文章编号:1671-4598(2019)10-0277-03 DOI:10.16526/j.cnki.11—4762/tp.2019.10.057 中图分类号:V243 文献标识码:A

民用航空电子系统网络安全验证方法研究

陈 杰
(中国民用航空上海航空器适航审定中心,上海 200335)

摘要:针对民用飞机适航中的网络安全特殊风险,通过研究美欧等民航审定机构的网络安全特殊风险的测试过程和方法,结合常用的符合性测试方法提出了民用飞机电子系统网络安全测试方法;基于DO—326A中的网络安全测试框架,提出航电系统适用的网络安全鲁棒性测试方法与网络安全脆弱性测试方法;该方法为民用飞机电子系统网络安全适航提供了可行的思路。

关键词:民用航空电子系统;符合性验证;网络安全;鲁棒性测试;脆弱性测试

Cybersecurity Verification Method Research for Civil Avionics System

Chen Jie
(Shanghai Aircraft Airworthiness Certification Center of CAAC, Shanghai 200335, China)

Abstract: In view of the special risks about civil aircraft airworthiness cybersecurity, the airborne system cybersecurity compliance verification is proposed by studying the cybersecurity certificate process and methods of the civil aviation certification agencies in the United States and Europe, combined with the commonly used compliance verification methods. Based on the network security verification activity framework proposed by DO—326A, the method was proposes the applicable cybersecurity robustness test method and cybersecurity vulnerability test method for civil avionics systems, and provides feasible ideas for the civil aircraft cybersecurity certification.

Keywords: civil avionics system; compliance verification; cybersecurity; robustness test; vulnerability test

0 引言

随着世界民用航空业的发展,飞机制造越来越精密,信息技术在航空界也得到了广泛应用。如今民用客机的运营涉及众多的利益关联方,如航空公司、空管、机场、乘客、飞行机组、通信运营商以及相关信息提供商等,构成了一个庞大复杂的业务关系网络,民用客机成为这个信息网络中的一个节点。多种通信技术的使用在为飞机与地面进行高带宽的、全阶段的实时通信,以及为飞机与地面网络系统信息交互提供便利的同时,也为飞机的飞行安全带来了信息安全威胁,包含非授权人员通过非法访问、使用、泄漏、破坏、修改数据或数据接口的行为等。对此,美国联邦航空局和欧洲航空安全局针对飞行控制域和航空公司信息服务域中关键系统的安全性、完整性和可用性提出了特殊要求,对民用飞机的网络安全适航提出了专用条件。同样的,中国民航局也将网络安全风险作为安全性中的一种特殊风险对待,针对多个在审查的客机型号提出了网络安全专用条件。

国内学者针对机载电子设备的适航符合性方法,进行了梳理,对开发过程中的常用方法进行了澄清[1];针对机载软件适航验证,提出了灰盒测试方法与应用过程[2];针对民用飞机机载系统的安全环境,提出了一种可量化的机载网络安全风险评估方法[3]。国外学者对综合模块化航电的安全操作系统给出了相应的验证方法。

收稿日期:2019-05-21; **修回日期**:2019-06-12。
基金项目:国家某重点科研项目资助(MJ—2016—S—42)。
作者简介:陈 杰(1976-),男,浙江湖州人,硕士,工程师,主要从事民用飞机适航技术方向的研究。

在国内外适航机构对民用航空电子系统仅提出了网络安全的验证目标,并没有提供相应的验证测试方法。由于我国在民用飞机网络安全适航审查方面尚未有成熟经验,因而尚无可借鉴的民用航空电子系统的网络安全验证方法。鉴于此,需要基于民用航空电子系统开展网络安全验证方法的研究[4]。

1 民用航空电子系统网络安全验证目标

信息化民用飞机机载系统面临的网络安全问题从安全性角度,分为与飞机安全性相关和与飞机安全性无关这两类问题。

适航审定方关注与飞机安全性相关的问题,关注针对电子信息或飞机电子接口的未授权电子干扰行为(如非授权访问、使用、泄露、拒绝、中断、修改或破坏),这些行为可能会影响飞机的安全性和适航性。

飞机制造方、航空公司、机场等利益相关方则关注下面与飞机安全性无关的网络安全问题,包括:

