http://myfj.cnjournals.com myfj_sadri@comac.cc (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2021.04.004

以液压系统功能模型为例的告警捕获方法研究

薛鄂涛 肖 刚*

(上海交通大学,上海 200240)

摘 要: 回顾民机某型号研制过程中出现被动的设计更改和优化问题,机组告警与指示设计方案不完全符合飞行员操作需求是其主要原因。在机组告警系统设计前期有着需求确认手段缺乏,需求确认不充分的困难,如果在机组告警系统设计前期能够采用正确的建模和评估方案,就能及时发现问题,避免后期出现重大问题。针对此问题,首先阐述了告警需求与失效模式之间的关系,针对告警所关注的特征信息搭建告警需求数据库,并根据告警需求捕获准则,以液压系统功能运行模型为例,通过系统失效模式分析和模型间映射关系得到需要告警的失效模式,最后结合型号经验和 ARP4102-4、FAR25.1322 及 AC25-1322 中的告警理念,完成系统告警定义。

关键词: 告警需求捕获;告警定义;MBSE;级联失效

中图分类号: TP393 **文献标识码**: A **OSID**:

0 引言

回顾某民机研制过程,发现在机组告警系统设计前期遇到了告警需求确认手段缺乏、需求确认不充分的困难,因此迫切需要丰富机组告警系统设计需求确认手段,提高设计效率,降低后期设计更改的风险。基于模型的系统工程方法(Model-Based Systems Engineering,简称 MBSE)能确保在项目前期实现需求捕获与需求确认,减少在项目后期进行设计更改及相应的验证等工作,避免巨额工程更改费用。

针对目前某型号告警需求捕获不充分的问题,本研究首先基于 ARP 4754A[1],ARP 4761[2]对告警必要性和重要性进行了分析,得到了告警信息的特征信息[3-4],然后基于已有的特征信息与型号研制经验搭建了告警需求数据库,利用基于 MBSE 建立的液压系统功能运行模型[5-8],根据告警需求捕获准则,对告警故障底事件进行综合模拟,自动化分析系统失效模式[9-11],通过模型间映射关系得到需要告警的失效模式,进而形成液压系统告警需求捕获方案的分析方法。

1 告警消息与告警需求分析

在飞机多告警成员系统集成的背景下,有必要确立合理的告警信息设计准则,捕获需要产生告警的异常状态或者事件,即告警需求。告警需求为判决告警信息必要性和重要性的重要来源,准确捕获告警需求的先决条件是建立对告警消息所表征信息类型的系统性理解。

1.1 告警消息分析

通过飞机典型告警成员系统的告警信息类型可知,告警的关注对象为系统的功能/性能/物理部件异常状态,即失效情况,因此后续告警需求的捕获方法将以系统内的失效模式作为主要分析对象。

除了明确告警消息类型,告警消息还将根据

* 通信作者. E-mail: xiaogang@sjtu.edu.cn

引用格式: 薛鄂涛,肖刚. 以液压系统功能模型为例的告警捕获方法研究[J]. 民用飞机设计与研究,2021(4):22-27. XUE Z T, XIAO G. Research on alarm capture based on hydraulic system model[J]. Civil Aircraft Design and Research,2021(4):22-27(in Chinese).

实际飞行状态进行触发/抑制，因此告警触发条件也是告警需求捕获过程中需要考虑的因素之一。选择通过告警逻辑方程解析告警的产生/抑制条件。图 1 中说明了告警逻辑方程的组成元素可划分为四个部分：主干信息、背景信息、控制信息、抑制信息。

