文章编号:1674-8190(2024)03-101-09

民用飞机刹车控制系统软件构型管理研究

刘莉,马晓军,张娟,杨茗
(西安航空制动科技有限公司 民用飞机事业部,西安 710065)

摘 要: 民用飞机刹车控制系统构型管理在系统设计开发过程和适航符合性验证过程中发挥着关键作用。为了提升民用飞机刹车控制系统软件构型管理能力,使该系统设计开发的软件满足适航要求,介绍刹车控制系统软件构型管理的概念和方法,描述如何运用系统思维和信息化流程手段将构型管理和软件设计相结合,开展软件全生命周期过程构型管理活动。结合DO-178C的要求,提出建立以产品构型为核心的构型数据数字化管理机制,实现刹车控制系统软件研制的单一数据源。结果表明:通过与构型基线管理相结合建立一个统一的构型数据库,在该构型数据库中严格按照阶段的状态进行准确记录,确保了状态信息的实时性、可追溯性、完整性及有效性,达到了最终构型控制目标,可以满足适航要求。

关键词: 软件构型管理(SCM);基线(BS);构型数据数字化管理;设计保证等级(DAL);DO-178C
中图分类号: V227; TP273 **文献标识码:** A
DOI: 10.16615/j.cnki.1674-8190.2024.03.10

Research on configuration management of civil aircraft brake control system software

LIU Li, MA Xiaojun, ZHANG Juan, YANG Ming
(Civil Aircraft Business Department, AVIC Xi'an Aviation Brake Technology Co., Ltd., Xi'an 710065, China)

Abstract: The configuration management of civil aircraft brake control system plays a key role in the process of system design and development and airworthiness compliance verification. In order to improve the configuration management capability of civil aircraft brake system, and make the software designed and developed meet the airworthiness requirements, this paper introduces the concept and method of brake system control software configuration management, and illustrates how to combine configuration management with software design by means of system thinking and information flow to carry out whole-life-cycle configuration management. By combining with the requirements of DO-178C, configuration data digital management mechanism based on product configuration is established, unique data source of brake control system development is created. The result shows that a unified configuration database is established with configuration baseline management combination, in which the information and status are accurately recorded strictly to ensure the real-time, traceability, integrity and effectiveness of status information, and achieve the final configuration control goal to meet the airworthiness requirements.

Key words: software configuration management (SCM); baseline (BS); configuration data digital management; design assurance level (DAL); software considerations in airborne systems and equipment certification (DO-178C)

收稿日期: 2023-04-03; **修回日期:** 2023-08-15

通信作者: 刘莉(1972—),女,学士,高级工程师。E-mail: nwliuli@126.com

引用格式: 刘莉,马晓军,张娟,等. 民用飞机刹车控制系统软件构型管理研究[J]. 航空工程进展, 2024, 15(3): 101-109,142.
LIU Li, MA Xiaojun, ZHANG Juan, et al. Research on configuration management of civil aircraft brake control system software [J]. Advances in Aeronautical Science and Engineering, 2024, 15(3): 101-109,142. (in Chinese)

0 引 言

构型管理的概念来源于美国，波音公司于1993年提出了基于产品数据管理的数字化构型管理系统DCAC/MRM（飞机构型定义与控制和制造资源管理），2001年在全球供应链中正式运行该系统[1]。经过20多年的总结和发展，构型管理规范ANSI/GEIA-649B—2010[2]已成为一个概念清晰的新规范，规范要求所有构型管理功能的应用是平衡的和一致的。构型管理的发展大致可分为3个阶段，即强制性阶段、自觉性阶段和走向市场驱动阶段，目前的构型管理处于第3个发展阶段[3]。

2013年7月美国联邦航空局（FAA）明确了新开发软件适航标准由DO-178B升级为DO-178C[4]。DO-178C/DO-178B标准是民航体系内各利益相关方普遍接受的一种符合性方法，在机载软件的研制及审查中发挥着重要的指导作用[5]。Rafael等[6]研究了一个SCM五轴参考模型，讨论了角色配置管理在商业产品和系统中发挥的作用，描述了不同的技术、组织和产品关注点之间的关系，提供了一个简单度量公司内部结构和运行环境适合的SCM解决方案。

刹车控制系统所用机载软件在开发过程中为了达到适航要求，通常会参考DO-178C/DO-178B标准进行软件开发，但是在构型管理特别是更改控制方面与适航要求还有差距。随着民用飞机综合航电和液压系统技术的提高，对软件的应用和通过软件实现的需求也越来越多。如何高效进行部件级机载软件的构型管理，使其既能满足适航要求、便于管理，又能满足项目需求、便于设计开发构型管理方案，成为民用飞机供应商亟待解决的理论与现实问题。

传统的构型管理研究局限于构型数据管理，缺少从流程体系角度对全生命周期构型管理的改造提升[3,7]。如果没有考虑基于全生命周期的软件平台数据化的构型管理，会出现很多问题。例如：①软件开发过程中数据的追溯性不便于关联查询；②软件构型管理对人员的依赖过高；③软件信息的时效性、完整性以及权属问题都得不到保证。随着民用飞机的高速发展与新技术的广泛应用，采用基于全生命周期的系统管理方法进行软件构型管理可以规范化刹车控制系统的软件开发过程，使得最终设计验证的软件达到适航要求，保障民用飞机刹车控制系统在采用新技术的同时保障安全。

