广西科学院学报
Journal of Guangxi Academy of Sciences

2017,33(1):53～58,64
Vol. 33, No. 1 February 2017

网络优先数字出版时间:2017-02-27 **DOI:10.13657/j.cnki.gxkxyxb.20170227.001**
网络优先数字出版地址:http://kns.cnki.net/kcms/detail/45.1075.N.20170227.1538.002.html

基于 CMDB 的规则推理的故障定位技术
Research on Fault Location of Information System based on CMDB and Rule Inference

曾明霏,谢朋宇
ZENG Mingfei, XIE Pengyu

(广西电网有限责任公司信息中心,广西南宁 530022)
(Information Center of Guangxi Power Grid Ltd., Co., Nanning, Guangxi, 530022, China)

摘要:【目的】帮助系统管理员从复杂的结构中寻找系统故障的根源,以进一步提高电网管理信息系统的可靠性。**【方法】**将配置管理数据库(Configuration management database,CMDB)结合故障树分析法(Fault tree analysis,FTA)进行故障规则推理,再通过 CMDB 确定故障设备之间的关系,从而通过监控告警结合故障规则分析定位到故障根源,并进行实例验证。**【结果】**基于 CMDB 的规则推理的故障定位技术可以有效地梳理信息系统各功能组件和故障表征之间的关系,实现快速故障定位。**【结论】**该技术可有效提高系统的可用率和运行率。

关键词:CMDB 配置管理 配置模型 故障规则 故障定位
中图分类号:TP39 **文献标识码:**A **文章编号:**1002-7378(2017)01-0053-06

Abstract:【Objective】Helping the system administrator to locate the source of system failure from complex system architecture, we can improve the reliability of information system in power grid corporation. **【Methods】**The configuration management database (CMDB) is combined with the fault tree analysis method to analyze the fault rules, and then the relationship between the faulty devices is determined by the CMDB. Finally the fault location is achieved and the instance is verified by monitoring warnings and fault analysis. **【Results】**This method can effectively sort out the relationship between the functional components and fault representation of the information system. We apply it in the core information system of Power Grid Corp. **【Conclusion】**The fault location can be done in a short time, which can effectively improve the system's availability and operating efficiency.

Key words:CMDB, configuration management, configuration model, fault rule, fault location

0 引言

【研究意义】信息系统是由网络与通讯设备、物理服务器、虚拟服务器、存储资源、平台软件、应用软件、信息资源等组成的以处理信息流为目的的人机一体化系统。电网企业的管理信息系统储存着企业的核心数据,为电网的生产、经营和管理提供全方位的保障。一旦管理信息系统出现故障,很可能会影响电网各项核心业务的正常开展,进而造成更严重的社会影响。因此,这些大型的信息系统为了保证可靠性和性能,往往有着复杂的内部结构。这些结构也给信息系统的故障定位带来很大的困难。如何帮助系统管理员从复杂的结构中寻找系统故障的根源,是进一步提高电网管理信息系统可靠性的必要条件。**【前人研究进展】**目前,国内外对信息系统故障定位的相关研究主要是基于配置管理数据库(Configuration management database,CMDB)和故障树分析法(Fault tree analysis,FTA)两大理论基础开展分析。范娟娟等[1]、刘权[2]和黄波[3]分别提出了一种基于 CMDB 的业务可用性评估方法。该

收稿日期:2016-12-20
作者简介:曾明霏(1984－),男,博士研究生,工程师,主要从事信息系统运维管理,E-mail:zeng_mf.xt@gx.csg.cn。