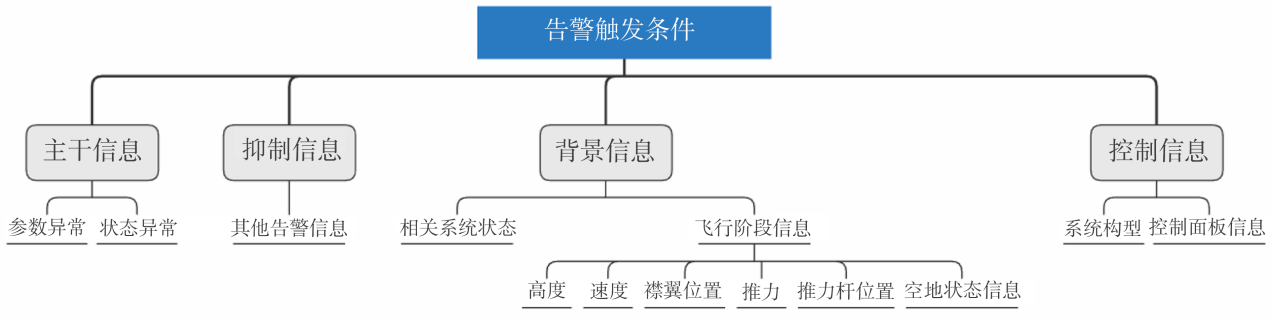

图 1　告警触发条件

主干信息包括与飞行过程中主要任务实现相关的错误的参数/状态信息，即上一小节所分析的告警关注对象；背景信息包括与该告警/失效相关的其他系统状态信息/外界场景信息以及飞行阶段信息；控制信息包括由驾驶舱设置的系统组件/部件的工作状态，以及系统构型状态/运行模式；抑制信息则为通过失效/告警级联关系或者包含关系推导出的，与本告警相关的其他告警信息的触发状态。

1.2 告警需求分析

通过分析告警消息类型和告警触发/抑制条件，可知告警主要关注较高层级/较重要的异常情况，并考虑飞行员的情景意识因素、外部环境因素等来决定是否进行告警。上述因素共同决定了告警的必要性，可进一步归纳为如下几种类型的告警需求：失效的直接和间接的安全性影响、飞行员的情景意识需求、外部环境等。除此之外，由于飞机要满足适航规章，因此从安全性角度考量，部分适航条款覆盖了告警需求，也可归纳至告警需求的必要性集合中。告警需求与告警逻辑方程各个组分的映射关系如图 2 所示。

