

doi:10.3969/j.issn.1001-893x.2014.07.023

引用格式: 阎芳, 谢文光, 赵长啸, 等. 机载软件数据质量评价参数及验证方法[J]. 电讯技术, 2014, 54(7): 990-995. [YAN Fang, XIE Wen-guang, ZHAO Chang-xiao, et al. Evaluation Parameters and Validation Method of Airborne Software Data Quality[J]. Telecommunication Engineering, 2014, 54(7): 990-995.]

机载软件数据质量评价参数及验证方法*

阎芳^{1,**}, 谢文光², 赵长啸¹, 王鹏²

(1. 中国民航大学 天津市民用航空器适航与维修重点实验室, 天津 300300;
2. 中国民航大学 民用航空器适航审定技术与管理研究中心, 天津 300300)

摘要:通过分析影响机载数据质量的因素,建立了机载软件数据传输模型。提出了机载软件数据质量的定性评价方法,按照机载软件对于数据的需求及相关工业标准要求,总结了层次化的机载软件数据质量评价参数。根据不同安全关键等级的数据需求,提出了针对性的数据质量确认、验证方法及其实现。本研究对于机载软件数据库的审定和机载软件数据质量的验证有一定的理论价值。

关键词:航空电子;适航;机载软件;安全性评估;验证方法;数据质量

中图分类号:V247.5 **文献标志码:**A **文章编号:**1001-893X(2014)07-0990-06

Evaluation Parameters and Validation Method of Airborne Software Data Quality

YAN Fang¹, XIE Wen-guang², ZHAO Chang-xiao¹, WANG Peng²
(1. Civil Aircraft Airworthiness and Repair Key Laboratory of Tianjin, Civil Aviation University of China, Tianjin 300300, China; 2. Civil Aircraft Airworthiness Certification Technology and Management Research Center, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Through analyzing the impact of airborne data quality factors, the software data model is established and a qualitative evaluation method is proposed. According to the needs of the airborne software for data, the data quality evaluation parameters of airborne software data are summarized. Based on different levels of safety-critical data requirements, different validation and verification methods of data quality and their implementation are presented. The research in this paper has a certain theoretical value for validation and verification of airborne software data quality.

Key words: avionics; airworthiness; airborne software; safety evaluation; validation method; data quality

1 引言

随着航空电子技术不断发展,现代飞机向着高度模块化、集成化的方向发展^[1],软件在航空电子系统中所占的比重越来越大^[2]。现代飞机几乎所有重要的功能系统都和机载软件相关,从第二代飞机起通过软件实现的功能随着每一代飞机而翻倍^[3]。机载软件系统的安全性问题得到了各国研

究机构和学者的关注,提出了基于模型的软件安全性评估方法^[4]、形式化验证方法^[5]、保证系统静态结构构件安全性依赖与认证目标之间的一致性评估方法^[6],以及面向适航认证的安全性评估方法^[7]等,民航当局也发布了相关资讯通告认可了 RTCA DO-178B^[8]作为机载软件的安全性评估指南。而对于机载软件重要组成的软件数据的安全性验证问

* 收稿日期:2014-03-01;修回日期:2014-06-04 Received date:2014-03-01;Revised date:2014-06-04
基金项目:中央高校基金项目(3122013p004);航空科学基金项目(20128067003);中国民航大学科研启动基金项目(2013QD04X)
Foundation Item: Fundamental Research Funds for the Central Universities(3122013p004); Aeronautical Science Foundation of China(No. 20128067003); The Scientific Research Foundation of Civil Aviation University of China(2013QD04X)

** 通讯作者: fyan@cauc.edu.cn Corresponding author: fyan@cauc.edu.cn

题,研究相对较少。

机载软件数据库是机载软件的一部分^[9],作为某些重要飞机功能的基础,其数据质量和安全性会直接影响航空器的安全。从 20 世纪 70 年代开始,就有机载系统以数据库作为其预期功能的基础,现代民用飞机上对数据库的应用越来越广泛,如基于性能的导航系统^[10]使航空器从传统的台(导航台)到台(导航台)飞行模式转变为点(航路点)到点(航路点)飞行模式,因此航空器极大依赖于导航数据库的相关信息,对机载导航数据的精度和时效性提出了更高要求。电子飞行包^[11]技术的应用将代替纸质资料为飞行员提供包括电子文档、飞行日志、性能计算、图形气象、电子化操作手册等功能,也给机载软件数据的采集、配置、更新带来了挑战。评估软件数据质量,提高软件数据库的安全性也是机载航电系统发展、应用亟需解决的问题。