方法充分利用CMDB丰富的数据模型，将应用基础架构和它们对业务服务的影响映射起来，可以缩短信息系统平均故障定位时间。徐定杰等[4]和董朝阳等[5]均认为通过CMDB配置项关系有向图调查基础设施及其可用信息分析事件关联关系，可对事件进行智能多层分析、建立关联以过滤冗余事件、提炼主要信息，从而确定事件背后存在的问题。同样地，马秀丽等[6]通过知识库定义IT环境中业务的类别和运行的流程，对业务数据建模，形成业务数据配置项，依靠业务和设备信息配置项的联结，自动判断节点间依赖关系，快速定位业务及设备故障根源。蔡宗平等[7]采用故障树分析法构造一个专家系统进行信息系统故障诊断，并描述了此专家系统的基本设计构想及实现方法。类似的还有卢燕等[8]和吴明强等[9]的研究等。邓歆等[10]的研究则是在通信网络中使用告警相关性分析的方法，从大量的告警中找出根源告警。**【本研究切入点】**由于CMDB数据和FTA分析并非尽善尽美，因此信息系统智能故障定位在实现时不能照搬理论框架，必须有所取舍，并加入专家系统和主动数据采集模块以弥补数据不完善带来的不良影响。同时，主动数据采集模块采用通用设计，除了数据采集外还能完善其他功能，为系统功能扩展提供基础。在信息系统中，各种软硬件都是以完成业务需求为目的进行安装部署，各种软硬件信息及相互的关系无直观统一的描述及展现。当故障发生后，无法直观的判断故障根源以及影响范围，运维人员需要凭经验或逐一排查系统软硬件故障。依托CMDB，将运维人员的故障排查经验梳理成故障规则，结合CMDB中配置项(Configuration item，CI)的关系数据，可以提高故障事件定位的准确性，快速准确的定位故障原因和评估影响范围，实现网管系统对事件的丰富和关联分析等功能，有效的改善网管系统的监控和分析能力。**【拟解决的关键问题】**本研究提出一种基于CMDB的规则推理的故障定位技术，主要是利用CMDB存储的CI之间的关联关系，构建CI网络模型，当CI本身或关联属性出现故障时，通过故障树分析法(FTA)进行规则推理，遍历CI树型结构，从而找出故障根源。

1 基于CMDB的规则推理模型构建

如图1所示，故障定位的基础是CMDB，从CMDB可以得到CI关系网、CI属性集和CI-服务模型。CI关系网按照信息系统的维度进行裁剪，每个信息系统裁剪成一棵信息系统CI树。通过专家经验，将CI关系与故障树的故障规则一一对应。信息系统CI树的CI关系替换为故障树的故障规则即可生成FTA故障树。

FTA故障树以信息系统CI为根，树中的节点是信息系统各组成部分的CI。非叶子结点CI的运行状态由下级CI的运行状态通过FTA推理机推导得到。叶子节点CI的运行状态由实际采集到的监控数据确定。在理论上，以叶子结点CI的运行状态(即CI属性集的子集)为输入，通过FTA故障树进行逻辑推理，可以推导出所有上级CI的运行状态，即信息系统各个组成部分的运行状态。故障的组件和正常的组件均可以通过运行状态计算出来，实现故障定位，定位的精度可达到CI级。

CI-服务模型则是用于故障影响分析。完成故障定位后，有故障的CI对应的服务就是受到影响的服务。受影响的服务主体的集合就是故障的影响范围。

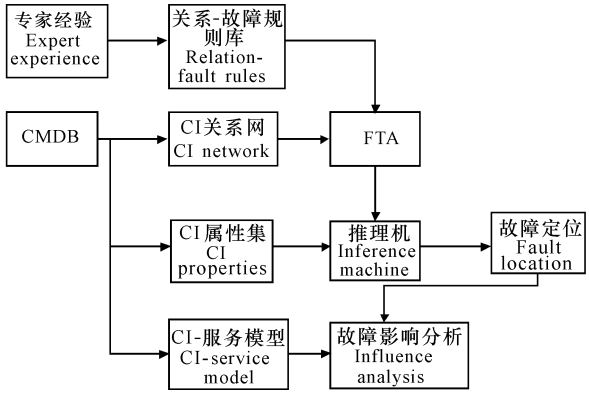

图1 信息系统故障定位理论框架

Fig. 1 Framework of fault location system

2 基于CMDB的规则推理实现

2.1 系统架构

如图2所示，信息系统故障定位系统的系统架构分为数据采集与适配、数据模型、应用功能、应用呈现4层。

数据采集与适配层负责现有CMDB数据采集和标准化工作，含采集和标准化两个子层。电网企业内部已实现包含了CMDB的IT服务管理系统，但其CMDB数据仅包含了图1模型中的分类与静态属性部分，关系、操作和动态属性的数据都不完整。因此，采集层除了从已有系统中采集信息外，还包含一个Agent端，该Agent端既可采集不完整的数据，也可执行相关脚本，为作业执行、故障自动处理等高级功能提供技术支撑。采集到的数据分为静态数据和动态数据。静态数据用于标准化为CMDB

