doi:10.11959/j.issn.1000-436x.2017001

适于双冗余系统的信任链生成和更新算法

王雷[1,2,3]，杨明华[3]，刘增良[2]，郑建群[3]
（1. 清华大学精密仪器系，北京 100084；2. 国防大学信息指挥与作战教研部，北京 100091；
3. 火箭军装备研究院，北京 100094）

摘 要：可信计算技术中传统的信任链构建方式只适用于单一系统，对于工业控制领域广泛采用的双冗余系统会造成信任传递的断裂，为此提出一种适于双冗余系统的信任链模型，通过双信任链设计以及 IMC/IMV 交互机制，实现信任链从一个计算单元到另一个计算单元的扩展。在此基础上，提出了双冗余系统信任链生成和更新算法。最后基于可信理论和实验分析，对所提出模型的有效性进行证明。
关键词：可信计算；工控计算机；双冗余系统；信任链；IMC/IMV
中图分类号：TP319 **文献标识码**：A

Trust chain generating and updating algorithm for dual redundancy system

WANG Lei[1,2,3], YANG Ming-hua[3], LIU Zeng-liang[2], ZHENG Jian-qun[3]
(1. Department of Precision Instrument, Tsinghua University, Beijing 100084, China;
2. Institute of Information Operation, National Defence University of PLA, Beijing 100091, China;
3. Rocket Force Equipment Research Institute, Beijing 100094, China)

Abstract: In trusted computing field, the traditional construction mode of trust chain is only applicable to a single system. For the dual redundancy system, it causes break of transitive trust. A trust model suitable for dual redundancy system was proposed. Through double trust chain design and IMC/IMV interaction mechanism, the trust chain extension of trust from a computing unit to another unit was realized. On this basis, a trust chain generating and update algorithm for dual redundancy system was proposed. Finally, the validity of the proposed model was proved based on the trusting theory.
Key words: trusted computing, industrial control computer, dual redundancy system, trust chain, IMC/IMV

1 引言

随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，病毒、木马等威胁开始向工业控制系统大规模扩散，工控系统信息安全问题日益突出。据统计，在所有的安全问题中，问题最集中的地方是终端。由于工控系统大量使用工控计算机作为系统终端设备，工控计算机已成为黑客对工控系统恶意攻击的首选目标，工控计算机的安全性面临巨大挑战，一旦发生安全事故，就有可能造成人员和财产的巨大损失。

目前，为了提高工控计算机的可靠性，工控计算机已普遍采用冗余容错技术，如采用双冗余热备设计，在一个机箱中配置 2 套计算单元(CPU 板)，通过心跳检测，在主控计算单元出现故障时由备份计算单元接替工作，以保证应用业务不间断。但在安全性方面，为了保证可用性和效率，大多数工控系统采取的防护措施十分有限，甚至不会安装任何杀毒软件或 IDS。因为即使安装了杀毒软件、入侵检测等安全产品，但杀毒软件的病毒库、入侵检测的规则库都需要不定期地升级，这一要求无法适应工业控制环境。

高安全性、高可靠性是用户对工控计算机的基本要求，也是当前工控计算机系统研究的热点。近

收稿日期：2016-01-08；**修回日期**：2016-12-18
基金项目：国家核高基重大专项基金资助项目（No.2014ZX01040501-002）
Foundation Item: Nucleus High Base Significant Special Project (No.2014ZX01040501-002)

年来，可信计算技术已经被证明是提高计算机系统安全性的一种有效手段[1,2]。但是现有的可信计算技术，其信任根、信任链的设计只适用于保障单一计算机系统自身的安全，不适合由多个计算单元组成的工控计算机，尤其是在主备计算单元发生失效切换时，信任将如何传递，现有研究没有给出模型或方法。本文将可信计算技术与冗余容错技术有效融合，提出一种双冗余系统的信任链模型，设计一种双信任链机制和提出的信任链生成、更新算法，为解决冗余系统信任链实现问题提供了一种方法。

2 相关研究

近年来，可信计算技术得到了快速发展[3]，将可信计算技术应用于工控计算机系统中，可显著提高系统的安全性。可信计算技术的最大特点是采用了可信平台模块（TPM）硬件，提供基于硬件的安全保护，其本质是一种通过硬件手段来保证平台安全性的技术，其发展可以追溯到对安全协处理器和密码加速器的研究[4-6]。依据国际可信计算组织（TCG）提出的可信计算规范，可信计算采用了信任链传递技术，通过一种链式的信任度量模型[7]，信任可从TPM→BIOS→OS_LOADER→OS逐级传递，构成了一个可信链，其中，信任的传递利用了散列值迭代计算的方式，即将当前值与新值相连，再计算散列值并作为新的完整性度量值存储起来，计算式为

$$\text{New PCR}_i = \text{HASH}(\text{OLD PCR}_i \,||\, \text{New Value}) \quad (1)$$