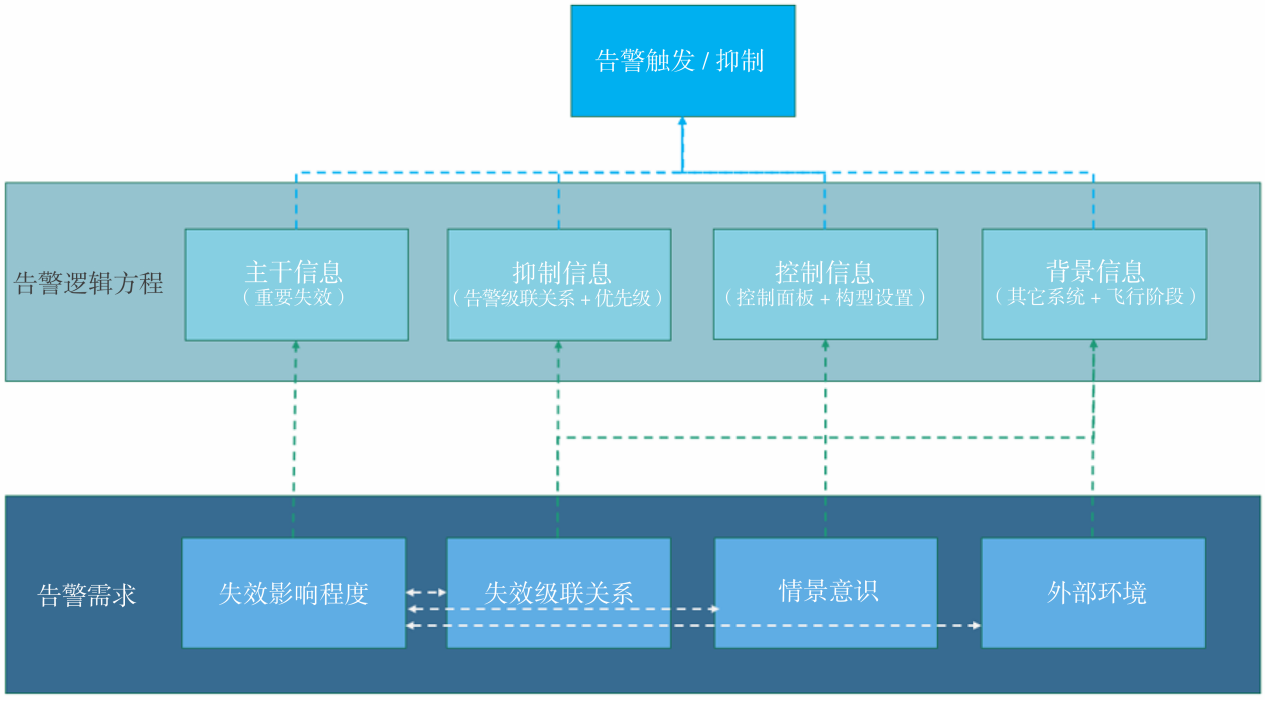

图 2　告警需求与告警逻辑方程映射关系

2　告警需求捕获方法

告警需求捕获的原理是通过对行业适航标准、飞行员情景意识、失效模式安全性影响等维度进行综合分析，提取飞行过程中有必要告知飞行员的情景模式。

2.1 告警需求库构建

告警需求数据库中存储了告警必要性有关的特征信息，包括适航条款、飞行员情景意识等，基于行业规则或者实际经验，为告警需求的提取进行表征。

1）适航条款

适航条款是决定告警的顶层约束，与告警必要性相关的适航条款将以模型的形式存储在数据库中，并为下文的告警相关性建立提供支持。

2）情景意识需求

告警信息与飞行员响应紧密耦合，是飞机向飞行员传递信息的重要接口，其有助于飞行员建立情景意识，为飞行员对当前飞机状态感知、决策判断等行为提供指导。因此，从飞行员的情景意识角度可以反向推测告警的必要性。

3）飞行员处理措施

飞行员处理措施模型对 FCOM 中已有的对于告警或异常情况的处理行为进行记录，并在 tagged value 中标注了处理措施的紧急程度和内容等信息。

2.2 告警需求捕获准则

告警需求产生的源头为飞机告警成员系统内的异常状态，聚焦于失效模式。因此，告警捕获规则旨在建立系统模型内潜在失效模式模型与告警需求之间的相关性。

从告警必要性分析和告警等级分析中的需求特征元素可知，主要从适航条款、情景意识、安全性影响、其他（包括对飞机结构、气动、环境的影响的分析）来建立告警需求与系统模型之间的映射。

2.3 系统模型搭建

在告警需求映射规则建立的基础上，根据告警成员系统的功能组成、物理架构和安全性因素，构建系统模型以提供用于告警需求分析的原始素材。如图 3 所示，系统模型的主要构成部分包括功能架构、物理架构、失效模式。

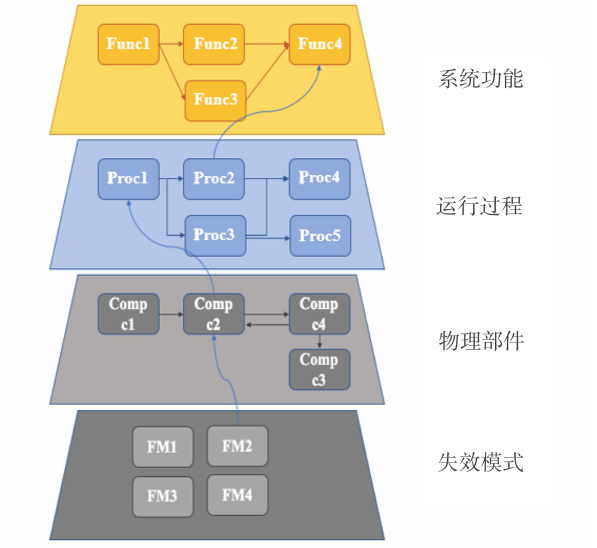

图 3　系统模型组成结构

不同功能架构元素通过功能参数建立上下游逻辑关系。如图 4 所示，物理部件对功能的影响通过

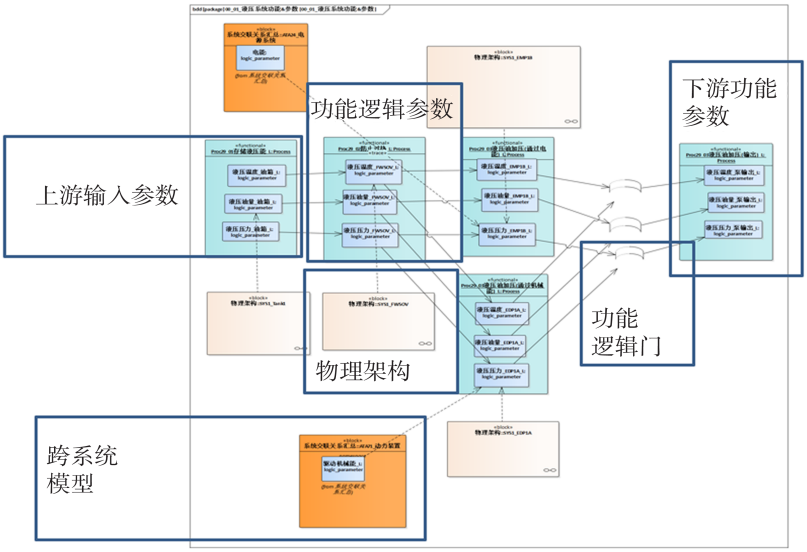

图 4　系统功能框架元素关系分析

物理部件模型（黄色）与功能参数的映射关系体现，外界功能对功能的影响通过外界功能模型（粉色）中的参数与功能模型中参数的映射关系体现，进而，功能运行过程模型链条的输出结果传递给系统级功能模型（粉色），并以其为媒介进一步向下合并至其他系统的功能运行框架中。