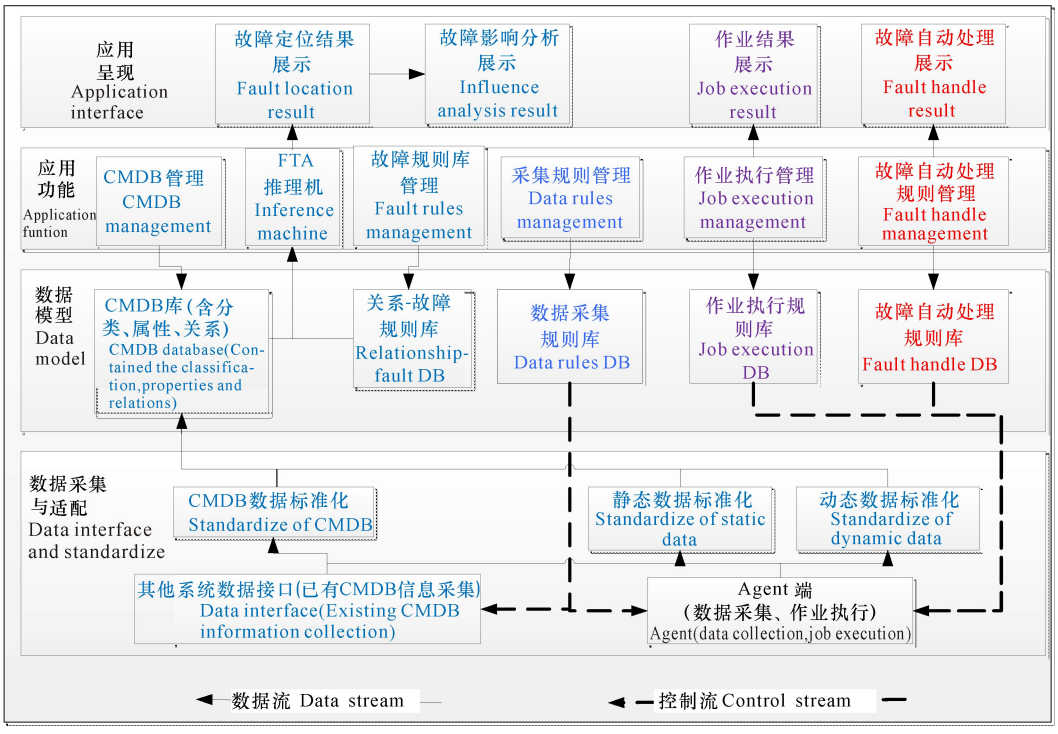

图 2 信息系统故障定位系统架构图

Fig. 2 System architecture of fault location system

库,即 CI 的技术参数属性;动态数据是故障定位需要的数据,即 CI 的运行状态属性。

数据模型层包含 CMDB 库、关系-故障规则库、数据采集规则库、作业执行规则库和故障自动处理规则库。CMDB 库是该层的核心,包括模型中的分类、属性和关系数据。它将数据采集层采集到的数据汇总,并通过 CMDB 管理功能提供数据录入的接口,以便人工修正可能影响故障定位的问题数据。此外,CI 关系网按照信息系统维度裁剪的需求也在 CMDB 库中实现,为故障定位提供技术保障。关系-故障规则库的功能和理论框架一致,实现将各类 CI 关系转化为 IF-THEN 条件转移结构的功能。这个库是专家经验的核心,通过故障规则库管理功能手工录入。数据采集规则库存储的是各类数据采集的方式和频率等信息。数据采集管理功能根据这个库存储的信息控制数据接口和 Agent 端的数据采集工作。作业执行规则库和故障自动处理规则库则存储了对应功能所需的数据。