由于在信任链中采用了这种逐级迭代的可信度量方法，从而能确保被度量部件的完整性。基于TPM构建起来的可信执行环境，使上层应用可以时刻处在安全可信的保护框架内。文献[8]基于TCG提出的可信计算原理和安全技术规范，提出一种柔性可信计算机模型(FTPC)。FTPC通过增强传统BIOS的安全功能，以BIOS核心代码为可信根核，将可信计算模块(TPM)封装成块设备，通过USB接口实现了TPM与BIOS和操作系统的交互。FTPC由于无需改变现有计算机硬件体系结构即可支持可信计算，因而具有易实施和应用灵活的特点。文献[9]提出了一种动态化的信任链传递模型，其基于无干扰理论将系统抽象为应用程序、动作和状态输出，通过度量应用程序及其动态库的完整性来保障应用的静态可信，通过分析有交互的应用之间的关系，来保障应用运行过程中的动态可信。

国内可信计算技术相关研究大概从2003年起步。中国拥有自主知识产权的可信计算规范被称为TCM（可信密码模块），与国际可信计算的TPM规范相对应[10,11]。文献[12]基于国产可信芯片、龙芯处理器、中标麒麟操作系统，结合可信计算技术，深入研究了基于龙芯处理器的可信计算机的体系结构、信任根的构建、信任链传递技术，以及用户身份认证和系统的完整性度量机制，最后通过原理样机验证了基于龙芯处理器可信计算机设计方法的可行性和正确性。文献[13]以我国自主研发的可信密码模块TCM为可信根，采用国产软硬件实现了自主可信计算机。为了保证系统资源的安全可信，专门设计了IC卡密钥加载、基于USB-KEY的用户身份认证和系统的完整性度量机制。针对BIOS的可信性，设计了可信BIOS，通过LPC总线与TCM和CPU连接，上电后TCM会对其进行主动度量验证，确保BIOS可信，然后BIOS继续完成硬件检测与初始化、外部设备扫描及驱动挂载、启动配置设置以及操作系统引导加载等工作。

综上所述，在可信计算技术研究方面，无论国内还是国外都已比较深入，相关的设计模型、解决方案、原型系统较多，技术也较为成熟，但已有的研究大多专注于提高单一计算机系统的可信性，对于具有多模冗余特点的工控计算机系统如何实现可信，尤其是如何构建可信链、如何实现度量算法还缺少相关研究。

3 双冗余系统信任链模型

为保证工控计算机在发生故障、存在不安全问题时仍然可以安全、稳定地工作，基于“可信≈安全+可靠”的理念，提出可信双冗余设计。可信双冗余设计是由2个计算单元、冗余电路等组成的*A*/*B*可信冗余系统，平时2个子系统同时运行，但只有一个子系统参与业务处理，在一个子系统出现软硬件故障、不安全问题时，由另一个子系统接替工作，如图1所示。

由于可信双冗余系统采用了冗余架构，其信任链传递机制不同于单机系统，尤其是在发生失效切换过程中，必须保证可信计算基（TCB）始终是可信的。

针对双冗余系统内部互联特点，按二元对等模型设计双冗余系统信任链模型如图2所示，在每个计算单元上集成TCM模块，分别建立信任链，通过完整性检测心跳实现信任链的交接。当一个计算单元不可靠时，由另一个计算单元接替工作，保证应用业务始终在可信的环境下运行。