本文针对刹车控制系统民用飞机构型管理的现状和薄弱环节，在构型管理平台的搭建、构型基线建立时机以及通过平台对软件构型项的更改控制机制等方面开展研究，重点分析如何运用科技手段，利用数字平台，将软件构型管理与产品的设计过程相结合，实现对机载软件全生命周期的技术状态管理、跟踪和控制。

1 刹车控制系统软件构型管理方案

机载软件构型管理的思想已经逐步在民用飞机研制过程中被认知和接纳，如何通过高效管理实现既可以保障开发的软件满足适航要求，又能兼顾软件研制进度就成了一个新命题。传统的做法是把机载软件视作机载设备的一部分，按照设备的管理方式进行管理，通过Testbed工具对软件代码进行静态测试，再通过黑盒测试验证技术条件是否满足合同要求。传统做法虽然简单高效，但有很多隐患和潜在的安全风险不易被识别，软件更改前后的追溯性及综合试验阶段软件的有效性都无法保障。本文提出一种基于DO-178C标准，结合软件设计开发过程，通过多平台交互开展构型管理活动的方案。

现代刹车控制系统（BCS）通常会被设计成电子控制液压刹车系统（brake-by-wire），并提供机械操控的液压停车/应急刹车系统作为备用停机刹车。其中，正常刹车系统包括一个刹车控制单元（BCU），刹车控制系统软件就嵌入在这个BCU中，实现数据采集、运算，实现控制功能、数据交互以及数据记录。刹车控制系统软件生命周期过程之间的信息流如图1所示。

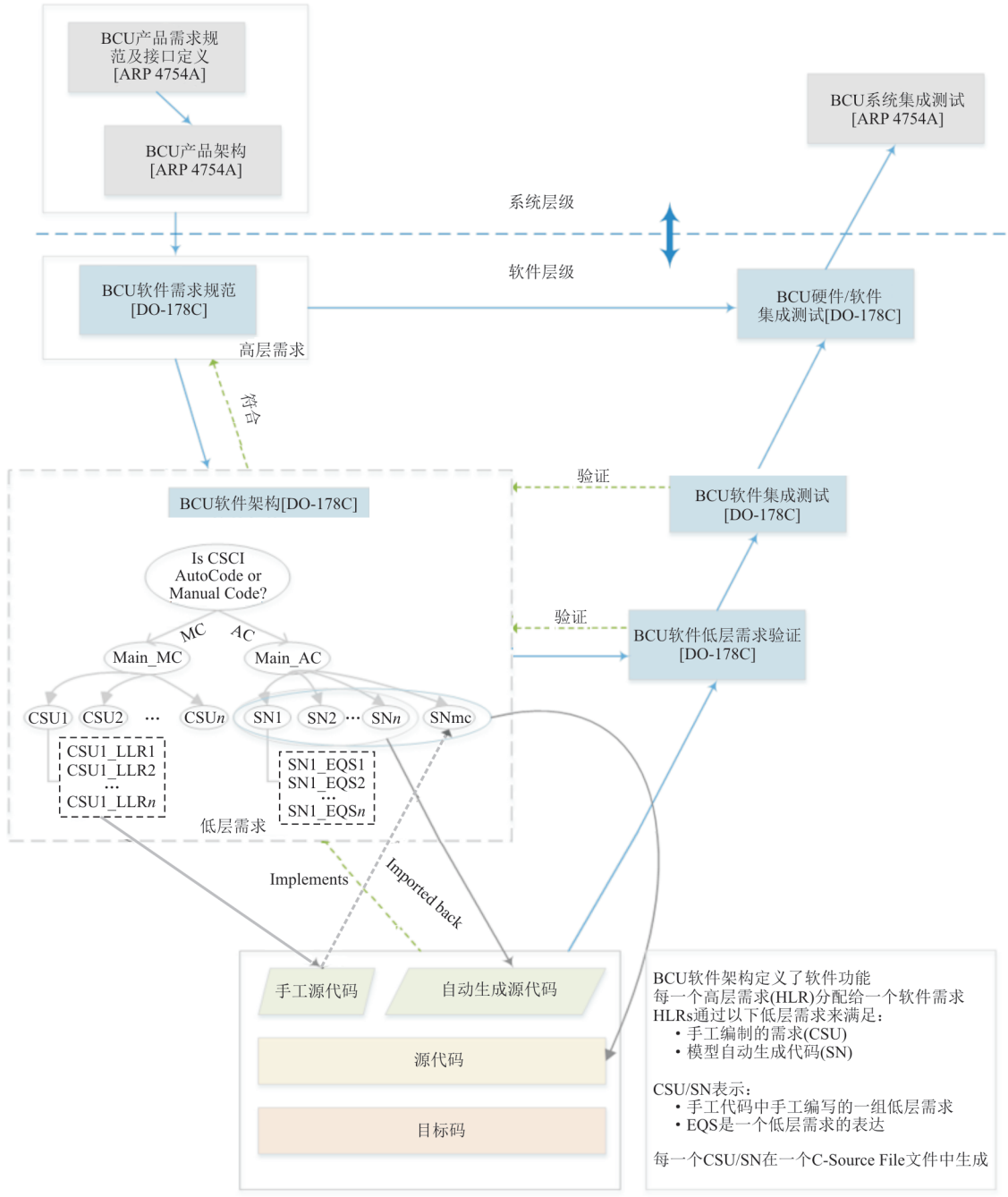

图 1　刹车控制系统软件生命周期过程之间的信息流

Fig. 1　Information flow between brake control system software lifecycle processes