1)针对飞机(或地面部件)进行的物理安全或物理攻击问题;

2)机场、航空公司或空中交通服务提供商的信息安全问题;

3)由国家机构或国际机构提供的通信、导航和监视等服务的信息安全问题。

从风险角度来看,飞机审查方将网络安全归类于新的一类特殊风险。由于针对这类风险的适航经验太少,尚没有针对网络安全审查发布相应的规章和指导性材料,现有的民机项目中,审查方都是通过向具体的机型发专用条件的方式实现对适航规章要求的补充。例如美国联邦航空局向波音787发布25—357—SC[5],向波音747—8发布25—

10－01－SC[6]，向空客 A350－900 发布 25－534－SC[7]。在这些专用条件中，美国联邦航空局提出了网络安全适航的符合性目标（审定基础要求），即：

1）保护飞机电子系统信息安全不会受到非授权的外部访问；

2）隔离或保护飞机电子系统信息安全不会受到非授权的内部访问。

我国大型客机 C919 型号在按照当今最新的适航标准取证过程之中，也同样存在网络安全适航的问题，因此中国民航 C919 飞机型号合格审查组制定并发布了网络安全适航专用条件，提出了相应的符合性目标。

2 民用航空电子系统网络安全符合性验证方法

为了证明飞机满足符合性目标，飞机制造方需采用符合性验证方法开展相应的试验活动，获得试验数据，作为符合性证据提供给审查方进行审查。航空器型号合格审定程序 AP－21－03－R4[8]对常用的符合性验证方法进行了分类，规定了 MC0～MC9 共 10 种常用符合性验证方法，见表 1。

表 1 常用符合性验证方法[8]

代码	名称	使用说明
MC0	符合性声明	通常在符合性记录文件中直接给出。
MC1	说明性文件	如技术说明，安装图纸，计算方法，技术方案，航空器飞行手册。
MC2	分析/计算	如载荷、静强度和疲劳强度，性能，统计数据分析，与以往型号的相似性。
MC3	安全性评估	如功能危害性评估、系统安全性分析等用于规定安全目标和演示已经达到这些安全目标的文件。
MC4	试验室试验	如静力和疲劳试验，环境试验…… 。试验可能在零部件、分组件和完整组件上进行。
MC5	地面试验	如旋翼和减速器的耐久性试验，环境等试验。
MC6	飞行试验	规章明确要求时，或用其他方法无法完全演示符合性时采用。
MC7	航空器检查	如系统的隔离检查，维修规定的检查。
MC8	模拟器试验	如评估潜在危险的失效情况，驾驶舱评估。
MC9	设备合格性	设备的鉴定是一种过程，它可能包含上述所有的符合性方法。

为了充分表明适航性，民用飞机网络安全适航符合性验证方法可能需要多种验证方法的组合。为了表明飞机系统满足网络安全风险可控的要求，采用 MC2 分析/计算的方法进行飞机网络安全风险评估，提供飞机级、系统级的网络安全风险评估数据。为了表明机载系统满足网络安全适航要求，在系统试验中开展 MC4 试验室试验，包括功能测试、网络安全鲁棒性测试、网络安全脆弱性测试等活动，提供系统级网络安全试验报告。为了表明飞机设备满足网络安全适航要求，开展 MC5 机上地面试验，提供飞机级网络安全试验报告。考虑到网络安全脆弱性测试可能会对机载系统造成安全性损伤，进而影响飞行安全，不建议选用 MC6 飞行试验作为符合性验证方法。

