基于安全性的航空发动机控制软件测试技术

高　虎,封二强,王　宁
(中国航空综合技术研究所,北京 100028)

摘要:针对航空发动机控制软件安全性需求的验证问题,提出了基于需求模型与安全性分析结果的软件测试技术。从软件需求的结构化描述和软件安全性分析结果中的失效和危险因果关系链出发,研究并制定了符合航空发动机控制软件特点的测试用例生成方案,给出了程序化的自动实现算法,并描述了在某重点发动机型号的工程实践情况。

关键词: 安全性分析;软件测试;航空发动机;需求模型
中图分类号: TP311.11　　**文献标识码:**A　　doi:10.13477/j.cnki.aeroengine.2018.01.017

Research on Aeroengine Control Software Testing Based on Safety

GAO Hu, FENG Er-qiang, WANG Ning
(**China Aero-polytechnology Establishment, Beijing 100028, China**)

Abstract: Aiming at the problem of safety requirements verification of aeroengine control software, a software testing technology based on requirements model and safety analysis was proposed. Starting from the structured description of software requirements and causal chain of failure and hazard in software safety analysis, the scheme of testing cases generation was developed according to characteristics of aeroengine control software, the automatic algorithm of programming was given and engineering practices in one type of aeroengine were described.

Key words: safety analysis; software test; aeroengine; requirements model

0　引言

航空发动机在航空技术的发展中起着关键性作用,其状态和性能直接影响飞行任务的完成和飞行安全,被称为飞机的"心脏"。随着全权限数字电子控制(FADEC)技术在国内外新型发动机中的应用,航空发动机控制软件(以下简称"发控软件")成为航空发动机系统最核心的控制决策单元[1]。近年来,由软件造成的航空发动机安全事故呈大幅度上升趋势,发控软件的质量与安全性问题成为航空发动机发展中亟待解决的问题之一。该问题的解决目前主要依赖于软件测试活动。

软件测试是目前确保软件可靠性和质量的最成熟而有效的方法[2]。航空无线电委员会(RTCA)规定软件测试目的在于证明软件满足其需求,并且以高置信度证明由系统安全性过程确定的失效状态得到消除[3]。而目前在中国航空软件测试工程实践中,更多关注软件实现对需求的符合性验证,而对软件安全性的验证尚未给予足够重视,缺乏系统性的理论基础,很大程度上依赖于测试人员的实践经验,成为航空发动机安全运行的重大隐患[4]。因此,基于安全性分析的发控软件测试技术成为保证我国发控软件有效运行进而保证飞机整体安全的重要途径。

软件安全性是指软件运行时不引起系统危害的能力[5]。软件安全性分析就是识别可能导致系统危险和软件自身失效的软件因素,从而形成软件安全性需求的过程。在软件安全性分析领域,采用基于模型的软件安全性分析与验证方法[6-7]可以获得软件安全性分析结果,该结果精确描述了软件行为导致的系统危险和软件失效情况。基于此类安全性分析结果,在软

收稿日期:2017-05-25　**基金项目:**国防基础科研项目(Z052013B009)资助
作者简介:高虎(1986),男,硕士,工程师,从事软件安全性分析、FPGA 软件测试工作;E-mail:gaohu_2009@163.com。

引用格式:*高虎,封二强,王宁.基于安全性的航空发动机控制软件测试技术[J]. 航空发动机,2018,44(1):91-96. GAO Hu, FENG Erqiang, WANG Ning. Research on aeroengine control software testing based on safety [J]. Aeroengine,2018,44(1):91-96.*

件测试过程中通过动态运行软件将导致安全性事件的软件行为进行复现,便可验证软件安全性需求的落实情况。

本文提出了基于需求模型与安全性分析的发控软件安全性测试技术方法,以实现对基于发控软件安全性分析的软件安全性需求的有效验证。

1 软件需求建模与安全性分析

1.1 基本方法

基于安全性的发控软件测试技术以软件需求模型和安全性分析技术为基础,以测试技术为验证手段,3 项技术共同构成了支撑发控软件安全性的基本方法。

建立软件需求模型是保证软件安全性分析客观、无歧义的有效手段,也是软件安全性分析流程化、自动化的基础。软件安全性分析结果与软件需求模型的不断迭代,最终形成满足安全性要求的软件需求。同时在基于需求的软件测试中,软件需求模型能够为程序化的软件测试用例设计提供依据。

