

## 基于故障树的复杂航天系统故障预测方法

李赣华<sup>1,2</sup>,董黎<sup>1,2</sup>,李显武<sup>1,2</sup>,邵能建<sup>1,2</sup>,夏克强<sup>1,2</sup>,邵文星<sup>1,2</sup>,安源<sup>1,2</sup>

(1.国家宇航动力学实验室,陕西西安710043;2.西安卫星测控中心,陕西西安710043)

**摘要:**针对航天数据处理中心运控管理系统长期不间断高可靠运行要求,采用了基于规则和故障树分析的故障预测方法,设计了航天数据处理中心运控管理系统的故障预测分系统。首先提出了航天数据处理中心软硬件故障诊断分系统架构;其次设计了可视化故障树和规则相结合的推理方法,实现了基于故障树和规则的系统故障诊断;然后在故障诊断的基础上,通过趋势预测方法的历史数据学习结合人工手段,选择预测方法进行故障预测;最后通过预测结果与实测数据比对,验证了方法的可用性和有效性,并通过系统应用,有效地提前避免了系统故障的出现。

**关键词:**复杂系统;故障预测;故障树;航天数据处理中心

中图分类号:TN820.4

文献标识码:A

DOI:10.16157/j.issn.0258-7998.222661

中文引用格式:李赣华,董黎,李显武,等.基于故障树的复杂航天系统故障预测方法[J].电子技术应用,2022,48(10):54-59.

英文引用格式:Li Ganhua, Dong Li, Li Xianwu, et al. A fault prediction method based on fault tree method for a complex space system[J]. Application of Electronic Technique, 2022, 48(10): 54-59.

## A fault prediction method based on fault tree method for a complex space system

Li Ganhua<sup>1,2</sup>, Dong Li<sup>1,2</sup>, Li Xianwu<sup>1,2</sup>, Tai Nengjian<sup>1,2</sup>, Xia Keqiang<sup>1,2</sup>, Tai Wenxing<sup>1,2</sup>, An Yuan<sup>1,2</sup>

(1.State Key Laboratory of Astronautic Dynamics, Xi'an 710043, China;

2.Xi'an Satellite Control Center, Xi'an 710043, China)

**Abstract:** The space data processing center should be on-line running without stop in highly reliability and availability, so this paper presents a fault prediction method based on rule and fault tree, and designs the fault prediction system for processing management system of space data processing center. Firstly, the architecture of fault detection is designed for software and hardware of the space data processing center. Secondly, the derivation method is presented based on fault tree and rule of visualization to realize the fault function of the processing management system. Then, based on the fault detection, the fault prediction method is proposed using auto-selection method and artificial method, after the learning method is used between prediction result and historical data. At last, the application of the system is realized with the using of the method presented in this paper. On the comparison of the prediction result with the real data, the method of this paper is proved effective and efficient.

**Key words:** complex system; fault prediction; fault tree; space data processing center

## 0 引言

随着我国航天工业尤其是商业航天的快速发展,我国在轨航天器数量迅猛增长。面向航天器高可靠控制管理要求,航天地面数据中心也出现了长期不停、多代并行、功能多样、系统复杂等特点。面向不断扩大的地面系统,稳定运行和高效运维是航天地面数据处理中心系统的首要要求,不同格式的数据传输异常、进程异常退出等应用软件问题,以及服务器宕机、CPU异常、磁盘故障、风扇损坏等底层硬件故障,都是严重影响系统运行的严重故障,会严重影响航天地面数据处理中心的正常运行,甚至影响航天器在轨应用。为了实现这种复杂航天地面数据处理中心故障提前发现,争取时间解决故障,本文提出了一种基于规则和故障树的软硬件系统故

障预测方法,并在航天数据处理中心系统进行了验证和应用,结果能够实现对故障的预测,更好地保障了航天数据处理中心系统连续运行的高可靠性<sup>[1-2]</sup>和高可用性<sup>[3]</sup>。