3 民用航空电子系统网络安全验证方法

3.1 民用航空电子系统网络安全验证过程

RTCA 发布的 DO－326[9]/DO－326A[10]中指出民用航空电子系统网络安全验证包括 3 种类型的测试：

1）网络安全功能需求测试；

2）网络安全鲁棒性测试；

3）网络安全脆弱性测试。

网络安全验证活动如图 1 所示。

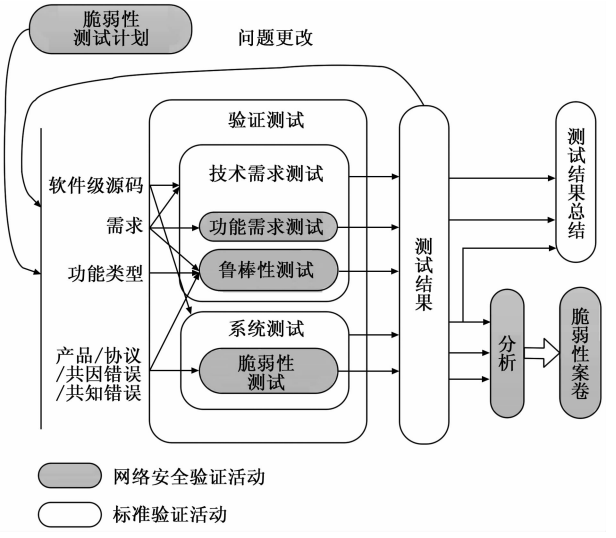

图 1 民用航空电子系统网络安全验证过程

针对上述 3 类网络安全验证活动，DO－356A[11]规范中提出了具体的验证目标：

1）网络安全功能与鲁棒性验证要素已开发、确认和执行。

2）网络安全功能与鲁棒性验证结果是完整的、正确的，偏离是合理的并可追溯的。

3）软件和/或硬件实现的测试覆盖已完成。

4）执行脆弱性分析以识别新的脆弱性。

5）执行脆弱性测试以评估脆弱性在网络安全环境中的暴露情况并挑战脆弱性评估。

6）脆弱性测试计划可用。脆弱性测试结果覆盖测试计划，并执行测试。测试结果已分析，偏离是合理的和可追溯的。

根据上述验证目标，需要具体开展相应的网络安全验证活动。

3.2 网络安全功能需求测试

网络安全功能需求测试是基于需求测试的一部分，它用于验证系统功能的实现是否满足详细需求。此外，其还包括测试系统在响应非授权事件时网络安全措施执行的正确性。

基于网络安全需求的验证主要针对功能需求测试，因此可以使用 DO－178 中提出的基于需求的验证方法，通常分为白盒测试和黑盒测试。白盒测试也称为“结构测试”或“逻辑驱动测试”，根据软件内部工作过程，检测软件内部动作是否按照设计正常进行。白盒测试对软件源代码进行直接测试。黑盒测试称为功能测试或基于需求的测试。黑盒测试根

据需求来检查程序的功能是否符合需求的要求，对应用的二进制执行码执行测试，而不需要了解源代码实现逻辑。大多数定制应用，由于可以获取其源代码，因此可以采用白盒测试。黑盒测试能检测到组件间接口的缺陷，识别到应用在编译链接或安装配置过程中产生的网络安全问题。

根据图 1 中描述的网络安全验证活动，基于网络安全功能需求的测试方法根据网络安全功能需求和功能类型开展，其测试活动的输入不包括软件源代码，因此在测试方法选取上采用黑盒测试方法更为适合。对于网络安全功能需求测试来说，由于它是预期功能测试的一部分，不同飞机型号的系统设计需求不同、网络安全需求也不同，有着个体的差异性，所以没有专门针对需求测试的通用方法。在实际操作中，通常是根据具体网络安全软件的功能需求去设计与其相匹配的测试用例。

3.3　网络安全鲁棒性测试

网络安全鲁棒性测试属于技术需求测试的一部分，用于验证在异常的输入和条件下，软硬件能否按照预定的功能执行。

Fuzzing 测试，即模糊测试，可用于网络安全鲁棒性测试。模糊测试的方法是将一组随机的数据作为软件的输入数据，监控软件运行过程中的异常行为，当出现异常行为时，记录引起异常出现的数据，通过分析数据和异常行为来发现和确定软件中的缺陷。模糊测试主要采用黑盒测试和灰盒测试方式进行。