软件安全性分析立足于软件全生命周期,以安全性为视角,分析软件的安全不确定性因素——软件是否存在导致系统危险和软件自身失效的可能性,从而在软件层面上识别危险与失效、补充危险与失效的控制策略,最终实现系统级安全性要求,提高系统级安全性水平。

动态测试作为最直接有效的手段,验证软件安全性分析产生的软件安全性需求在软件代码中能否得到准确而充分的落实。软件安全性测试即验证软件安全性需求的动态测试过程,基于软件需求模型将软件安全性分析的因果关系进行实例化,形成安全性测试用例,在动态测试过程中执行安全性测试用例,提供软件安全性验证结论。

软件需求建模、安全性分析与测试的关系如图 1 所示。

1.2 发控软件需求建模

发控软件实时性强,输入输出接口多,功能逻辑复杂且耦合性强,大量存在闭环控制功能,软件具有明显的任务特性和状态特性[8-9]。因此发控软件的需求模型一方面需要清晰客观地描述发动机地面起动、运行、加力、停车以及空中起动等主要控制流程的软件控制及故障处理要求,另一方面还应对安全性分析所需

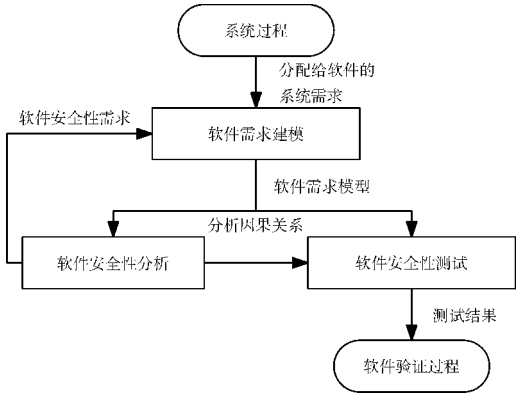

图 1 软件需求建模、安全性分析与安全性测试的关系

的各类复杂逻辑信息,如状态迁移、功能时序约束、机构控制策略等进行描述。建立发控软件需求模型包括:

(1)外部交联关系模型,描述发动机控制系统外部交联设备、总线、接口的连接关系,信号的闭环反馈关系,以及信号间的耦合关系;

(2)状态迁移模型,描述发动机控制系统的任务状态,状态之间的迁移条件;

(3)状态流程模型,描述各状态内部控制流程,各状态控制律算法和输出组合逻辑,以及状态内部异常处理逻辑;

(4)公共功能模型,描述发动机控制系统各任务状态公共功能逻辑和时序,如发动机消喘、防冰、应急放油等。

1.3 发控软件安全性分析

针对发控软件特点,软件安全性分析基于需求模型对状态、流程、输入、输出的描述,重点关注发动机控制状态迁移、动态处理流程以及功能和接口的耦合关联关系等方面引起的危险和失效,分析其原因和影响,并提出改进措施,形成软件安全性需求。

初步危险分析(PHA)[10]、失效模式与影响分析(FMEA)[11]、故障树分析(FTA)[12-13]等方法,能够有效地为发控软件安全性分析提供帮助。

上述软件安全性分析方法的出发点都来自于系统危险或软件失效,且均通过对原因和影响的分析最终产生系统危险或软件失效的因果关系链。

软件安全性分析的目标是在软件层面上识别危险与失效并补充危险与失效的控制策略。如果发控软件在进入安全性分析前已经正确实现了软件需求,则系统危险或软件失效的因果关系链的最顶层原因均能够反映在软件的外部输入中。因此,系统危险或软

件失效的发生均可通过软件的外部输入激发产生。而软件动态测试过程也是以软件外部输入为激励,因此基于软件安全性分析结果设计测试用例,并在测试环境中执行测试用例,成为一种验证软件安全性需求的有效手段。