## 1 国内外现状分析

不论国外还是国内,当前系统监控主要依托3种方式开展系统管理:(1)硬件平台自带的监控管理系统,如浪潮服务器自带的性能监视软件;(2)云管理平台提供的监视系统,如华为FusionSphere管理平台;(3)用户自研的集中监控管理平台。航天数据处理中心因为系统复杂,高可靠不间断运行要求高,系统软硬件平台都需要监控,多采用独立建设集中监控管理平台。但是一旦发生故障,对于航天数据处理中心以及航天器运行都是灾难性。对于航天数据处理中心故障的预测和提前处置就

是系统运行的关键技术。

在系统运维监控方面,陈建译从计算机连锁系统原理和硬件结构出发,提出了基于现场运维故障数据的系统寿命预测方法<sup>[4]</sup>;翟永开展了计算机硬件设备的运维决策和评估数据模型分析,基于设备和子系统可靠度和可用性理论,分析了资产残值、业务重要度和不可靠度等运维重要度变量的测算方法<sup>[5]</sup>。

在故障预测方面,郭建综述了基于状态的系统故障预测与维修决策的发展现状,分别将基于可靠性、基于数据驱动、基于统计、基于失效物理和综合集成的故障预测进行了总结分析<sup>[6-9]</sup>;缪巍巍提出了针对IMS业务特点的故障树构建方法,实现了一种基于故障树知识库的故障诊断专家系统<sup>[10]</sup>;宋俊花提出新的故障树简化规则和模块扩展分解算法,对现有的线性时间算法进行改进,解决大型故障树的分析需要耗费大量的计算资源,导致分析效率低下、时间消耗过多问题<sup>[11]</sup>。故障树的预测和诊断方法还在计算机系统的状态分析、网络安全管理、系统容错等方面进行应用和研究<sup>[12-15]</sup>。

## 2 系统架构

故障诊断系统的目的是在中心综合监视系统的基础上,引入故障诊断技术,通过计算机系统的各类参数状态信息、任务过程信息、设备属性信息,进行故障诊断,实现对中心系统运行状态的准确感知,降低系统故障虚报漏报的概率,并实现故障的精确定位,形成一个具有专家智能的故障检测平台,提高故障诊断的智能化水平,提升中心系统的维护效率。该平台具备自动报警、辅助诊断和快速故障定位的功能。系统整体架构如图1所示。

系统工作流程:故障诊断系统接收数据采集模块推送的相关设备告警名称、告警设备标识符、告警类型等参数,经过规则转化,再综合运用知识库中的知识进行复杂的逻辑推理,同时利用反馈机制及时判断事件发生与否,最终诊断出可能导致设备发生故障的位置、故障原因置信度及修复建议。系统采用反向演绎推理策略并结合深度优先搜索遍历的方法,以实现对计算机系统设备故障原因的快速定位,并给出排除故障的措施。

系统分为转化规则管理、知识库管理、故障推理管理以及故障预警管理四大模块。在系统内部数据处理过程中,信息存储至少包含转化规则信息记录、知识库相关信息记录(包含事件信息记录和故障树相关记录)、故障推理相关记录(推理条件记录和推理结果记录)以及故障预测相关记录(包含预测条件记录和预测结果记录)。

## 3 可视化故障树和规则相结合的推理

根据人工诊断先验知识,构建故障树,模型如图2所示。其中“L1:显示网收不到数据”作为故障树的顶事件。

采用故障树和规则推理相结合的工作方式,首先根据故障树的构成,转化成如下的推理规则:

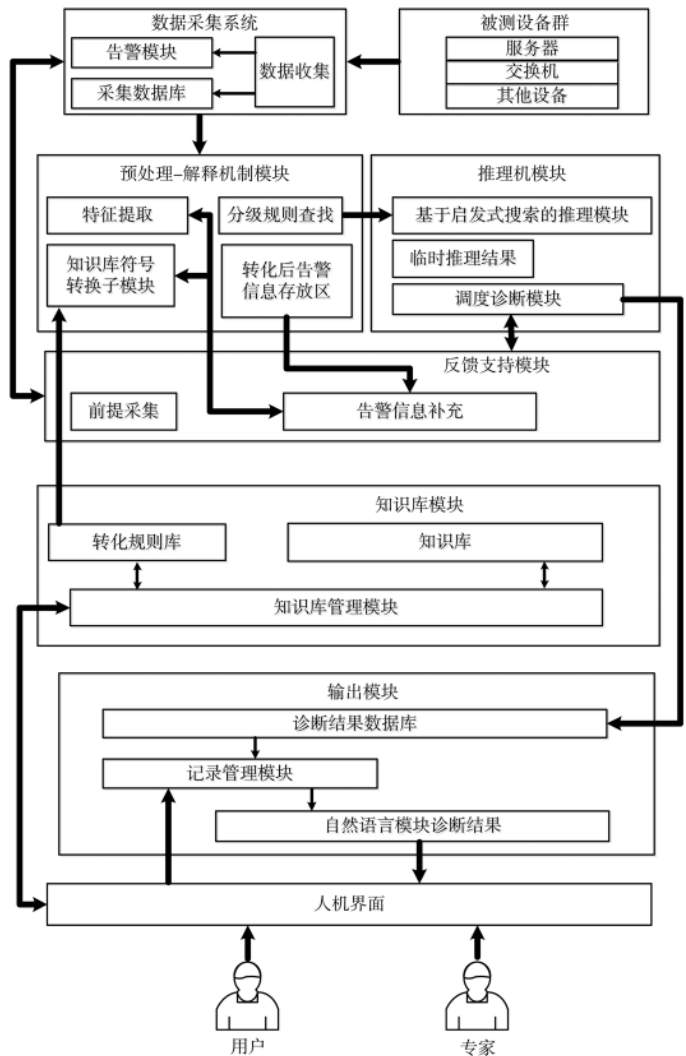


图1 故障诊断系统架构

规则1: IF 显示网收不到数据 THEN 显示网交换机异常; 前件可信度  $T=0.8$ , 规则强度  $C=0.2$ ;

规则2: IF 显示网收不到数据 THEN 显示网计算机异常; 前件可信度  $T=0.8$ , 规则强度  $C=0.3$ ;

规则3: IF 显示网收不到数据 THEN 非显示网问题; 前件可信度  $T=0.8$ , 规则强度  $C=0.5$ ;

规则4: ……

然后采用反向推理策略搜索故障来源, 搜索的优先顺序是首先搜索较大概率的下一级事件, 判断该事件是否是叶子节点。若是叶节点则从数据采集端确认是否有消息证实该事件的真实性; 若不是叶节点, 则搜索其他下一级事件, 直到确认故障发生的原因及位置, 同时更新相应的节点概率。

将故障诊断系统的诊断结果显示给系统管理员, 方便管理员及时针对故障诊断结果进行故障修复。

故障名称: 显示网收不到数据

设备信息: Windows50

诊断时间: 2015-04-24 14:45:49

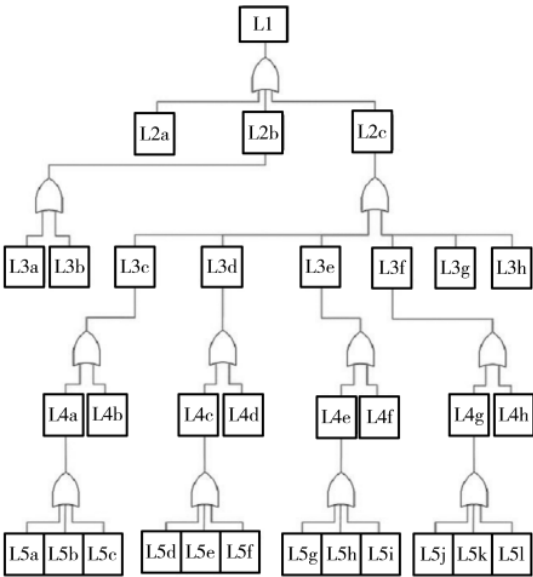


图 2 某故障示例的故障树示意图

诊断结果:未完成  
诊断步骤:见表 1  
处理意见:重新启动 EADS 设备,或人工检查 DODS 软件状态。

4 基于故障树和规则的故障诊断系统

规则管理界面如图 3 所示,用于管理系统告警推理时所需规则库,表中的属性字段和故障树的门事件紧密相关,故障树的逻辑关系描述了表中属性字段的父子关系,并给出诊断结果的处理意见。该表中的规则需在诊断前手动添加,该表中的规则越丰富,诊断结果越准确。