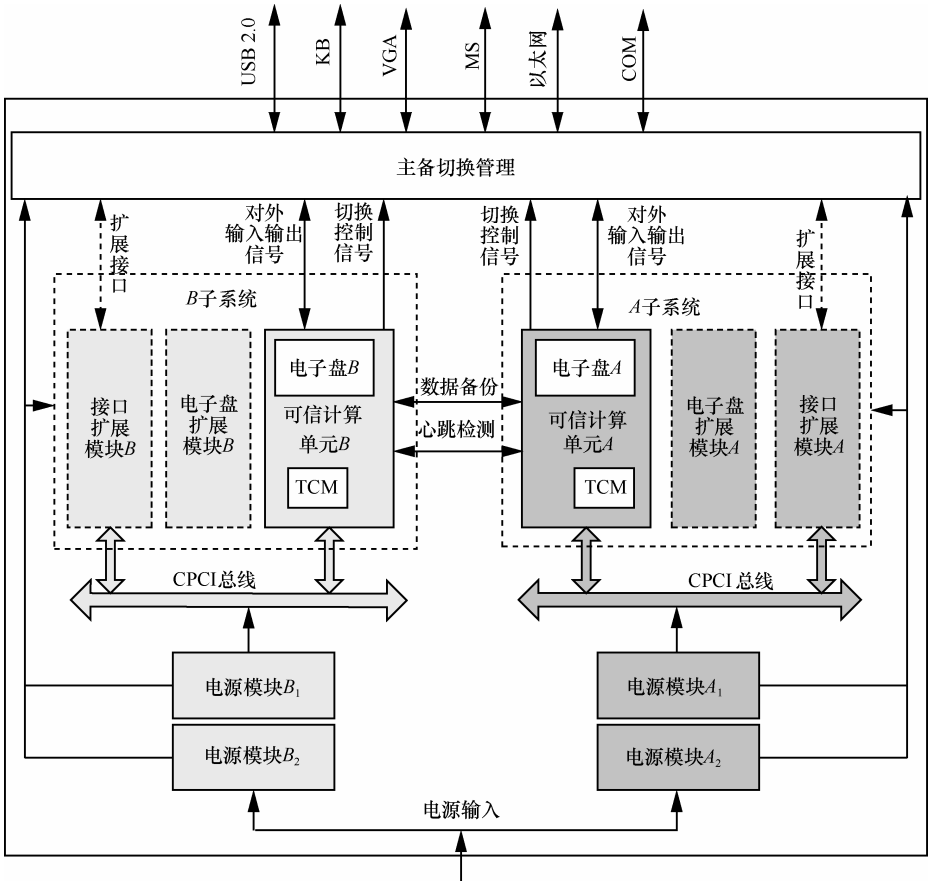


图 1　工控计算机可信双冗余系统组成结构

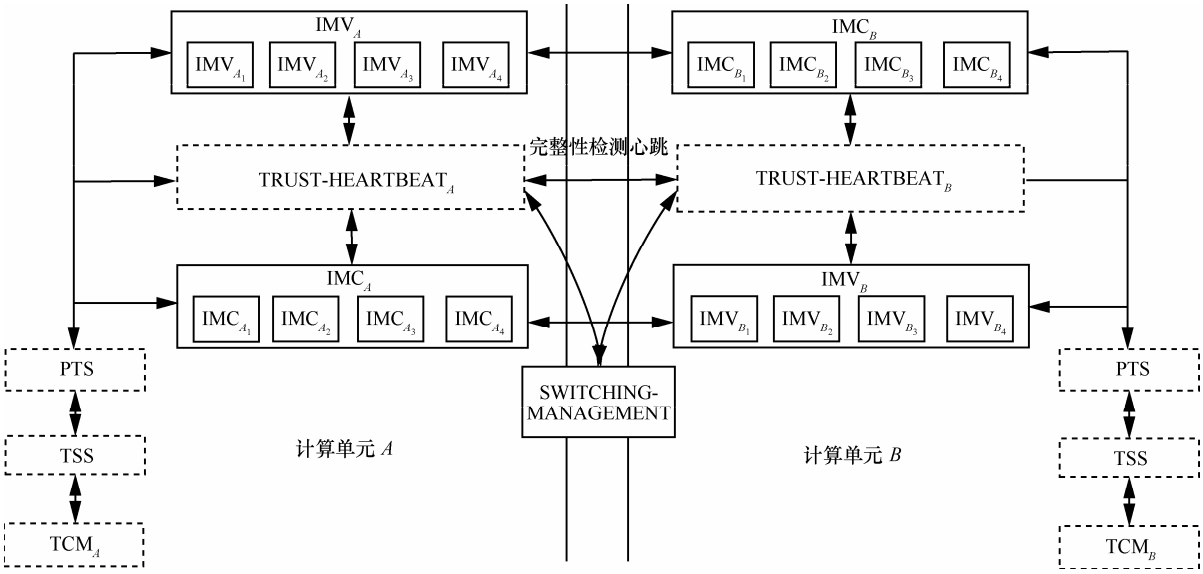


图 2　双冗余系统可信模型

在图 2 中，TSS（trust software stack）为可信软件栈，PTS（platform trust service）为平台可信服务。PTS 负责收集完整性度量器（IMV，integrity measurement verifier）、完整性收集器（IMC，integrity measurement collector）以及可信心跳（TRUST-HEARTBEAT）组件的完整性状态，如果这些组件在未被授权的情况下被篡改就会被发现，并且 PTS 构建完整性报告供 IMC 和 IMV 之间进行远程证明。当 IMC 需要向远端的 IMV 报告平台某组件完整性信息时会通知 PTS，由 PTS 负责向 TCM 报告度量

需求并将度量报告返回给远端的 IMC。

IMC 为完整性度量收集器，负责收集用户身份、平台身份、平台完整性信息以及其他安全属性信息[14]，并通过 TRUST-HEARTBEAT 将上述信息发送给远端对应的 IMV。