数据质量评价方法一般分为定性方法和定量方法,定性评价法主要是针对数据质量定性元素的评价,是基于数据的相关信息进行演绎推理确定数据集的数据质量状况;定量评价法主要是针对数据质量定量元素的评价,通过与内部或外部的参照信息进行对比来评定数据集的数据质量状况^[12]。

本研究针对机载软件数据质量评价问题,提出一种定性的质量评价方法,总结了影响机载软件数据库数据质量的 7 个因素,并针对不同安全等级需求的数据提出了不同的确认和验证方法,并给出了确认和验证方法的实现。

2 机载软件数据

机载软件数据库是指以电子形式存储的为地面或航空器中的航空应用服务的数据库,其为某些航空应用(如导航、飞行计划、飞行仿真、地形告警等)提供服务。与普通数据不同,机载软件数据的质量和安全性关系到整个航空器的安全性。机载软件数据库中数据的采集、集成、更新、应用涉及到航空器设计、制造、运营、维护等各个阶段,因此对于其安全性的验证需要关注数据传输过程的每个环节,检查每一个影响数据库安全性的环节,实现对于数据库整个生命周期的数据质量验证。

机载软件数据传输链代表的是机载软件数据的一个元素或一个集合从产生到最终被使用的整个过程。在机载软件数据传输链中,每个环节均与相邻的环节相连,组成机载软件数据传输链的环节可能是机构、机构中的部门、个人或者具体设备,不同的机载软件数据传输链环节都可能为最终使用数据的

用户提供服务。

机载软件数据传输链由一系列的中间环节组成,每个环节提供相应的功能,这些功能推进机载软件数据为具体目的而进行的采集、转换以及应用,有 5 类典型环节(机载软件数据传输链的长度可能会不同,每种环节在同一数据链传输中也可能出现多次)。这典型的 5 类环节包括采集、传输、准备、应用集成以及最终使用。机载软件数据的最终使用又决定着机载软件数据的采集过程,因此,机载软件数据传输链也可以视作一个信息环路。典型的机载软件数据传输链如图 1 所示。

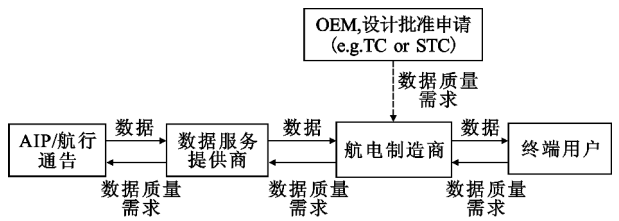


图 1 机载软件数据传输链示意图
Fig. 1 The transmission chain of airborne software data

3 机载软件数据质量定性评价方法

定性评价法需要根据事先确定的评价指标,通过演绎推理等方法对数据目的、用途,以及用户自定义项目进行评价,从而判定数据集的质量是否合格,因此,对定性评价方法,其评价指标体系的建立和对应验证方法的选择直接影响评价结果的可用性。

3.1 数据质量评价指标体系

机载软件数据传输链中的所有成员机构都必须确保针对数据的预期应用为其建立了正确的数据质量要求。与其他系统的软件数据不同,机载软件数据质量直接关系到飞机的飞行安全,因此安全性是其重要的需求^[13]。另一方面,经济性也是民机产业的重要考量,而数据的可维护性直接决定了维护成本。为了客观描述这种数据质量要求,我们从机载软件数据的可用性、安全性和可维护性方面对数据质量定义了七个方面的具体要求,如图 2 所示。

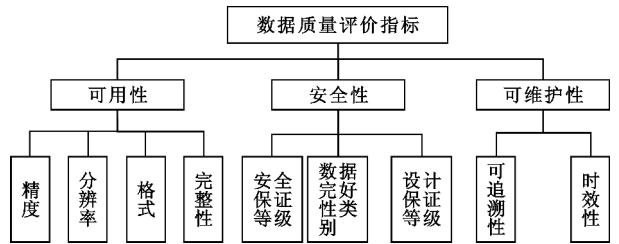


图 2 机载软件数据质量评价指标
Fig. 2 The quality evaluation criterion of airborne software data

