DOI：10.13890/j.issn.1000-128X.2023.06.018　　文章编号：1000-128X(2023)06-0147-09

云联锁系统冗余结构研究

何志彬[1]，邢科家[2]，梁志国[2]，魏东冬[2]，郑长宗[2]
（1.中国铁道科学研究院 研究生部，北京　100081；
2.中国铁道科学研究院集团有限公司 通信信号研究所，北京　100081）

摘　要：为保障联锁系统在云平台中的运行安全，文章通过对既有计算机联锁系统冗余结构进行分析，结合云平台特征，提出了基于虚拟机容错技术的云联锁系统冗余结构。首先，阐述了云联锁冗余结构的特点和优势。其次，通过对云联锁冗余结构的工作模式和服务器失效因素进行分析，建立服务器故障树模型、云联锁系统冗余结构关于危险失效概率PFD和安全失效概率PFS的动态故障树模型。最后，对云联锁冗余结构的可靠性进行研究，对动态故障树模型进行仿真分析。研究结果表明：云平台更适合部署形如*M*oo*N*结构的多重冗余结构联锁系统，开展云联锁冗余结构研究对云联锁的发展具有一定的借鉴意义。

关键词：铁路联锁系统；云计算；冗余结构；动态故障树；失效概率；高速铁路
中图分类号：U284.3　　**文献标识码：**A

Research on redundant structure of cloud-based interlocking systems

HE Zhibin[1], XING Kejia[2], LIANG Zhiguo[2], WEI Dongdong[2], ZHENG Changzong[2]

(1. Postgraduate Department, China Academy of Railway Sciences, Beijing 100081, China;
2. Signal & Communication Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China)

Abstract: In order to ensure the operational safety of interlocking systems within cloud platforms, this paper presented a redundant structure for cloud-based interlocking systems based on virtual machine fault tolerance technology, through analyzing the redundant structure of the existing computer-based interlocking systems and considering the characteristics of cloud platforms. Firstly, the characteristics and advantages of the redundant structure of cloud-based interlocking systems were elaborated. Subsequently, this paper analyzed the working mode and server failure factors, and established a server fault tree model and dynamic fault tree model to evaluate the probability of failure on danger (PFD) and probability of failure to safety (PFS). Finally, the reliability of the redundant structure of cloud-based interlocking systems was assessed by simulation analysis using the dynamic fault tree model. The results indicate that cloud platforms are more suitable for deploying interlocking systems in multiple redundant structures such as *M*oo*N* structures. This research on the redundant structure for cloud-based interlocking holds certain reference significance for the development of cloud-based interlocking systems.

Keywords: railway interlocking system; cloud computing; redundant structure; dynamic fault tree; failure probability; high-speed railway

0　引言

计算机联锁系统是铁路信号系统中核心的关键子系统之一，对于列车安全平稳运行起着至关重要的作用[1-2]。计算机联锁系统通常采用二乘二取二、三取二等冗余结构来提高系统的可靠性和安全性。近年来，云计算服务应用越来越广泛[3]。云计算利用虚拟化技术

基金项目：中国国家铁路集团有限公司科技研究开发计划项目（J2021G006）；中国铁道科学研究院集团有限公司科研项目（2022YJ063）
通信作者：梁志国（1982—），男，副研究员，主要从事计算机联锁方面的研究；E-mail: liangzhiguo@139.com
引用格式：何志彬, 邢科家, 梁志国, 等. 云联锁系统冗余结构研究[J]. 机车电传动, 2023(6): 147-155.
Citation: HE Zhibin, XING Kejia, LIANG Zhiguo, et al. Research on redundant structure of cloud-based interlocking systems[J]. Electric drive for locomotives,2023(6): 147-155.

将商用现货服务器集群资源池化，统一资源配置，提供大规模的计算资源、数据存储和软件服务，有助于降低成本，提高资源利用率、灵活性和可拓展性，虚拟化作为实现云计算资源共享的核心技术，在铁路行业探索信号系统的云服务方面的项目研究不断增加。云平台可以为联锁系统等应用提供大量的计算资源，并以集中的方式执行大量的计算任务。通过将联锁的逻辑计算任务迁移到位于中心的云平台上，联锁系统性能、可用性和可扩展性也将大幅提升。作为新型联锁发展方向之一，云联锁将联锁软件部署在云平台上，以通用平台替代专用平台。云联锁如何保证联锁系统的安全性是一个新的课题，本文将分析既有计算机联锁系统冗余结构，结合云平台特性，提出基于虚拟机容错技术的云联锁系统冗余结构，针对冗余结构建立动态故障树模型，通过仿真分析对云联锁冗余结构的可靠性进行研究，对云联锁的冗余结构的选择进行分析并给出建议。开展云联锁相关研究，有助于推动铁路信号领域的技术创新和发展，提升我国铁路信号安全相关系统的智能化水平和综合竞争力。

1 传统计算机联锁系统冗余结构分析

计算机联锁系统采用典型的分层架构，联锁系统典型的分层结构如图 1 所示。人机接口层的主要功能是提供信号值班员操作和显示界面，值班员通过在人机接口层进行必要的逻辑处理后，将控制命令发送到主控层，同时人机接口层接收主控层发来的站场信号设备的状态信息，并在屏幕上加以显示。主控层的联锁机是系统安全平台的核心，主要用于实现安全平台管理逻辑的处理、联锁逻辑运算、与外部其他安全苛求系统的通信等功能；执行层能够根据主控层联锁运算发出的指令完成规定的动作[4]。

