海上设施自动化系统软件认可流程与技术要求研究

张本伟[1],李文华[2]

(1. 中国船级社海工技术中心 北京 100007;2. 大连海事大学轮机工程学院 大连 116026)

摘要:随着计算机及通信技术的发展,海上设施自动化水平的不断提高,海上设施运营的安全可靠性越来越依赖于自动控制系统,尤其是软件部分。由于软件本身在设计和开发中可能存在的缺陷引起系统故障或失效,将给设施及利益方带来不可估量的损失。文章结合IEC61508系列标准、ISO9000—3标准,针对自动化系统软件有关要求和国际船级社协会及船级社等机构有关规范和标准的内容进行分析研究,系统地分析总结出海上设施软件的认可流程及对应技术要求,为我国海工装备设计制造业提供指导。

关键词:海上设施;自动化系统;软件;认可流程;技术要求

中图分类号:U675;P75 **文献标志码**:A **文章编号**:1005-9857(2018)03-0062-05

Software Approval Process and Technical Requirements of Offshore Facility Automation System

ZHANG Benwei[1], LI Wenhua[2]

(1. Offshore Engineering Technology Center, China Classification Society, Beijing 100007, China;
2. Department of Marine Engineering, Dalian Maritime University, Dalian 116026, China)

Abstract: Software is the core of control system based on computer. With the development of computer and communication technology, the level of automation of offshore facilities has been improving constantly. The security and reliability of offshore facilities are more and more dependent on the automatic control system, especially the software part. Due to the defect of software causing in the design and development, the failures which will bring immeasurable losses to the facilities and stakeholders may existing. This paper analyzed combining relevant requirements for automation system software from the IEC61508 series standard, ISO9000—3 standard with relevant norms and standards of relevant institution such as the International Association of Classification Societies (IACS), Classification Society, systematically analyzed and summed up the offshore facilities software approval process and corresponding technical requirements to provide guidance for China's marine equipment design and manufacturing industry.

Key words: Offshore facilities, Automation system, Software, Approval process, Technical requirement.

收稿日期:2017-08-01;**修订日期**:2018-02-06

基金项目:工信部项目"自升式平台中央控制系统研制与应用示范"(工信部联装〔2016〕26号);国家自然科学基金项目(51779026).

作者简介:张本伟,高级工程师,硕士,研究方向为船舶电气

通信作者:李文华,副教授,博士,研究方向为海洋工程装备

随着我国经济发展的需要和海洋强国战略的实施，我国海上设施及配套产品迎来了突飞猛进的发展。越来越多的高集成度的自动控制系统被应用在海上设施上，关于自动控制系统软件的可靠性的要求也在不断进步，这就需要对软件进行专业认可，确保其质量和安全运营。图 1 为高集成度海上设施的自动系统控制及系统图[1]，其中部分控制系统是独立的，而又通过现场总线与其他系统进行通信，大大增加了系统的复杂性。由于集中控制和无人控制要求的自动控制系统集成度和复杂性越来越高，随之而来的风险性也就越来越高，故自动控制系统软件的认可度越发显得重要。

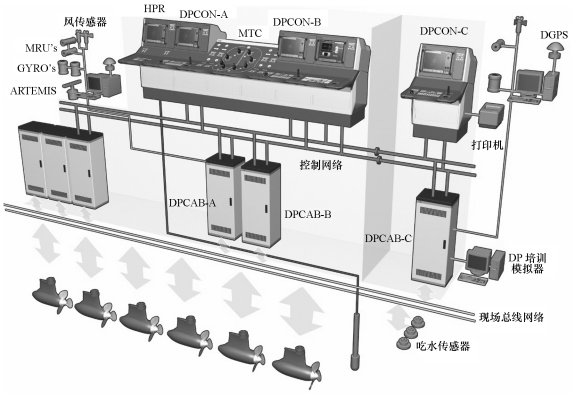

图 1　海上设施自动控制系统组成

1　系统分类[1]