1.1　软件等级

软件等级通常是指机载软件的设计保证等级(DAL),是由飞机安全性分析过程决定的。供应商应和主制造商一起完成系统级的功能危害性评估(FHA)和初步系统安全评估(PSSA),再通过PSSA分析后即可得到软件的DAL。由于机轮刹车控制系统是飞机在着陆安全时的重要保障,通常刹车系统软件会被定级为A级或B级,本文重点研究A级和B级软件的构型管理。

根据DO-178C的要求,结合产品研制目标以及DAL,通过完成的构型管理活动实现对数据的管控。软件生命周期数据的构型管理需要通过编制和执行软件构型管理计划,标识软件构型项并对其进行构型控制、变更控制、维护构型项状态记录、构型审核,来建立和维护工作产品的完整性和一致性。软件的生命周期数据流如图2所示。

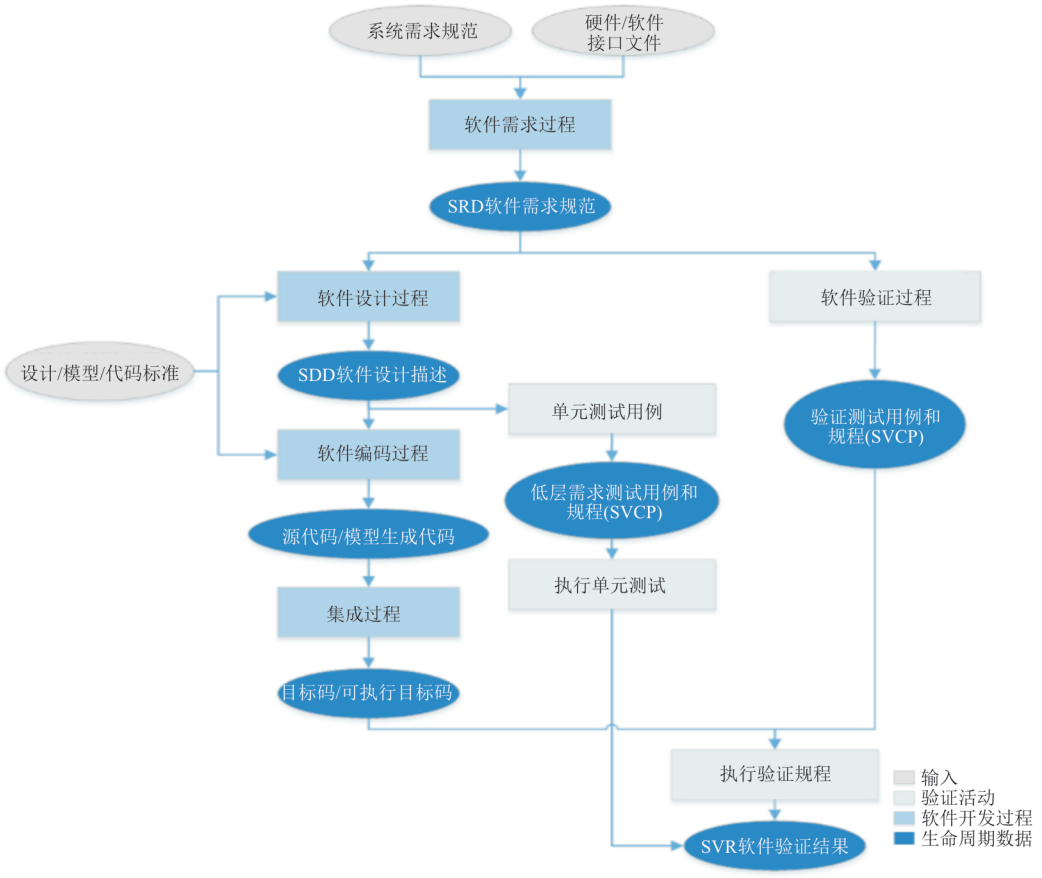

图 2 软件生命周期数据流

Fig. 2 Software lifecycle data flow

对于不同类型的软件生命周期数据，其至少应完成的构型管理活动有所不同。软件构型管理过程主要包括如下活动：策划构型管理过程[2-3,8-13]、建立并跟踪基线、问题报告与更改控制[2-3,8-13]、构型状态纪实[2-3,12]、软件归档、检索与发布、软件加载控制以及软件生命周期环境控制。

1.2 构型管理

构型管理是指：用技术和行政的手段建立规范化的产品研发秩序，确保产品从立项、设计、试验、生产、验证、维护和使用到报废清理的全生命周期过程中，产品所达到的功能特性、物理特性和需求与其构型信息之间的一致性[3,12,14]，保证设计目标能够如期实现。软件构型管理是指为保证软件构型项的完整性和正确性，在整个软件生存周期内应用构型管理的过程。

1.3 构型标识

构型标识是一项构型管理活动，包括：识别构型项，确定每个构型项所需的构型文件，确定构型项及相应文件的标识号。每个构型项必须使用唯一的标识[11-12]，应为软件生命周期数据建立构型标识，并通过项目软件构型项标识规则予以充分定义。

将定义好的项目构型标识规则作为一个工作包加载到构型管理数据平台中，配置完成后，每个构型项由计算机按照规则分配唯一的构型标识。

1.4 基 线

基线(BS)是在某一时间节点上对产品特征的一致性的描述，包括当前已批准和发放的由某版本的软件及相关构型文件所组成的一系列文档，它作为更改定义的基础。

基线的确立原则：建立基线的目的是为进一步的工作定义一个基础，以便保证构型项目间的可追溯性、可参照性和可控性。第一次基线建立时应包含构型基线申请单、构型文件清单、构型项清单及软件源代码和软件目标码，且纳入基线的

