称为激励。其操作语义规则定义如下：$S \xrightarrow[\alpha]{e}{}_f S'$，$e$ 为激励，α 为输出事件，标记 f=1 表示当处于 s 状态时，激励 e 发生，至少发生一次以上变迁，f=0 则表示不发生变迁。

3.2 管理单元状态模型

根据所描述的管理机制，可得单系 MCU 管理单元状态转移模型，包括 HOST 状态开始的主工作模式及 STANDBY 状态开始的备工作模式在内，所建立的有限状态机模型共包含 37 个状态节点以及 50 个激励（当系统在某一状态时，促使其向下一状态转移的条件即激励），如图 2 所示，对系统运行的所有状态迁移过程进行了描述。当系统上电自检的次数超过 3 次时，会自动进入断电模式，在图中用虚线表示。

在正常完成系统上电、自检及初始同步过程后，双系会通过 SCMU 进行主、备运行状态判定，此时，先收到数据并完成校验的一系会向另一系发送做主信息请求，并开启定时，当收到另一系反馈信号时间隔为 t，此时，主、备模式判定完成，主模式系向备模式系发送同步命令，并在 $\frac{t}{2}$ 后开始自身主模式运行，以此实现两系间的同步，分别以主、备模式运行。当运行至某一状态时，且仅当对应激励事件发生才能实现向下一节点的跳转。若系统发生故障，会自动跳转到故障状态（图 2 中以加粗进行标注）。

3.3 管理单元主备、运行模式

在安全计算机实际运行过程中，双系的 SCMU 分别以主、备模式（分别为图 2 中的 HOST、STANDBY）运行，通过自身状态的转移对单系中的 GCU 及 SIOU 进行控制，使整个系统完成数据的输入、运算及输出任务，实现其管理机制。

