

民机航电系统虚拟化计算平台功能安全评估研究

杨欢¹, 王晓东¹, 李庚¹, 张双², 郭阳明³

(1.西北工业大学 计算机学院, 陕西 西安 710072; 2.航空工业西安航空计算技术研究所, 陕西 西安 710068;
3.西北工业大学 网络空间安全学院, 陕西 西安 710072)

摘要:围绕虚拟化后影响机载计算平台安全的时空隔离性、故障隔离性、可调度性等主要问题,开展虚拟化环境下机载计算平台的安全等级评定研究,考虑虚拟化后航电系统的特点,提出了一种基于层次分析法(AHP)和灰度关联分析法(GARD)的安全性计算方法。建立了机载虚拟化计算平台安全评估判断树,利用 AHP 方法计算了各安全能力的权重,给出了系统整体安全性得分,在此基础上,结合 GRAP 方法,参照航空电子系统安全性评估,计算得出了测试系统与 DAL 安全等级要求适配度最高的安全等级。

关键词:民机;计算平台;虚拟化;功能安全;层次分析

中图分类号:V247

文献标志码:A

文章编号:1000-2758(2024)01-0045-08

国外飞机制造商波音、空客等为了提升飞机舒适性和经济性,对民用客机进行 E 化(在我国被称之为民机信息化)^[1-2]。航空电子系统是实现这一改进的重要手段,几乎所有的机载信息化都依赖于航空电子系统实现^[3-4]。虚拟化商用现成产品和技术(commercial off-the-shelf, COTS)成为了民用客机信息化的一种新方法,它降低了民机研发成本和周期、减少设备的冗余、减轻了飞机的质量,同时也能实现绿色低碳发展^[5-7]。在航空电子系统机载计算环境虚拟化之后,机载计算平台实现计算资源与操作系统的解耦,极大地提升了资源的利用率,但同时也改变了航空电子系统计算平台的现有功能和架构,引入了航空电子系统安保的新问题^[8]。虚拟化方式与以往航空领域设计的专用产品和技术有所不同,COTS 更加关注高性能和通用性,对航空电子系统领域的高可靠性和高确定性研究不足^[9]。现有的信息技术安全评估通用准则(the common criteria for information technology security evaluation, CC)不能完全适用于航空电子系统虚拟化计算平台的安全评估。目前航空电子系统制造商和航空公司主要关

注的是其功能安全,因此需要通过定性和定量相结合的方法评估虚拟化后的航空电子系统机载计算平台的功能安全性(safety)。对于这种安全性和实时性要求高的航空电子系统来说,功能安全和由不确定性问题导致的安全风险对民机的飞行安全具有致命威胁。

目前,在对具有跨学科、高复杂性的综合化航空电子系统进行适航符合性安全评估时,国内外航空相关研究机构提出了许多安全评估方案,但针对虚拟化计算平台目前还没有一套适用的功能安全评估方案,目前大部分的研究都是以单一指标研究为主。

虚拟化最重要的安全特征就是它的隔离性。分区隔离机制的主要目的是让机载计算平台各分区之间不会相互感知、影响,就好像它们分别运行在不同的物理设备上,以此来保障分区系统的安全性和机密性,为不同安全级别的分区提供了时空隔离和故障隔离^[10-12]。时间隔离性方面, Kim 等^[13]在四核处理器系统上进行实验,其结果数据表明,相比于每个任务单独运行时的完成时间,处理器间共享缓存干扰会将任务完成的预期时间增加 40%。空间隔离性方面,作为虚拟化分区空间隔离性的重要保障,访问控制技术一直以来是研究的重点。为解决虚拟化环境中的访问控制问题, Jakub 等^[14]利用机密性和完整性保护表对内存中每个物理页标注 Hypervisor