3.1.1 可用性

(1)精度

某一具体数据要求的精度是基于其预期的功能,通常只有可测量的数据值才有相应的精度规定,而定义的数据值没有精度的概念。实际应用过程中应该根据数据所在系统的上一层精度要求来规定该数据的精度要求(如导航数据的精度要求可具体参见 RTCA DO-201A^[14]的表 2-1~2-8)。

(2)分辨率

某一具体数据要求的分辨率是基于其预期的功能,通常只有可测量的数据值才有相应的分辨率规定,而定义的数据值没有分辨率的概念。分辨率的设置对数据的精度有影响,因此在设置分辨率时要考虑精度要求。在对分辨率进行规定之后,应在数据格式中体现。

(3)格式

交付数据的格式应进行详细定义,以保证该数据在加载到应用终端时能够按照与预期功能相一致的方式进行解读。数据格式同时定义了数据传输的分辨率。数据格式有两个层级:基本格式和压缩格式。基本格式为通常意义上理解的数据格式要求,例如参数定义、符号含义、单位、编码方法(例如二进制码-十进数、二进制补码)等。数据压缩用于在加载数据时缩小存储容量。因此,也将数据压缩方法

作为数据格式要求的一部分。经压缩的数据必须保证与其压缩前一致。

(4)完整性

完整性是指对执行预期功能所需的最小数据集合的全部要求进行定义。最小数据集合通常在设备批准时用到,更大的数据集合一般由用户确定。很多系统的数据库规模限制了全部数据的存储,这种情况下需要有数据选择准则以缩小数据库数据规模。例如,导航数据库应包含国内所有的进近航路,又如地形数据库应包含所有带有 1 km 以上长度的完整机场区域。

3.1.2 安全性

应用于不同功能软件的机载软件数据其安全性需求不同,再次以安全保证等级定义数据的安全关键性程度,保证等级是对数据处理过程要求的指标。对数据处理过程的保证等级要求基于整个系统架构中风险的分布。由于数据处理过程的完好性要求无法定量表述,因此采用定性的保证等级的概念进行描述。等级应该与飞机的其他安全性分析结果(研制保证等级)相兼容(典型的导航数据可具体参见 RTCA DO-200A^[15]的表 2-1~2-8)。

在系统安全性分析过程中确定的针对功能的等级定义方式,分为 A、B、C、D、E 5 个等级,与 5 类失效状态类别相对应,具体如表 1 所示。

表 1 数据处理的保证等级与数据类别和研制保证等级的对应关系
Table 1 Correspondence between the data processing level and data assurance level

失效状态类别	失效影响	设计保证等级	安全关键等级
灾难性的	妨碍飞机继续安全飞行和着陆,将会导致多人死亡,通常会使飞机坠毁。	A	关键
危险的	失效状态降低飞机的性能,降低机组人员处理飞机不利运行状态的能力,包括:急剧降低飞机安全裕度或功能性能;造成身体伤害或工作负担增加使飞行机组人员不能准确或完整的完成工作;除飞行机组人员外,相当少的旅客受到严重或致命的伤害。	B	
重大的	失效状态会降低飞机的性能或机组人员处理飞机不利运行状态的能力,例如在安全裕度和功能性能显著降低,机组人员的负担显著增加或在这种状态下降低机组人员的效率,对飞行机组人员造成身体不适,对客舱人员或旅客造成危险,可能受伤。	C	
轻微的	失效状态对安全性没有显著影响,机组成员的工作也在其能力范围内。例如在安全裕度或功能性能方面轻微降低,机组成员的工作负担轻微增加,诸如常规飞行计划的改变,对乘客或客舱内人员造成一些身体不适。	D	重要
无安全影响	失效状态对安全无影响;失效状态对飞机使用能力和机组成员的工作无影响,并且不增加机组成员的工作量。	E	常规