故障树管理界面如图 4 所示,绘制完成了一个可视

注:L1:显示网收不到数据;L2a:显示网交换机异常;  
L2b:显示网计算机异常;L2c:非显示网问题;  
L3a:计算机硬件异常;L3b:显示软件异常;  
L3c:开发系统异常;L3d:转发系统异常;  
L3e:协议转换器异常;L3f:保密系统异常;  
L3g:中心交换机异常;L3h:通信异常;  
L4a:开发系统硬件异常;L4b:开发系统软件异常;  
L4c:转发系统硬件异常;L4d:转发系统软件异常;  
L4e:协议转换器硬件异常;L4f:协议转换器软件异常;  
L4g:保密系统硬件异常;L4h:保密系统软件异常;  
L5a:开发系统 CPU 异常;L5g:协议转换器 CPU 异常;  
L5b:开发系统内存异常;L5h:协议转换器内存异常;  
L5c:开发系统磁盘异常;L5i:协议转换器磁盘异常;  
L5d:转发系统 CPU 异常;L5j:保密系统 CPU 异常;  
L5e:转发系统内存异常;L5k:保密系统内存异常;  
L5f:转发系统磁盘异常;L5l:保密系统磁盘异常。

表 1 诊断系统诊断表

检测项	检测结果	阈值(无单位)
显示网交换机异常	正常	0.20
中心交换机异常	正常	0.15
通信软件异常	人工待检测	0.15
数据处理硬件异常	正常	0.10
监控报警软件异常	异常	0.10
协转器硬件异常	正常	0.10
通信异常	正常	0.10
...	...	...

化故障树实例。故障树中的元素可以随意拖动,门元素

事件管理 检索规则管理 故障树管理 转化规则管理 故障管理 规则管理 故障预警管理						
条件查询选择						
<input type="checkbox"/> 事件分类: 页事件 <input type="checkbox"/> 名称关键字: 更新						
事件信息						
第1页共25条记录 首页 上一页 下一页 尾页 1 跳转						
事件编号	事件分类	事件名称	标识	事件描述	前置条件检索规则	处理意见
45	服务器事件	服务器宕机	La1	服务器宕机了		要重启服务
46	中间事件	CPU异常	La2	CPU异常		更换CPU
47	中间事件	磁盘异常	Lb1	磁盘异常		更换磁盘
48	底事件	CPU温度过高	Lb2	CPU温度过高	温度过高	给CPU降温
49	底事件	风扇异响	Lb3	风扇异响	风扇异响	更换风扇
50	底事件	磁盘已满	Lb4	磁盘已满	磁盘已满	清理磁盘
51	底事件	磁盘使用率过高	La	磁盘使用率过高	磁盘使用率过高	降低磁盘使用率
52	底事件	CPU利用率异常	Lb1	cpu温度高了		降低温度
53	底事件	风扇异响		风扇坏了		更换风扇
54	底事件	磁盘异常		磁盘异常	磁盘异常	磁盘可能满了
64	底事件	新增用户A无法接收组播数据异常		新增用户A无法接收组播数据异常		
67	底事件	三层路由配置检索规则		三层路由配置检索规则		
68	底事件	组播路由配置检索规则		组播路由配置检索规则		
69	底事件	组播信息配置检索规则		组播信息配置检索规则		
70	中间事件	配置正确		配置正确		
71	中间事件	服务器与交换机互联端口检索规则		服务器与交换机互联端口检索规则		
72	中间事件	交换机与路由器互联端口检索规则		交换机与路由器互联端口检索规则		
73	中间事件	路由器与防火墙互联端口无故障		路由器与防火墙互联端口无故障		
74	底事件	硬件故障检索规则		硬件故障检索规则		检查硬件