网络安全鲁棒性测试主要通过网络协议模糊测试进行，其主要操作步骤如下。

1）报文捕获。可使用 wireshark、pcap 等抓包工具在以太网线路上捕获相关的报文数据。

2）报文分析。对报文的帧格式进行分析，标记出关键字段。

3）生成模糊测试的异常输入数据。模糊测试工具根据报文分析的结果，使用内置的变异算法进行模糊测试用例的自动生成。

4）测试执行。模糊测试工具将自动执行测试用例代码。

5）测试监控。模糊测试工具监控被测目标设备在各测试用例注入后的执行情况，如果发生故障，则记录测试上下文现场情况。

6）测试结果分析。所有测试用例都执行完成后，模糊测试工具对测试数据进行收集，分析故障出现原因，确定被测目标设备是否存在漏洞。

在模糊测试中，生成测试用例的方法主要有以下 4 种。

1）预生成测试用例：该方法首先需要研究目标软件的输入数据规约，理解输入中每个字段支持的数据结构以及可接受的值的范围；然后依据这些已经获得的知识生成用于测试边界条件或是违反归约的测试用例；接着利用这些测试用例来测试该归约实现的完备性。

2）随机生成测试用例：该方法是产生一段随机的数据，并将其输入给目标软件，试图使目标软件崩溃或者诱发一些异常行为。这种方法可以用来快速地识别目标软件中是否存在有缺陷的代码。随机生成输入在实现上比较简单，却能发现软件中一些严重的错误，同时这种方法比较容易自动化与并行化实现。

3）变异或强制性生成测试用例：该方法从一个正确有效的协议样本或数据样本开始，不断地变异数据包或者文件中的字节、字、双字、字符串等来生成测试用例。

4）自动协议生成测试用例：该方法首先需要对目标软件的输入数据格式进行深入学习与研究，理解和解释协议归约或文件格式定义。在获取知识的基础上，创建一个描述协议规约如何工作的文法。使用这种方法，测试者可以识别出数据包或文件中的静态和动态部分，其中静态部分是不可修改的部分，动态部分是可被替代的部分。

3.4　网络安全脆弱性测试

网络安全脆弱性测试是一种特殊的网络安全测试活动，包括脆弱性扫描方法，试图破坏、旁路或篡改网络安全措施的攻击测试，以及渗透测试，以此证明攻击者能否利用飞机系统的脆弱性导致系统失效。网络安全脆弱性测试包括脆弱性扫描、攻击测试和渗透测试等测试方法。

3.4.1　脆弱性扫描

脆弱性扫描的目的是探测指定网络内的计算节点、网络设备、网络安全设备等设备的漏洞，包括硬件、软件、协议的具体实现或系统安全策略方面存在的安全缺陷，并给出相应的漏洞修补建议，从而使系统更加安全可靠。

脆弱性扫描常用的测试技术包括：

1）缓冲区溢出：向一个软件发送大量的输入而导致其失效，这种漏洞能够允许攻击者对被测系统实施流氓命令；

2）供应商遗留在软件中的后门：后门的本意是方便技术支持，但是一旦暴露，攻击者就获取了进入系统的机会。

3）软件缺陷：软件缺陷一旦被利用，能使得软件执行非授权操作。

通常情况下，脆弱性测试依据公知脆弱性进行覆盖性测试，保证在应用环境中至少没有可被利用的公知脆弱性。

3.4.2　攻击测试

由于现代航空电子系统基于以太网技术构建数据网络，因此攻击测试主要的测试目标是网络核心交换设备、网络端系统设备、网络协议、操作系统、应用软件等。通过攻击测试，可以测试和发现被测设备是否存在的公知脆弱性。攻击测试包括主动攻击测试和被动攻击测试。

1）主动攻击测试：测试时使用专用攻击测试设备，基于公开漏洞库，向被测目标设备发送网络攻击报文或包含恶意代码的报文，监测被测目标设备是否能够抵御这些网络攻击行为。

2）被动攻击测试：通常采用网络嗅探或端口扫描的方式对被测目标设备进行攻击，获取被测目标设备的信息。

3.4.3　渗透测试

渗透测试是一种网络安全反证测试方法，通过渗透测试可以证明被测目标设备的网络安全保护能力，发现是否存在未知的脆弱性。渗透测试与测试人员能力相关性很强，需要其具备相应的技术能力和经验，同时要有很强的洞察力和想象力。渗透测试通常需要人工和测试工具协作执行。

渗透测试基于测试工具，模仿真实世界的网络攻击，

（下转第 284 页）