应用功能层除了对应的数据管理功能外,还有一个 FTA 推理机的功能。该功能是故障定位的核心功能,将专家经验和 CMDB 库结合,自动进行故障树分析,实现故障定位。

应用呈现层包含故障定位结果展示、故障影响分析展示、作业结果展示、故障自动处理展示 4 个展示功能,用于展示各个系统功能的执行结果。

2.2 系统功能

信息系统故障定位系统主要包括故障定位及影响分析、作业执行、故障自动恢复和 Agent 端 4 个功能。其中,Agent 端相对独立,安装在目标信息系统的相关服务器上,根据系统的要求在目标信息系统上执行相应的命令,是各个功能的实现的基础。故障定位及影响分析是本系统的核心功能,它的各个组件的功能和相互关系在前文已有介绍,这里不再重复。

作业执行是通用 Agent 端在目标信息系统上执行标准作业的模块。每个信息系统都有其标准作业,例如启动、停止、巡检、定期维护等。这些作业很重要又很繁琐,必须按照作业指导书的要求执行。但是由人执行的操作总会存在遗漏或差错的可能,进而影响系统的运行。作业执行功能就是将目标信息系统的标准作业操作通过脚本的形式固化在作业执行规则库中,并设定好执行的周期或条件。当作业执行管理模块检测到符合条件时,自动调用脚本通过 Agent 端在目标服务器上执行,并自动采集执行结果,实现作业指导书在执行层面的标准化,减少系统管理员执行遗漏或者差错,提高信息系统的维护水平。

故障自动恢复功能用于自动/半自动地恢复一

些简单故障。它的实现和作业执行功能类似。首先针对一些简单故障,预先编制故障处理脚本,例如清理磁盘空间的脚本、增加数据库表空间的脚本、重启中间件特定节点的脚本、回滚死锁数据库进程的脚本。这些脚本存储在故障自动处理规则库中,然后设定这些脚本的执行条件,可以和故障定位结果联动,最后检测脚本执行的条件是否满足,满足即通过 Agent 端在目标服务器上执行脚本,并采集执行结果。该功能实现了部分故障的自动处理,可以大大提高系统故障处理的效率,并且可以通过脚本实现故障处理经验的积累与分享。

2.3 CMDB 库的构建

构建 CMDB 库,通过对 IT 信息系统进行梳理,明确故障定位的逻辑与可定位的对象,去除非关注的 CI 信息,尽可能的降低 CI 复杂度,以分析与定位故障为目标,根据 IT 信息系统软硬件特点构建 CMDB 模型,如图 3 和图 4 所示。

