

引用格式:王鹏,张帆,董磊,等.基于概率模型检验的民机平视显示系统建模与安全性分析[J].电光与控制,2017,24(11):64-69. WANG P, ZHANG F, DONG L, et al. Probability model check based modeling and safety analysis of HUD system on civil aircrafts[J]. Electronics Optics & Control, 2017, 24(11):64-69.

基于概率模型检验的民机平视显示系统建模与安全性分析

王鹏^a, 张帆^b, 董磊^a, 赵长啸^a

(中国民航大学, a. 天津市民用航空器适航与维修重点实验室; b. 适航学院, 天津 300300)

摘要: 民机平视显示系统(HUD)作为安全关键系统,由于其高度复杂且与其他机载系统结合使用,使得传统系统安全性评估方法难以满足定量安全性分析需求。因此,需要开发基于形式化模型的安全性评估(MBSA)方法,在明确概率模型检验原理及系统高层建模规范基础上,研究平显系统概率模型分层建模方法,建立平显系统概率模型,并描述系统定量安全性属性,展开自动概率模型检验,得出定量安全性分析结论,提高安全性分析效率与运算结果精确度。

关键词: 平视显示器; 民机; 概率模型检验; 形式化模型; 定量分析; 安全性

中图分类号: V240.2 **文献标志码:** A **doi:**10.3969/j.issn.1671-637X.2017.11.013

Probability Model Check Based Modeling and Safety Analysis of HUD System on Civil Aircrafts

WANG Peng^a, ZHANG Fan^b, DONG Lei^a, ZHAO Chang-xiao^a

(Civil Aviation University of China, a. Civil Aircraft Airworthiness and Repair Key Laboratory of Tianjin;
b. College of Airworthiness, Tianjin 300300, China)

Abstract: Head-Up Display (HUD) onboard civil aircrafts is a crucial safety system. Because of its high complexity and other airborne systems combined with it, the traditional system-safety-assessment method has difficulty in meeting the requirements of a quantitative safety analysis. Therefore, it's necessary to develop a Model-Based Safety-Assessment (MBSA) method. On the basis of clearly defining the principles of the probability model check and the high-level system-modeling specifications, we studied the method for hierarchical modeling of the probability model of the HUD system, built the probability model of the HUD system, described the quantitative safety properties of the system, and carried out automatic probability model checks. The conclusion of the quantitative safety analysis was obtained, which can improve the efficiency of the safety analysis and the accuracy of the calculating results.

Key words: head-up display; civil aircraft; probability model check; formalized model; quantitative analysis; safety

0 引言

作为民用飞机航行新技术,平视显示系统(HUD)与其他系统相互综合,将重要的飞行参数(如飞行高

度、飞行速度、姿态、航向等)以图形、字符的形式,通过光学部件投影到座舱正前方组合仪上^[1]。由于该组合仪高度大致与飞行员的眼睛处于水平位置,因此飞行员透过平显观察舱外景物时,几乎不用改变眼睛焦距就能同时观测到平显上显示的图形和字符信息,从而及时修正飞行姿态,对于减轻飞行员负担,提高飞行员环境感知能力,增强飞行安全性具有重要意义。

随着平显系统集成化程度的提高,平显系统部分功能以模块化形式集成到综合模块化的航电系统(IMA)中,且通过飞控系统、增强视景系统等获取数据及视频信息,使得平显系统高度复杂。作为航电安全关键系统,由于传统基于双V的安全性评估方法^[2]存

收稿日期:2017-01-13

修回日期:2017-03-29

基金项目:国家自然科学基金委员会-中国民航局民航联合研究基金资助(U1533105);中国民航大学科研启动基金项目(2013QD04X);天津市自然科学基金联合资助项目(15JCQNJC42800);中国民航大学科技创新基金(Y17-25)

作者简介:王鹏(1982—),男,天津人,硕士,副教授,研究方向为民机系统安全性设计与评估、机载电子硬件适航技术。

在工作量大、依赖于专家经验且易于出错等问题^[3],需要开发新型的基于模型的自动化分析方法,对民机平显系统展开定量分析,提高安全性评估效率。

针对上述问题,采用基于概率模型检验的形式化安全性分析技术,在分析平显系统物理架构及功能基础上,探索平显系统分层建模方法,深入分析系统内部失效转移逻辑,对系统定量安全性属性展开自动化验证,得出分析结论。