和 DMA 的访问权限,以此来避免虚拟机内存被 Hypervisor 和 DMA 恶意访问,并把这种技术称作 HyperWall。故障隔离方面,郝继锋等^[15]对虚拟化环境下 ARINC 653 分区的故障隔离进行实验测试,但是仅考虑了故障情况下对其他分区调度的影响。王心然^[16]对虚拟容器的 2 类故障进行分析并给出了故障隔离能力测试方案。可调度性方面,符宁等^[17]提出了将 AADL (architecture analysis and design language) 模型转换为 UPPAAL 模型进行可调度性验证的方法,但仅考虑了相同任务的情况。雷煜靓等^[18]提出了一种用于对包含周期及非周期任务的单处理器多分区 ARINC 653 系统可调度性分析的方法,采用全局 SMC 与组合 MC 相结合的方式定位不可调度任务,但是没考虑多核情况。

综上所述,本文提出了一种基于层次分析-灰色关联分析 (AHP-GRAP) 评估方法。该方法综合考虑了机载计算平台隔离性、可调度性和故障隔离性等安全性因素。由于单一的数据指标无法直观地提供反馈,因此需要综合评估这些安全性指标,并确定航空电子系统的安全等级。同时,对虚拟化环境下机载计算平台的功能安全评估方法进行了实例验证。该方法对于机载虚拟化计算平台的功能安全评估具有一定的参考意义。

1 机载虚拟化计算平台安全性描述

民用飞机航空电子系统的安全性被理解为系统可持续提供正常功能,或者以不破坏其他系统并威胁人员生命安全的方式中断服务的能力^[19]。在机载计算平台中,除了原本系统本身的不确定性导致故障或失效外,一些信息安全 (security) 方面的漏洞也会改变系统运行情况,进而影响到系统的安全性,许多安全性机制也是从信息安全领域的的安全机制发展而来^[20-21]。

陈刚等^[6]对虚拟化多核架构下的安全性提出了三方面的担忧:保证系统行为的可预测性、多核系统并行任务对实时应用程序的实时性保证,以及在充分利用处理器性能的前提下保证系统行为的时间正确性。虚拟化引入 3 个对飞机适航安全性的考验:①虚拟化共享系统中的硬件资源,并根据分区需求进行资源分配,但共享资源之间可能存在干扰,同驻虚拟机之间可能会因软件错误或外界攻击而越权访问。②虚拟化后,所有分区集中在同一个物理平

台上,如果一个分区发生故障,是否能将故障控制在该分区内,不影响其他分区甚至虚拟机管理器。③虚拟化后,硬件资源的动态调度影响机载计算系统行为的可预测性,而机载操作系统中的实时系统,尤其是硬实时系统对调度行为的可预测性要求非常严格。

综合上述 3 个问题发现,虚拟化对机载计算系统适航符合性带来的安全影响主要有三方面:①由于资源争用,共享硬件资源的分区间会发生不确定性干扰;②同驻分区可能存在软件错误或外部攻击造成的安全性隐患;③混合安全关键级系统中的调度场景更复杂,导致高安全等级任务的可调度性变得不可预测。前 2 个影响源于虚拟化后物理隔离的消失,而后一个影响源于复杂场景下无法通过简单的数学模型对可调度性进行分析。因此,在虚拟化机载计算平台中,需要关注系统隔离性和可调度性的安全性评估。

特别是当虚拟化商业化技术应用于航空电子系统领域后,未来的机载云构想将面临越来越普遍的功能和信息安全威胁。本文综合考虑了时间不确定性等功能安全威胁,并部分考虑了信息安全威胁,以评估整体系统的功能安全性。因此,综合考虑虚拟化后机载计算平台安全状态的变化,将虚拟化环境下的机载计算平台安全性分为时空隔离性、故障隔离性和可调度性,如图 1 所示。