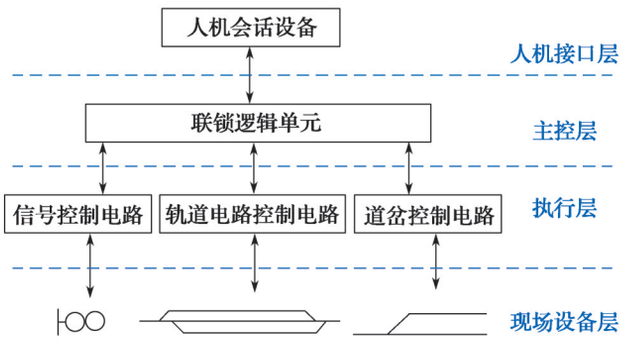
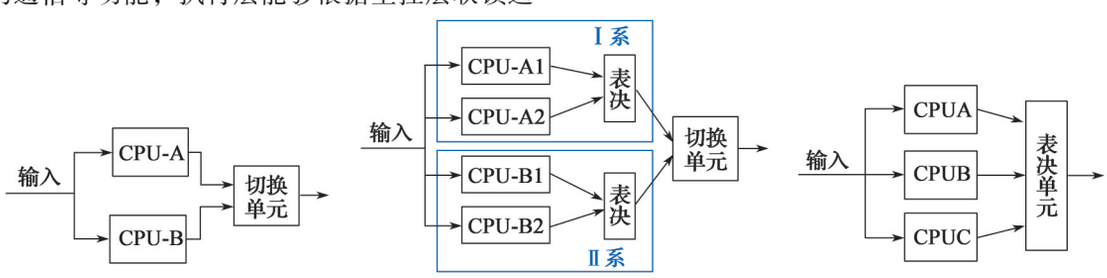


图 1 联锁系统典型分层结构

Fig. 1 Typical hierarchical structure of an interlocking system

随着计算机联锁系统安全苛求越来越高，使得系统的复杂性日益增加，同时，对联锁系统可靠性的要求也在持续提高，在铁路信号计算机联锁系统中，采用冗余技术作为提高系统可靠性和可用性有效的技术手段[5]。图 2 展示了 3 种联锁系统的冗余结构，其中，双机热备是基于故障检测并能自动切换的最基本的可靠性冗余结构，该结构中的两个基本单元完全相同，只要有一个单元完好就能正常地执行规定的功能；二乘二取二是由两个具有二取二安全结构互为热备构成的组合式冗余结构，其中的二取二由两个单元构成，功能完全相同，只有两个单元运算结果完全相同时才能够执行规定功能，否则导向安全侧；三取二是多重系冗余结构，兼顾了可靠性和安全性，它由 3 个功能相同的单元构成，其输出符合多数表决原则。三取二结构能够屏蔽任意单一单元的故障，若仅其中一个单元的输出与其余两个单元的输出不同，整个系统的输出状态不会因此而改变，使系统的整体功能在一单元故障时能够保持正常。



(a) 双机热备 (b) 二乘二取二 (c) 三取二

图 2 联锁典型冗余结构

Fig. 2 Typical redundant structure of interlocking system

2 云联锁冗余结构分析

目前，计算机联锁系统主要采用二乘二取二的安全冗余结构，以兼顾整个系统的安全性与可靠性。云联锁由于其中心服务平台的特性，能通过增加运算节点数量，经多重表决比对数据这种冗余方式，保证联锁系统逻辑运算数据的可用性。在这种架构中，在增加运算节点的同时面临着如何实现同步表决或多节点一致性等问题。如何设计基于云平台的联锁系统冗余结构是新一代数字化联锁系统面临的关键问题。

2.1 基于虚拟机容错技术的冗余结构

借鉴既有计算机联锁系统设计经验，设计了云联锁总体结构，如图 3 所示。该结构设计的总体思路为：由云平台负责联锁逻辑运算处理任务，并运用多重冗

余机制，屏蔽系统中出现的错误。由独立于云平台的SIL4级表决设备对联锁处理进行安全输出控制，确保控制符合故障–安全原则。云联锁系统采用通用硬件取代了专用硬件设备，将联锁逻辑处理部分部署在资源集中化的云平台中，所有车站的联锁应用通过云上的虚拟化技术相互隔离地在云平台上执行，轨旁配置对象控制单元，对象控制单元是一个用于控制轨旁设备（如道岔、信号和轨道电路）的固有安全单元。为保障联锁命令的正确性，云平台与对象控制单元的信息交互需经由参与决策的SIL4级安全表决设备，表决设备作为云平台与对象控制单元的交互的唯一通道，将信号、道岔和轨道电路等轨旁设备状态信息传输到云平台中，经联锁运算处理后再由表决设备发送到轨旁对象控制单元，由轨旁对象控制单元控制轨旁设备。云平台、表决设备和对象控制单元三者协作，共同完成联锁服务。同时，“空–地”交互通道的严格管理有益于将网络入侵的风险最小化。云平台中的任务处理都基于统一的时钟。为实现异地冗余备份，进一步提升云联锁的可靠性，采用主/备两套云联锁平台配置。

从上述描述的云联锁总体架构可以看出，联锁服务虽然建立在非SIL4级的云平台上，云平台本身不具备数据一致性比较等安全性功能，其运算必须经由SIL4级安全表决设备监控才能输出，以保障联锁功能的安全性。