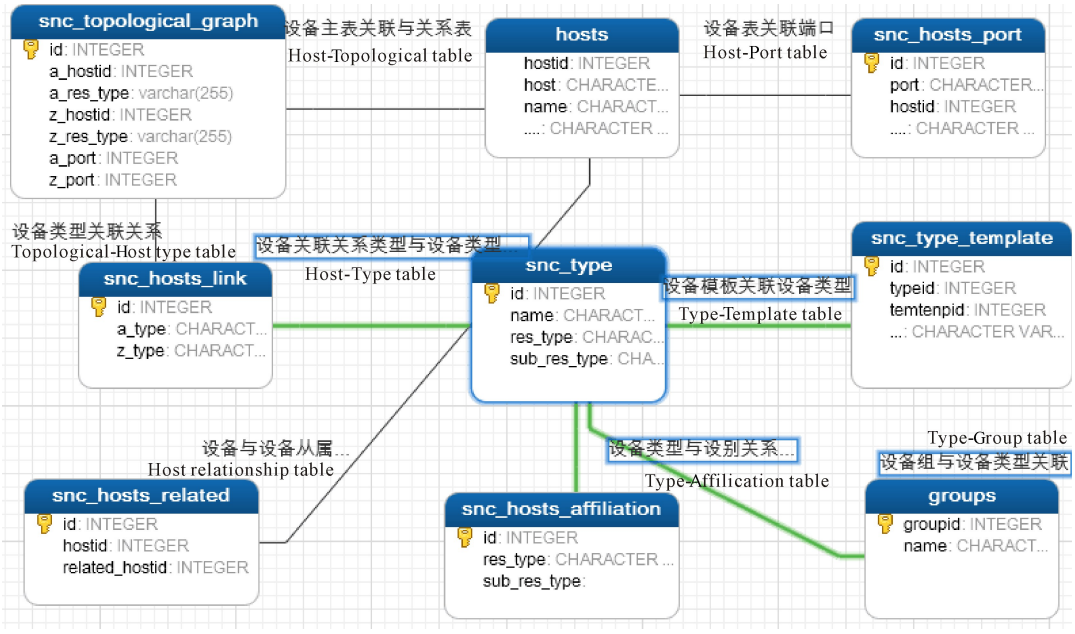

图 3 CMDB 库主要模型表

Fig. 3 Primary model of CMDB

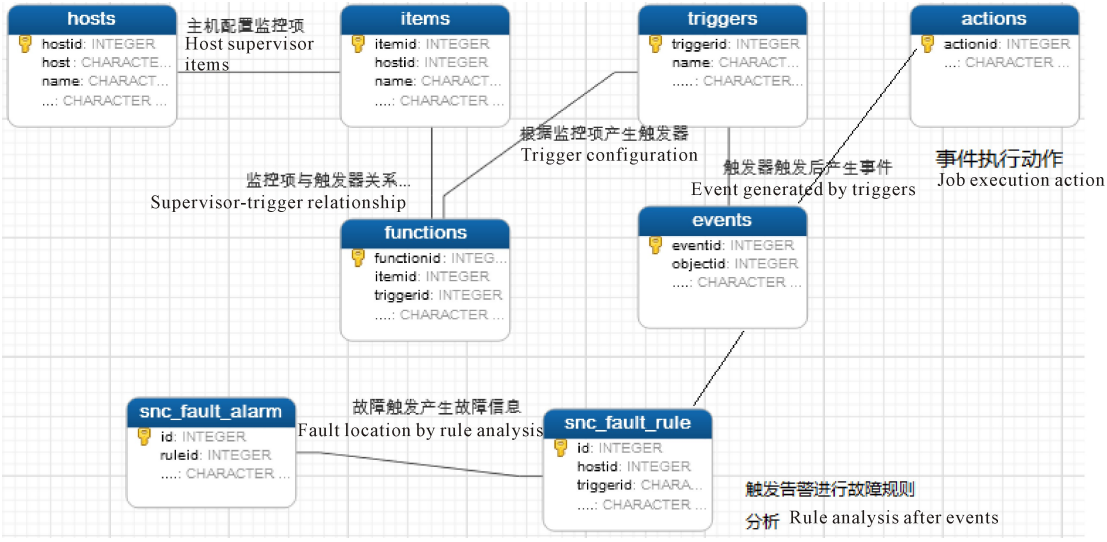

图 4 CMDB 库 ER 图

Fig. 4 E-R diagram of CMDB

2.4 推理机的实现

推理机主要通过告警事件分类、告警事件预处理、规则推理 3 大功能实现。其中,告警事件分类和告警事件预处理理论已比较成熟,本研究采用邓歆等[10]提出的告警相关性分析规则。规则推理则是使用故障树分析法得到的故障规则进行推理。

告警事件分类:在做规则推理分析之前,对采集上来的信息进行统一格式化处理,格式化后的信息大体上具有如下信息:告警时间、告警对象名称、告警级别和告警描述等,然后对格式化后的信息进行事件规则推理分析。事件通常包括(1)相同事件,指来自同一告警源的相同故障描述的持续告警信息;(2)相反事件,指两个来自同一告警源的信息,一个说明告警,另一个说明告警已恢复;(3)同源事件,指来自同一告警源,但不同告警类型的多个信息;(4)拓扑关系事件,指来自不同且有拓扑连接关系的告警源,告警类型相同或不同的多个信息。