2　软件安全性测试策略

2.1　软件安全性测试目的

软件安全性测试的目的是通过设计和执行测试用例,复现软件安全性分析过程中产生系统危险或软件失效的场景,查看系统危险和软件失效是否均得到有效的控制和处理,从而验证软件安全性需求的落实情况。

软件安全性测试的输入是软件安全性分析过程产生的包含系统危险或软件失效的因果关系链,以及系统的外部交联关系模型;软件安全性测试的过程形成软件安全性测试用例,并根据软件安全性测试用例的执行结果,最终输出软件安全性需求的验证结论。

2.2　发控软件安全性测试特点分析

发控软件具有时序逻辑强、输入输出接口关系复杂的特点[14],发控软件安全性分析生成的危险或失效原因一般描述为特定时间点和特定输入接口的异常行为。而在发控软件测试过程中,一般需要执行完整的发动机运行流程,不但需要与危险或失效原因相对应的相关输入激励,还要对与危险或失效原因耦合的其他输入激励进行实时调整,以保证发控软件运行所必须的数据需求。由此可见,发控软件安全性测试用例描述的是一个在完整的发动机控制系统运行场景下注入了危险和失效原因的实时性运行过程。

另外,发控软件安全性分析结果多数来源于对发动机危险及软件失效等异常情况的考虑,这些异常情况一旦在实际发动机系统中产生而未得到有效控制,将造成严重的后果。所以发控软件的安全性测试如果在实物或半实物环境下执行,将面临较大的危险和成本,因此必须采用仿真测试技术,通过建立交联环境的全数字模型,模拟发动机运行数据以及各类异常情况来完成。在仿真测试环境中,交联设备的危险和失效等行为改变在很多情况下体现为仿真模型的参数变化[15],因此在安全性测试用例设计中,可将危险和失效原因落实在仿真模型参数中,通过仿真模型的运行间接实现包含失效和危险状态的测试激励。

2.3　发控软件安全性测试方案

(1)将软件的外部输入接口划分为被控对象输入和操作输入。被控对象输入主要包括发动机系统的传感器采集输入,如转速、温度、压力等信号;操作输入主要包括飞机其他系统或驾驶员对发动机系统的输入,如油门杆、各类按钮等。

(2)建立从软件控制指令输出到被控对象输入的全数字仿真模型,并根据正常的发动机操作流程确立软件所有操作输入的时序变化关系,实现对发动机正常使用场景的模拟。

(3)将软件安全性分析获得的危险或失效原因定位于软件的外部输入,或间接定位于仿真模型的参数输入,然后依据软件外部交联关系对系统输入范围及时序的约束将相关的系统输入进行实例化。

(4)依据危险或失效原因的产生时机,将实例化的系统输入注入到已确定的描述发动机正常使用场景的输入序列中,形成安全性测试用例。

(5)软件安全性分析获得的危险或失效原因可通过优化算法(如故障树最小割集算法)进行组合,以降低测试成本。

(6)发控软件安全性测试用例可根据格式化的软件需求模型和安全性分析结果通过自动化的手段生成。

3　软件安全性测试用例自动生成方法

3.1　基本原理

软件安全性分析产生系统危险或软件失效的因果关系链,其最底层的危险和失效原因均可描述为软件输入的数值或时序行为;利用数字化的软件交联环境模型,可将这些软件输入的数值或时序行为实例化为具体的软件输入;将由危险和失效原因产生的软件输入注入到软件运行场景中,形成软件安全性测试用例。

3.2　算法描述

定义发控软件输入向量

$$p^T=[p_e \quad p_f]^T \tag{1}$$

式中:p_e 为被控对象输入;p_f 为操作输入。

定义发控软件输出向量

$$q^T=[q_e \quad q_f]^T \tag{2}$$

式中:q_e 为仿真模型的输入;q_f 为发控软件的其他输出。

发控软件的行为可用矩阵 S 描述

$$q(t)^T=S\cdot p(t)^T \tag{3}$$

建立发动机系统仿真模型 M,则仿真模型运行可描述为

$$p_e(t)^T=M(t)\cdot q_e(t-1)^T \tag{4}$$

其中仿真模型存在可变参数 b,定义该参数随发动机运行时间序列为 b(t)

$$M(t)=b(t)^T\cdot M_0 \tag{5}$$

同时,建立发动机正常操作流程为 $p_f(t)$,因此,发动机的运行过程可描述为

$$[q_e(t)\quad q_f(t)]^T=M\cdot\begin{bmatrix} b(t)^T\cdot M_0\cdot q_e(t-1)^T \\ p_f(t)^T \end{bmatrix} \tag{6}$$