海上设施用到的基于计算机系统比较复杂，典型的系统组成和层次关系如图 2 所示，图中虚线表示尚未开发的分支。

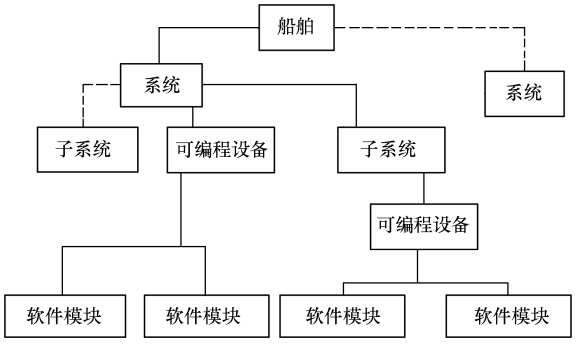

图 2　典型的海上设施自动化系统组成和层次关系

参照最新要求[1]中船用计算机系统分类，按照系统功能的影响，把海上设施自动化系统分为 3 类，分别对应 I 类、II 类、III 类。其中，I 类系统的故障不会对人员、设施的安全以及环境产生危害，主要实现信息/管理任务的监视功能；II 类系统的故障最终会对人员、设施的安全以及环境产生危害，主要实现监视和报警功能、维持船舶正常运行和可居住条件所必需的控制功能；III 类系统的故障即刻会对人员、设施的安全以及环境产生危害，主要实现保持设施推进和操舵的控制功能、设施安全功能。

通常，根据对所有操作工况的风险评估，确定系统准确分类，以下系统分为 III 类：①设施推进系统，即产生和控制机械以移动设施，不包含仅在操纵工况使用的设备，例如首侧推；②操舵控制系统；③设施电站系统，包括功率管理系统（Power Management System，PMS）；④设施安全系统，包括火气探测、进排水监测、内部报警、救生系统；⑤加装有 DP-2（Class 2 Dynamic Positioning）或 DP-3（Class 3 Dynamic Positioning）的动力定位系统；⑥钻井系统/油气处理系统。

根据对所有操作工况的风险评估，确定系统准确分类，以下系统分为 II 类：①液货装卸控制系统；②舱底水探测和舱底泵相关控制；③燃油处理系统；④压载水阀门遥控系统；⑤推进系统的报警和监测。

2　质量体系要求[2]

软件开发是一个系统工程，常见的软件开发流程包含了概念设计、工程设计、工程开发、检测与测试和操作与维护 5 个阶段[3]。

为了保证软件的质量和可靠性，并为软件认可奠定基础，开发者在开发软件之前，应自身建立并实施标准[4]或等效标准的质量管理体系并持有有效证书。按照标准[4]的要求，开发者应对其管理活动、资源提供、软件产品实现和测量、分析和改进有关的过程进行控制。II、III 类系统的制造厂还应满足标准[2]的适用要求。

同时，开发者应制订针对软件开发生命周期的质量计划。软件质量计划应规范该软件整个生命周期的活动，明确相关程序、职责和系统文件，包括配置管理。所制订的质量计划可参照标准[5]的要求。对于 II 类、III 类系统的软件，质量计划中应包

含安全功能要求部分，应设计具体保证方法，以验证和确认安全功能要求是否得以满足。

开发者应具有针对产品的质量控制文件，该质量控制文件应准确描述产品的生产工艺流程，并用文字以及图表清晰描述各工艺流程的质量控制要求，还应包含明确的控制对象、控制标准、控制方法及检验方法和生产质量保证措施落实的证明文件。对于安全相关功能的产品，还要求提供通过“试验和模拟”的证明文件。

制造厂应对产品进行最终测试并提供报告。最终的试验报告是根据成品试验和试验结果记录生成的报告。

软件可追溯性要求：必须按程序对编程内容和数据的修改以及版本的变化进行标志并文档化。确保在需要时对软件产品质量形成过程实行可追溯。通过软件配置管理及软件版本说明等质量保证文件，明确编程内容、数据的修改以及版本的变化所必须遵循的流程，并确定在文件中记录这些修改或变化。

在软件开发生命周期阶段中，应制定船用计算机系统的软件配置管理，保证当某些可交付项有改变时，几种开发的可交付项的一致性。

3 系统生命周期[6]

依据上述质量体系要求，软件开发分为 5 个阶段，系统整个生命周期也由这 5 个阶段组成。但 5 个阶段的目的范围又做了不同划分，其关系和要求如图 3 所示。

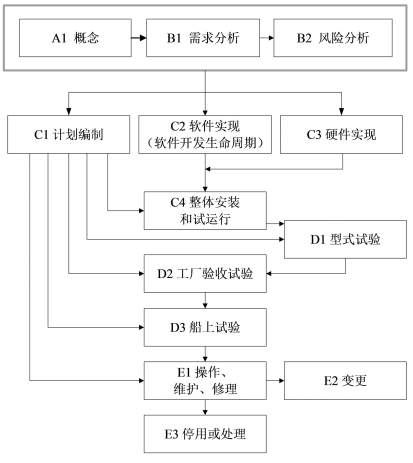

图 3 软件开发 5 个阶段的要求关系划分

从认可角度，依据标准[6]，上述各阶段软件开发的要求和依据如下。

(1)A1 概念。要求对受控设备及其要求的控制功能和实际环境进行全面的了解；确定可能的危险源；获取确定危险的有关信息；获取当前的安全法规；考虑相邻近的受控设备之间相互作用所产生的危险；以上所要求的信息和结果应文档化。依据：满足该条要求所必需的所有有关信息。