IMV 为完整性度量校验器，与远端的 IMC 一一对应，负责检验远端的 IMC 发来的完整性度量值。必须所有的 IMV 都判定可信的情况下，才能认为远端可信。

SWITCHING-MANAGEMENT 为切换管理单元，负责接收 TRUST-HEARTBEAT 的主备切换指令，完成 *A*/*B* 子系统的主备切换控制。

TRUST-HEARTBEAT 为完整性心跳检测器，周期性地将本地 IMC 产生的度量报告完整性心跳数据分组发送给远端 TRUST-HEARTBEAT，同时接收远端 TRUST-HEARTBEAT 发来的远端 IMC 的度量报告。TRUST-HEARTBEAT 接收本地 IMV 对远端的可信判定结果，若判定远端不可信，则通知 SWITCHING-MANAGEMENT，进行主备切换。

为实现双冗余系统的可信，初始化每个计算单元，分别建立信任链，之后通过信任链的交接，实现信任链从本地计算单元向远端计算单元的扩展。信任链传递过程如下所示。

1) 操作系统启动之前：TCM→BIOS→OS_LOADER→OS。

2) PTS 启动之前：OS→TSS→PTS。

3) PTS 启动之后：PTS→(TRUST-HEARTBEAT、IMV、IMC)。

4) PTS→IMC：PTS 向 IMC 报告从 TCM 开始的可信链。

5) IMC→TRUST-HEARTBEAT：IMC 向 TRUST-HEARTBEAT 报告从可信状态。

6) TRUST-HEARTBEAT→远端 IMV：通过 TRUST-HEARTBEAT 组件，向远端 IMV 报告其他组件完整性信息。

7) 远端 IMV→（远端 TCM、远端 BIOS、远端 OS_LOADER、远端 OS、远端 TSS、远端 PTS、远端 IMC、远端 TRUST-HEARTBEAT）：由远端 IMV 进行完整性检测，若检测结果为可信，则实现信任链扩展到远端。

4 信任链生成和更新算法

4.1 信任链协议

系统开机启动后，每个计算单元按现有的信任链生成方法独立地建立信任链，分别确保各个计算单元可信，如图 3 所示。

其中，每个计算单元 TRUST-HEARTBEAT 中的 IMC/IMV 的交互过程是实现双冗余系统每个计算单元信任链安全交接的关键。IMC 的任务是根据 IMV 的要求收集平台完整性信息，发送 IMC 的度量值给 IMV 并接受来自 IMV 挑战者的响应消息，以便 IMV 校验 IMC 完整性状态来决定其是否可信。这些交互通常是发生于完整性校验握手过程之中。在 *N* 次交互信息过程中，IMC 将平台完整性度量值及其他安全属性值分片发送给 IMV，IMV 根据预置策略有选择性地对消息进行回应，如修补命令，需要更多平台完整性信息等。在这之间的通信会一直持续到 IMV 有自己的推荐行为时终止。在 IMC/IMV 的交互过程中，IMC/IMV 不是直接通信的实体，必须依靠 TRUST-HEARTBEAT 来传递信息。每一条消息都包括消息体、消息类型和接收类型，但 TRUST-HEARTBEAT 不能解析和分析消息体信息，消息体的解释由最终的信息接收方端的 IMC 或 IMV 来进行。信任链协议交互过程如图 4 所示。

4.2 算法描述

计算单元 *A* 与计算单元 *B* 之间按照一定的时间节拍彼此发送完整性检测心跳，证明彼此可以信任。当一个计算单元已被证明不可信时，由可信心跳组件通知失效切换单元可信状态发生改变，由失效切换单元完成主备切换。每个计算单元同时执行信任链生成、更新算法。

设 TCM 表示可信密码模块，BIOS 表示计算机基本输入输出系统固件，OS_LOADER 表示操作系统加载器，OS 表示操作系统，TSS 表示可信软件栈，PTS 表示平台可信服务，IMV 表示完整性度量器，IMC 表示完整性收集器，TRUST-HEARTBEAT 表示可信心跳组件，SWITCHING-MANAGEMENT 表示主备切换管理单元，具体算法描述如下所示。