告警事件预处理:(1)对相同事件,认为频度发生变化的同一个告警信息,只显示一条故障信息;(2)对于相反事件,将这两个信息关联起来,自动将相应的告警事件清除,并存入已清除的历史告警页面中,不产生故障事件;(3)对于同源事件,通过相关规则的定义,将其中一条根源性的告警挑选出来,产生故障事件,并将其它的同源事件定义为被抑制信息;(4)对于拓扑关系事件,利用 CMDB 中 CI 关系模型为依据,通过相关规则的定义推理,挑选出最具根源性的告警或产生一条根源性告警,同时将其它的拓扑关系事件定义为被抑制信息,只产生一条根源故障事件。

规则推理实现:(1)在应用程序中调用规则引擎提供的相应的接口以创建规则引擎对象、工作内存对象和规则集对象;(2)监控对象告警数据采集上来后经过处理加入到规则引擎工作内存;(3)应用程序中首先将规则库加载到规则集中,规则引擎会自动将工作内存中的监控告警对象实例结合 CMDB 中 CI 信息,与内存中加载规则库进行匹配,再在应用程序中调用相应接口指令进行故障树规则推理遍历 CI 树型结构,将工作内存中经过推理分析的告警与故障定位规则进行匹配,最终输出故障事件,包括故障源、故障原因等参考信息。

3 实例验证

将上述模型及实现应用于某电网公司一个核心生产 IT 信息系统,该系统当前故障为“系统整体运行缓慢”,具体规则如下:(1)目录 IO 异常或读写过高;(2)CPU 主机资源紧张;(3)MEM 主机资源紧张;(4)数据库存在大量等待事件;(5)数据库表空间使用率 100%。由于上述规则单独出现时并不一定会导致系统运行过于缓慢,因此需要在所有规则都生效时才会产生“系统整体运行缓慢”告警(图 5)。

红色方框部分表示信息系统故障定位系统 4 个功能的组成部分

Red box means 4 components of fault location system

图 5 故障规则界面

Fig. 5 Interface of fault rules

随着系统压力持续上升，故障中所有规则的告警都已经触发，产生故障(图 6 和图 7)。

CMDB 在此过程中提供主机、中间件等与所有监控项之间的关系，使推理机能找出符合所有故障条件的对应故障源，从而准确定位故障。实例验证表明，CMDB 结合系统规则推理的自动诊断分析能力可以有效的梳理现有各信息系统各功能组件和故障表征之间的关系，实现快速故障定位和展现，有效地提高了运维人员定位 IT 系统问题的效率与处理问题的准确性。

图 6 告警界面

Fig. 6 Interface of warnings

图 7 故障界面

Fig. 7 Interface of faults

4 结论

本研究描述了信息系统故障定位系统的理论基础和具体实现，在深入研究配置管理数据库(CMDB)的基础上结合规则推理进行故障定位，实现故障事件与 CMDB 的关联，通过 CMDB 确定故障设备之间的关系数据，从而通过监控告警结合故障规则分析定位到故障根源，并展示了应用范例。该系统除了实现故障定位外，还实现了作业执行和故障自动恢复的功能，不仅提高了信息运维水平，还可以通过各类规则库实现经验的积累与分享。此外，由于 Agent 端的通用性很强，只要能开发出相应的脚本，系统的功能可以进一步扩展，例如规范各组件参数配置、简单的日志分析等，有助于提升故障处理效率。

参考文献：

[1] 范娟娟，刘宇，刘亮，等. 铁路 IT 综合运维管理中 CMDB 子系统的设计与实现[J]. 铁路计算机应用，2015，24(8)：30-33.
FAN J J，LIU Y，LIU L，et al. CMDB subsystem in railway IT integrated operation and maintenance management system[J]. Railway Computer Application，2015，24(8)：30-33.

[2] 刘权. 基于 CMDB 的网管系统业务可用性监控平台的设计与实现[J]. 电信工程技术与标准化，2012，25(10)：29-32.
LIU Q. Design and implementation of a platform based on CMDB for service availability monitoring of network management systems[J]. Telecom Engineering Technics and Standardization，2012，25(10)：29-32.