(2)B1 需求分析。软件开发依据从概念至整体范围获取的信息。

(3)B2 风险分析。要求应采取适当的方法进行分析，如：①故障树分析；②风险分析；③故障模式及影响分析（Failure mode and effects analysis，FMEA）或故障模式、影响及危害性分析（Failure mode effects and criticality analysis，FMECA）。依据：计算机系统要求规范。

(4)C1 计划编制。要求拟定工厂验收试验（Factory acceptance test，FAT）试验大纲和船上试验大纲，大纲中需包括安全相关功能试验。依据计算机系统要求规范 ，功能安全相关规范要求。

(5)C2 软件实现。满足软件开发要求，依据计算机系统要求规范。

(6)C3 硬件实现。软件开发依据计算机系统要求规范。

(7)C4 整体安装和试运行。软件开发依据计算机系统安装、操作和维护计划进行软件开发。

(8)D1 型式试验。要求按 GD01—2006 进行试验。依据计算机系统要求规范；安全相关功能要求规范；型式试验大纲进行软件开发。

(9)FAT 试验。要求 FAT 报告应记录：使用的工具和设备；FAT 活动的记录；实际结果和预期结果的差异及处理。依据计算机系统要求规范；FAT 试验大纲进行软件开发。

(10)D3 船上试验。要求完全系统试验应验证在实际硬件部件及最终应用软件的条件下，功能可以正常实现。集成试验应验证所有系统集成状态下的功能可以正常实现。依据计算机系统要求规范；船上试验大纲进行软件开发。

(11)E1 操作、维护、修理。依据计算机系统安

装、操作和维护计划进行软件开发。

(12)E2 变更。要求变更应返回生命周期合适阶段，并加以验证。记录应文档化。制造厂应对修改进行记录。对 II、III 系统的软件和硬件进行的后续重大修改应提交给船级社进行批准。依据计算机系统要求规范、软件质量计划、相应阶段的试验大纲进行软件开发。

(13)E3 停用或处理。要求在进行停用或处理活动之前应进行影响分析，并制订一个计划，包括系统的关闭、系统的拆除。在计算机系统使用说明书中提示对敏感信息的销毁和处理。根据功能安全管理规程对停用或处理的请求进行软件开发。

4　软件开发生命周期[6-7]

开发者应制订针对软件开发生命周期的质量计划。应在软件的生命周期中使用行政和技术手段加以控制，以便于管理软件变化和保证有关软件安全方面的要求得到满足，证明制造厂存在有效的、能够满足软件开发生命周期的各阶段的质量控制程序。

软件开发生命周期与质量保证计划关系如图 4 所示，对周期内每一阶段要求解释如下。

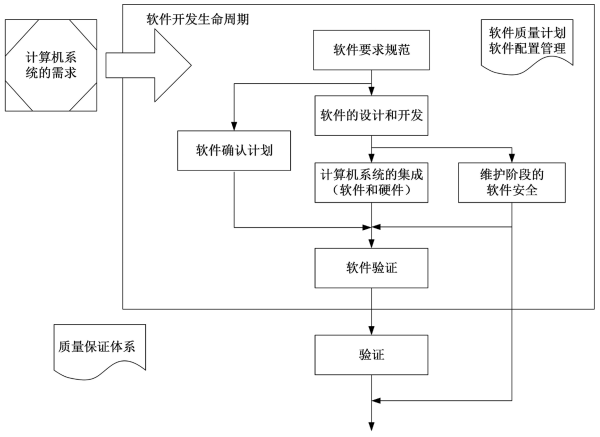

图 4　软件开发生命周期与质量保证计划关系

(1)软件要求规范。包括：①在前述系统分类规定的系统类别等级范围内，软件安全的规定要求应得到表达和组织；②确认软件安全功能的要求；③对软件和硬件间的任何与安全有关的或相应的约束进行规范并文档化；④应将计算机系统的非安全功能和安全功能清晰区分，清晰地表达出系统的安全属性。

(2)软件确认计划。包括：①受控设备(EUC)[8]操作的有关模式的识别和操作的每一模式软件的识别；②确定符合软件功能规定要求的每一功能的措施和规程；③确认软件的通过/失败准则。

(3)软件的设计与开发。包括：①软件结构的要求，软件结构是定义软件主要组件和子系统，包括它们如何实现内部连接，如何获得所要求的属性，特别是安全完整性；②支持工具和编程语言的要求。