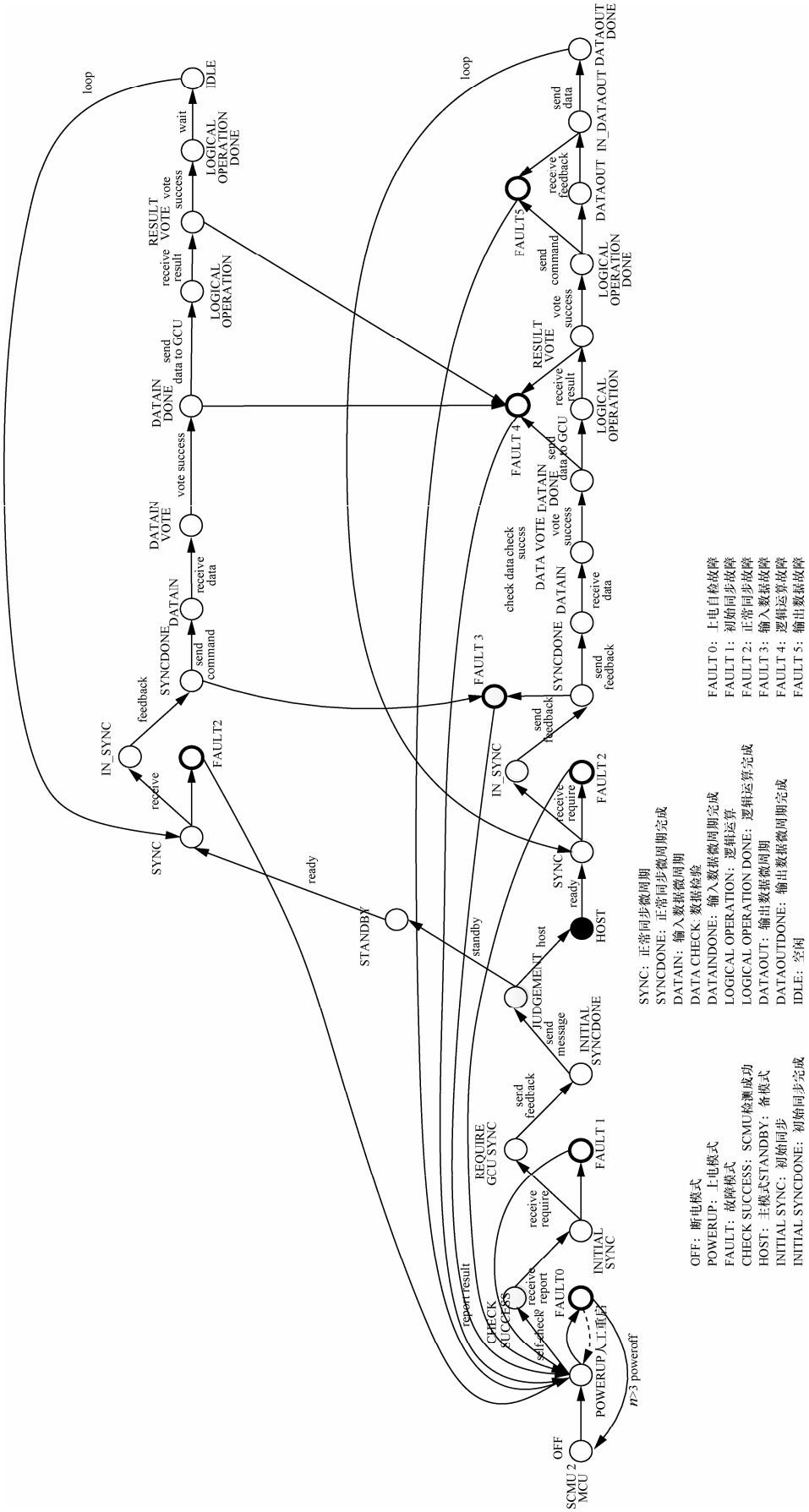

图 2　SCMU 状态机模型

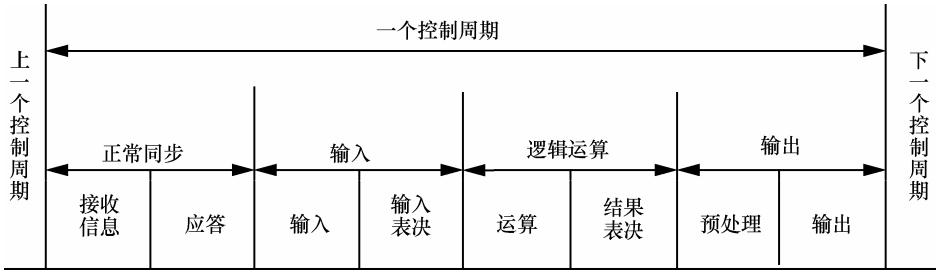

图 3　主模式控制周期划分

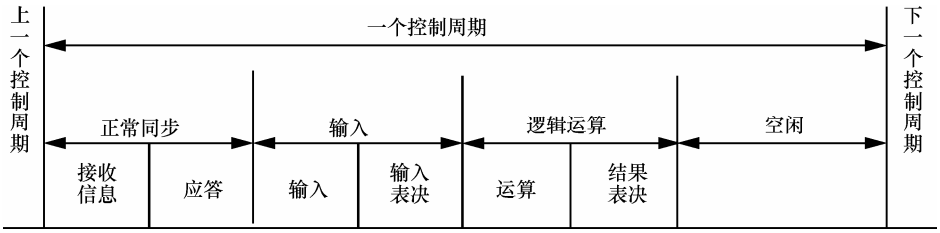

图 4　备模式控制周期划分

无论 SCMU 进入主模式工作状态还是备模式工作状态，其都会按照预先设定的周期或微周期运行。主模式的控制周期具体划分如图 3 所示。

备模式不向外输出数据，为了能够与主模式系同时进入下一控制周期，需以空闲时段进行备模式控制周期的填补。其具体划分如图 4 所示。

2 种模式下都对运行过程进行了设定，并且在每个微周期的规定时间内系统只能执行规定的任务，若超出规定的时限或是运行过程中发生错误，两系将通过 SCMU 进行通信，自动完成主、备切换或重启，以保障输出数据的安全可靠。