[3] 黄波. 基于 CMDB 的业务可用性评估[J]. 微计算机信息，2012(6)：133-135.
HUANG B. Business usability evaluation base on CMDB[J]. Microcomputer Information，2012(6)：133-135.

[4] 徐定杰，郑笑天. 基于 CMDB 的银行故障管理优化实现[J]. 黑龙江科技信息，2010(6)：70.
XU D J，ZHENG X T. The improve and apply of bank failure management based on CMDB[J]. Heilongjiang Science and Technology Information，2010(6)：70.

[5] 董朝阳，陈珂，葛新. 基于 CMDB 的 ITIL 决策支持研究[J]. 机械设计与制造，2011(9)：266-268.
DONG C C，CHEN K，GE X. Study for ITIL decision support based on CMDB[J]. Machinery Design & Manufacture，2011(9)：266-268.

(下转第 64 页 Continue on page 64)

University,2010.

[15] 王桐明,杨琳. 基于 osg 粒子系统的海洋场景中下雪的仿真[J]. 电脑编程技巧与维护,2016(5):84-85.
WANG T M,YANG L. Simulation of snow in ocean scene based on OSG particle system[J]. Computer Programming Skills and Maintenance,2016(5):84-85.

[16] 陆灏铭,陈玮. 船舶运动可视化仿真平台的设计与实现[J]. 计算机仿真,2012,29(8):277-281.
LU H M,CHEN W. Design and realization of visualizing simulation platform for ship motion[J]. Computer Simulation,2012,29(8):277-281.

[17] 王正山,华芳,顾耀林. 带碰撞自反馈的分布式虚拟环境实现[J]. 计算机工程与应用,2006,43(6):82-84.
WANG Z S,HUA F,GU Y L. Implementing of distributed virtual environment with collision self-response[J]. Computer Engineering and Applications,2006,43(6):82-84.

[18] 马登武,叶文,李瑛. 基于包围盒的碰撞检测算法综述[J]. 系统仿真学报,2006,18(4):1058-1061.
MA D W,YE W,LI Y. Survey of box-based algorithms for collision detection[J]. Journal of System Simulation,2006,18(4):1058-1061.

(责任编辑:米慧芝)

(上接第 58 页 Continue from page 58)

[6] 马秀丽,王红霞,张凌云. 网络故障管理系统中告警相关性分析实现技术研究[J]. 沈阳理工大学学报,2009,28(3):9-14.
MA X L,WANG H X,ZHANG L Y. Research on the implementation of alarm dependency analysis in network faults management system[J]. Transactions of Shenyang Ligong University,2009,28(3):9-14.

[7] 蔡宗平,汤正平,闵海波. 故障树分析法的专家系统在故障诊断中应用[J]. 微计算机信息,2006,22(22):135-137.
CAI Z P,TANG Z P,MIN H B. Application of expert system based on fault tree technique in fault diagnosis[J]. Microcomputer Information,2006,22(22):135-137.

[8] 卢燕,潘宏侠. 基于 B/S 模式的远程故障诊断专家系统[J]. 仪器仪表与分析监测,2007(1):7-8,17.
LU Y,PAN H X. Remote fault diagnosis system based on B/S Model[J]. Instrumentation Analysis Monitoring,2007(1):7-8,17.

[9] 吴明强,史慧,朱晓华,等. 故障诊断专家系统研究的现状与展望[J]. 计算机测量与控制,2005,13(12):1301-1304.
WU M Q,SHI H,ZHU X H,et al. Research and prospect of fault diagnosis expert system[J]. Computer Measurement & Control,2005,13(12):1301-1304.

[10] 邓歆,孟洛明. 告警相关性分析模型在通信网故障诊断中的应用[J]. 北京邮电大学学报,2006,29(3):66-69.
DENG X,MENG L M. Application of alarm correlation model for fault diagnosis in communication networks[J]. Journal of Beijing University of Posts and Telecommunications,2006,29(3):66-69.

(责任编辑:陆 雁)