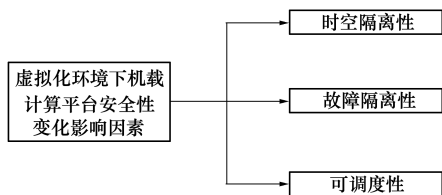


图 1 虚拟化环境下机载计算平台安全性变化因素

2 安全等级指标体系构建

在安全等级评估中,涉及到的指标通常不应只是单维度或片面的,而应该是包含多个维度的集合。这些指标应能根据具体的评估对象设定合适的评估准则,其中每一个评估准则对应评价对象的一个能力。因此,可以将机载虚拟化计算平台的每一项能力转化为对应的安全性指标。然而,采用多个指标来描述机载计算平台的安全性时很难明确哪些能力是机载计算平台的安全性、哪些能力是关键的。因

此,有必要采用客观地选取流程区分指标的重要性,本文采用层次评估法进行评估。

在建立层次评估体系后,需要进一步完成指标体系的构建工作,指标体系的确立步骤如下所示,流程如图 2 所示。

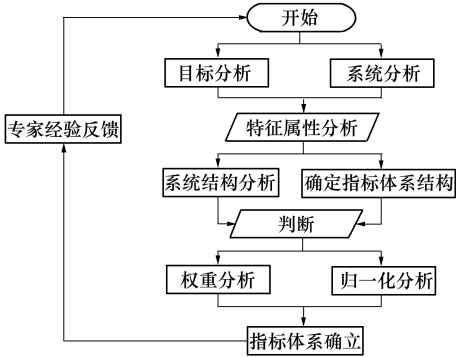


图 2 指标体系确立流程图

安全评估指标体系中第一层为目标层:虚拟化环境下机载计算平台安全性 (E);第二层为安全类层 ($C_1 \sim C_3$):将虚拟化环境下的系统安全性分解为时空隔离性(包含时间隔离性和空间隔离性)、可调度性(包含调度正确性)以及故障隔离性,综合所有因素考虑整体的安全性;第三层安全子类层($H_1 \sim H_8$),将第二层不同的安全子类具体化,使用不同的指标来度量,如访问控制能力、分区可扩展能力等。因此,本文选取了虚拟化计算平台的安全功能组件,如表 1 所示。从表中可以得出安全评估判断树,如图 3 所示。

表 1 安全功能组件选取	
安全功能要求类	安全功能要求子类
时空隔离性	抑制共享资源干扰能力
	分区可扩展能力
	访问控制能力
	防御虚拟机逃逸能力
可调度性	紧急情况响应能力
	优先级反转抑制能力
故障隔离性	共享资源故障隔离能力
	系统调用故障隔离能力

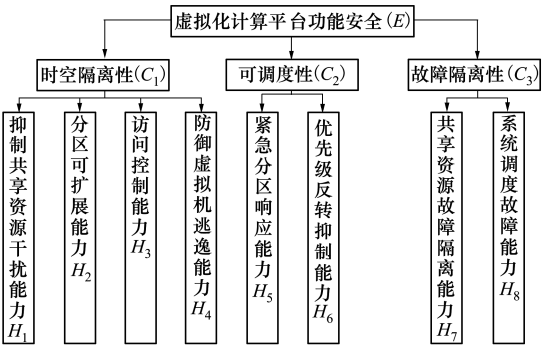


图 3 安全评估判断树

3 机载虚拟化计算平台安全计算方法

目前,信息安全领域以 CC 为代表的通用评估方法更多关注系统的机密性、完整性等与信息安全(security)相关的安全性,对一些不确定因素造成的系统的安全威胁关注较少。本文使用层次分析法(AHP),综合考虑了虚拟化环境下的各因素受影响程度,计算并给出了每项指标不同的权重,最后对系统安全性进行了综合评估。

3.1 基于 AHP 的权重计算

从本质上来说,AHP 方法是一种将研究的目标按支配的关系拆解成多层模型的方法。它通过一定的方法确定每一层次中所有指标相对于上一层次中父元素的权重排序,最终确定每一层次中所有指标相对重要性^[21]。简单来说,AHP 确定指标权重的过程主要包括构造判断矩阵和决定权重并检查一致性。AHP 权重计算的步骤为:

1) 建立分层结构:安全评估指标体系中的第一层为目标层,用于系统整体评估目标;第二层为安全类层,用于将安全性分类为影响系统安全的各个方面;第三层为子类层,用于对上一层指标进行细化,以更细粒度的指标评价系统安全性。

2) 构造两两比较的判断矩阵:在建立分层结构模型的基础上,根据专家经验对所有因素进行两两比较,并使用 1~9 标度法由定性转化为定量。具体的 1~9 标度法如表 2 所示。最后建立判断矩阵 U ,其函数表示为

$$U = (u_{ij})_{n \times n} \quad i, j = 1, 2, \cdots, n \tag{1}$$

表 2 构造判断矩阵

标度	定义
1	两者重要性,A 等于 B
2	两者重要性,A 略大于 B
5	两者重要性,A 大于 B
7	两者重要性,A 明显大于 B
9	两者重要性,A 远远大于 B
2,4	表示 2 个相邻判断的中值
6,8	表示 2 个相邻判断的中值

以 C 表示总指标, C_i 表示第 i 层指标, $C_i \in C$ ($i=1,2,\cdots,n$), n 是因素的层数, 表示 C_i 与 C_j 的相对重要性数值($j=1,2,\cdots,n$), $U_{ij}=U_i/U_j$, 还满足

$$U_{ij}=1/u_{ji} \tag{2}$$

3) 层次单排序: 层次单排序是对当前层次中所有指标相对于上一层次对应的父指标重要程度进行排序。计算结果是判断矩阵 U 的最大特征根 $\lambda_{\max}$ 对应的特征向量。最后进行归一化, 得到单一权重向量。具体计算公式为

$$W = \frac{\sqrt[n]{\prod_{j=1}^n u_{ij}}}{\sum_{i=1}^n \sqrt[n]{\prod_{j=1}^n u_{ij}}} \quad i, j = 1, 2, \cdots, n \tag{3}$$

式中, u_{ij} 是判断矩阵 U 的各个元素, $W=[w_1, w_2, \cdots, w_n]^T$ 为判断矩阵 U 的特征向量, 即单一权重向量。

4) 检查一致性: 完成层次单排序后, 需要对判断矩阵进行校验, 需要计算一致性指标 C_I

$$C_I = \frac{(\lambda_{\max} - n)}{(n - 1)} \tag{4}$$

根据特征向量计算可得最大特征值 $\lambda_{\max}$

$$\lambda_{\max} = \sum_{i=1}^n \frac{(U \cdot W)_i}{nw_i} \tag{5}$$

依据公式(3)计算出最大特征根后, 计算检查一致性指标

$$C_R = \frac{C_I}{R_I} \tag{6}$$

公式(6)中, R_I 是随机性指标, 取值如表 3 所示, 在实际应用中, 如果随机一致性比例小于 0.1, 则认为其一致性良好。

表 3 R_I 取值表

n	1	2	3	4	6	7	8	9
R_I	0	0	0.58	1.12	1.24	1.32	1.41	1.45

5) 层次总排序: 在获得同一层中所有单个排序结果后, 可以计算本层中所有指标相对于上一层的重要性权值。

3.2 安全判断矩阵

安全评估判断树顶层为机载计算平台安全性, 第一层编号为 E ; 第二层编号为 C , 第二层的因素编号为 C_1, C_2, C_3 ; 第三层编号为 H , 第三层因素编号为 H_1, H_2, H_3 等, 以此类推。根据 AHP 法, 构造机载计算平台安全性能各层的判断矩阵分别见表 4 ~ 7 所示。

表 4 机载计算平台安全判断矩阵

计算平台安全	C_1	C_2	C_3	权值
C_1	1	2.19	3.35	0.52
C_2	0.46	1	1.53	0.31
C_3	0.3	0.65	1	0.17