图 3 规则管理界面

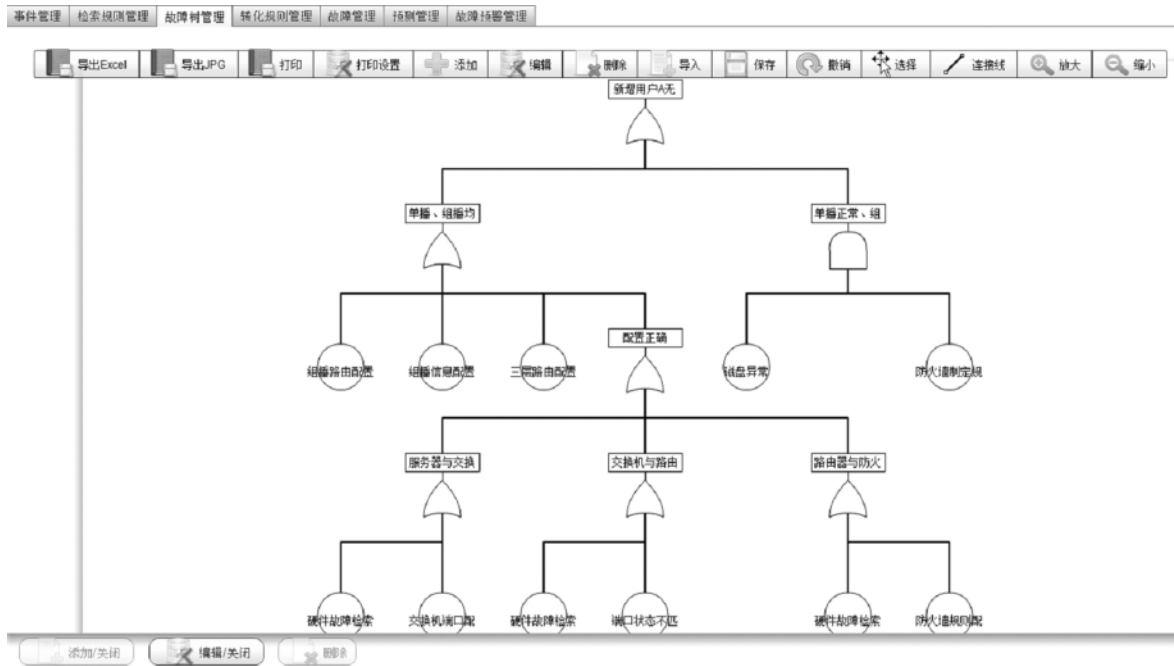


图4 故障树管理界面

中绑定的事件也可以随意修改,故障树绘制过程中会进行故障树合法性检查,例如故障树中是否有环路、门节点的孩子数是否大于等于2等。

## 5 基于趋势拟合的故障预警方法

故障预警是通过建立预测模型,根据设备性能参数的历史记录,推断出未来某一段时间内设备运行的状况,及时发现设备潜在故障,提前进行故障维修,降低设备故障引起的事故风险。故障预测分为以下几步。

### 5.1 确定预测目标

中心系统是一个复杂的系统,反映系统运行状态的参数很多,如设备路由表、设备运行时间、板卡温度、CPU使用率、内存、硬盘使用率、端口流量、端口丢包率、SYSLOG日志等。在选择故障特征量时应选择对设备运行有直接和重大影响的参数。实践表明,选择内存使用率、CPU使用率、硬盘使用率、端口流量等参数作为故障预测参数,是有实际意义的。