根据式(6)可通过计算机递推方法计算发控软件输入 $p(t)^T$,实现发动机正常操作流程的动态仿真运行。

安全性分析结果中的危险或失效原因可分解为某个变量(或模型参数)在某中时序下的行为,可采用结构化的方式描述为:“A 状态 B 操作中,C 变量(或参数),产生 D 数值改变或 E 时序改变”。

根据软件需求模型对状态和操作的描述,可通过危险或失效原因在正常操作序列 $p_f(t)$中查找获得该危险或失效产生的基准时间 t_0,并可在 p_f(或 b)向量中定位到发控软件运行模型中的输入(或模型参数)p_{f_x}(或 b_x)。

根据危险或失效原因中对“E 时序改变”既有方式的选择,可通过查表的方法,并结合需求模型中对时序参数(时间分辨率、响应时间等)的设置,确定危险或失效的实际激发时间 $t_0+\delta$;同时根据危险或失效原因中对“D 数值改变”既有方式的选择,可通过查表的方法,结合 $p_f(t_0)$(或 $b(t_0)$)的正常输入以及需求模型中对接口参数(上下限、精度等)的设置,确定产生危险的系统输入 $p_{f\_x}(t_0+\delta)$(或 $b_x(t_0+\delta)$)。

最后,根据安全性分析结果将单点或组合的危险或失效原因实例化输出结果叠加于原模型参数和操作输出序列中,未影响的输入(或模型参数)填充为“null”,即

$$sel(X,Y)=\begin{cases} X,X=null \\ X,Y\neq null \end{cases} \tag{7}$$

$$[q_e(t)\quad q_f(t)]^T=S\cdot\begin{bmatrix} sel(b(t),b_x(t))^T\cdot M_0\cdot q_e(t-1)^T \\ sel(p_f(t),p_{f\_x}(t))^T \end{bmatrix} \tag{8}$$

根据式(8)形成新的发控软件运行序列,作为该危险或失效原因所对应的安全性测试用例。

4 工程应用

某型号航空发动机控制系统由 FADEC 控制器、传感器、液压机械装置和电气系统组成。其中发控软件是 FADEC 控制器的核心部分,该软件接收来自飞机、发动机和机械液压装置的信号,经过数字运算、逻辑判断发出各种控制信号给相应的执行机构以控制发动机状态,同时传输信号给飞机机载装置显示和记录。

2014 年 9 月至 2016 年 8 月,对该发控软件开展了安全性分析和测试工作。其中安全性分析工作通过自研的“软件安全性分析工具”开展,在依据系统和软件需求建立外部交联关系模型、状态迁移模型、状态流程模型和公共功能模型的基础上,采用 PHA 和 FMEA 方法进行了软件安全性分析,分析识别系统危险 45 项,分解危险原因 69 条,识别软件失效 138 项,获得失效原因 155 条。典型安全性分析结果见表 1。

表 1 典型安全性分析结果

系统危险或软件失效	失效原因	控制措施
冷运转过程误执行消喘控制,进行点火	冷运转状态满足消喘条件(压气机后总静压差变化幅值大于阈值)	冷运转状态强制禁止点火
P3 传感器故障,导致 P3 取安全值为标准大气压,造成燃油给定值计算量瞬间减小,导致发动机熄火	起动及运行状态,P3 出现瞬间峰值。	修改 P3 双通道故障处理对策,将取安全值改为取上一次正确值
根据燃油 PI 控制算法,燃油给定值将瞬间增大或减小,造成发动机超转或熄火	在运行状态,驾驶员迅速增大或减小油门杆角度	增加对油门杆变化率的限幅和超限保护功能