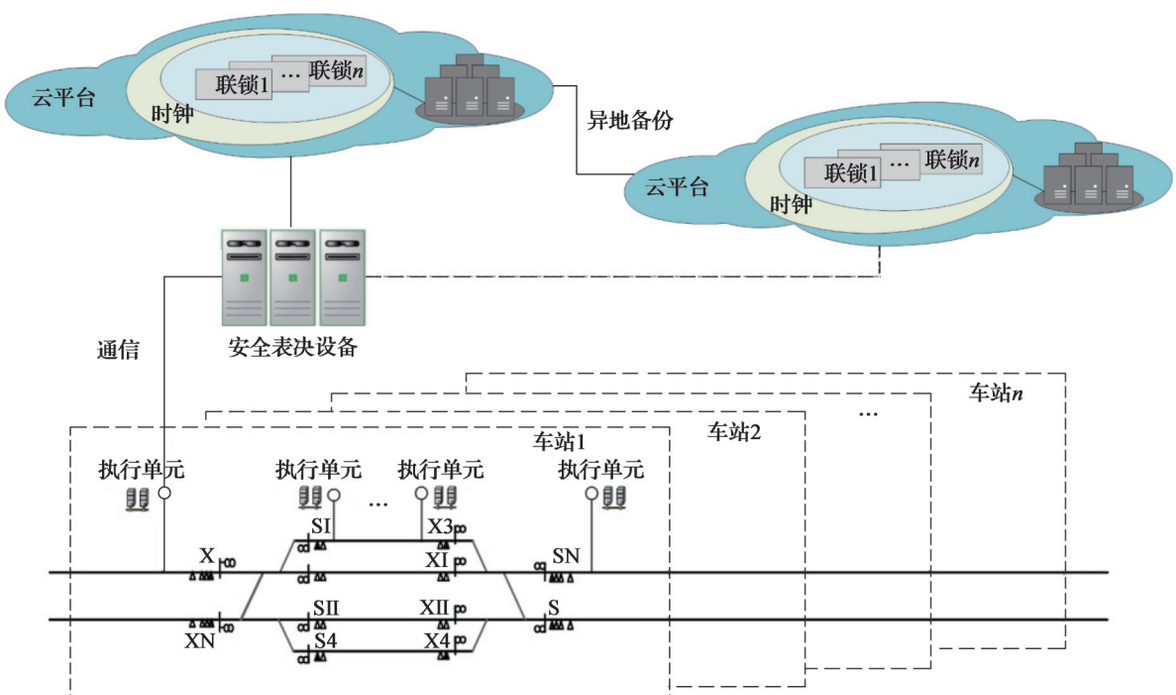


图3　云联锁总体结构

Fig. 3　Overall structure of cloud-based interlocking system

本节以最小冗余结构–具备容错机制的二取二（2oo2 FT）结构为例进行分析，其结构如图4所示。从形式上看，2oo2 FT结构与传统二乘二取二联锁系统结构相似，但其热备及切换机制与二乘二取二结构不同。以联锁应用1为例对该冗余结构进行说明，联锁应用1-1、1-1′、1-2和1-2′是同一车站4个相同的联锁应用（以下简称为1-1、1-1′、1-2和1-2′），分别位于不同的服务器集群中。1-1和1-2作为二取二中的两个子系，对于联锁应用执行功能，只有当这两个子系的联锁应用运算的结果经由SIL4级安全表决设备进行比较判决一致时，表决设备才能够执行输出，可以有效防止错误驱动的发生，达到故障导向安全的目的。1-1′和1-1构成双机热备子系统，若1-1或其所在的虚拟机发生故障，则虚拟机1-1′无缝接替虚拟机1-1继续运行，且虚拟机1-1′的工作状态（CPU、内存和存储等）与虚拟机1-1故障发生前一时刻的工作状态是相同的。1-1′和1-2重新组成二取二的两个子系，此时，1-2（工作正常）不会因为1-1发生故障而一并切换到1-2′。同理，1-2′和1-2的热备关系也是如此。

在软件配置方面，对承载联锁的系统采用基于虚拟机的容错技术，在主用虚拟机正常工作过程中，通过运用该容错技术，使得备用虚拟机不断和主用虚拟机在磁盘数据、内存状态数据和CPU寄存器数据上保持同步传输[6-8]。在主用虚拟机出现故障时刻前，备份虚拟机和主用虚拟机时刻保持同步，以确保备份虚拟机的实时性和准确性。备份虚拟机在主用虚拟机正常运行期间不对外提供服务，只对主用虚拟机运行状态进行监听，在发现主用虚拟机发生故障后，备份虚拟机立即启动代替主用虚拟机继续对外提供服务，在此过程中，用户感知不到虚拟机发生故障这一情况，实现联锁服务7×24 h正常运行，确保联锁应用服务的连续性，增加了系统的可用性。云平台的应用，实现在