### 5.2 选择预测方法建立预测模型

设备运行状况的变化趋势一般通过预测模型来模拟和仿真,从而预测设备未来的运行状态。目前主要的故障预测技术有统计方法、数学方法、人工智能方法和信息融合方法等。

### 5.3 评价预测模型

利用建立好的模型进行预测,预测的准确性将直接决定着系统性能的好坏,因此应根据一定的指标来评价预测模型的好坏,并对模型进行改进。

故障预测的基本模型如图5所示。

## 6 实验结果及系统验证

系统采用二次曲线拟合的数学模型,利用最小二乘

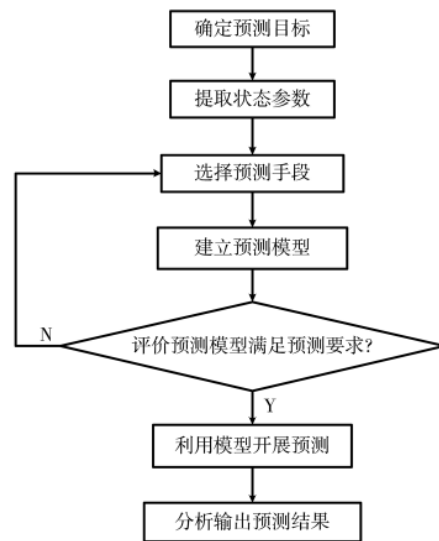


图5 故障预测基本模型

数学方法,回归分析历史数据,并拟合出与历史数据相一致的曲线,然后根据这条曲线预测设备未来一段时间的健康状态。该方法具有原理简单、易于实施的特点。每次预测时根据最新采集的历史数据重新生成拟合曲线,在使用过程中拟合次数可以进行配置,下面介绍具体实现过程。

### 6.1 选择拟合公式

$$y = ax^2 + bx + c \quad (1)$$

其中, $a$ 、 $b$ 、 $c$ 为公式系数, $x$ 为时间值, $y$ 为时间值对应的具体监控参数值。

### 6.2 历史数据训练

数据以 $x$ 、 $y$ 值的形式表示, $x$ 值为时间值,每个 $x$ 值



之间的间隔取决于监控系统中采集频率(一般为 60 s),  $y$  值为  $x$  轴各个时间点上采集的监控参数值, 如图 6 中采集的数据为时间在 0~20 个单位之间的数据。

6.3 代入拟合公式

历史数据的  $x$  值(时间值)和  $y$  值(时间上对应的监控参数值)为已知数据, 带入二项式曲线拟合式(1)求出公式系数  $a$ 、 $b$ 、 $c$  值。

6.4 选择预测范围

取预测条件中的预测时间范围, 监控系统中的采集频率分隔预测时间为若干采样点, 如图 6 中预测的范围为 20~40 个单位时间的情況。

6.5 产生预测数据

将采样点作为预测  $x$  值(预测时间值)加到已采集的历史数据  $x$  值(历史时间)后, 带入到式(1)中求出  $y$  值,

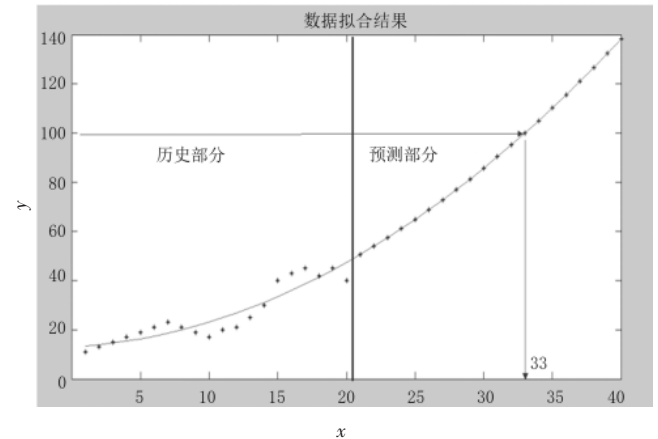


图 6 历史曲线及预测曲线图

即从 0~40 个单位时间内的拟合值(图 6 中的曲线)。

6.6 按预测阈值报警

图 6 中的垂直的实线左侧为历史部分, 图上点为采集的历史实际数据, 在拟合曲线附近波动; 垂直实线右侧为预测部分, 图上点为拟合后的预测数据, 预测的目的就是用这些拟合值与预测条件中设置的阈值表达式比较。如果预测条件中设置的阈值表达式为大于 100, 那么预测过程中就会用该阈值表达式遍历比较拟合值, 当遍历到第 33 个单位时间时超出阈值, 此时会发出报警信息; 如果阈值表达式设置为大于 200, 则在这个预测周期(20~40 的单位时间)内就不会发生报警。

从曲线图中可以看出曲线拟合方法的直观性, 该方法能实时地预测某个设备性能参数在未来某个时间区间内的走向, 在任务过程中已多次成功预测 CPU 使用率、硬盘使用率、网络端口流量引起的设备故障风险, 有效避免了重要时段设备故障, 提高了系统的稳定性。