表 5 时空隔离性判断矩阵

时空隔离	H_1	H_2	H_3	H_4	权值
H_1	1	1.38	0.91	1.6	0.29
H_2	0.72	1	0.66	1.17	0.21
H_3	1.10	1.52	1	1.78	0.32
H_4	0.62	0.86	0.56	1	0.18

表 6 可调度性判断矩阵

可调度性	H_5	H_6	权值
H_5	1	0.79	0.44
H_6	1.27	1	0.56

表 7 故障隔离性判断矩阵

故障隔离	H_7	H_8	权值
H_7	1	0.61	0.38
H_8	1.63	1	0.62

综合表 4~7, 可以得到机载虚拟化计算平台各级指标的权重值得到表 8。

表 8 综合安全判断矩阵

一级指标	二级指标	二级指标权重	一级指标权重
C_1	H_1	0.15	0.52
	H_2	0.11	0.52
	H_3	0.16	0.52
	H_4	0.10	0.52
C_2	H_5	0.14	0.31
	H_6	0.17	0.31
C_3	H_7	0.06	0.17
	H_8	0.11	0.17

综合上述,系统整体的安全性评估应该对这八项能力得分进行无量纲化处理后,再进行加权计算安全性得分。

4 机载计算平台安全等级评定

安全等级评定采用 GRAP 方法的目的是通过指标计算的方式得出当前虚拟化平台对航空电子系

统不同安全级别应用的适应度。其中, ω 表示安全等级适应度, $\omega_i(k)$ 表示只考虑相关指标情况下组件符合航空电子安全关键等级 DAL 要求为 i 的可能性(1~5 分别对应 DAL E/D/C/B/A 5 个安全等级),假设有 n 个组件,则这 n 个组件的安全等级适应度矩阵如公式(7)所示。

$$\omega = \begin{bmatrix} \omega_1(1) & \omega_1(2) & \cdots & \omega_1(n) \\ \omega_2(1) & \omega_2(2) & \cdots & \omega_2(n) \\ \vdots & \vdots & & \vdots \\ \omega_5(1) & \omega_5(2) & \cdots & \omega_5(n) \end{bmatrix}$$

(7)

GRAT 的具体步骤为:

1) 优先值数列 ω_0

$$\omega_0 = \{ \omega_0(k) \mid (k = 1, 2, \cdots, n) \}$$

(8)

公式(7)中, $\omega_0(k)$ 表示在所有的安全级要求中 k 的可能性最高,即

$$\omega_0(k) = \max \{ \omega_1(k), \omega_2(k), \omega_3(k), \omega_4(k), \omega_5(k) \}$$

(9)

所求得虚拟化计算平台符合度最优值代表的元素就是系统最适配的安全等级。

2) 计算关联系数

$$\xi_i(k) = \frac{\min_i \min_k | \omega_0(k) - \omega_i(k) | + \rho \max_i \max_k | \omega_0(k) - \omega_i(k) |}{| \omega_0(k) - \omega_i(k) | + \rho \max_i \max_k | \omega_0(k) - \omega_i(k) |}$$

(10)

公式(10)中, ρ 为分辨系数,根据经验通常取 0.5。

计算完所有 $\xi_i(k)$ 后,可得到关联系数矩阵 E

$$E = \begin{bmatrix} \xi_1(1) & \xi_2(1) & \cdots & \xi_5(1) \\ \xi_1(2) & \xi_2(2) & & \xi_5(2) \\ \vdots & \vdots & & \vdots \\ \xi_1(n) & \xi_2(n) & \cdots & \xi_5(n) \end{bmatrix}$$

(11)

公式(11)中, $\xi_i(k)$ 中 i 的取值为 1~5,分别代表对每个安全等级的关联系数。

3) 得出评估结果

$$R = P \cdot E$$

(12)