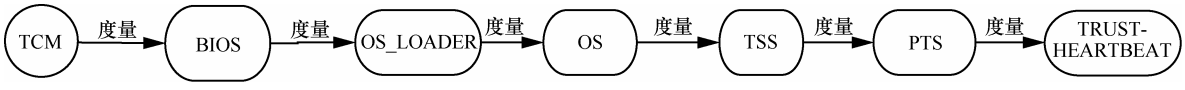


图 3 单一计算单元可信链构建过程

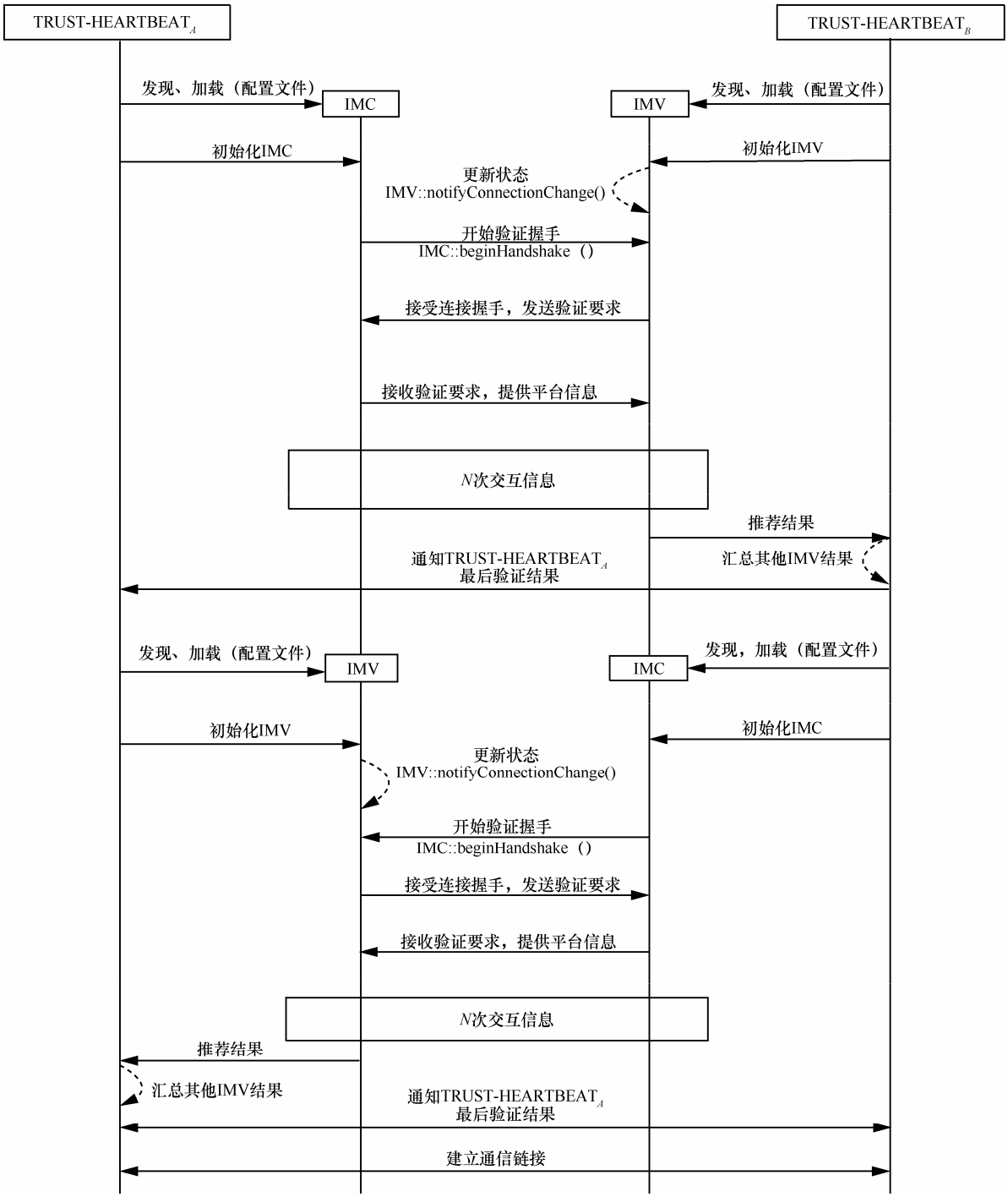


图 4　信任链协议交互过程

1) 执行一般的可信链建立过程 TCM→BIOS→OS_LOADER→OS；如果在建立过程中，出现不可信，则跳转至 9)。

2) 为扩展后面的可信链增加对 TSS 和 PTS 度量；TCM→BIOS→OS_LOADER→OS→TSS→PTS；如果不可信，则跳转至 9)。

3) 如果 PTS 是可信的，PTS 就可以通过度量 IMC、IMV 和 TRUST-HEARTBEAT 把信任传递到本计算单元的边界，确保本地报告平台完整性信息的组件是可信的，即 TCM→BIOS→OS_LOADER→OS→TSS→PTS→(TRUST-HEARTBEAT、IMV、IMC)；如果不可信，则跳转至 9)。

4) 通过 IMC 收集本地平台完整性信息。

5) 通过 TRUST-HEARTBEAT 向远端报告平台

完整性信息，使远端相信 TRUST- HEARTBEAT 组件是经过一条完整的信任链度量过程的，是可信的。

6) IMC 度量其他组件，并通过 TRUST-HEARTBEAT 报告给远端，由于远端已经知道报告的 TRUST-HEARTBEAT 组件是可信的，所以可以相信 IMC 报告的其他完整性信息。