图 7 为实现的预测管理模块界面, 该模块主要完成对指定设备的特定事件的录入, 设置告警阈值、预测周期、提取的历史数据点数以及预测开始的时间, 作为故障预警管理模块显示展示的数据来源。

图 8 为对某个设备的具体预测结果。在曲线图中以虚线显示所选设备下对应事件的阈值; 一次拟合线为中间曲线; 二次拟合线为下部曲线; 三次拟合曲线为上方曲线; 实时采集的历史数据点与中间的一次拟合曲线重合。最新预测结果状态栏会实时滚动显示预测的结果, 系统会根据预测数据与实测数据差自动或手动选择拟

事件管理 检索规则管理 故障树管理 转化规则管理 故障管理 预测管理 故障预警管理							
条件查询选择							
<input type="checkbox"/> 预测条件状态: 正常 <input type="checkbox"/> 名称关键字: <input type="text"/> <input type="button" value="更新"/>							
预测信息							
第1页共1页 共13条记录 首页 上一页 下一页 尾页 1 跳转							
预测设备	预测事件	报警阈值	预测周期(单位: 秒)	提取历史数据量	预测开始时间	最后预测时间	状态
20000	CPU温度过高	>30	1小时	22	2015-10-05 00:00:00		停用
20000	风扇损坏	>20	1分钟	22	2015-10-21 00:00:00		正常
20000	磁盘已满	>90	1分钟	11	2015-10-12 00:00:00		停用
20000	磁盘使用率过高	>60	1小时	3	2015-10-13 00:00:00		正常
20000	磁盘异常	=1	1小时	3	2015-10-05 00:00:00		停用
20001	磁盘使用率过高	<22	3小时	332	2015-10-04 00:00:00		停用
20032	磁盘已满	>90	2小时	12	2015-10-12 00:00:00		正常
20200	CPU温度过高	>29	1小时	24	2015-10-05 00:00:00		正常
31000	磁盘使用率过高	>80	1小时	3	2015-10-12 00:00:00		正常
50400	磁盘异常	=1	1小时	3	2015-10-12 00:00:00		正常
53000	风扇损坏	=0	1小时	3	2015-10-05 00:00:00		正常
100003	CPU温度过高	>0.8	1小时	50	2015-04-01 00:00:00	2015-06-07 17:14:55	停用
100008	CPU温度过高	>0.9	1分钟	50	2015-06-02 00:00:00	2015-10-29 17:41:15	正常