根据由于数据错误造成的对所支持功能的影响对数据进行的类别划分,分为关键数据、重要数据、常规数据 3 类。

(1)关键数据——保证等级 1

该数据如果有错误会阻碍飞机继续安全飞行和着陆,或会降低机组处理不利运行条件的能力到一

定程度,以至于飞机安全裕度或功能能力很大程度的降低。如果使用了这类已损毁的关键数据,飞机上乘员生命受到威胁的可能性很高。

(2)重要数据——保证等级 2

该数据如果有错误,会降低机组处理不利运行条件的能力到一定程度,以至于飞机安全裕度降低很多。如果使用了这类已损毁的关键数据,飞机上乘员生命受到威胁的可能性较低。

(3)常规数据——保证等级 3

该数据如果有错误,不会对飞机的安全有很大影响。如果使用了这类已损毁的关键数据,飞机上乘员生命受到威胁的可能性很低。

3.1.3 可维护性

(1)追溯性

数据使用方对数据的追溯性要求通常体现为数据的留存时间问题。通常建议数据在使用期间都应该进行保留并可以追溯。

(2)时效性

多数数据有确定的有效期限。有效期限的设定取决于供应商的更新周期或数据本身的特性。如导航系统使用符合国际民航组织要求(ICAO)的数据库,每 28 天更新一次。而地形数据的有效期取决于该数据本身的特性,需要在对系统进行评估的基础上确定地形数据的可接受性。该评价要素的最终目的是为了能够使用有效、现行的数据。

3.2 数据质量验证方法

对于不同安全等级的机载软件数据,需采用不同的数据质量验证方法,以在满足数据安全性、可用性等因素条件下降低数据质量辨识成本。

3.2.1 确认方法

数据确认是通过对数据的检查确保其值完全符合数据特性,或确保一组数据适用于其预期目的。数据确认有 3 种方法。

(1)应用

在数据正式发布前,对数据进行试用是最有效的确认方法。例如在通过飞行检查最终进近数据的正确性。

(2)逻辑一致性判断

通过对两组数据进行逻辑方面的比较来进行数据确认。例如第一组数据是公布的方向,第二组数据是通过两个方位点的计算得到的方向,将这两组数据分别比较,检查是否一致。但是这种方法可能无法对数据全面的确认,因为这两组数据中有

可能包含相同的错误。因此,为提高这种确认方法的有效性,应该严格控制相比较数据之间的独立性。

(3)语义一致性判断

语义一致性判断是根据数据特性将被测数据与某一期望值或指的区间进行比较。但是这种方法可能无法对数据全面的确认,因为相比较的这两组数据中有可能包含相同的错误。例如将某一高度值与高度的有效区间范围进行比较。

3.2.2 验证方法

数据验证是对数据完好性的检查。通过对数据的检查确保其值完全符合数据特性,或确保一组数据适用于其预期目的。数据确认有 4 种方法。

(1)数字错误检测

数字错误检测方法可以用来检测数据传输和数据存储过程中的错误。典型的检测方法包括循环冗余检查(CRC)、同位元检查、汉明码、里德-所罗门码等,这些编码技术与传输介质(例如存储卡、互联网)的影响。

当确定了数据的保证等级后,需要对错误检测方法的有效性进行定量评估,并满足表 2 的要求。数据处理过程中,只有数字错误检测可以进行概率数值评估,其他过程均不适用。

表 2 保证等级和数字错误检测有效性的对应关系
Table 2 Correspondence between the level of assurance and the effectiveness of error detection

保证等级	未检测到数据损坏的可能性
1	$\leq 10^{-8}$
2	$\leq 10^{-5}$
3	不适用

(2)反馈测试

反馈测试是将一组数据的输出和输入进行比较,将数据进行中间的数据处理过程后再对得到的输出进行反向处理,得到另一组“输入”数据,将两组输入数据进行比较,看是否一致,如图 3 所示。

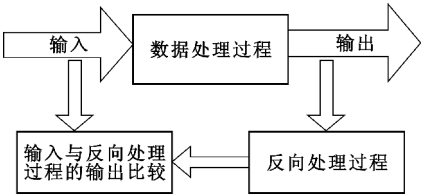


图 3 反馈测试
Fig. 3 Feedback test

(3) 独立性冗余测试

独立性冗余测试是将同一组数据经过两个目的相同但相互独立的处理过程,并将输出结果进行比较,如图 4 所示。

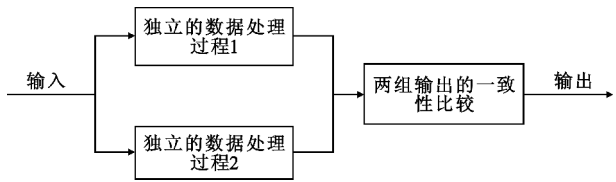


图 4 独立性冗余比较测试
Fig. 4 The independence test for the redundancy

(4) 数据更新比较

数据在处理过程中经常会有频繁的更新。通过分析更新后的数据可以确定该次被更新了的数据清单。同时,在更新数据之前,数据处理方通常会有一份欲更新数据的清单。将这两份清单进行比较,如果存在差异,则说明数据存在问题。这种比较的方法也可以用来降低其他验证方法的工作量,在验证过程中只需要针对被更新部分的数据进行处理。