构型内容应该全部是已批准的最新技术状态。基线冻结之后,基线内构型项所发生的任何更改需发起正式的问题报告流程。基线的建立管控流程如图 3 所示。

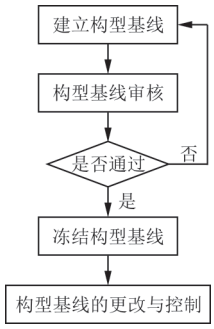

图 3　基线建立管控流程图

Fig. 3　Baseline establishment control process

刹车控制系统软件的基线管理是通过内部资源平台 PDM(Product Date Management,是一个企业级的产品研发协同管理平台)实现的。基线平台管理示意图如图 4 所示。

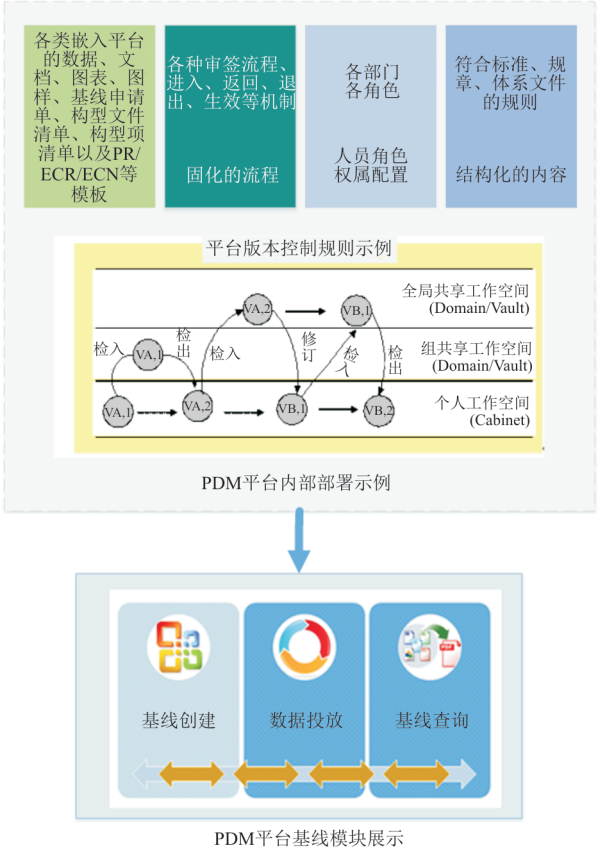

图 4　基线平台管理示意图

Fig. 4　Baseline platform management demonstration

PDM 平台的二次开发中在产品数据满足规定的特定功能特性和物理特性时,记录当时数据结构中各具体版本的组合关系,形成产品的技术状态记录和控制的起点,系统可以有效、实时、全面地控制产品从规划、设计等全生命周期中的各种庞大而复杂的数字化信息,通过对不同产品基线的管理,企业就可以合理调配产品的多样化、多状态,轻松控制产品配置,促使相互间相辅相成,充分发挥各自的作用。

平台在软件的部分参考了 DO-178C/DO-178B 标准,将要求以模板、结构化的内容、固化的流程等方式嵌入在 PDM 平台中,并通过后台对人员角色、基线审批流程及用户权限进行了约束和定义。

1.5　构型控制

构型控制是一项构型管理活动,是指构型基线建立后,为控制构型项的更改而对提出的更改建议(工程更改、偏离、超差)所进行的论证、评定、协调、审批和实施的活动。

为了提升产品研发过程中,不同专业和部门之间紧密协同,以既分工又互相协作的方式共同完成研制任务,对 Polarion 平台(西门子公司开发的一套一体化应用程序,提供软件生命周期管理的一体化解决方案)也进行了二次开发,目的是打造一个端到端的研发管理平台,实现不同研制阶段的数据共享与协同,将需求、设计、开发、软件配置管理、测试、项目管理等工作无缝衔接、统筹管理,实现技术相关项关联追溯,实现技术状态有效管理。刹车控制系统的软件构型控制通过内部资源平台 PDM 实现对构型项的申请、审签、更改及发布,软件的构型数据更改控制逻辑以及在平台间交互情况示例如图 5 所示;通过软件平台 Polarion 进行软件的需求、设计、开发和更改申请控制,软件的更改控制流程如图 6 所示;通过内部资源平台 SVN(SVN 是 Subversion 的缩写,是一个开放源代码的版本控制系统)进行构型数据存储;通过高效沟通管理软件(Effective Communication Management,简称 ECM)与客户进行数据交互,软件平台交互关系示意图如图 7 所示。