图 7 预测管理界面

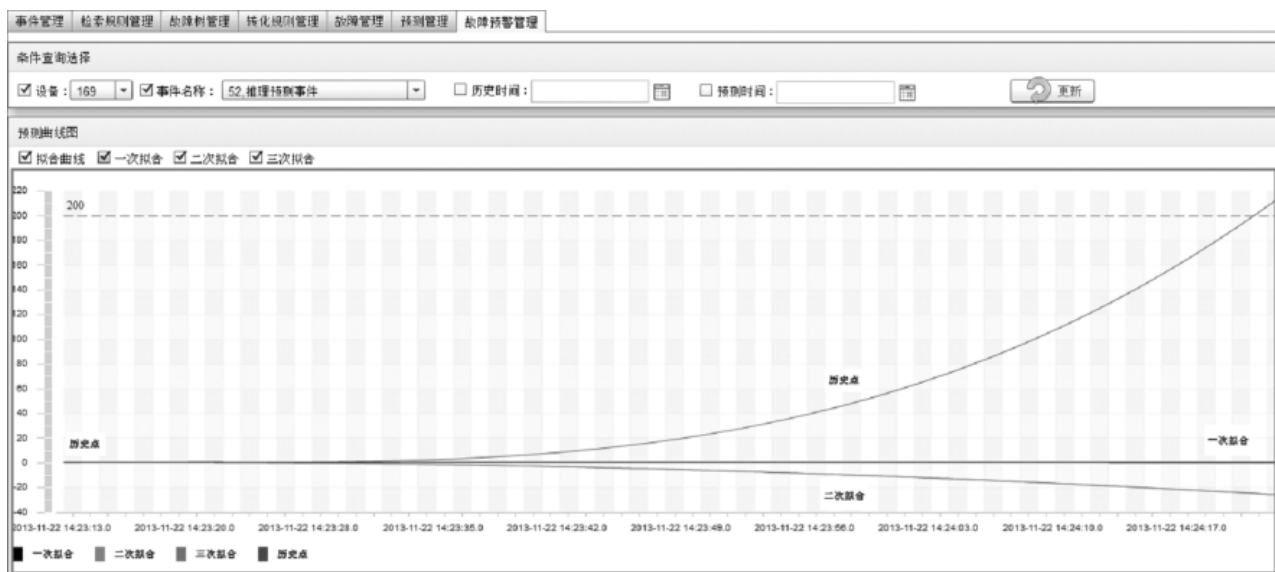


图8 故障预测结果

合方法,适应数据变化。

## 7 结论

针对航天数据处理中心软硬件监控系统,本文提出了一种基于故障树的故障预测方法,实现了系统监控故障诊断和预测系统。通过需检测的硬件平台和航天数据处理软件系统的监控系统验证,说明方法对各种大量的软硬件系统参数适用,验证了方法的有效性。

## 参考文献

- [1] 卢明银,徐人平,李乃梁,等.系统可靠性[M].北京:机械工业出版社,2008.
- [2] PECHT M, KAPUR K C, KANG R, et al. Foundations of reliability engineering[M]. China: Publishing House of Electronics Industry, 2011.
- [3] 王海鹏,周兴社,张涛,等.面向用户的普适计算系统可用性度量模型[J].计算机科学,2006,33(11):89-93.
- [4] 陈建译,周荣,乔高锋,等.基于故障数据的计算机联锁系统寿命预测方法[J].铁路计算机应用,2017,26(1):22-28.
- [5] 翟永,刘津,陈杰,等.计算机硬件设备的运维决策和评估数学模型分析[J].计算机科学,2018,45(6A):568-579.
- [6] 郭建,徐宗昌,张文俊.基于状态的装备故障预测技术综述[J].火炮发射与控制学报,2019,40(2):103-108.
- [7] Wu Yingnian, Huang Xiaohong. Hard drive failure prediction for large scale storage system[D]. Los Angeles: University of California, 2017.
- [8] AHMED EL-SHIMI. Predicting storage failures[C]//Linux Storage and File Systems Conference Cambridge MA, 2017.
- [9] Xu Yong, Sui Kaixin. Improving service availability of cloud

systems by predicting disk error[C]//Proceedings of the 2018 USENIX Annual Technical Conference (USENIX ATC'18), 2018.

- [10] 缪巍巍,吕顺利,蒋承伶,等.基于故障树的电力IMS业务故障诊断专家系统研究应用[J].计算机与数字工程,2018,46(8):1558-1563.
- [11] 宋俊花,魏欧.基于线性时间算法的故障树模块扩展分解方法[J].计算机科学,2019,46(1):226-231.
- [12] RUIJTERS E, STOELINGA M. Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools[J]. Computer Science Review, 2015, 15-16: 29-62.
- [13] FOVINO I N, MASERA M, DE CIAN A. Integrating cyber attacks within fault trees[J]. Reliability Engineering & System Safety, 2009, 94(9): 1394-1402.
- [14] DUGAN J B, BAVUSO S J, BOYD M A. Dynamic fault-tree models for fault-tolerant computer systems[J]. IEEE Transactions on Reliability, 1992, 41(3): 363-377.
- [15] 程明华,姚一平.动态故障树分析方法在软、硬件容错计算机系统中的应用[J].航空学报,2000,21(1):35-38.

(收稿日期:2022-02-20)

## 作者简介:

李赣华(1977-),通信作者,男,博士,高级工程师,主要研究方向:航天测控总体、信息工程, E-mail: liganhua666@163.com.

董黎(1978-),女,本科,工程师,主要研究方向:航天测控通信。

李显武(1975-),男,硕士,高级工程师,主要研究方向:航天测控总体。



扫码下载电子文档

## 版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所