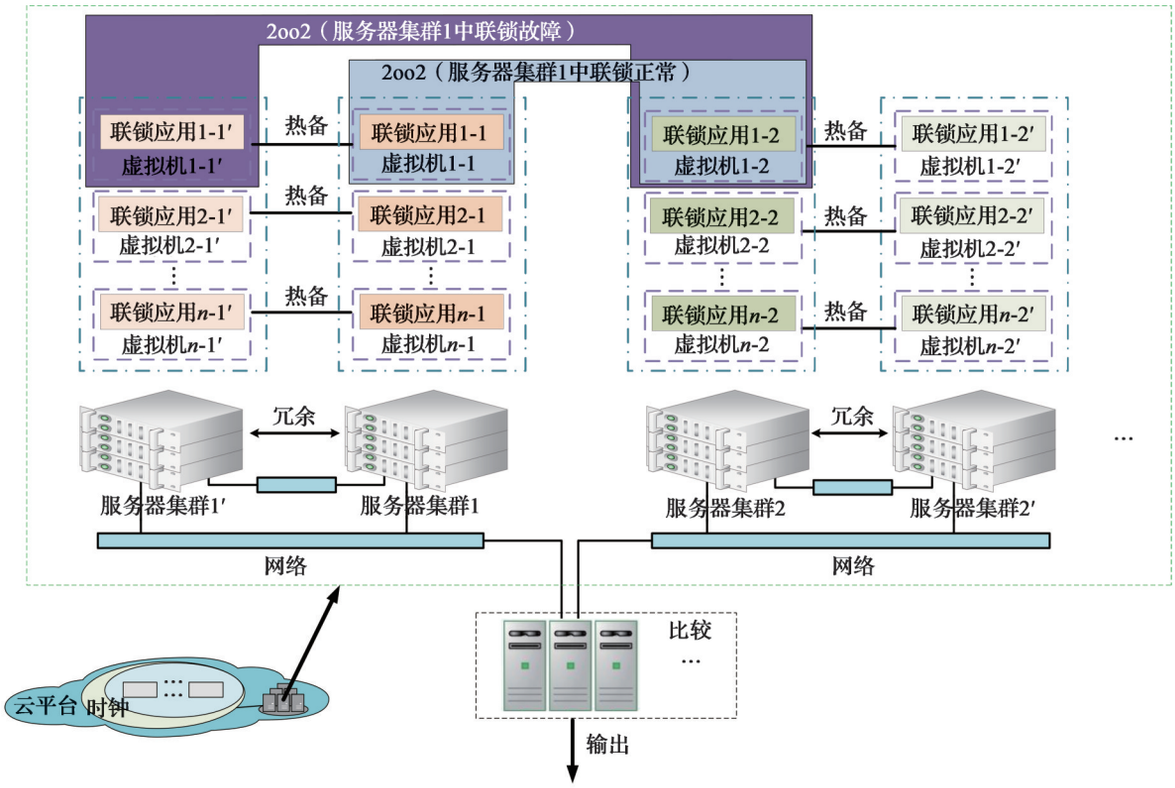


图4　2oo2 FT结构示意图

Fig. 4　Structure diagram of 2oo2 FT

单台服务器中部署多个不同车站的联锁应用，应用资源隔离和虚拟机迁移等技术，消除服务器单点故障等问题。资源隔离是将云平台中资源分隔为不同的服务器集群，将同一车站相同的联锁应用分别部署在云环境下不同的服务器集群中。每一个服务器集群采用不同的虚拟化方案，避免同一车站的联锁应用互相影响，由此出现因系统共因故障导致危险输出的问题。基于容错虚拟机，可构建二取二、三取二等多重冗余机制。若检测到虚拟机所在的服务器出现故障，在虚拟机热迁移和容错机制下，将虚拟机迁移到健康的服务器节点，在虚拟机迁移过程中运行的服务不会停止，同时不会因系统升级、维护影响系统运行，因此不会对铁路运营造成影响。虚拟机迁移情形如图 5 所示。

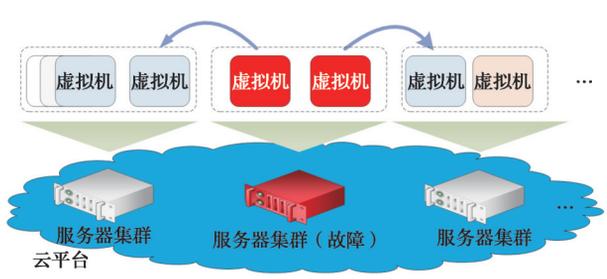


图5　服务器故障迁移示意图

Fig. 5　Schematic diagram of server fault migration

2.2　结构特点

在云平台中，运用冗余结构来实现不同的目标，例如提高可用性、检测和屏蔽故障以及系统扩展等。在冗余结构中，系统的安全关键功能“复制”在不同的计算单元上。冗余设计也有助于避免系统中的单点故障。

①高可用性系统的冗余：在此配置中，所有冗余节点同时激活并执行关键功能。负载在处于运行的计算节点(运行应用程序的所有相关镜像或副本)之间分配，如果一个计算节点出现故障，那么，故障计算节点的负载将被转移到其余的健康节点。这种配置为云联锁系统提供了高可用性。

②用于故障检测的冗余系统：在 *M*oo*N*（$M \leqslant N$）配置中的冗余系统提供故障检测。例如，在2oo2结构中，由两个独立的联锁应用处理相同的输入，产生的结果由表决设备进行比较。当表决设备检测到结果不一致时，该结果被标记为无效，同时平台将采取相应的故障处理操作。

③用于容错性的冗余：硬件容错（硬件故障裕度）是指部件或子系统在硬件出现一个或多个危险故障时，仍具备能继续执行所需安全功能的能力。硬件故障裕度为1意味着在一个拥有两个独立设备的结构中，当其中任意一个设备发生危险故障时不会阻止安全动作的执行。在三通道系统中，当有两个通道发生故障时，那么另外一个通道可继续执行安全功能，如果将该结构表示为 *M*oo*N*，则硬件故障裕度为 *N*−*M*。换言之，1oo3架构的硬件故障裕度为2，表明该结构可以承受2次故障并继续工作。表 1 列出了几种冗余体系结构的硬件故障裕度。

表 1　几种冗余体系结构的硬件故障裕度

Table 1　Hardware fault tolerance of different redundant architectures

冗余结构	硬件故障裕度
1oo2	1
2oo2	0
2oo3	1
1oo3	2

采用适合的冗余技术可提高系统的可用性，在虚拟机容错技术的支持下，可以在不影响系统正常运行的情况下对主虚拟机进行维护和升级。对于基于云平台的联锁系统而言，为运行的联锁应用创建多个备份虚拟机镜像，确保备用联锁应用和主控联锁应用之间的数据时刻同步，保障联锁应用能连续、不间断地提供服务。

3　云联锁 2oo2 FT 结构可靠性研究

3.1　2oo2 FT 结构分析

2oo2 FT 基本结构如图 6 所示，该冗余结构由 A1、A2、B1 和 B2 共 4 个具有相同联锁功能的单元组成，将容错机制具体描述为容错单元 S1/S2，A1 和 A2 在同一时刻只有 1 个联锁单元对外输出（其余联锁单元不对外提供联锁服务），A1 和 A2 之间通过容错单元进行热备。联锁单元 B1 和 B2 也是如此。以 A1 和 B1 组成二取二提供联锁服务为例，两个联锁单元同步执行相同的联锁运算，A2 和 B2 分别对 A1 和 B1 进行热备，当 A1 和 B1 的数据处理经 V 比较一致时对外输出，若 A1 或 B1 发生故障，容错单元 S1/S2 将故障单元切除，并切换到备用 A2/B2 单元，备用单元无缝替代故障单元继续输出运算结果并与另一组中正常的工作单元的运算结果进行比较，作为 2oo2 FT 结构的输出[9]。

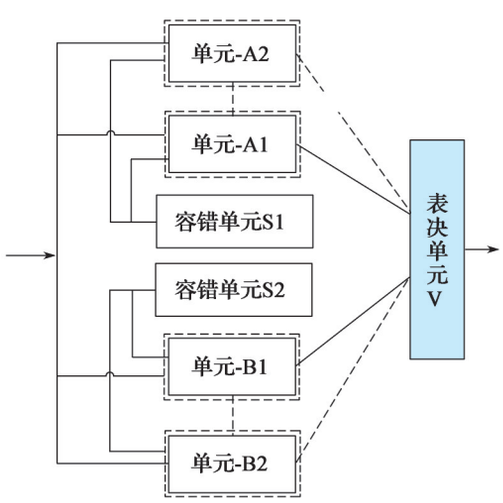


图 6　2oo2 FT 基本结构

Fig. 6　Basic structure of 2oo2 FT

3.2　2oo2 FT 冗余结构分析基本假设 Redundant

在 2oo2 FT 结构中，对同一站联锁应用进行冗余配置，此外，同站联锁应用必须分布在不同的服务器中，即使服务器发生故障，在容错机制下，虚拟机和其中运行的联锁应用可迁移到其他完好的服务器中，且迁移过程中，虚拟机和联锁应用不会停止运行。从这个角度来说，服务器硬件对系统造成的影响较小。对容错单元建立在线监测机制，实现故障及时维护。对于云平台的管理软件、虚拟化软件等，都采取冗余配置，避免单点故障。