7) TRUST-HEARTBEAT 接收远端 TRUST-HEARTBEAT 发送的完整性信息，交由 IMV 进行可信性判断。

8) IMV 根据可信基准值判断远端是否可信，如果可信则跳转 4)，否则跳转 9)。

9) 通知 SWITCHING-MANAGEMENT，进行主备切换，将应用业务迁移到可信的计算单元上运行。

5 证明

双冗余系统信任链的有效性证明如下。由可信计算理论[15,16]可知以下定理和推理。

定理 1 设 R 为组件域，R 具有交换性。$Trust(A)$ 表示一个组件 A 是可信的。对于任意 A，$B\in R$，则 $<A, B>$表示 A 信任 B。若存在 A，$B\in R$，且$<A, B>$，则由 R 中组件的交换性可知：$<A,B> \rightarrow <B, A>$，即存在 B 信任 A。

定理 2 设 R 为组件域，R 具有传递性。$Trust(A)$ 表示一个组件 A 是可信的。对于任意 $A, B\in R$，则$<A, B>$表示 A 信任 B。若存在 A，B，$C\in R$，且$<A, B>$、$<B, C>$，则由 R 中组件的传递性可知：$<A, B>, <B, C>\rightarrow <A, C>$，即存在 A 信任 C。故信任可由 A 传递到 C。

推理 1 由定理 1 可知，当组件链 M 满足下列 3 个条件时，则 M 是可信的。

1) M 始于可信根。

2) 传递过程满足单步隔离性。

3) M 满足交换性、传递性。

证明 1) 在系统启动后，A、B 计算单元分别建立始于可信根 TCM 的可信链，其中，计算单元 A 的可信链为

$$TCM_A\rightarrow BIOS_A\rightarrow OS\_LOADER_A\rightarrow OS_A\rightarrow TSS_A\rightarrow PTS_A\rightarrow(TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A) \quad (2)$$

计算单元 B 的可信链为

$$TCM_B\rightarrow BIOS_B\rightarrow OS\_LOADER_B\rightarrow OS_B\rightarrow TSS_B\rightarrow PTS_B\rightarrow(TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B) \quad (3)$$

2) 由于 $TRUST\text{-}HEARTBEAT_A$ 与 $TRUST\text{-}HEARTBEAT_B$ 的 IMC-IMV 交互过程加密并经数字签名，且传递是在冗余系统内部完成，即传递过程具有单步隔离性，可得

$$(TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A)\rightarrow(TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B) \quad (4)$$

$$(TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B)\rightarrow(TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A) \quad (5)$$

3) 由于可信链具有交换性，由式(2)可得

$$<TCM_A, BIOS_A>\rightarrow<BIOS_A, TCM_A> \quad (6)$$

$$<BIOS_A, OS\_LOADER_A>\rightarrow<OS\_LOADER_A, BIOS_A> \quad (7)$$

$$<OS\_LOADER_A, OS>\rightarrow<OS_A, OS\_LOADER_A> \quad (8)$$

$$<OS, TSS_A>\rightarrow<TSS_A, OS> \quad (9)$$

$$<TSS_A, PTS_A>\rightarrow<PTS_A, TSS_A> \quad (10)$$

$$<PTS_A, (TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A)>\rightarrow<PTS_A, (TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A)> \quad (11)$$

由式(6)~式(11)及可信传递性可得

$$(TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A)\rightarrow PTS_A\rightarrow TSS_A\rightarrow OS_A\rightarrow OS\_LOADER_A\rightarrow BIOS_A\rightarrow TCM_A \quad (12)$$

由式(3)可得

$$<TCM_B, BIOS_B>\rightarrow<BIOS_B, TCM_B> \quad (13)$$

$$<BIOS_B, OS\_LOADER_B>\rightarrow<OS\_LOADER_B, BIOS_B> \quad (14)$$

$$<OS\_LOADER_B, OS_B>\rightarrow<OS_B, OS\_LOADER_B> \quad (15)$$

$$<OS_B, TSS_B>\rightarrow<TSS_B, OS_B> \quad (16)$$

$$<TSS_B, PTS_B>\rightarrow<PTS_B, TSS_B> \quad (17)$$

$$<PTS_B, (TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B)>\rightarrow<PTS_B, (TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B)> \quad (18)$$

由于式(13)~式(18)及可信链具有传递性，可得

$$(TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B)\rightarrow PTS_B\rightarrow TSS_B\rightarrow OS_B\rightarrow OS\_LOADER_B\rightarrow BIOS_B\rightarrow TCM_B \quad (19)$$

由式(4)和式(12)可得

$$TCM_A\rightarrow BIOS_A\rightarrow OS\_LOADER_A\rightarrow OS_A\rightarrow TSS_A\rightarrow PTS_A\rightarrow(TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A)\rightarrow(TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B)\rightarrow PTS_B\rightarrow TSS_B\rightarrow OS_B\rightarrow OS\_LOADER_B\rightarrow BIOS_B\rightarrow TCM_B \quad (20)$$