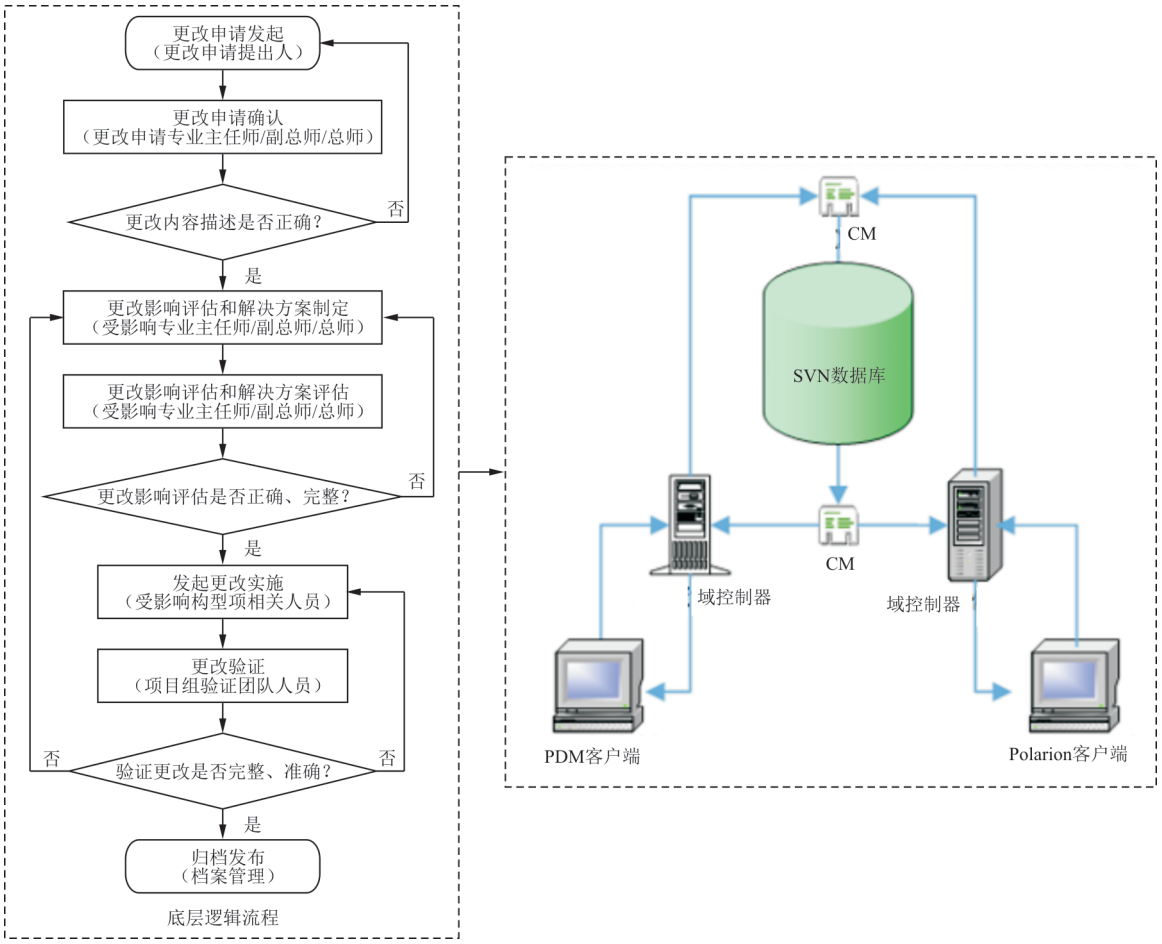

图 5 软件构型更改控制示意图

Fig. 5 Software configuration change control demonstration

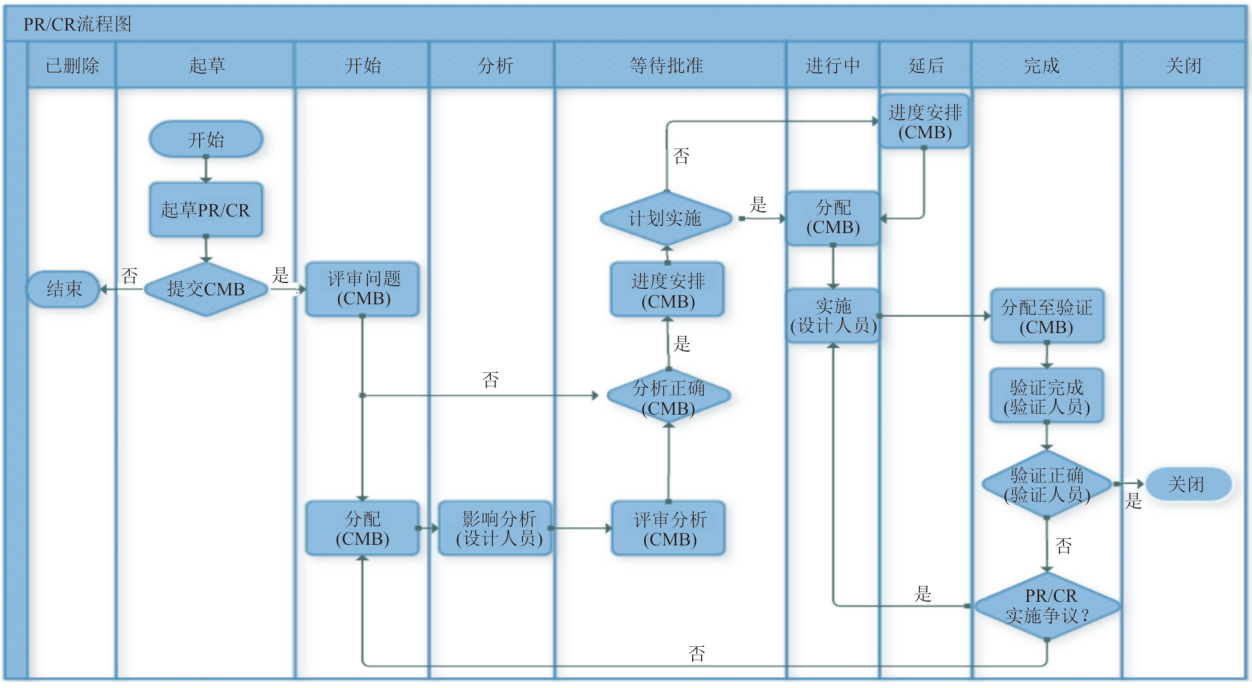

图 6 软件 PR/CR 流程图

Fig. 6 Software PR/CR control process

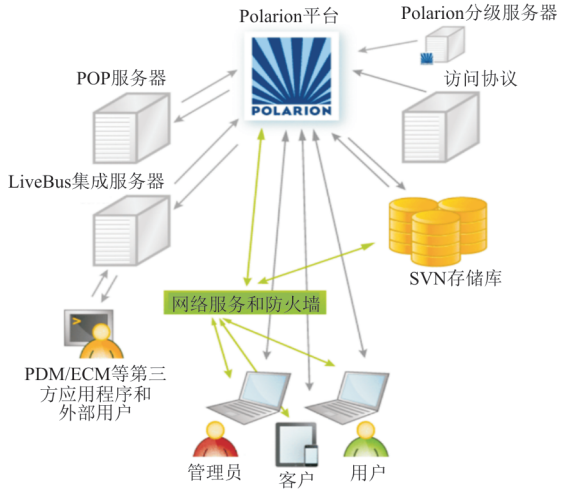

图 7　软件管控平台交互示意图

Fig. 7　Software control platform interaction

2　刹车控制系统软件构型管理研究

运用系统思维和信息化流程的技术手段,通过和构型基线管理相结合建立一个统一的构型数据库,集中存放各类构型数据,并在构型库 SVN 中严格按照阶段的状态进行准确记录,确保状态信息的实时性、可追溯性、完整性及有效性,实现刹车系统软件研制的单一数据源。