其中,32 条危险原因和 101 条失效原因均已采取相应的控制措施,形成为软件安全性需求,并在软件的升级版中得到落实。对失效或危险原因进行优化和合并后,设计软件安全性测试用例 117 个(其中 92 个采用软件安全性测试用生成算法自动生成),执行了全部测试用例,软件安全性需求得到有效验证。

针对发控软件的特点,要求安全性测试环境具备实时性、自动化、支持仿真模型运行的能力,因此在项目实施过程中,构建软件安全性测试环境如图 2 所示。

该测试环境通过测试执行计算机中的测试主控模块实现测试用例的自动组织和执行。测试用例和测试模型通过以太网加载到测试执行计算机中,并通过测试执行计算机集成的总线接口加载到被测设备中,

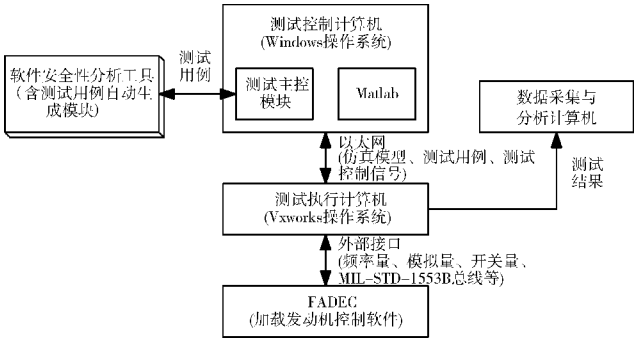

图 2　某发动机控制软件安全性测试环境

测试执行计算机采用 VxWorks 实时操作系统，能够以较高的时间精度实现仿真模型的运行和测试用例的执行[16]。

根据表 1 中描述的典型软件安全性分析结果设计测试用例,在已落实安全性需求的软件中执行的结果见表 2。

表 2　典型安全性测试用例

失效原因	测试用例简述	执行结果
冷运转状态满足消喘条件(压气机后总静压差变化幅值大于阈值)	建立 t_1 冷运转,t_2 停车工作场景，在 t_1 <t< t_2 时刻设置压气机后总静压差变化幅值为 Δ p	通过。未进行点火
起动及运行状态,P3 出现瞬间峰值	建立 t_1 地面起动,t_2 中间位置运行,t_3 停车工作场景，分别在 t_1 <t< t_2 和 t_2 <t< t_3 设置 P3 在 t 到 t+Δ t 时刻由 p MPa 改变为 (p+1)MPa,之后 P3 恢复模型计算结果	通过。t 到 t+Δ t 时刻范围发动机燃油流量平稳,t+Δ t 时刻后恢复正常控制
在运行状态,驾驶员迅速增大或减小油门杆角度	建立 t_1 地面起动,t_2 中间位置运行,t_3 停车工作场景,在 t_2 <t< t_3 设置油门杆迅速在 r~(r+50)~r 变化	通过。发动机转速和燃油流量均平稳上升和下降,未出现超转

通过对某型发动机控制软件安全性分析和测试，使潜在导致系统危险和失效的软件原因得到了有效的识别和控制。在安全性测试工作中,已形成安全性需求的危险或失效原因均通过测试用例进行覆盖,危险和失效得到有效复现,软件安全性需求得到验证。

5　结束语

本文提出了针对航空发动机控制软件的安全性测试新方法,并给出了软件安全性测试用例自动生成的算法和原理,开发形成了原型工具平台,型号发控软件的工程应用表明该方法具有较高的实用性和可操作性,能够为发控软件的质量提升和安全性保证提供支撑。后续工作中,可将软件安全性分析与安全性测试结果相结合,采用软件安全性分析的方法对安全性测试数据进行采集,作为迭代开展软件安全性分析的输入;此外,软件安全性分析结果到软件安全性测试用例的转换算法是通过形式化描述实现的,因此需要对软件安全性分析结果进行进一步优化,使其能够与测试用例生成模块直接对接,从而避免人工进行形式化转化工作,进而大大提高测试效率。

参考文献:

[1] 姜彩虹. 航空发动机双余度控制规律设计方法 [J]. 航空动力学报,2011,26(10):2364-2370.
JIANG Caihong. Method of dual-redundant control law design for aeroengine [J]. Journal of Aerospace Power,2011,26(10):2364-2370.(in Chinese)

[2] Antona Bertoling. Software testing research: achievements, challenges, dreams [C]//Future of Software Engineering, Minneapolis, 2007: 85-103.