由式(3)和式(19)可推出

$$TCM_B\rightarrow BIOS_B\rightarrow OS\_LOADER_B\rightarrow OS_B\rightarrow TSS_B\rightarrow PTS_B\rightarrow(TRUST\text{-}HEARTBEAT_B、IMV_B、IMC_B)\rightarrow(TRUST\text{-}HEARTBEAT_A、IMV_A、IMC_A)\rightarrow PTS_A\rightarrow TSS_A\rightarrow OS_A\rightarrow OS\_LOADER_A\rightarrow BIOS_A\rightarrow TCM_A \quad (21)$$

由此证明所构建的双冗余系统的信任链是可信的。

6　实验分析

为验证所设计模型和方法的有效性，基于两单元机架式服务器搭建了实验环境。两单元机架式服务器由 2 个计算单元、2 个交换单元、1 个共享存储单元和 1 个管理单元组成。每个计算单元集成可信模块。系统基本配置如表 1 所示。

表 1　　系统基本配置

基本配置项	主要技术参数
可信模块	国产 TCM
计算单元处理器	国产龙芯 3A
操作系统内核	Linux 2.6.32
操作系统	中标麒麟 4.1.1
数据库	达梦 7.0

分别采用接入非法 USB 设备、关闭杀毒软件、篡改核心配置文件、打开非法网络端口这 4 种方式，对系统失效切换的有效性进行测试，测试结果如表 2 所示。

表 2　　主备切换测试

测试项目	测试次数	首次成功切换次数	成功率
插入非法 USB	150	148	98.6%
关闭杀毒软件	150	150	100%
篡改核心文件	150	150	100%
打开非法网络端口	150	150	100%
合计	600	598	99.6%

从测试结果可以看出失效切换成功率达 99.6%。经对切换失败的原因分析，主要是操作系统对 USB 设备识别过程有一定延迟，这 2 次实验的时间间隔过短，导致系统首次切换失败。但在系统再次执行切换动作时，可以顺利完成切换，能够满足实际应用需要。

失效切换时间测试如图 5 所示。失效切换时间主要受系统服务启动时间、应用服务启动时间、心跳间隔时间、可信度量时间影响。

经 600 次测试，系统平均切换时间为 5.5 s，最大切换时间为 7.1 s，最短切换时间为 3.9 s。其中，对切换时间影响最大的是应用服务，尤其是数据库。进一步实验表明，通过优化相关参数配置可进一步缩短切换时间。

7　结束语

随着工控系统信息化程度的加速，工业控制系统产品越来越多地依赖通用协议、通用硬件和通用软件，导致工控系统信息安全问题日益突出。本文针对工业控制领域对关键系统的高安全性要求，提出一种双冗余系统可信模型，通过设计的双信任链机制以及冗余系统信任链的生成和更新算法，实现了信任在双冗余工控计算机各计算单元间的可信传递、扩展，为解决工控计算机的可信机制实现问题提供了一种可行方法。考虑到在面临攻击时，同构冗余设计仍有一定的风险，尤其是在一个计算单元被攻破的情况下，另一个被攻破只是时间问题，下一步将在此研究基础上进一步开展异构冗余系

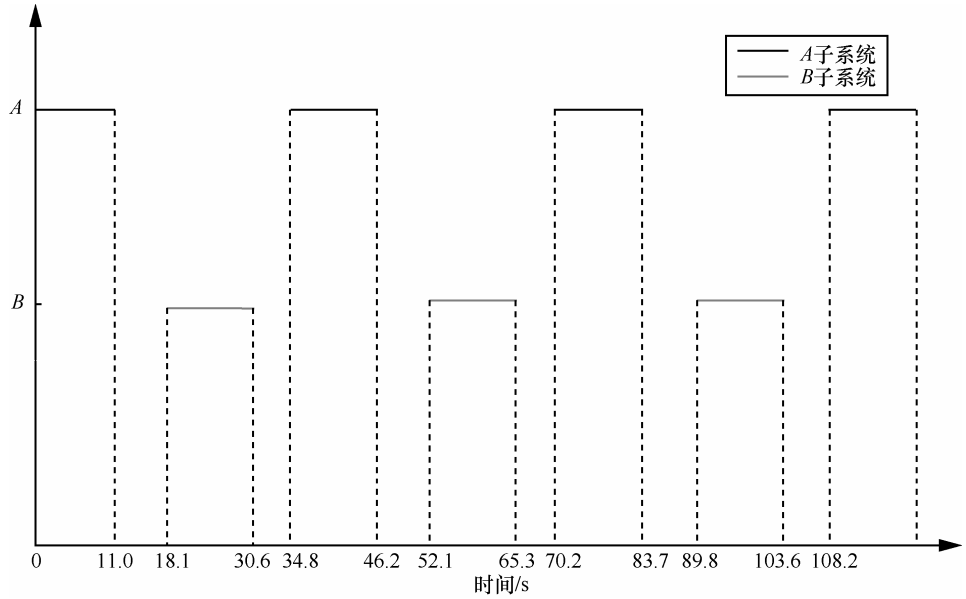


图 5　*A*/*B* 子系统失效切换时间

统的信任链构建技术研究。

参考文献：

[1] 冯登国. 可信计算——理论与实践[M].北京：清华大学出版社, 2013.
FENG D G. Trusted computing theory and practice [M]. Beijing: Tsinghua University Press, 2013.