公式(12)中, P 表示通过前面介绍的 AHP 方法所得到的全部组件权值, $P = [P_1, P_2, \cdots, P_5]$, E 为上文得到的关联系数矩阵, $R = [\omega_1, \omega_2, \omega_3, \omega_4, \omega_5]$ 。 ω_i 代表整个系统对虚拟化安全等级不同级别的适应度。假设 $\max(R) = \omega_3$ 代表系统能满足的最高研制保证等级是 DAL D 级。

5 验 证

考虑机载计算平台的整体安全性指标,参考 GB/T 18336.1-2015 和 DO-178B/C,明确了在虚拟化机载场景下不同安全等级应用要求。利用 GRAP 方法结合各组件的安全性评估结果,得到了表 9 中的安全性结果。

表 9 组件安全等级评估表

二级指标	DAL E	DAL D	DAL C	DAL B	DAL A
H_1	0.20	0.50	0.15	0.10	0.05
H_2	0.15	0.60	0.10	0.10	0.05
H_3	0.05	0.05	0.55	0.25	0.10
H_4	0.05	0.75	0.10	0.05	0.05
H_5	0.05	0.70	0.10	0.10	0.05
H_6	0.05	0.05	0.65	0.15	0.10
H_7	0.10	0.55	0.15	0.10	0.10
H_8	0.10	0.60	0.15	0.10	0.05

1) 依据表 9,得到航空电子系统中机载信息系统(DAL D 级)的优先值数列 $\omega_0=[0.50,0.60,0.05,0.75,0.70,0.80,0.55,0.60]$,关联系数矩阵

$$E = \begin{bmatrix} \xi_1(1) & \xi_2(1) & \cdots & \xi_5(1) \\ \xi_1(2) & \xi_2(2) & \cdots & \xi_5(2) \\ \vdots & \vdots & & \vdots \\ \xi_1(8) & \xi_2(8) & \cdots & \xi_5(8) \end{bmatrix} = \begin{bmatrix} 1.00 & 1.80 & 0.93 & 0.87 & 0.82 \\ 0.82 & 1.80 & 0.77 & 0.77 & 0.73 \\ 0.77 & 0.77 & 1.80 & 1.00 & 0.82 \\ 0.63 & 1.80 & 0.69 & 0.63 & 0.63 \\ 0.66 & 1.80 & 0.69 & 0.69 & 0.66 \\ 0.69 & 0.73 & 1.80 & 0.77 & 0.69 \\ 0.82 & 1.80 & 0.87 & 0.82 & 0.82 \\ 0.77 & 1.80 & 0.82 & 0.73 & 0.77 \end{bmatrix} \quad (13)$$

得 $P=[0.15,0.11,0.16,0.10,0.14,0.17,0.06,0.11]$, $R=[0.77,1.45,1.13,0.80,0.74]$,因此,根据 GRAP 方法得出的评估结果认为被测系统最适配于 DAL D 级应用的要求。

2) 客舱系统(DAL E 级)的优先值数列 $\omega_0=[0.20,0.15,0.05,0.05,0.05,0.05,0.10,0.10]$,得 $P=[0.15,0.11,0.16,0.10,0.14,0.17,0.06,0.11]$,根据

公式(11)可以得到关联系数矩阵为 $R=[1.47,1.21,0.89,1.11,0.77]$,得出的评估结果认为被测系统最适配 DAL E 级应用的要求。

3) 机载维护系统(DAL C 级)的优先值数列 $\omega_0=[0.15,0.10,0.55,0.10,0.10,0.65,0.15,0.15]$,得 $P=[0.15,0.11,0.16,0.10,0.14,0.17,0.06,0.11]$,根据(11)式可得到关联系数矩阵为 $R=[0.90,1.22,1.38,0.87,0.73]$,得出的评估结果认为被测系统最适配 DAL C 级应用的要求。