3.4　性质验证及结果分析

NuSMV（new symbolic model verifier）是一款基于二元决策图的经典符号模型检测工具，可有效地控制状态爆炸，从而实现高效的检验过程[10]。本文采用 NuSMV 的形式化建模工具，主要采用数学分析的方式，通过 CTL 公式对模型性质进行详细描述，以验证模型是否符合设计规范。

1) 活性的 CTL 验证如式(1)所示。

$$\mathrm{AG}(\mathrm{EF}(\mathrm{state}=s_1)) \tag{1}$$

表达含义为：系统可以从任一状态实现到 s_1 的转移。此处以 HOST 状态为例，对其进行活性的验证，验证结果如图 5 所示。

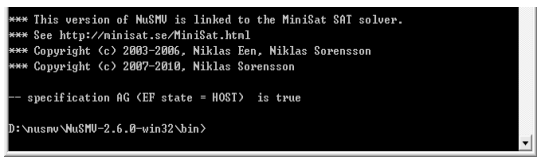

图 5　活性验证结果

结果表明，所建立的系统模型满足系统活性验证的规范。

2) 可达性的 CTL 验证如式(2)所示。

$$\mathrm{EF}(\mathrm{state}=s_1|\mathrm{state}=s_2) \tag{2}$$

表达含义为：系统可以从其他状态到达 s_1 状态或 s_2 状态。此处以 HOST 状态和 STANDBY 状态为例，对其进行可达性的验证，验证结果如图 6 所示。

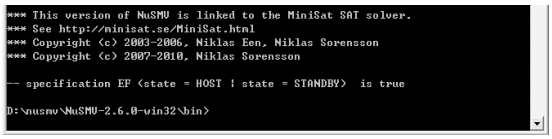

图 6　可达性验证

结果表明，系统能够实现由其他状态到 HOST 或 STANDBY 状态的迁移，满足系统可达性的验证规范。

3) 转移性质的 CTL 验证如式(3)所示。

$$\mathrm{EF}(\mathrm{state}=s_1\&\mathrm{EX}(\mathrm{state}=s_2)) \tag{3}$$

表达含义为：系统的 s_1 状态与 s_2 状态之间存在能够一步到达的迁移。此处以 JUDGEMENT 到 HOST 状态、JUDGEMENT 到 STANDBY 状态为例对其进行转移性质的验证，其验证结果如图 7 所示。

图 7　转移性质验证结果

结果表明，系统在 JUDGEMENT 状态时，能够通过一步迁移到达 HOST 或 STANDBY 状态，验

证了其状态转移的性质。

4) 反应性的 CTL 验证如式(4)所示。

$$AG(S \rightarrow AF(R)) \tag{4}$$

表达含义为：当 S 条件发生时，系统必然会转移到 R 状态。此处以 HOST 状态为例，状态机系统需要接收到做主信息后才能进入 HOST 做主状态，HOST 事件发生即迁移路径 t_{11} 发生，现对 t_{11} 与 HOST 状态的因果关系进行验证，如图 8 所示。

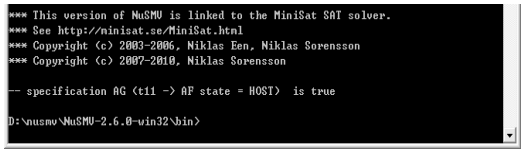

图 8　反应性验证结果

结果表明，当 t_{11} 发生时，即条件 HOST 发生时，系统定会进入到 HOST 状态，验证了其反应性。

5) 死锁性质的 CTL 验证如式(5)所示。

$$AG(EX(state=s_1)) \tag{5}$$

表达含义为：对于全局中的任何状态而言，在条件满足的情况下，系统的下一个运行状态可以为 s_1。现对系统 HOST 状态进行验证，结果如图 9 所示。

图 9　死锁性质验证结果

结果表明：系统可从任意状态进行跳转，而不会一直处于 HOST 状态。证明所检验的模型中不存在死锁现象。

6) 互斥性的 CTL 验证如式(6)所示。

$$!EF(state=s_1 \& state=s_2) \tag{6}$$

表达含义为：对于 s_1 和 s_2 系统状态而言，二者不会同时出现。此处以 HOST、STANDBY 两状态为例，对其进行互斥性的验证，验证结果如图 10 所示。