[2] SHEN C X, ZHANG H G, WANG H M, et al. Research on trusted computing and its development[J].Science China:Information Sciences, 2010, 53(3): 405-433.

[3] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学, 2010, 40(40): 139-166.
SHEN C X, ZHANG H G, WANG H M, et al. Research and development of trusted computing [J]. Science China, 2010, 40 (40): 139-166.

[4] TCG. TPM specifications v2.0[EB/OL]. http://www. trustedcomputinggroup. org/.

[5] LI H, HU H. UCFS: building a usage controlled file system with a trusted platform module[C]//1st Chinese Conf on Trust Computing Theory and Practice. 2009: 10-23.

[6] YU A M, FENG D G, LIU R. TBDRM: a TPM based secure DRM architecture[C]//Int Conf on Computational Science and Engineering, Los Alamitos, CA. 2009: 671-677.

[7] 徐明迪, 张焕国, 赵恒. 可信计算平台信任链安全性分析[J]. 计算机学报, 2010, 33(7): 1167-1176
XU M D, ZHANG H G, ZHAO H. Security analysis of trust chain in trusted computing platform[J]. Chinese Journal of Computer, 2010, 33(7): 1167-1176.

[8] 周振柳, 陈榕, 池亚平, 等.一种柔性可信计算机模型与实现方法[J]. 计算机工程, 2007, 33(20): 156-158.
ZHOU Z L, CHEN M, CHI Y P, et al. A model and implementation of a flexible trusted computer [J]. Computer Engineering, 2007, 33 (): 156-158.

[9] 司丽敏, 蔡勉, 陈银镜, 等.一种信任链传递模型研究[J]. 计算机科学, 2011, 38(9): 36-42.
SI L M, CAI M, CHEN Y J, et al. A study on trust chain transfer model[J]. Computer Science, 2011, 38 (9): 36-42.

[10] 国家密码管理局.可信密码支撑平台技术规范[EB/OL]. http://www.osscca.gov.cn.
STATE ENCRYPTION ADMINISTRATION. Technical specification for trusted cryptographic support platform [EB/OL]. http://www.osscca.gov.cn.

[11] 中国可信计算工作组. 可信计算密码支撑平台功能与接口规范[EB/OL]. http://www.tcmu.org.cn/.
TRUSTED COMPUTING WORKING GROUP OF CHINA. The function and interface specification of trusted computing cryptographic support platform [EB/OL]. http://www.tcmu.org.cn/.

[12] 吴小强. 基于龙芯处理器的可信计算机研究与设计[J]. 工业控制计算机, 2011, 24(11): 26-30.
WU X Q. Research and design of trusted computer based on Godson processor[J]. Industrial Control Computer, 2011, 24 (11): 26-30.

[13] 朱小波, 舒棚, 周晓霞. 基于TCM的国产可信计算机的设计[J]. 信息技术, 2013, 12(12): 102-105.
ZHU X B, SHU P, ZHOU X X. Design of a domestic trusted computer based on TCM[J]. Information Technology, 2013, 12 (12): 102-105.

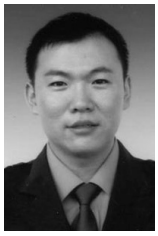
[14] 秦宇，冯登国.基于组件属性的远程证明[J].软件学报, 2009, 20(6): 1625-1640.
QIN Y, FENG D G. Component property based remote attestation[J]. Journal of Software, 2009, 20(6): 1625-1640.

[15] CHALLENER D. 可信计算[M]. 北京：机械工业出版社, 2009.
CHALLENER D. A practical guide to trusted computing[M]. Beijing: China Machine Press, 2009.

[16] 张焕国, 赵波. 可信计算[M]. 武汉：武汉大学出版社, 2011.
ZHANG H G, ZHAO B. Trusted computing[M]. Wuhan: Wuhan University Press, 2011.

作者简介：

王雷（1967-），男，江苏扬州人，火箭军装备研究院研究员，主要研究方向为指挥通信、信息安全。



杨明华（1977-），男，黑龙江哈尔滨人，博士，火箭军装备研究院高级工程师，主要研究方向为可信计算技术、无线传感器网络技术。

刘增良（1958-），男，河北深泽人，国防大学教授、博士生导师，主要研究方向为信息对抗、C3I。

郑建群（1973-），男，江苏建湖人，火箭军装备研究院高级工程师，主要研究方向为信息化应用、网络安全。