6 结 论

本文基于现有航空电子虚拟化技术的进展,分析了虚拟化对机载计算平台安全隔离性和可调度性的影响因素。针对这些因素,建立了模型进行评估,并使用 AHP 方法计算了每个因素的权重;通过 GRAP 方法,确定了被测系统最适应的安全等级。根据模型计算得到的安全能力指标,确定了虚拟化机载计算平台的安全性,并计算加权的安全评分,利用灰度关联模型,对系统符合的具体安全等级进行评定。

参考文献:

[1] 张军才,茹伟,胡宇凡.民用客机 E 化趋势及其对航电系统的影响[J].航空计算技术,2016,46(5):115-118
ZHANG Juncai, RU Wei, HU Yufan. Civil aircraft e-enabling trend and influence on avionics system[J]. Aeronautical Computing Technique, 2016,46(5):115-118 (in Chinese)

[2] MARKO W, MORITZ M, MARTIN M. Information technology security threats to modern E-enabled aircraft: a cautionary note [J]. Aerospace Information Systems, 2014,11(7):154-164

[3] 张军红,童强.基于软件虚拟化技术的新一代航空机载软件设计[J].南京航空航天大学学报,2019,51(6):772-777
ZHANG Junhong, TONG Qiang. New generation aeronautical airborne software design based on software virtualization technology [J]. Journal of Nanjing University of Aeronautics & Astronautics, 2019,51(6):772-777 (in Chinese)

[4] 赵光.多核处理器在综合模块化航空电子系统中的应用[J].科技视界,2016(13):140
ZHAO Guang. Application of multicore processor in IMA[J]. Science & Technology Vision, 2016(13):140 (in Chinese)

[5] 汪恺,张功萱,周秀敏.基于容器虚拟化技术研究[J].计算机技术与发展,2015(8):138-141
WANG Kai, ZHANG Gongxuan, ZHOU Xiumin. Research on virtualization technology based on container[J]. Computer Technology and Development, 2015(8):138-141 (in Chinese)

[6] 陈刚,关楠,吕松鸣,等.实时多核嵌入式系统研究综述[J].软件学报,2018,29(7):2152-2176
CHEN Gang, GUAN Nan, LYU Songming, et al. State-of-the-art survey of real-time multicore system[J]. Journal of Software, 2018,29(7):2152-2176 (in Chinese)

[7] 崔德龙,夏曼.虚拟化技术在航空计算领域的应用[J].航空工程进展,2022,13(2):71-77
CUI Delong, XIA Man. Application of virtualization technology in aeronautical computing field[J]. Advances in Aeronautical Science and Engineering, 2022,13(2):71-77 (in Chinese)