3.2.3 确认和验证的实现

不同保证等级的数据,其质量对航空器安全性的影响不同,因此验证和确认的工作要求也有差别。

(1) 保证等级 1

对于保证等级 1 的机载软件数据,必须保证在数据处理过程中没有可能引入人为差错;并且,如果使用的工具可以以一种不被发现的方式修改数据,则必须对数据按照其可能导致的灾难性失效状态或危险的失效状态进行鉴定。

(2) 保证等级 2

对于保证等级 2 的数据不要求进行确认,但是数据应用仍然是进行数据确认最有效的方法。逻辑检查和语义一致性检查也可以用于整个确认过程。数据通常在数据产生方进行确认。一旦数据确认完成,需要通过验证手段确保在接下来的每个过程中数据都没有被修改。

(3) 保证等级 3

保证等级 3 的数据不要求进行确认和验证,属于推荐开展的工作。

表 3 说明了不同验证方法的适用阶段。

表 3 各种验证方法的适用阶段
Table 3 Various authentication methods for different stage

适用阶段	验证方法			
	数字错误检测	反馈测试	独立性冗余测试	数据更新比较
数据接收 数据集成 数据选择 数据分发	有效,可以给出定量的数据概率	在数据移动和存储之后,是有效的检查方法。人工反馈检查可以部分用于 C 级过程。	在数据移动和存储过程中,是有效的检查方法。	在数据移动和存储过程中,是有效的检查方法。
翻译 格式化	不适用	可以在数据转换过程中使用。为将转换后输出与输入进行比较,需要将数据全部转换成统一格式(如 ASCII)。因此,只有当验证所使用的转换方法与被验证的转换方法相独立时此方法才可使用。	对人工格式转换可进行有效验证;对工具进行的自动转换,需要对工具鉴定。	无法检查数据转换,因为转换过程可能在数据更新过程中引入相同的错误。可以用于确保上一次的更新被确认。

4 结 论

本研究以机载软件数据库为研究对象,在建立数据传输模型的基础上,提出了机载软件数据质量的定性评价方法,总结了影响数据质量要求的可用性、安全性和可维护性三方面的 7 项指标;针对不同保证等级的数据,分别给出了数据确认和数据验证的方法。本研究对于机载软件数据库的审定和数据质量验证有一定的理论价值。

参考文献:

[1] 王鹏,赵长啸,马赞. 综合模块化航电系统失效模型分析[J]. 电讯技术,2013,53(11):1406-1411.
WANG Peng,ZHAO Chang-xiao,MA Zan. Failure Model Analysis of Integrated Modular Avionics System[J]. Telecommunication Engineering,2013,53(11):1406-1411. (in Chinese)
[2] 郑澜,王运盛. 适用于民机 IMA 的通用机载软件开发平台[J]. 电讯技术,2012,52(6):1027-1030.
ZHENG Lan,WANG Yun-sheng. A General Airborne