结合软件设计过程如图 8 所示,需要经历 4 个阶段(计划阶段、开发阶段、验证阶段和最终合格审定阶段)[3,12,15]及软件开发模型开展软件全生命周期过程构型管理,建立以产品构型为核心的构型数据管理机制。

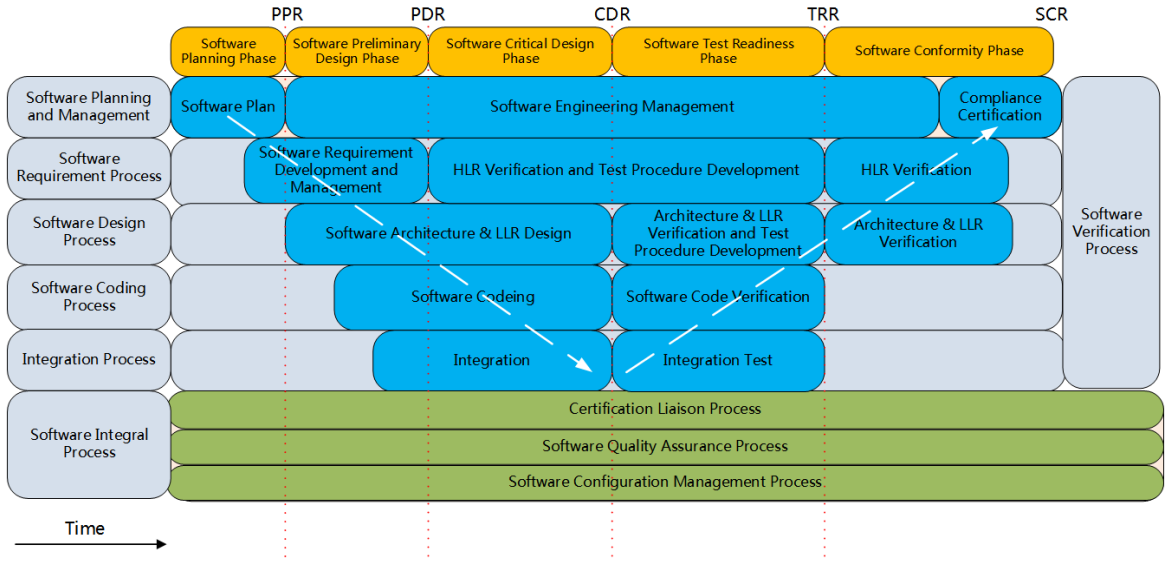

图 8　V 模型过程关系图[9]

Fig. 8　V model process relation[9]

刹车控制系统结合软件设计过程需要经历的 4 个阶段,在软件全生命周期过程通常会建立 5 条或者 6 条正式基线(例如,软件计划评审基线、软件需求评审基线、软件设计评审基线、软件集成评审基线、软件验证评审基线及软件最终评审基线)。根据具体情况,为了便于软件的研发还可以建立多条工程基线(例如,需求基线、设计发放基线、产品基线等)。工程基线存储在 SVN 的设计开发库中。构型和基线之间的逻辑关系如图 9 所示。