为简化分析过程，明确分析内容，对于上述系统进行了如下简化和假设[10]：

①云平台中不同服务器集群各个单元失效率相互独立，在不考虑共模故障时，某一时刻只有一个单元发生失效；

②考虑云平台中不同服务器集群中各个单元（容错单元和表决单元等）因相同错误结果导致的多重非共因故障；

③为便于分析，对于表决单元和容错单元，不设置相应的故障诊断电路，故将表决单元和容错单元的失效认为是不可测失效；

④2oo2 FT 系统初始状态为正常工作状态。

3.3　故障树分析

云平台容易受到硬件、软件、网络和 IO 故障的影响。这些故障会影响云平台的性能，同时也会降低运行应用程序的性能[11-12]。文献[13]指出，在导致云平台故障的各种影响因素中，硬件故障占比约为 38.9%，而软件故障约为 3.8%，网络中断和电源故障约为 1.3%。联锁系统的可靠性很大程度上取决于其依托的硬件的可靠性。本文主要针对云平台的硬件方面，针对其冗余结构进行分析。

以服务器故障为例，服务器故障主要分为硬件故障、系统崩溃、网络中断和输入输出故障子事件。对以上事件发生的原因进行进一步分析。硬件故障的基本事件包括电源故障、电路板故障和驱动程序故障；系统崩溃的基本事件包括应用程序崩溃、操作系统崩溃和虚拟机崩溃；网络中断的基本事件为通信故障、软件问题和计划中断；输入输出故障的基本事件分为硬盘问题、光纤问题和 SAN 问题。构建服务器失效故障树如图 7 所示。

服务器产品常用 λ_{AFR}（年化故障率）和 t_{MTBF}（平均无故障工作时间）指标定义故障概率[如式(1)]，如企业级服务器硬盘的 MTBF 达到了 10^6 h（故障率为 0.87%/年）。

$$\lambda_{AFR}=\frac{1}{\frac{t_{MTBF}}{8760}}\times 100 \tag{1}$$

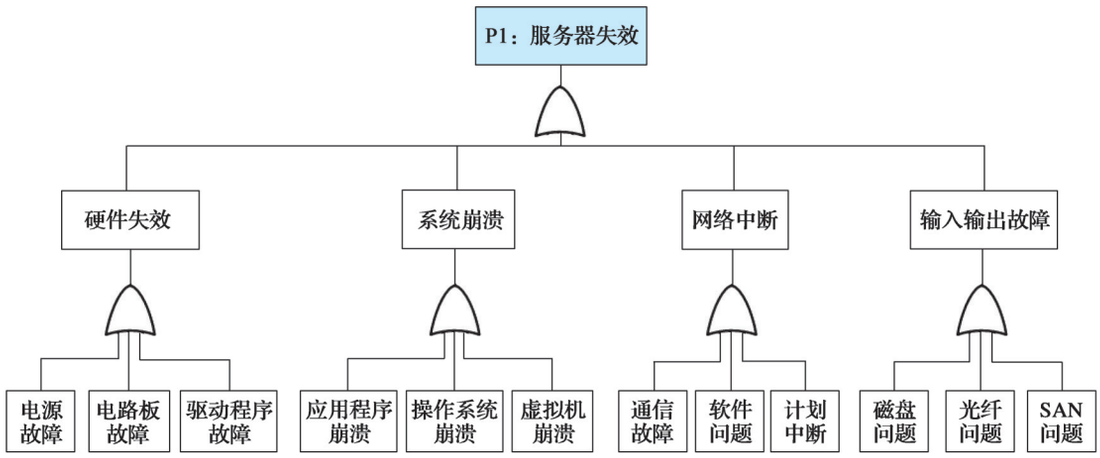


图7　服务器故障树

Fig. 7　Schematic diagram of server fault tree

系统崩溃是导致云平台故障最严重的原因。系统崩溃的原因包括应用程序崩溃、操作系统崩溃和虚拟机崩溃。其中，导致应用程序崩溃原因可分为分段故障、无效系统调用和参数错误；操作系统崩溃的原因包括注册表损坏、驱动程序损坏和内核错误；虚拟机崩溃的原因包括资源争用、虚拟机映像损坏和虚拟机重启[14]。系统崩溃的故障树如图 8 所示。

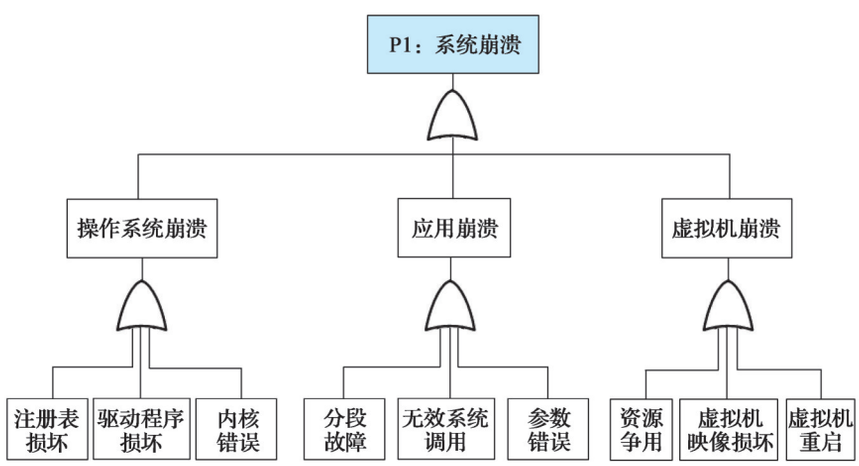


图8　系统崩溃故障树

Fig. 8　Schematic diagram of fault tree for system crash

通过对服务器故障树进行分析，对服务器故障进行估计。服务器故障概率为

$$P_{(\mathrm{Se})}=\sum_{i=1}^{4}P\left(S_i\right)-\left[\left(\sum_{i=1}^{3}P\left(S_i\right)\cdot P\left(S_{i+1}\right)\right)-\left(P\left(S_1\right)\cdot P\left(S_4\right)\right)\right] \tag{2}$$