[3] RTCA/DO-178C. Software considerations in airborne systems and equipment certification[S]. Washington.DC: Requirement s and Technical Concepts for Aviation(RTCA), 2011:31.

[4] 何鑫,郑军,刘畅. 软件安全性测试研究综述[J]. 计算机测量与控制,2011,19(3):493-496.
HE Xin, ZHENG Jun, LIU Chang. A survey on research of software safety test [J]. Computer Measurement & Control,2011,19 (3): 493-496.(in Chinese).

[5] MIL-STD-882D, Standard Practice for System Safety Program Requirements [S]. Department of Defense, Washington.DC: USA Military, 1996:4.

[6] 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 Bingfeng, HUANG Zhiqiu, 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)

[7] Hendzik Post, Carsten Sinz, Florian Merz, et al. Linking functional requirements and software verification [C]//17th IEEE International Requirements Engineering Conference, 2009: 295-302.

[8] 李华聪,王鑫,韩小宝,等. 航空发动机线性变参数建模方法研究[J]. 推进技术,2007,28(4):418-421.
LI Huacong, WANG Xin, HAN Xiaobao,et al. Study of aeroengine linear parameter varying modeling [J]. Journal of Propulsion Technology, 2007,28(4):418-421.(in Chinese).

[9] 胡卫红,李述清,孙健国.控制问题中航空发动机飞行包线区域最优划分[J].推进技术,2011,32(3):391-395.
HU Weihong, LI Shuqing, SUN Jianguo. Flight-envelope optimization partition for aeroengines control [J]. Journal of Propulsion Technology, 2011,32(3):391-395.(in Chinese)

[10] NASA.NASA-GB-8719.13 Software safety guidebook [S]. Washington. DC: National Aeronautics and Space Administration, 2004:6.

[11] SAE.SAE ARP4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment[S]. Warrendale: The Engineering Society For Advancing Mobility Land Sea Air and Space, 1996:6.

[12] 宋晓秋.GJB/Z 102A-2012 军用软件安全性设计指南 [S]. 北京:中国人民解放军总装备部,2012:13.
SONG Xiaoqiu.GJB/Z 102A-2012 Guide for military software safety design[S]. Beijing:General Armament Department of the People's Liberation Army,2012:13.(in Chinese)

[13] 赵跃华,朱媛媛. 基于故障树分析的软件安全性测试研究[J]. 计算机应用研究,2013,30(6):1760-1763.
ZHAO Yuehua, ZHU Yuanyuan. Research on software safety testing based on fault tree analysis [J]. Application Research of Computers, 2013,30(6):1760-1763.(in Chinese)

[14] 蒋文亮,王少永,营笑,等. 一种应用于航空发动机全权限数字电子控制系统的解算器处理技术[J]. 推进技术,2017,38(3):666-672.
JIANG Wenliang, WANG Shaoyong, YING Xiao, et al. A resolver technology for full authority digital electronic control systems of aero-engine[J]. Journal of Proplsion Technology,2017,38(3):666-672.(in Chinese)

[15] 杨伟,冯雷星,彭靖波,等. 求解航空发动机数学模型的混合智能方法[J]. 推进技术,2008,29(5):614-616.
YANG Wei, FENG Leixing, PENG Jingbo, et al. An intelligent algorithm for solution of nonlinear mathematical model for aeroengine[J]. Journal of Propulsion Technology, 2008,29(5):614-616.(in Chinese)

[16] 刘畅,刘斌,阮镰. 航空电子软件仿真测试环境软件体系结构研究[J]. 航空学报,2006,27(5):877-882.
LIU Chang,LIU Bin,RUAN Lian. Software architecture of simulation testing environment for software in avionics [J]. Acta Aeronautica Et Astronautica Sinica,2006,27(5):877-882.(in Chinese)

(编辑:刘 静)