1 概率模型检验

1.1 概率模型检验概述

概率模型检验 (Probabilistic Model Checking) 通过形式化方法,验证具有随机行为的系统定量属性^[4]。基于平显系统的概率模型检验框架如图 1 所示,包括以下两项输入^[5]。

1) 系统高层模型。基于严格的平显系统物理架构及功能分析,捕获平显系统内部各模块失效模式、失效概率及失效转移路径,对系统进行高层模型建模。

2) 形式化属性规范。通过分析平显系统定量安全性需求,将其以时序或稳态逻辑形式表达为系统属性规范。

完成上述平显系统建模与属性规范表达后,基于状态机原理进行自动化底层系统失效状态转移建模,分析失效路径并计算各状态定量概率,得出安全性分析结论。

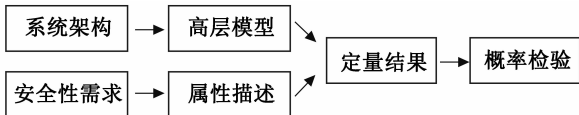


图 1 概率模型检验框架

Fig. 1 An overview of probabilistic model checking

1.2 概率模型检验原理

自动分析系统概率行为并建立系统高层模型,是概率模型检验的关键内容。概率模型检验支持离散时间 Markov 链 (DTMC)、连续时间 Markov 链 (CTMC) 及 Markov 决策过程 (MDP)^[6]。在民机系统安全性分析过程中,采用 CTMC 对系统行为进行分析。

1) 连续时间 Markov 链定义。

设过程 $\{X(t), t \geq 0\}$ 为连续时间的随机过程,若对于一切 $s, t \geq 0$ 和非负整数 $i, j, x(u), 0 \leq u \leq s$, 有

$$P\{X(t+s) = j | X(s) = i, X(u) = x(u), 0 \leq u < s\} = P\{X(t+s) = j | X(s) = i\} \quad (1)$$

则称过程 $\{X(t), t \geq 0\}$ 是一个连续时间 Markov 链^[7]。通常,以 $P_{ij}(t)$ 表示当前处于状态 i 的 Markov 链在附加时间 t 后处于状态 j 的概率,即

$$P_{ij}(t) = P\{X(t+s) = j | X(s) = i\} \quad (2)$$

2) 状态转移及运算原理。

连续时间 Markov 链能够表示随着时间变化,系统可能出现的各种状态及状态间的转移关系。在基于概率模型检验的民机系统安全性分析中,各状态指的是系统可能出现的失效模式,转移关系指正常模式与失效模式以及各失效模式之间的转换逻辑。完成系统高层建模后,概率模型基于 CTMC 将高层模型转换为底层模型,进行概率计算,以支持定量安全性分析。对应底层模型举例如图 2 所示,并得到其相应的微分方程组。

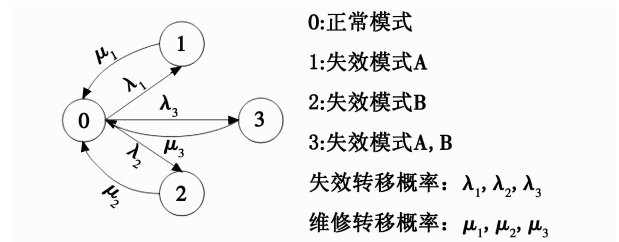


图 2 CTMC 底层模型

Fig. 2 CTMC bottom-level model

$$\begin{cases} \frac{dP_0(t)}{dt} = -(\lambda_1 + \lambda_2 + \lambda_3)P_0(t) + \mu_1P_1(t) + \mu_2P_2(t) + \mu_3P_3(t) \\ \frac{dP_1(t)}{dt} = \lambda_1P_0(t) - \mu_1P_1(t) \\ \frac{dP_2(t)}{dt} = \lambda_2P_0(t) - \mu_2P_2(t) \\ \frac{dP_3(t)}{dt} = \lambda_3P_0(t) - \mu_3P_3(t) \end{cases} \quad (3)$$