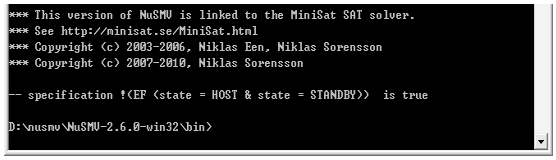

图 10　互斥性验证结果

结果表明，系统中的 HOST 和 STANDBY 状态不能同时出现，对于单步运行时，存在的状态间的互斥性进行了验证。

7) 确定性的 CTL 验证如式(7)所示。

$$!AG\ (state=s_1 \leftrightarrow state=s_2) \tag{7}$$

表达含义为：系统不会同时处于 s_1 状态和 s_2 状态。其对应于系统的无限运行状态，此处仍以 HOST、STANDBY 状态为例进行确定性的验证，其验证结果如图 11 所示。

图 11　确定性验证结果

结果表明，系统不能同时处于 HOST 和 STANDBY 状态，对于无限运行中，任意两状态间的确定性进行验证。

4　安全计算机管理单元的实现与测试

4.1　管理单元的软硬件设计与实现

本文所设计的基于 MCU 的管理单元的硬件结构如图 12 所示。

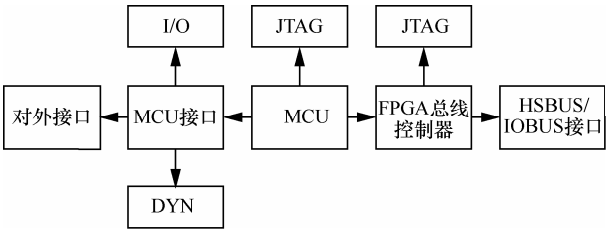

图 12　MCU 逻辑板硬件结构

MCU 逻辑板及其子模块所需的电源主要由电源模块进行提供；对外接口主要接收动态信号及 FPGA 管理单元传送的时钟同步信号；I/O 部分主要对信号进行隔离及相应的处理；DYN 动态转直流模块对故障进行检查；FPGA 部分主要与 MCU 通信，同时与专用总线接口模块进行连接，实现数据访问的功能；专用总线接口模块通过对电平的转换，实现 FPGA 与总线的连接，为专用总线提供物理连接入口。

软件方面，为了保证可靠运行以及方便后期维护操作，采用 MISRA-C 进行实现。根据具体设计功能对状态机的各个状态及转移条件进行定义，通过 switch/case 语句对条件进行判断，实现状态转移逻辑。

4.2　调试环境设计与实现

为确定状态机能够实现逻辑功能及数据传输功能，本文设计了状态监控软件，使用 PC 机作为

平台并通过 Windows 操作系统进行运行，对如下功能进行实现。

1) 对 $SCMU_2$ 的内部状态进行监控。

2) 模拟 FPGA 管理单元与 MCU 进行数据交互，对数据的收发状态进行显示。

3) 通过故障注入的检测方法验证 MCU 管理单元的可靠性及故障处理能力。

这种状态监控软件的优点在于：事先对所有状态进行顺序编排，只需点击 NEXT 按钮即可实现切换状态过程，亦可通过循环按钮实现状态的自动跳转及测试；并且对于同一状态节点的故障测试不需要手动输入各个激励事件，使测试过程的操作变得简单易行，达到自动测试的效果。可对测试过程中所有输入条件的测试结果进行记录，通过表格形式直观地显示出来。

4.3　测试结果分析

在测试的过程中，两机运行至判定状态时，能够实现主、备运行模式的判定，并且在各自做主的情况下继续运行，完成主、备模式控制周期中的各项任务，直接最终的数据输出状态。

通过对所述 MCU 内部状态机的运行情况及测试过程的分析可知：MCU 状态机与 PC 机模拟的 FPGA 通信状况保持良好，其内部软件状态机程序在对应的正确激励条件发生时，能够实现状态的正确跳转，对于故障信息不会产生错误响应而发生状态乱跳的情况，实现了预期的状态转移功能。