式中：$P(S_i)$，i=1，2，3，4，分别为硬件故障、系统崩溃、网络中断和输入输出故障的概率。

系统崩溃故障的概率为

$$P(S_2)=\sum_{i=1}^{3}P\left(L_i\right)-\left[\left(\sum_{i=1}^{2}P\left(L_i\right)\cdot P\left(L_{i+1}\right)\right)-\left(P\left(S_1\right)\cdot P\left(S_3\right)\right)\right] \tag{3}$$

式中：$P(L_i)$，i=1，2，3，分别为操作系统崩溃、应用程序崩溃和虚拟机崩溃的概率。

同理可求硬盘失效、网络中断和输入输出故障的概率。

设$R(t)$表示服务器Se的可靠性，$P_{(\mathrm{Se})}$表示服务器在时间t发生故障的概率。式(4)给出了服务器的可靠性$R_s(t)$。

$$R_s(t)=1-P_{(\mathrm{Se})} \tag{4}$$

在(t，$t+\Delta t$)时刻的失效率$\lambda(t)$为

$$\lambda(t)=\frac{\mathrm{d}\left(P_{(\mathrm{Se})}\right)}{R_s(t)} \tag{5}$$

3.4　云联锁动态故障树模型的建立与评估

基于上述分析，对2oo2 FT系统进行进一步研究。将系统故障状态区分为系统故障–安全状态、系统危险状态(A1、A2、S1和S2发生危险输出导致系统处于危险状态)。得到动态故障树系列模型如图 9 和图 10 所示。2oo2 FT云联锁工作模式分析情况如表 2 所示。

表2　2oo2 FT云联锁的工作模式分析

Table 1　Analysis of operational modes for 2oo2 FT cloud-based interlocking

故障说明	系统状态
I组无故障，S1发生不可测故障，V无故障	由S1的失效状态决定
I组无故障，S1无故障，V发生不可测故障	由V的失效状态决定
I组A1发生可测故障，S1无故障，V发生不可测故障	由A1与V的失效状态共同决定
I组A2先发生不可测故障，A1后发生不可测故障，S1无故障，V发生不可测故障	由A1和V的失效状态共同决定
I组A1发生不可测故障，S1无故障，V发生不可测故障	由A1与V的失效状态共同决定
I组A2先发生可测故障	系统正常
I组无故障，V无故障，II组无故障	系统正常
I组A2发生可测故障，S1无故障，V无故障，A1无故障	系统正常
I组A2发生不可测故障，S1无故障，V无故障，A1无故障	系统正常
I组A2发生可测故障，S1无故障，V无故障，A1发生故障	由A1的失效状态决定
I组A2发生不可测故障，S1无故障，V无故障，A1发生故障	由A1的失效状态决定
I组A2发生可测故障，S1无故障，V无故障，II组B1/B2共因失效	由B1和B2的失效状态共同决定
I组A2发生不可测故障，S1无故障，V无故障，II组B1/B2共因失效	由B1和B2的失效状态共同决定
I组A2先发生不可测故障，A1后发生不可测故障，S1无故障，V无故障	由A2的失效状态决定
I组A2先发生不可测故障，A1后发生可测故障，S1无故障，V无故障	由A2的失效状态决定
I组A1发生可测故障，S1发生不可测故障	由A1与S1的失效状态共同决定
I组A2先发生不可测故障，A1后发生不可测故障，S1发生不可测故障，V无故障	由A1和S1的失效状态共同决定
I组A2先发生不可测故障，A1后发生可测故障，S1发生不可测故障，V无故障	由A1和S1的失效状态共同决定
I组A1发生不可测故障，S1发生不可测故障，V无故障	由A1与S1的失效状态共同决定
I组A2先发生不可测故障，A1后发生可测故障，S1无故障，V发生不可测故障	由A1和V的失效状态共同决定
I组A1和A2共因失效，S1无故障，V无故障	由A1和A2的失效状态决定