通过拉氏变换,概率模型检验将自动求解上述微分方程,可得到经过确定的时间 t ,处于上述 4 种状态的概率,完成定量计算过程。

1.3 概率模型高层建模规范

概率模型检验方法通过结构化的高级语言对系统建模,该语言由最基本的模块及变量组成。通过建立一系列表示系统各组分的并行模块,以变量形式定义各模块的失效模式及其概率,并采用逻辑等式的方式,表达模块中变量之间、模块与模块间的相互关系。模块的失效行为由一系列命令表示,对于 CTMC,采用以下语法表达命令: $[action](guard) \rightarrow (rate) : (update)$;其中,命令起始于 $[]$, $action$ 为同步符号; $(guard)$ 表示模块中的变量,在系统安全性分析建模中,变量通常为失效模式; \rightarrow 表示状态转移,执行该状态转移的条件是 $(guard)$ 为真; $(update)$ 表示转移后的状态; $(rate)$ 表示发生该转移的概率。

概率模型采用标准的 CSP 并行代数处理器将各模块进行集成,可更精确地指定模块间的同步关系。同时,对于模块中各状态之间、模块与模块之间的逻辑关

系,通过逻辑等式的形式描述。基于布尔表达式,逻辑等式将模块变量以基础逻辑形式(如 NOT:!, AND:&, OR:|)衔接,在系统安全性分析建模时,便于模块及功能的封装。

2 基于概率模型检验的平显系统建模

2.1 平显系统物理架构与典型功能分析

典型的民用飞机平显系统主要是由平显计算机(HUDC)、组合仪(HCU)、投影组件(HPU)组成^[8]。通过ADN数据网络及航空总线,由左右两侧HUDC接收来自于飞机其他航电设备的各种数据,如速度、加速度、姿态、位置、风速、导航信息、引导提示、告警信息等^[9],经处理、融合后生成HUD显示图像,再经过总线分别传递至左右两侧HPU,最终显示于机长与副驾HCU。根据平显系统的主要功能,识别其交互界面,如表1所示。

作为概率模型检验的系统安全性需求输入之一,通过功能危害性评估(FHA)识别出平显系统的失效状

态及影响等级,其中,灾难性失效状态(I类)如表2所示。此处,选取双侧HUD姿态误指示这种失效状态,作为安全性分析的对象。图3是HUD在显示飞行姿态功能下对应的系统物理架构。

表1 平显系统主要功能及交互界面
Table 1 Main functions and interfaces of HUD

交互界面	功能
惯性基准组件(IRU)	显示姿态
大气数据计算机(ADC)	显示空速、垂直速度
气压高度计(BA)	显示气压高度
无线电高度表(RA)	显示无线电高度
无线电接口单元(RIU)	进近着陆、导航信息
侧滑传感器(SS)	显示侧滑信息
综合处理机柜(IPC)	显示航向、航迹信息
空中防撞系统(TCAS)	显示TCAS数据
地形规避警告系统(TAWS)	显示近地告警、风切变信息
中央维护系统(CMS)	提供维护信息支持

表2 平显系统灾难性失效状态

Table 2 HUD catastrophic failure conditions

功能	失效状态	飞行阶段	影响	等级	验证方法
提供空速显示	双侧HUD空速误指示且无失速、超速告警	ALL	飞机:可能失控,导致机毁人亡。 机组:可能按错误空速指示操纵,导致飞机损毁。 乘客:可能大部分或全部死亡。	I	定量FMEA、定量FTA CCA
提供姿态显示	双侧HUD姿态误指示	ALL	飞机:可能失控,导致机毁人亡。 机组:可能按错误姿态指示操纵,导致飞机损毁。 乘客:可能大部分或全部死亡。	I	定量FMEA、定量FTA CCA
提供气压高度显示	双侧HUD气压高度误指示	ALL	飞机:可能失控,导致机毁人亡。 机组:可能按错误气压高度指示操纵,导致飞机损毁。 乘客:可能大部分或全部死亡。	I	定量FMEA、定量FTA CCA