2.4 告警需求捕获

在告警需求关联规则建立与系统模型建立的基础上，将开展告警需求捕获。告警需求捕获包括以下三个子步骤：建立告警需求的模型，建立模型间的映射关系，进而筛选需要告警的情况。

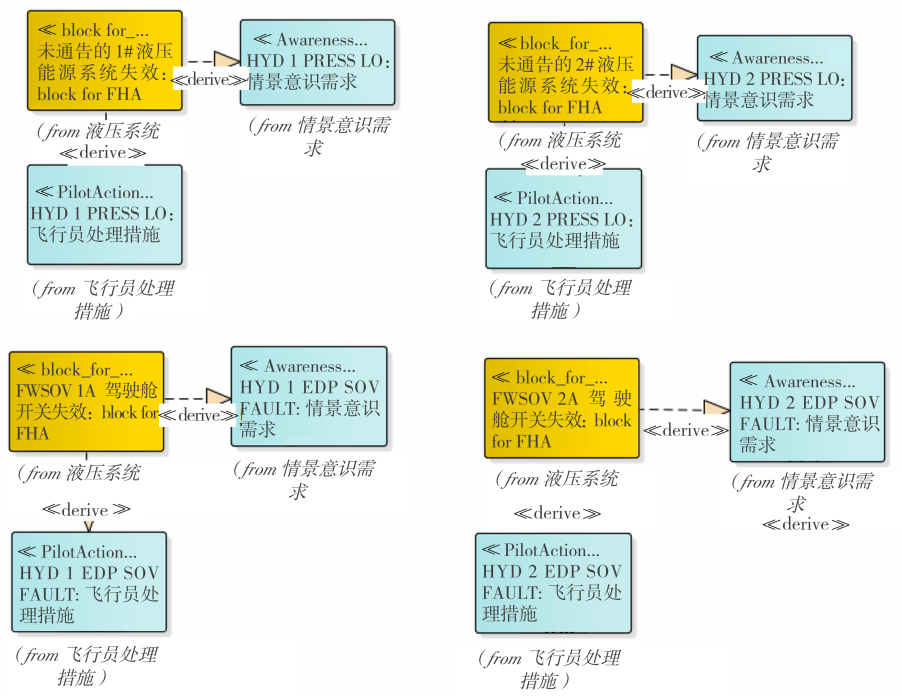

图 5　失效模式与告警需求模型映射关系

另一方面，如图 6 所示，建立失效模型与物理部件、功能参数模型之间的关联性，用于表现和推导失效的安全性影响。

3）筛选需要告警的情况

以系统的失效模型为分析对象，基于告警需求捕获准则，搜索存在上述映射关系的对象，以及其级联效应导致严重失效的对象。通过以下两方面对失效模式的安全性影响进行精细化：图 7 说明了一方面

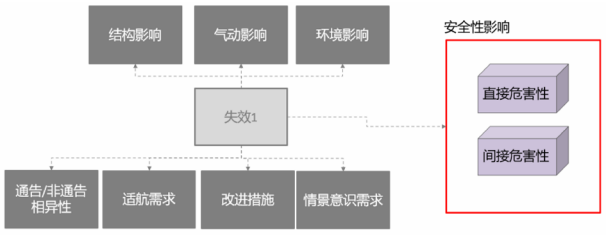

图 6　失效与其他模型的映射关系汇总

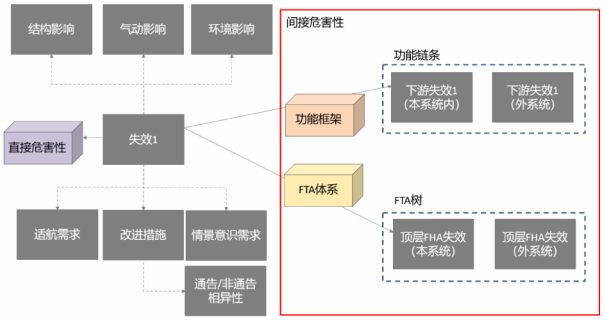

图 7　失效的间接危害性搜索框架

分析该失效的直接危害性，另一方面推导该失效可能导致的潜在危害，进一步分解为本系统内的安全性影响和外系统内的安全性影响。

2.5 告警等级判定

告警等级判定考量告警的紧急程度和飞行员响应的必要性。根据适航标准中对于告警等级的定义，通过飞行员知晓的紧急程度、处理措施的紧急程度和安全性影响等级，对告警等级进行约束。