软件构型管理过程同软件设计过程相结合的流程如图 10 所示。

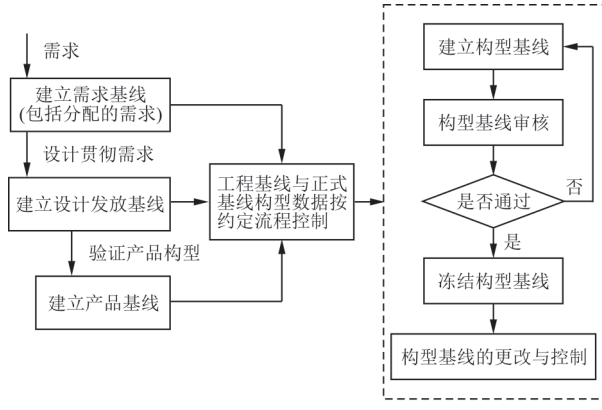

图 9　构型基线关系图

Fig. 9　Configuration baseline relation

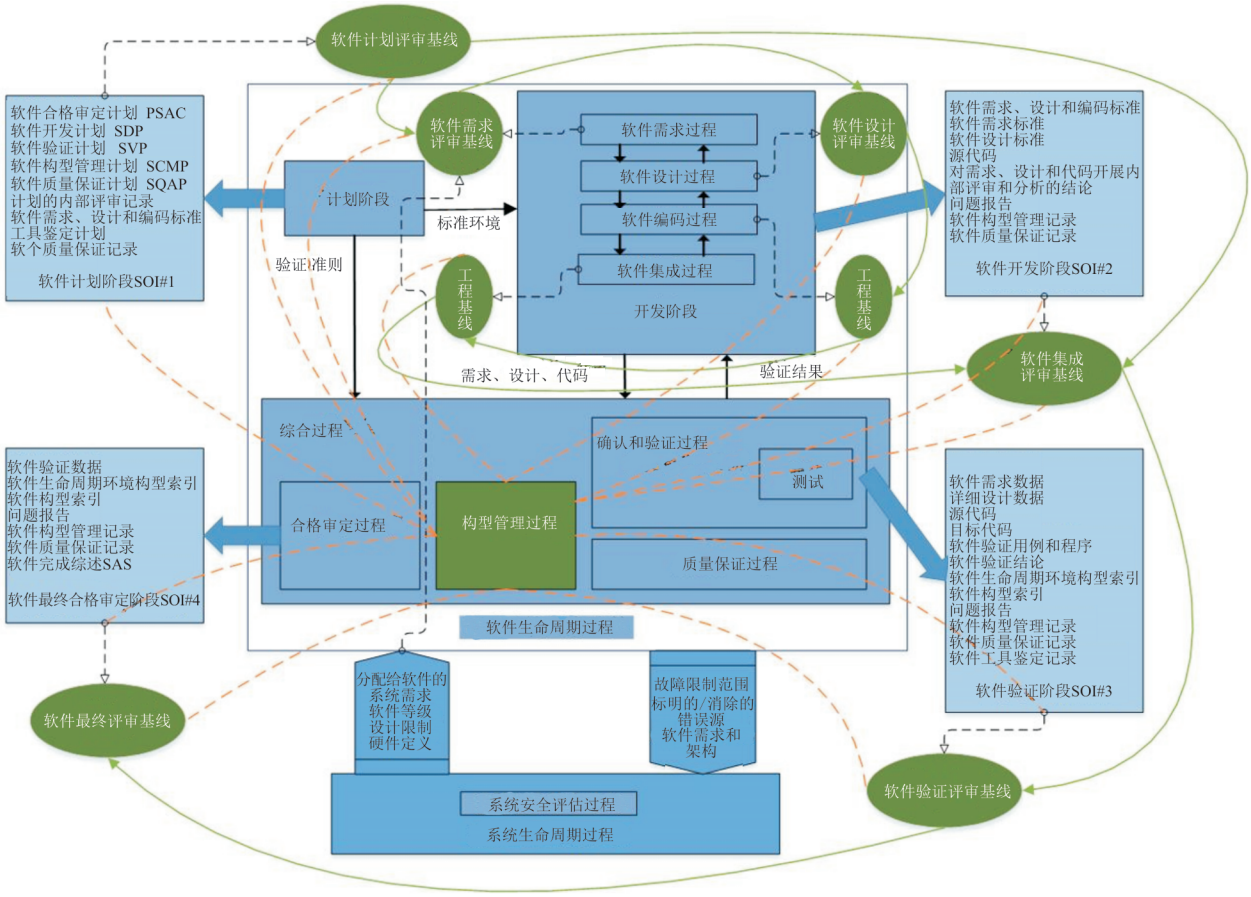

图 10 软件构型管理与软件设计过程结合图

Fig. 10 Software configuration management and software design process interaction

2.1 软件的计划阶段

如图 10 左上部分所示，在软件的计划阶段策划输入输出数据、活动、活动的环境（包括人、工具）等过程需要依照的标准和规则以及保障要求，并将经过评审后的构型数据纳入软件计划评审基线进行构型控制。

2.2 软件的开发阶段

如图 10 右上部分所示，按照纳入构型数据库的软件计划进行软件开发，这是一个循环往复的过程。它将需求获取、分析合二为一，循环执行直到完整、准确地分析所有的需求，经过评审后建立软件需求评审基线；在软件设计过程中，输入包括软件高层需求、软件开发计划以及软件设计标准等，通过一次或多次迭代，对软件高层需求进行细化，开发出软件架构和软件低层需求，编写源代码，经过评审后建立软件设计评审基线；在这个过程中还可以根据需要建立多条工程基线。按照图 10 所示的流程将开发阶段产生的所有构型数据通过评审后纳入软件集成评审基线进行构型控制并作为下一个阶段的输入。