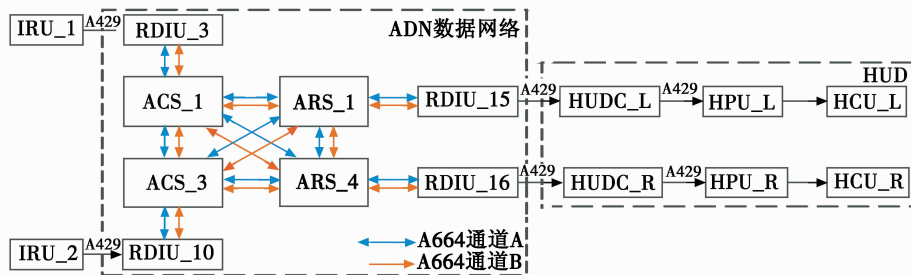


图3 基于飞行姿态显示功能的平显物理架构

Fig. 3 HUD physical architecture based on attitude display

2.2 平显系统概率模型分层建模方法

平显系统作为重要航电系统,关系到飞机整机的可靠性与安全性。由于平显系统具备模块化、资源共

享等特点,因此对其进行概率模型建模与安全性分析面临技术困难。此外,由于模型检验方法的本质是基于对状态空间的穷举搜索,对于并发系统,其状态数目

会随着并发量的增加而呈指数增长,出现状态爆炸问题^[10]。解决上述问题,对其进行概率模型建模时,采用基于不同粒度的分层建模方法,降低系统复杂程度,减少状态空间数量。

由于在进行初步系统安全性评估(PSSA)时,需要根据 ARP 4754A^[11],将功能研制保证等级由系统向子系统、设备及软硬件分解,因此,在概率模型分层建模时,以功能为上下层级连接依据,从软硬件功能模块或内部元件开始建模,通过逻辑等式逐步向上一级封装,分别建立元件级/功能模块级、设备级、子系统级、系统级 4 层模型,建模层次如图 4 所示。

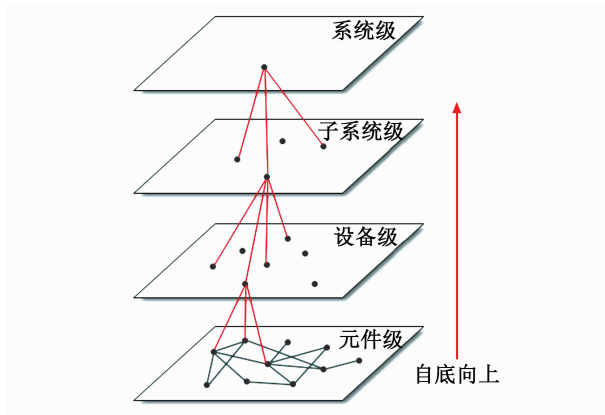


图 4 概率模型层次图

Fig. 4 Hierarchical probabilistic model

2.3 平显系统概率模型建模

2.3.1 功能模块级概率模型建模

平显系统概率模型建模从设备内部软硬件功能模块开始。由于平显系统为复杂航电系统,因此设备内部软硬件功能模块复杂,不再详细描述。此处以图 3 中左侧 HUDC(HUDC_L)为例,根据选定的失效状态,双侧 HUD 飞行姿态误显示,识别相应失效信息如表 3 所示,对应概率模型为 3 个模块,图形处理、图形存储与数据传输;每个模块内定义了失效模式及发生概率。

表 3 左侧 HUDC 故障模式与影响分析

Table 3 Left HUDC FMEA

功能模块	失效模式	失效影响	失效率
图形处理	图形反走样功能丧失	图形失真,造成误显示	$3.56E-5$
	预畸变处理功能丧失	图形畸变,造成误显示	$1.27E-5$
	图形旋转缩放功能丧失	图形旋转缩放不当,造成误显示	$6.17E-6$
图形存储	图形读写功能丧失	图形缺陷,造成误显示	$4.33E-6$
数据传输	数据丢失或误码	图形缺陷,造成误显示	$1.78E-6$