5　结束语

本文针对下一代列控安全计算机平台的功能需求以及预期实现的通信管理机制，对其中的管理单元进行了状态机模型的建立，进而使用形式化验证工具对其进行验证，证明管理机制中不存在死锁等现象，满足设计规范的要求。并以此为基础对管理单元进行软硬件实现。通过故障注入的方式对管理单元进行状态转移的测试，对运行数据进行记录。结果表明，本文针对通信管理机制所设计与实现的管理单元，能够实现预期的管理机制及状态机的状态转移功能。

参考文献：

[1] 郑升, 曹源, 张玉琢, 等. 通用型列控系统的安全计算机设计与验证[J]. 北京交通大学学报, 2014, 38(3): 128-134.
ZHENG S, CAO Y, ZHANG Y Z, et al. Design and verification of general train control system's safety computer[J]. Journal of Beijing Jiaotong University, 2014, 38(3): 128-134.

[2] LEE J D, BHOJWANI P S, MAHAPATRA R N. A safety analysis framework for cots microprocessors in safety-critical applications [C]// Ninth IEEE International Symposium on High-Assurance Systems Engineering. Plano, US, 2007: 407-408.

[3] 苟冬荣, 刘海清. 双机容错计算机系统的设计与实现[J]. 计算机工程, 2008, 34(15): 255-258.
GOU D R, LIU H Q. Design and implementation of dual-computer fault-tolerant system[J]. Computer engineering, 2008, 34(15): 255-258.

[4] 马连川, 高倍力. 一种高安全、容错控制计算机的设计与实现[J]. 中国安全科学学报, 2004, 14(8): 101-105.
MA L C, GAO B L. Design and realization of highly safe fault tolerant control computer[J]. China Safety Science Journal, 2004, 14(8): 101-105.

[5] 齐志华, 王海峰. 一种嵌入式二乘二取二容错计算机联锁系统设计[J]. 北京交通大学学报, 2006, 30(5): 96-100.
QI Z H, WANG H F. Design of an embedded double 2-vote-2 fault tolerant computer-based interlocking system[J]. Journal of Beijing Jiaotong University, 2006, 30(5): 96-100.

[6] SCHERRER C, STEININGER A. Dealing with dormant faults in an embedded fault-tolerant computer system [J]. IEEE Transaction on Reliability, 2003, 52(4): 512-522.

[7] 郭志良, 郜春海, 马连川, 等. 基于时间自动机模型的安全计算机平台的形式化验证[J]. 铁道学报, 2011, 33(6): 68-73.
GUO Z L, GAO C H, MA L C, et al. Formal verification of safety computer platform based on timed automata model [J]. Journal of the China Railway Society, 2011,33(6):68-73.

[8] CENELEC EN50129-2006. Railway applications: safety related electronic systems for signaling[S]. 2006.

[9] IEC61508-2. Functional safety of electrical/electronic/programmable electronic safety-related systems-part II[S].2010.

[10] PAOLO A, ANGELO G, ELVINIA R. A model advisor for NuSMV specifications[J]. Innovations in System & Software Engineering, 2011, 7:97-107.

作者简介：

梁靓（1987-），女，内蒙古赤峰人，北京交通大学硕士生，主要研究方向为列控系统安全计算机技术。

曹源（1982-），男，回族，河南开封人，博士，北京交通大学副教授，主要研究方向为高速铁路通信技术。

马连川（1970-），男，河北唐山人，北京交通大学副教授，主要研究方向为列控系统安全计算机技术。

张玉琢（1990-），男，河南信阳人，北京交通大学博士生，主要研究方向为形式化建模与验证。

李恒奎（1977-），男，山东肥城人，中车青岛四方机车车辆股份有限公司高级工程师，主要研究方向为高速动车组及地铁车辆设计。