2.3 软件的验证阶段

如图 10 右下部分所示，软件验证是对软件计划过程、软件开发过程和软件验证过程输出的技术评估，贯穿于整个软件研制过程，软件验证活动如图 11 所示。根据 DO-178C，软件验证不仅包含测试，还包含核查和分析以及对构型数据库开发阶段产生的构型项进行验证。将通过软件测试和集成验证满足系统需求符合 DO-178C 标准的构型数据作为构型项在通过评审后纳入软件验证评审基线进行构型控制。

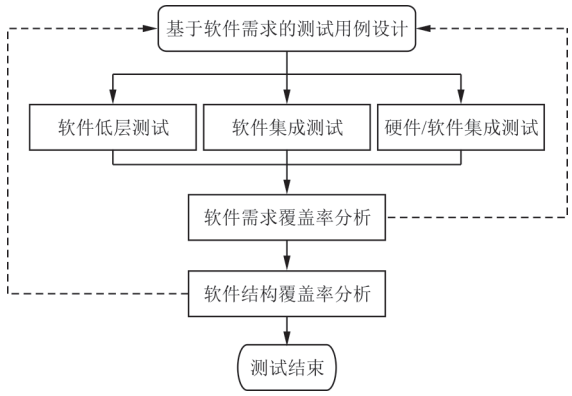

图 11　软件验证活动图

Fig. 11　Software verification process

2.4　软件的最终合格审定阶段

如图 10 左下部分所示,当所有的试验项目均已完成,验证阶段构型数据库的构型项及软件达到了最终构型,并进行了符合性评审,将软件构型索引、软件生命周期环境构型索引和软件完结综述提交适航批准[16-18],并将批准后的所用构型项的最新状态冻结纳入基线进行构型控制。

软件达到构型控制目标的最终基线后,供应商提交能够充分描述交付软件构型的用于软件最终批准数据给客户,之后再发生的变更由双方按约定的更改控制方式进行双控和追溯。

3　结　论

1) 通过研究确立了参照 DO-178C 标准建立以产品构型为核心的软件构型数据管理机制;将构型基线建立时机与软件研发设计过程相结合,通过平台化手段确保刹车控制系统软件在全生命周期过程中的单一数据源,满足适航要求。

2) 将构型数据通过计算机平台运用数字化管理代替人力手工管理,通过权限的设置和平台账户的分配管理既保障了数据的安全性,也通过平台流程实现了追踪,保障了软件在全生命周期的实时有效管理。

参 考 文 献

[1] 年丽云, 刘雅星, 吕潇超. 飞机谱系化构型管理模型研究与应用[J]. 航空科学技术, 2021, 32(3): 34-39.
NIAN Liyun, LIU Yaxing, LYU Xiaochao. Research and application of aircraft lineage configuration management model[J]. Aeronautical Science and Technology, 2021, 32(3): 34-39. (in Chinese)

[2] ANSI. National consensus standard for configuration management: GEIA-649B—2010[S]. US: ANSI, 2010.

[3] 王庆林, 余国华, 王睿. 构型管理[M]. 上海: 上海科学技术出版社, 2010.
WANG Qinglin, YU Guohua, WANG Rui. Configuration management[M]. Shanghai: Shanghai Science and Technology Press, 2010. (in Chinese)

[4] RTCA. Software consideration in airborne systems and equipment certification: DO-178C[S]. US: RTCA, 2011.

[5] 邢亮, 牟明. DO-178B/C 目标分析及阶段介入评审过程研究[J]. 航空计算技术, 2015, 45(5): 97-101.
XING Liang, MOU Ming. DO-178B/C objective analysis and stage intervention review process research[J]. Aeronautical Computing Technique, 2015, 45(5): 97-101. (in Chinese)

[6] RAFAEL C, JUAN C, KRIKHAAR D R. Managing software development information in global configuration management activities[J]. Systems Engineering, 2012, 15(3): 112-121.

[7] 占红飞, 李晓蕊, 孟旭. 一种基于统一构型管理流程的企业流程体系[C]// 第四届体系工程学术会议——数字化转型中的体系工程. 长沙: 国防科技大学, 2022: 202-206.
ZHAN Hongfei, LI Xiaorui, MENG Xu. An enterprise process system based on unified configuration management process [C]// The 4th systems engineering academic conference—systems engineering in digital transformation. Changsha: National University of Defense Technology, 2022: 202-206. (in Chinese)

[8] FAA. Software approval guidelines: Order 8110.49[S]. US: FAA, 2003.

[9] PETER H F. Configuration management models in commerical environment: SEI-91-TR-7[R]. US: SEI, 1991.

[10] 蔡喁, 郑征, 蔡开元. 机载软件适航标准 DO-178B/C 研究[M]. 上海: 上海交通大学出版社, 2013: 129-130.
CAI Yong, ZHENG Zheng, CAI Kaiyuan. Research on DO-178B/C for airborne software airworthiness standards[M]. Shanghai: Shanghai Jiao Tong University Press, 2013: 129-130. (in Chinese)

[11] 陈勇, 严林芳, 孙景华. 民用飞机机载软件管理[M]. 北京: 航空工业出版社, 2015.
CHEN Yong, YAN Linfang, SUN Jinghua. Civil aircraft airborne software management[M]. Beijing: Aviation Industry Press, 2015. (in Chinese)

[12] 孙景华. ARJ21-700 飞机研制项目的机载软件构型管理方案研究及应用[D]. 上海: 复旦大学, 2009.
SUN Jinghua. Research and application of airborne software

(下转第 142 页)