根据表 3 失效信息,建立左侧 HUDC 概率模型

如下。

```

ctmc
moduleHUDC_processor
HUDC_antialiasing_failure_mode;boolinit false;
HUDC_predistortion_failure_mode;boolinit false;
HUDC_rotate_failure_mode;boolinit false;
[ ](! HUDC_anatialiasing_failure_mode -> (3.56 - 5) : (HUDC_
analialiasing_failure_mode' = true) ;
[ ](! HUDC_predistortion_failure_mode) -> (1.27E - 5) :
(HUDC_predistortion_failure_mode' = true) ;
[ ](! HUDC_rotate_failure_mode) -> (6.17E - 6) : (HUDC_ro-
tate_failure_mode' = true) ;
endmodule
moduleHUDC_storage
HUDC_storage_failure_mode;boolinit false;
[ ](! HUDC_storage_failure_mode) -> (4.33E - 6) : (HUDC_
storage_failure_mode' = true) ;
endmodule
moduleHUDC_data
HUDC_data_failure_mode;boolinit false;
[ ](! HUDC_data_failure_mode) -> (1.78E - 6) : (HUDC_data_
failure_mode' = true) ;
endmodule
    
```

2.3.2 设备级概率模型建模

设备级建模指的是设备内部软硬件建模。建立设备级概率模型时,首先需要分析设备整体的失效路径,即分析失效模式组合导致设备特定功能失效的失效逻辑。作为 HUD 内部的一个 LRU(航线可更换单元),左侧 HUDC 内部模块失效模式造成姿态误显示的失效逻辑如下: $formula_{HUDC_L_wrong_attitude} = (HUDC_antialiasing_failure_mode) \mid (HUDC_predistortion_failure_mode) \mid (HUDC_rotate_failure_mode) \mid (HUDC_storage_failure_mode) \mid (HUDC_data_failure_mode)$ 。

其中,formula 为等式标签,等号左端为 HUDC_L 原因造成姿态误显示,等号右端为 HUDC_L 内部各功能模块失效模式间失效逻辑。通过建立上述逻辑等式描述,完成设备内部功能模块失效模式向设备级封装,即完成设备级建模过程。按上述方法依次完成平显系统其他设备的设备级建模,在此不再赘述。

2.3.3 子系统级概率模型建模

平显系统包括两个子系统,分别为平显及 ADN 数据网络。同理,在明确子系统内部各设备特定功能失效的条件下,通过建立各设备失效逻辑,可完成设备向子系统的封装,即子系统级概率模型建模。首先分析左侧平显子系统姿态误显示失效逻辑,左侧平显姿态误显示是由 HUDC_L 图像缺陷、左侧 HPU 图像缺陷及 A429 误码导致,对应子系统级建模如下: $formula_{HUD_L_wrong_attitude} = (HUDC_L_wrong_attitude) \mid (HPU_L_$

wrong_image_failure_mode)|(A429_7_wrong_data_failure_mode)。

对于另一子系统,ADN 数据网络原因导致姿态误显示,当来自左侧惯性系统的姿态数据经过 ADN 网络后出现错误,则会导致左侧平显姿态误显示,ADN 网络为双通道网络,当 A,B 两个通道均失效时,对应左侧平显姿态误显示。子系统建模如下:formula ADN_L_wrong_attitude = (RDIU_3_data_failure_mode) | (((A664_1_wrong_data_failure_mode) | (ACS_1_data_failure_mode) | (A664_5_wrong_data_failure_mode) | (ARS_1_data_failure_mode) | (A664_7_wrong_data_failure_mode) | (RDIU_15_data_failure_mode) | (A429_3_wrong_data_failure_mode)) & ((A664_2_wrong_data_failure_mode) | (ARS_4_data_failure_mode) | (A664_8_wrong_data_failure_mode) | (RDIU_16_data_failure_mode) | (A429_5_wrong_data_failure_mode)))。

2.3.4 系统级概率模型建模

完成上述子系统建模后,对子系统进行逻辑等式封装,得到左侧平显姿态误显示系统级概率模型,其失效由惯性系统或 ADN 数据网络或平显导致;同理可得右侧系统级概率模型,二者同时发生,导致失效状态双侧平显姿态误显示发生。对应左、右两侧及双侧系统级模型为:

formulasystem_L_wrong_attitude = (IRU_L_attitude_failure_mode) | (A429_1_wrong_data_failure_mode) | (ADN_L_wrong_attitude) | (HUD_L_wrong_attitude);

formulasystem_R_wrong_attitude = (IRU_R_attitude_failure_mode) | (A429_2_wrong_data_failure_mode) | (ADN_R_wrong_attitude) | (HUD_R_wrong_attitude);

formulasystem_wrong_attitude = (system_L_wrong_attitude) & (system_R_wrong_attitude)。