注：A1和A2为I组，B1和B2为II组，S1为容错单元，V为表决单元。

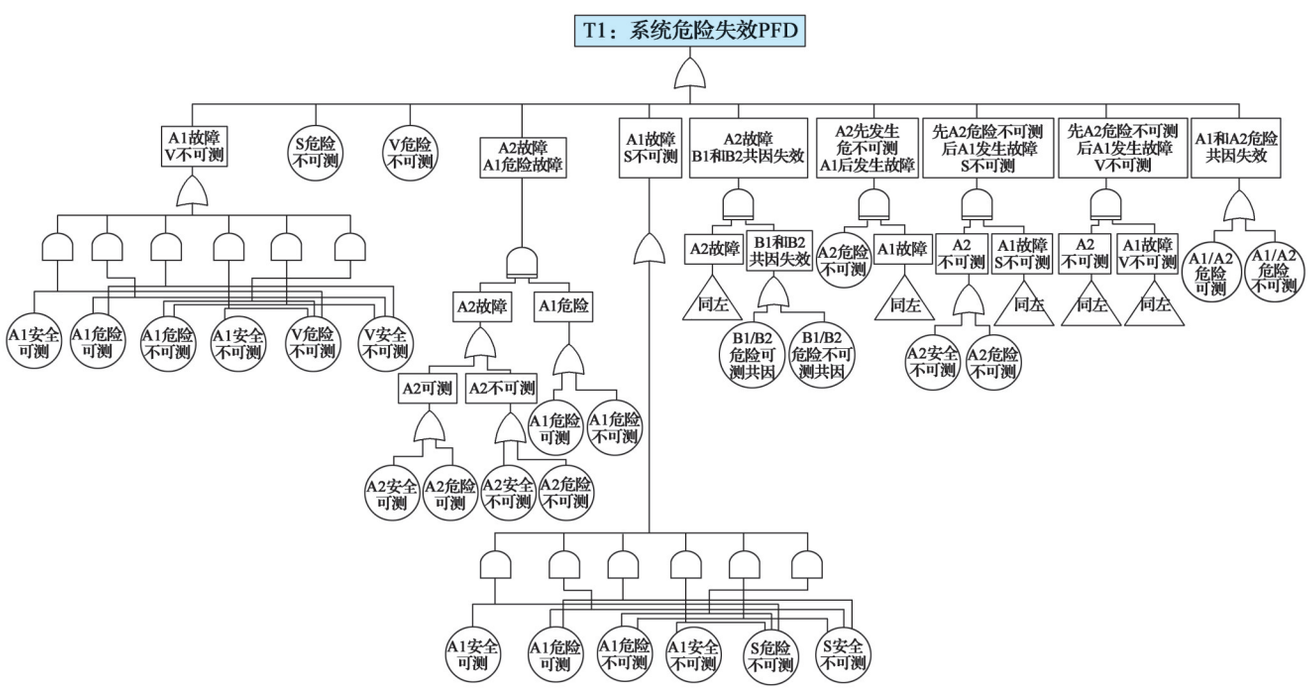


图9　2oo2 FT云联锁的PFD动态故障树模型

Fig. 9　Dynamic fault tree model of PFD for 2oo2 FT cloud-based interlocking system

在计算安全冗余结构可靠性的过程中，由于计算模型创建不完整、人为的计算错误、各输入参数的假定约束条件等因素，会导致最终的计算结果产生不确定性。根据IEC 61508安全标准及相关文献[15-17]，IEC 61508根据历史统计数据，对危险失效率λ_D给出了推荐值的取值范围，λ_D可以选择服从三角分布，λ_D ~ T(a,c,b) ~ T(5E-8,1E-6,2.5E-5)；对于共因失效因子β，由于缺少历史统计数据支持，应该选择一个较大取值分布范围[18]，选取(2%~20%)作为β的取值范围，即β ~ U(0.02 , 0.2)；对于故障诊断覆盖率α_c，将α_c的取值范围

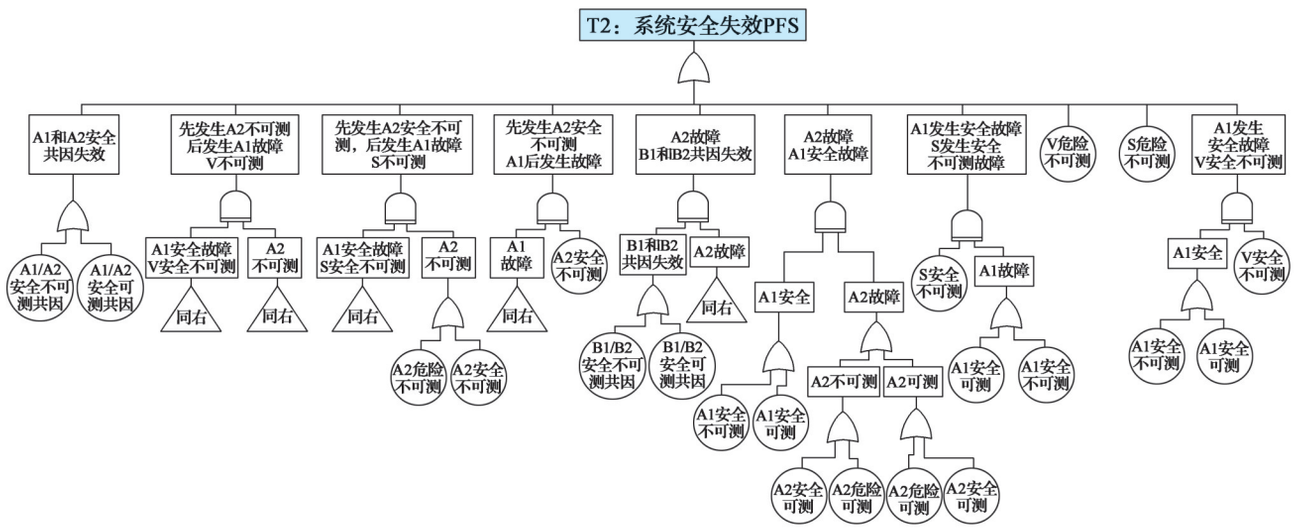


图 10　2oo2 FT 云联锁的 PFS 动态故障树模型

Fig. 10　Dynamic fault tree model of PFS for 2oo2 FT cloud-based interlocking system

规定为 90%~99% 区间内均匀分布，即 $\alpha_c \sim U(0.90, 0.99)$；定期维修周期取固定值 8 760 h。

IEC 61508 列出了可靠性分析措施，其中有提及蒙特卡洛模拟方法[15]。蒙特卡洛分析方法将安全性、可靠性计算的问题以统计量的形式进行描述，其以概率分布为研究对象，通过随机抽样并计算样本统计值，以估计目标变量的特性或值。蒙特卡洛分析方法基于概率统计学理论，借助随机抽样和统计试验的手段，获得目标对象的估计值以及置信区间，广泛应用于不确定性计算、风险评估等领域。蒙特卡洛方法不仅可以用来计算安全完整性等级（SIL），还能够处理可靠性数据的不确定度。本节通过蒙特卡洛法对云联锁冗余结构进行分析，将基于虚拟机容错的热备方案应用于二取二和三取二结构中，并进行仿真分析，结果如图 11 所示。从图 11 可以看出，在云平台中应用容错技术条件下，三取二结构可靠性总是大于二取二结构。采用云计算技术，从可靠性角度考虑，云平台更适用于多重冗余结构。