2.6 告警需求确认

在基于模型分析系统失效情况，得到潜在告警需求的基础上，对所导出的表格内容进行核查，以对告警需求进行确认。

核查方式主要包括以下两个方面：

1）表格内部信息的正确性。

2）根据失效分析得到的告警和已经存在的告警的一致性。

3　液压系统案例验证

3.1 液压系统

液压系统由发动机驱动泵（EDP）、电动泵（EMP）、能源转换装置（PTU）、液压油箱及油滤组件和液压系统综合控制单元（HLRM）等组成。飞机液压系统采用三套相互独立的 1#、2#、3#分系统，其主要功能是为飞机液压用户提供液压能源。系统与外界交互的参数为液压油，与该系统交互的上游系统包括电源系统、动力系统，下游系统包括主飞行控制系统、高升力控制系统、起落架控制系统等。仿真验证选取了飞机液压系统为告警需求的分析对象，对系统功能架构、物理架构、安全性模型进行了构建，并在此基础上开展了告警需求分析。

3.2 液压系统模型搭建

根据飞机级功能列出液压系统进行系统级功能清单，并对系统级功能清单进行分类梳理，以为用户提供恒压液压能源为核心建立主干功能框架，并将各辅助功能合并到框架中。

3.3 液压系统告警需求搜索结果

根据失效模式与适航条款需求维度，飞行员情景意识需求维度以及安全性维度的功能架构、故障树架构的交联关系，液压系统告警需求的搜索结果如图 8 所示。

进而对比分析告警需求捕获结果和已有告警信息的分布情况可知，通过软件分析平台开展告警需求捕获，发现了 47 个告警需求，其中每个告警需求均存在相对应的失效模式，并且同样存在相对应的告警信息，从而验证了分析方法的正确性。

	章节号	失效模式	失效模式编号	失效影响等级与概率	飞行阶段	安全性影响	告警有无对安全性影响	条款要求	发生该失效后是否需要机组知晓的原因	机组知否能及
1	ATA34	有通告的1#液压能源系统失效	29-F01-05	IV	T，F1-F4，L		偏航控制功能完全丧失， 非指令性偏航超过限制， 方向舵偏航控制功能丧失， 方向舵方向控制功能丧失， 方向舵非指令性运动超过可接受限制， 非指令性俯仰超过限制， 滚转控制功能完全丧失， 一块副翼急偏或振荡超过可接受限制， 未通告的丧失襟翼自动收回功能， 未通告的丧失缝翼伸出、收回功能， 丧失襟翼或缝翼位置信号（提供给主飞控系统）， 5#缝翼出现倾斜，系统未探测或锁止， 未通告的丧失缝翼低速大迎角锁定功能， 错误的缝翼低速大迎角锁定功能， 通告的丧失缝翼伸出、收回功能 襟翼或缝翼半速运动， 通告的丧失缝翼低速大迎角锁定功能		1,2,3	
2	ATA34	有通告的2#液压能源系统失效	29-F01-06	IV	T，F1-F4，L		未通告的丧失襟翼自动收回功能， 未通告的丧失缝翼伸出、收回功能， 丧失襟翼或缝翼位置信号（提供给主飞控系统）， 5#缝翼出现倾斜，系统未探测或锁止， 未通告的丧失缝翼低速大迎角锁定功能， 错误的缝翼低速大迎角锁定功能， 通告的丧失缝翼伸出、收回功能 襟翼或缝翼半速运动， 通告的丧失缝翼低速大迎角锁定功能		1,2,3	
3	ATA34	有通告的3#液压能源系统失效	29-F01-07	IV	T，F1-F4，L		通告的丧失襟翼伸出、收回功能 未通告的丧失襟翼伸出、收回功能， 丧失襟翼或缝翼位置信号（提供给主飞控系统）， 襟翼或缝翼半速运动， 通告的丧失襟翼自动收回功能， 通告的丧失襟翼载荷减缓功能		1,2,3	
4	ATA34	全部液压能源系统失效	29-F01-01	I5.84e-10	ALL				N/A	
5	ATA34	有通告的1#和2#液压能源系统失效	29-F01-02	III5.7e-9	T，F1-F4，L				1,2,3,4需要立即改航	
6	ATA34	有通告的1#和3#液压能源系统失效	29-F01-03	III4.86e-9	T，F1-F4，L				1,2,3,4需要立即改航	
7	ATA34	有通告的2#和3#液压能源系统失效	29-F01-04	III4.87e-9	T，F1-F4，L				1,2,3,4需要立即改航	