3 平显系统定量安全性分析

3.1 系统属性规范描述

验证系统行为是否满足定量安全性需求,必须将系统行为进行形式化描述,即系统属性规范描述。针对 CTMC 的定量属性验证,应在捕获系统定量属性需求的基础上,采用 CSL 连续随机逻辑语言对系统属性进行形式化规范。基于 CSL 语言的逻辑形式包括两种,时序逻辑和稳态逻辑^[12]。通常,稳态逻辑用于检验系统长时间运行条件下,某状态出现的概率。然而由于稳态逻辑受限于平衡状态,对于飞机系统安全性评估中需要检验的属性,如平均每飞行小时某失效状态出现的概率,应采用时序逻辑形式描述。如果系统在 2 h 之内发生失效状态 A 的概率可以表示为:

$P = ? [\text{true } U \leq 2(\text{system_FC_A})]$ 。完成属性描述后,概率模型将自动展开属性检验,得出结论。

3.2 定量安全性分析

完成平显系统概率模型建模后,对其定量安全性属性展开自动化验证。根据系统安全性需求,要求双侧 HUD 姿态误指示发生概率应小于等于 $1E-9$ 平均每飞行小时,设该机型飞机每次飞行平均飞行小时为 2 h,根据这个需求从设备级起逐级展开定量验证,相应左侧系统、右侧系统及系统整体失效的时序逻辑如下:

$$\begin{cases} P = ? [\text{true } U \leq 2(\text{system_L_wrong_attitude})] / 2 \\ P = ? [\text{true } U \leq 2(\text{system_R_wrong_attitude})] / 2 \\ P = ? [\text{true } U \leq 2(\text{system_wrong_attitude})] / 2 \end{cases}$$

概率模型检验器基于 Markov 状态转移原理,建立系统底层运算模型,并通过基于符号模型检测的 MTBDD(多终端二叉决策图)对状态进行归并与化简,且进一步利用稀疏引擎、MTBDD 引擎及混合引擎^[13]展开自动定量概率运算后,得到双侧平显系统姿态误指示的定量安全性分析结果如表 4 所示。

表 4 双侧平显系统失效概率分析

Table 4 Bilateral HUD failure probability analysis

定量属性	概率/平均每飞行小时
左侧平显系统姿态误指示	7.1422E-5
右侧平显系统姿态误指示	8.4498E-5
双侧平显系统姿态误指示	6.0350E-9

经过对双侧平显系统姿态误指示的概率模型自动验证,共分析了 4 194 304 个状态,可能的状态转移达 46 137 345 个,通过遍历验证,最终得到失效状态“双侧平显系统姿态误指示”的概率为平均每飞行小时 $6.035E-9$ 。根据系统安全性需求,该值应小于等于平均每飞行小时 $1E-9$,因此,不满足系统安全性需求,可通过提供计算保守性证明或重新设计调整物理架构,以进一步满足该安全性需求。

在此,考虑对物理架构重新调整,使系统满足安全性需求。逐级检验左侧平显系统定量属性,得到安全性结果如表 5 所示。

表 5 左侧平显系统失效概率分析

Table 5 Left HUD failure probability analysis

定量属性	概率/平均每飞行小时
左侧 ADN 失效导致姿态误指示	3.2292E-6
左侧 HUDC 失效导致姿态误指示	6.0564E-5
左侧 HPU 失效导致姿态误指示	6.3214E-5

根据表 5 结果可知,左侧 HUDC 及 HPU 失效导致姿态误指示发生的概率较大,因此对两侧 HUDC 物理架构重新进行安全性设计。由于 HUDC 功能模块中图形处理模块承担着图形反走样、预畸变处理以及分辨

率调整等重要功能,且这些功能均由同一个 FPGA 执行,因此,考虑在 HUDC 内部设置 CPU,对该功能模块进行监控,当处理后的图像不符合处理前信息时,由 CPU 发出错误指令,终止图像显示。在该物理架构下,经过属性验证,HUDC 失效导致姿态误指示的概率为平均每飞行小时 $6.3828E-9$,平显系统姿态误指示的定量安全性分析结果如表 6 所示。