- Software Development Platform for Civil Aircraft IMA[J]. Telecommunication Engineering, 2012, 52 (6): 1027 - 1030. (in Chinese)
- [3] Yin Y, Liu B, Su D. Research on formal verification technique for aircraft safety-critical software[J]. Journal of Computers, 2010, 5(8): 1152-1159.
- [4] Esposito C, Barbosa R, Silva N. Safety-Critical Standards for Verification and Validation[C]//Proceedings of Innovative Technologies for Dependable OTS-Based Critical Systems. Milan: Springer, 2013: 41-53.
- [5] Chen Z, Gu Y, Huang Z Q, et al. Model checking aircraft controller software: a case study[J]. Software: Practice and Experience, 2013, 44(8): 2242.
- [6] Panesar-Walawege R K, Sabetzadeh M, Briand L. A model-driven engineering approach to support the verification of compliance to safety standards [C]//Proceedings of 22th Software Reliability Engineering. [S. l.]: IEEE, 2011: 30-39.
- [7] 徐丙凤, 黄志球, 胡军, 等. 面向适航认证的模型驱动机载软件构件的安全性验证[J]. 航空学报, 2012, 33(5): 796-808.
- XU Bing-feng, HUANG Zhi-qiu, HU Jun, et al. Model-driven Safety Dependence Verification for Component-based Airborne Software Supporting Airworthiness Certification[J]. ACTA Aeronautica ET Astronautica Sinica, 2012, 33(5): 796-808. (in Chinese)
- [8] RTCA DO-178B/ED-12B, Software Considerations in Airborne Systems and Equipment Certification[S].
- [9] 苏志刚, 李志勃, 吴仁彪, 等. 实现 PBN 技术的陆基 DME 台选择算法[J]. 系统工程与电子技术, 2013, 35(10): 2170-2175.
- SU Zhi-gang, LI Zhi-bo, WU Ren-biao, et al. DME selection algorithm for implementation of PBN technology [J]. Systems Engineering and Electronics, 2013, 35(10): 2170-2175. (in Chinese)
- [10] 孙志强. 电子飞行包的适航和运行批准研究[J]. 装备制造技术, 2012(12): 165-167, 173.
- SUN Zhi-qiang. Research for Airworthiness and Operational Approval of Electronic Flight Bag[J]. Equipment Manufacturing Technology, 2012 (12): 165 - 167, 173. (in Chinese)
- [11] GB/T 28441-2012, 车载导航电子地图数据质量规范[S].
- GB/T 28441-2012, Data quality specification for navigation electronic map in vehicle[S]. (in Chinese)
- [12] 周庆, 刘斌, 余正伟. 面向机载软件适航验证的灰盒测试方法[J]. 系统工程与电子技术, 2012, 34(8): 1729-1734.
- ZHOU Qing, LIU Bin, YU Zheng-wei. Grey-box testing method for airworthiness certification of airborne software [J]. Systems Engineering and Electronics, 2012, 34

(8): 1729-1734. (in Chinese)

- [13] RTCA DO 201A, Standards for Aeronautical Information [S].
- [14] RTCA DO 200A, Standards for Processing Aeronautical Data[S].

作者简介:



阎芳(1982—),女,山东人,2005年于法国国立航空工程大学获硕士学位,现为中国人民航大学适航审定技术与管理中心副研究员,主要从事民机系统安全性设计与评估、机载电子软件适航技术研究;

YAN Fang was born in Shandong Province, in 1982. She received the M. S. degree from the Institut Supérieur de l'Aéronautique et de l'Espace in 2005. She is now an associate researcher of Civil Aircraft Airworthiness Certification Technology and Management Research Center Civil Aviation University of China. Her research concerns aircraft system design and evaluation of safety, software airworthiness technology.

Email: fyan@cauc.edu.cn

谢文光(1984—),男,汉,黑龙江人,2010年于西北工业大学获硕士学位,现为助理研究员,主要从事民机机载软件适航审定技术研究;

XIE Wen-guang was born in Heilongjiang Province, in 1984. He received the M. S. degree from Northwestern Polytechnical University in 2010. He is now an assistant researcher of Civil Aircraft Airworthiness Certification Technology and Management Research Center Civil Aviation University of China. His research concerns aircraft system design and evaluation of safety, avionics software airworthiness technology.

赵长啸(1989—),男,山东人,2013年于北京航空航天大学获博士学位,现为中国人民航大学适航审定技术与管理中心研究人员,主要从事民机航电系统设计与评估、航空电子综合研究;

ZHAO Chang-xiao was born in Shandong Province, in 1989. He received the Ph. D. degree from Beihang University in 2013. He is now a researcher of Civil Aircraft Airworthiness Certification Technology And Management Research Center Civil Aviation University of China. His research concerns avionics system design and evaluation.

王鹏(1982—),男,天津人,2005年于法国国立航空工程大学获硕士学位,现为中国人民航大学适航审定技术与管理中心副主任,副研究员,主要从事民机系统安全性设计与评估、机载电子硬件适航技术研究。

WANG Peng was born in Tianjin, in 1982. He received the M. S. degree from the Institut Supérieur de l'Aéronautique et de l'Espace in 2005. He is now an associate researcher and also the Deputy Director of Civil Aircraft Airworthiness Certification Technology and Management Research Center Civil Aviation University of China. His research concerns aircraft system design and evaluation of safety, electronic hardware airworthiness technology.