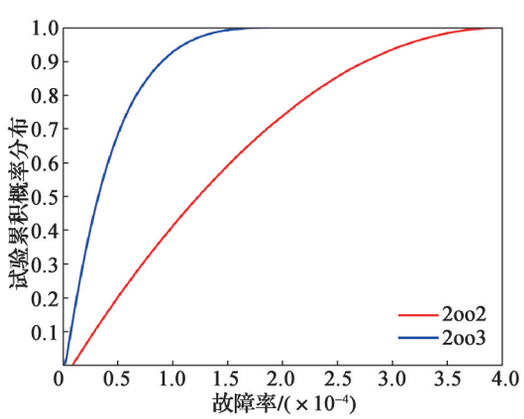


图 11　二种结构故障率比较

Fig. 11　Comparison of the failure rate of the two structures

4　结论

本文根据计算机联锁系统不同冗余结构特点，结合云平台特性，提出了基于虚拟机容错的 2oo2 FT 冗余结构的云联锁方案，并以最小冗余结构 2oo2 FT 冗余结构为例，对该冗余结构的特点进行了分析，2oo2 FT 采用了具有 SIL4 级安全完整性等级的表决单元实现对云平台数据的安全表决和安全协议解析的功能，具有冗余度更高、可用性更好和维护更便利的特点。运用动态故障树分析 2oo2 FT 冗余结构的云联锁系统的工作情况，采用优先与门表示事件之间发生的关系，建立了故障模式下云联锁系统的 PFD 和 PFS 动态故障树模型，对基于容错的云联锁冗余结构的云联锁可靠性进行了分析，分析结果表明，从可靠性角度出发，云联锁更适合采用多重冗余结构。随着技术的不断进步，作为面向未来联锁系统的发展方向之一，云联锁将会极大程度改变信号系统维护的工作方式，增强我国高速铁路信号系统的核心竞争力。

参考文献：

[1] HUANG Lujiang. The past, present and future of railway interlocking system[C]//IEEE. 2020 IEEE 5th International Conference on Intelligent Transportation Engineering. Beijing: IEEE, 2020: 170-174.

[2] VAN DONGEN S F M, CANTEKIN S, ELEMANS J A A W, et al. Functional interlocked systems[J]. Chemical society reviews, 2014, 43(1): 99-122.

[3] ATHAVALE J, BALDOVIN A, PAULITSCH M. Trends and functional safety certification strategies for advanced railway automation systems[C]//IEEE. 2020 IEEE International Reliability Physics Symposium. Dallas, TX: IEEE, 2020: 1-7.

[4] 王培. 铁路计算机联锁系统仿真测试平台的研究[J]. 机车电传动, 2019(3): 148-150.
WANG Pei. Research on computer interlocking system simulation and test platform[J]. Electric drive for locomotives, 2019(3): 148-150.

[5] 中国铁路总公司. 计算机联锁系统[M]. 北京: 中国铁道出版社, 2015: 48-60.
China Railway Corporation. Computer interlocking system [M]. Beijing: China Railway Publishing House, 2015: 48-60.

[6] 万仔仁. 基于KVM虚拟机双机热备技术研究与实现[D]. 武汉: 华中科技大学, 2015.
WAN Ziren. Research and implementation of virtual machine hot standby system based on KVM[D]. Wuhan: Huazhong University of Science and Technology, 2015.

[7] ITO M, HE Fujun, OKI E. Backup resource allocation of virtual machines for probabilistic protection under capacity uncertainty[J]. IEICE transactions on communications, 2022, E105.B(7): 814-832.

[8] FARZANEH S M, FATEMI O. HRAV: Hierarchical virtual machine placement algorithm in multi-hierarchy RF cloud architecture[EB/OL]. (2023-01-16) [2023-09-22]. https://doi.org/10.21203/rs.3.rs-2466859/v1.

[9] 北京全路通信信号研究设计院有限公司. 铁路车站计算机联锁技术条件: TB/T 3027—2015[S]. 北京: 中国铁道出版社, 2016.
CRSC. Computer based interlocking technical specifications: TB/T 3027—2015[S]. Beijing: China Railway Publishing House, 2016.

[10] 许崇. 二乘二取二系统的可靠性和安全性[D]. 合肥: 合肥工业大学, 2013: 10-35.
XU Chong. Reliability and safety of double 2-vote-2 redundancy system[D]. Hefei: Hefei University of Technology, 2013: 10-35.

[11] ATTALLAH S M A, FAYEK M B, NASSAR S M, et al. Proactive load balancing fault tolerance algorithm in cloud computing[J]. Concurrency and computation: practice and experience, 2021, 33(10): e6172.

[12] XU Limin, WANG Suoping, GAO Ping, et al. The method of realize the cloud based generic function safety platform [C]//Springer. 2021 6th International Conference on Intelligent Transportation Engineering. Beijing: Springer, 2021: 600-608.

[13] LEELIPUSHPAM G J, JEBADURAI I J, JEBADURAI J. Fault tree analysis based virtual machine migration for fault-tolerant cloud data center[J]. Journal of integrated design and process science, 2019, 23(3): 73-89.

[14] GALA G, CASTILLO RIVERA J, FOHLER G. Work-in-progress: cloud computing for time-triggered safety-critical systems[C]//IEEE. 2021 IEEE Real-Time Systems Symposium. Dortmund: IEEE, 2021: 516-519.

[15] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems: IEC 61508: 2010 [S]. Geneva: IEC, 2010.

[16] WANG Haifeng, LI Wei. Component-based safety computer of railway signal interlocking system[C]//IEEE. 2008 ISECS International Colloquium on Computing, Communication, Control, and Management. Guangzhou: IEEE, 2008: 538-541.

[17] 闫剑平, 汪希时. 两种方式双机热备结构的可靠性和安全性分析[J]. 铁道学报, 2000, 22(3): 124-127.
YAN Jianping, WANG Xishi. Reliability and safety analysis of two modes of dual module hot spare architecture[J]. Journal of the China railway society, 2000, 22(3): 124-127.

[18] KING A G. SIL determination: recognising and handling high demand mode scenarios[J]. Process safety and environmental protection, 2014, 92(4): 324-328.

收稿日期：2023-07-07
修回日期：2023-10-10