表 6 新架构下双侧平显系统失效概率分析

Table 6 Bilateral HUD failure probability analysis with new architecture

定量属性	概率/平均每飞行小时
左侧平显系统姿态误指示	$1.0866E-5$
右侧平显系统姿态误指示	$2.3946E-5$
双侧平显系统姿态误指示	$2.602E-10$

架构调整后,失效状态“双侧平显系统姿态误指示”的概率为平均每飞行小时 $2.602E-10$,满足系统安全性需求,定量系统安全性分析工作完成。

上述定量安全性分析均由概率模型检验器 PRISM 完成,该工具是由英国伯明翰大学、牛津大学及格拉斯哥大学共同设计开发的形式化建模与定量验证工具。目前已广泛应用于不同领域,包括通信、多媒体协议、安全协议、动态资源管理规划、生物系统等,为系统安全性分析提供了巨大支持^[4]。在此基础上,将其运用于民机复杂航电系统定量安全性分析,具有一定价值与意义。

4 结论

本文提出了基于概率模型检验的形式化安全性分析方法,有效解决了平视显示系统高复杂性、模块化程度高的问题。基于 Markov 理论,将系统内各模块失效模式作为 Markov 状态,在明确各状态间的转移关系基础上,采用分层建模技术,建立各层级概率模型,有效降低了系统复杂程度;最后通过时序逻辑描述检验系统定量安全性需求,以遍历方式自动完成所有状态及转移检验,得出定量概率验证结果,该结果能为系统安全性评估提供有效支持,降低安全性评估工作量,提高定量分析精度。

参 考 文 献

- [1] 吴连慧. 机载平显图形生成与视频处理算法研究及其 FPGA 实现[D]. 南京:南京航空航天大学,2014.
- [2] SAE. ARP4761 guidelines and methods for conducting the safety assessment process on civil airborne systems[S]. [S. l.];SAE International, 1996.
- [3] KWIATKOWSKA M, NORMAN G, PARKER D. Advances and challenges of probabilistic model checking[J]. Communication, Control, & Computing, 2010, 111(2): 1691-1698.
- [4] NORMAN G, PARKER D. Quantitative verification: formal guarantees for timeliness, reliability and performance[R]. London: London Mathematical Society and Smith Institute, 2014.
- [5] KWIATKOWSKA M, NORMAN G, PARKER D. PRISM: probabilistic model checking for performance and reliability analysis[J]. ACM Sigmetrics Performance Evaluation Review, 2009, 36(4): 40-45.
- [6] ELMQVIST J, NADJM-TEHRANI S. Formal support for quantitative analysis of residual risks in safety-critical systems[C]//HASE'08 Proceedings of the 11th IEEE High Assurance Systems Engineering Symposium, Washington: IEEE Computer Society, 2008:154-164.
- [7] ROSS S M. 随机过程[M]. 龚光鲁,译. 2版. 北京:机械工业出版社,2015.
- [8] 王全忠,高文正. 平视显示器在民用飞机上的应用研究[J]. 电光与控制,2014,21(8):1-5.
- [9] 费益,季小琴,程金陵. 平视显示系统在民用飞机上的应用[J]. 电光与控制,2012,19(3):95-99.
- [10] 侯刚,周宽久,勇嘉伟,等. 模型检测中状态爆炸问题研究综述[J]. 计算机科学,2013,40(s1):77-86.
- [11] SAE. ARP4754A guidelines for development of civil aircraft and systems[S]. [S. l.];SAE International, 2010.
- [12] GE X C, PAIGE R F, MCDERMID J A. Analysing system failure behaviours with PRISM[C]//Fourth International Conference on Secure Software Integration and Reliability Improvement Companion, IEEE Computer Society, 2010: 130-136.
- [13] YAN S, ZHANG H, ZHANG Y. Reliability prediction of a hydraulic system with probabilistic model checking [C]//International Conference on Reliability Systems Engineering, IEEE, 2016:1-7.

[1] 吴连慧. 机载平显图形生成与视频处理算法研究及其