图 8　液压系统告警需求搜索结果

4　结论

本文针对当前在民机告警系统前期设计中遇到的告警需求捕获不充分的困难,提出将模型和告警需求捕获方法相集成,并通过液压系统案例分析演示了告警需求捕获结果。

告警需求数据库和告警需求捕获准则的建立是基于工程实际经验与相关适航验证所得到的,其如何优化与完善仍然值得研究。

参考文献:

[1] Society of Automotive Engineers(SAE). Guidelines for development of civil aircraft and systems: SAE ARP 4754 [S]. U. S. :SAE,2010.

[2] Society of Automotive Engineers(SAE). Guidelines and methods for conucting the safety assessment process on civil airborne system and equipment: SAE ARP 4761 [S]. U. S. :SAE,1996.

[3] 熊华钢. 先进航空电子综合技术[M]. 第一版. 北京:国防工业出版社, 2009:246-298.

[4] 郭晓博,张鹏程,郭鼎. 飞行机组告警系统软件设计[J]. 航空电子技术,2017,48(3):32-36.

[5] BALMELLI L. An overview of the systems modeling language for products and systems development[J]. Journal of Object Technology, 2007, 6:8-24.

[6] BOOCH G,JACOBSON I,RUMBAUGH, J. The unified modeling language reference manual[M]. First? Edition. BeiJing:China Machine Press, 2006:126-156.

[7] ZHANG T, JOUAULT F, Bézivin J. An MDE-based method for bridging different design notations[J]. Innovations in Systems & Software Engineering, 2008, 4(3):203-213.

[8] ZHU Y, HUANG Z Q, CAO Z N, et al. Method for generating software architecture model based on formal specifications[J]. Journal of Software, 2010, 21(11):2738-2751.

[9] WU Y Q, XIAO G, WANG M. Cascading failure analysis method of avionics based on operational process state [J]. IEEE Access, 2020, 8: 148425-148444.

[10] WU, Y Q, XIAO G, WANG M. State-based safety analysis method for dynamic evaluation of failure effect [J]. Aerospace Systems, 2021, 4:49-65.

[11] WU Y Q, XUE, Z T, XIAO G. Parameter-orientated functional modeling method based on flight process: In Proceedings of International Conference on Aerospace System Science and Engineering[C] Shanghai: Springer-Verlag, 2020:55-69.

作者简介

薛鄹涛　男,硕士。主要研究方向:航电综合与仿真测试。E-mail: xzt0407@ sjtu. edu. cn

肖　刚　男,博士,研究员,博士生导师。主要研究方向:智能信息处理,航电综合与仿真测试,民机产业链与通用航空。E-mail: xiaogang@ sjtu. edu. cn

Research on alarm capture based on hydraulic system model

XUE Zoutao　XIAO Gang *

(Shanghai Jiaotong University, Shanghai 200240)

Abstract: Reviewing the passive design changes and optimization problems that occurred during the development of a certain type of civil aircraft, the main reason is that the design plan of the crew warning and indication does not fully meet the pilot's operational needs. In the early stage of the warning system design, there is a lack of alarm requirements confirmation means and the difficulty of insufficient demand confirmation. If the correct modeling and evaluation plan can be used in the early stage of the warning system design, problems can be found in time and major problems can be avoided in the later stage. Aiming at this problem, this paper first elaborates the relationship between alarm requirements and failure modes, builds an alarm requirement database for the characteristic information of alarms, and captures the criteria according to alarm requirements. Taking the hydraulic system function operation model as an example, obtain the failure mode that needs to be alarmed through the system failure mode analyzing and the mapping relationship between the models, finally combining the model experience and the alarm concept in ARP4102-4, FAR25.1322 and AC25-1322 to complete the system alarm definition.

Keywords: alarm demand capture; alarm definition; mbse; cascade failure

* Corresponding author. E-mail: xiaogang@ sjtu. edu. cn