- [8] 王卫东, 邸海涛, 张伟栋, 等. 面向 IMA 应用的多核处理器系统研究与实现[J]. 微电子学与计算机, 2019, 36(6): 10-14
WANG Weidong, DI Haitao, ZHANG Weidong, et al. Research and implement of a multicore processing system used for IMA system[J]. Microelectronics & Computer, 2019, 36(6): 10-14 (in Chinese)
- [9] Federal Aviation Administration. Assurance of multicore processors in airborne systems[S]. DOT/FAA/TC-16/51
- [10] 程广辉. 基于微内核的操作系统设计及其嵌入式虚拟化应用的研究[D]. 兰州: 兰州大学, 2013
CHENG Guanghui. The study of OS design based on microkernel and application of embedded virtualization[D]. Lanzhou: University of Lanzhou, 2013 (in Chinese)
- [11] 陈昊. 高可信嵌入式系统软件的关键技术研究[D]. 成都: 电子科技大学, 2018
CHEN Hao. Research on key issues in high assurance system software of embedded systems[D]. Chengdu: University of Electronic Science and Technology of China, 2018 (in Chinese)
- [12] YORICK D B, SIEGFRIED M, JAN B, et al. Real-time virtualization with Xvisor[J]. Internet of Things, 2020(11): 1-13
- [13] KIM H, KANDHALU A, RAJKUMAR R. A coordinated approach for practical OS-level cache management in multi-core real-time systems[C]//2013 25th Euromicro Conference on Real-Time Systems, 2013: 80-89
- [14] JAKUB S, RUBY B L. Architectural support for hypervisor-secure virtualization [C]// Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems, 2012
- [15] 郝继锋, 虞保忠, 周霆, 等. 一种多核混合分区调度算法设计与实现[J]. 微电子学与计算机, 2016, 33(7): 140-144
HAO Jifeng, YU Baozhong, ZHOU Ting, et al. Design and implementation of the multicore hybrid partition scheduling algorithm [J]. Microelectronics & Computer, 2016, 33(7): 140-144 (in Chinese)
- [16] 王心然. 安全虚拟化容器的性能优化[D]. 上海: 上海交通大学, 2020
WANG Xinran. Performance optimization of secure virtualization containers[D]. Shanghai: Shanghai Jiaotong University, 2020 (in Chinese)
- [17] 符宁, 杜承烈, 李建良, 等. AADL 分级调度模型的分析与验证[J]. 计算机研究与发展, 2015, 52(1): 167-176
FU Ning, DU Chenglie, LI Jianliang, et al. Analysis and verification of AADL hierarchical schedulers[J]. Journal of Computer Research and Development, 2015, 52(1): 167-176 (in Chinese)
- [18] 雷煜靓, 胡宁, 陈福, 等. ARINC653 实时任务可调度性验证方法[J]. 单片机与嵌入式系统应用, 2021, 21(4): 15-20
LEI Yuliang, HU Ning, CHEN Fu, et al. Verification method of schedulability for real-time task in ARINC653[J]. Microcontrollers & Embedded Systems, 2021, 21(4): 15-20 (in Chinese)
- [19] BUI B D, CACCAMO M, SHA L, et al. Impact of cache partitioning on multi-tasking real-time embedded systems[C]//2008 14th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2008: 101-110
- [20] ALTMAYER S, DOUMA R, LUNNISS W, et al. On the effectiveness of cache partitioning in hard real-time systems[J]. Real-Time Systems, 2016, 52(5): 598-643
- [21] 杨仕平. 分布式任务关键实时系统的防危技术研究[D]. 成都: 电子科技大学, 2004
YANG Shiping. Research on crisis prevention technology of distributed mission-critical real-time system [D]. Chengdu: University of Electronic Science and Technology of China, 2004 (in Chinese)

Safety assessment of virtualization computing platform
for avionics system of civil aircraft

YANG Huan¹, WANG Xiaodong¹, LI Geng¹, ZHANG Shuang², GUO Yangming³

- (1.School of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China;
2.Xi'an Aeronautical Computing Technique Research Institute, Xi'an 710068, China;
3.School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Aiming at the main problems that affect the security of airborne computing platform after virtualization, such as time-space isolation, fault isolation and schedulability, this paper studies the security level evaluation of airborne computing platform under virtualization environment. Considering the characteristics of virtualized avionics system, a security calculation method based on analytic hierarchy process (AHP) and gray correlation analysis (GARD) is proposed. The safety evaluation decision tree of airborne virtualization computing platform is established, and the weight of each safety capability is calculated by AHP method, and the overall safety score of the system is given. On this basis, combined with GRAP method and referring to the safety evaluation of avionics system, the safety level with the highest adaptability between the test system and DAL safety level requirements is calculated, realizing security grade evaluation of airborne computing platform under virtualization environment.

Keywords: civil aircraft; computing platform; virtualization; functional safety; analytical hierarchy process

引用格式: 杨欢, 王晓东, 李庚, 等. 民机航电系统虚拟化计算平台功能安全评估研究[J]. 西北工业大学学报, 2024, 42(1): 45-52

YANG Huan, WANG Xiaodong, LI Geng, et al. Safety assessment of virtualization computing platform for avionics system of civil aircraft[J]. Journal of Northwestern Polytechnical University, 2024, 42(1): 45-52 (in Chinese)