(4)详细设计与开发。包括：软件系统设计和单个软件模块设计[9]。其中：①软件的详细设计与开发需对每一软件组成提供逻辑语言，并产生详细设计文件以定义内部结构和组成部分的界面，包括每一组成部分单元的测试部分；②软件的开发应具有模块化、可测试性、安全修改能力；需提供软件系统设计规范和单个模块设计规范；③清晰的描述文档。

(5)软件模块测试。包括：①开发者应采用测试方法对软件模块的逻辑及需求进行全面的模块测试；②开发者应对 II 类、III 类系统的每一软件模块均根据软件模块测试规范的要求进行验证，该测试规范是在软件系统设计阶段制定的；③开发者可采用白盒测试的方法执行模块测试，根据边界值分析、错误推测、等价类或输入划分等方法设计测试用例。可根据软件的安全等级要求及船用可编程设备的特性要求选择上述方法。

(6)软件集成测试。包括：①软件集成根据规定的软件集成测试要求进行测试。这些测试应表明所有软件模块和软件组件/子系统内部正确作用以执行其预定的功能而不执行非预定的功能。②软件集成测试的记录应文档化，说明测试结果是否满足目的和测试准则，如果出现失效，记录失效原因。③在软件集成过程中，应对软件的任何修改或改变进行影响分析，以确定对所有软件模块的影响和所需要的再验证和再设计活动。

5　试验和验证[1]

依据最新要求，最终软件认可需要提交的图纸资料和要求，包括：①质量计划，需提交船级社认

可。②风险评估报告，Ⅱ类、Ⅲ类系统需提交船级社认可。③软件模块功能描述，Ⅱ类、Ⅲ类系统需提交船级社备查。④软件代码验证证据，Ⅱ类、Ⅲ类系统需提交船级社认可。⑤软件模块、子系统和系统层级上，Ⅱ类和Ⅲ类系统的元器件功能测试证据需提交船级社备查。⑥功能测试和故障测试流程，包含船级社可能要求的 FMEA 分析，Ⅱ类、Ⅲ类系统需提交船级社认可。⑦工厂验收试验，包括功能测试和故障测试，Ⅱ类、Ⅲ类系统由验船师见证。⑧最终集成前的模拟测试流程，Ⅱ类、Ⅲ类系统需提交船级社认可。⑨最终集成前的模拟测试，Ⅱ类、Ⅲ类系统由验船师见证。⑩船上的试验流程，Ⅱ类、Ⅲ类系统需提交船级社认可。⑪船上的集成试验，Ⅱ类、Ⅲ类系统由验船师见证。⑫软件版本号、功能描述、维护和使用手册、与其他系统接口列表，Ⅱ类、Ⅲ类系统提交船级社备查。⑬更新的软件注册表，Ⅱ类、Ⅲ类系统提交船级社备查。⑭安保相关程序和文件，Ⅱ类、Ⅲ类系统提交船级社备查。⑮配套的硬件试验报告，需提交船级社认可。

6 小结

本研究对 ISO9001 及 IEC61508 系列标准、IACS 等机构颁发的与自动控制系统软件开发、认可等相关的标准、规范及指南内容进行了系统分析研究，围绕软件开发的 5 个阶段，详细分析各个阶段的技术准备和要求，最终给出海上设施自动控制系统软件认可程序和依据，对于海工装备设计制造行业具有一定的指导和参考意义。

参考文献

[1] 国际船级社协会统一要求：IACS.UR E22[S].英国：国际船级社协会，2017.

[2] 国际标准组织.质量保证标准在计算机软件开发、供应、安装和维护中的应用指南：ISO9003[S].瑞士：国际标准组织，2015

[3] 张金男，张本伟，李文华，等.国际海工装备自动控制系统检验标准建设研究[J].海洋开发与管理.2015，32(8)：16－19.

[4] 国际标准组织.质量管理体系：ISO9001[S].瑞士：国际标准组织，2015.

[5] 国际电子和电气工程师协会.软件质量保证计划：IEEE 730—2014[S].美国：国际电子和电气工程师协会，2014.

[6] 国际电工委员会.电气/电子/可编程电子安全相关系统的功能安全 第 3 部分：软件要求：IEC 61508—3：2010[S].英国：国际电工文员会，2010.

[7] 国际标准组织.系统和软件工程－系统生命周期过程：ISO12207[S].瑞士：国际标准组织，2010.

[8] 国际电工委员会.电气/电子/可编程电子安全相关系统的功能安全 第 4 部分：定义：IEC 61508—4：2010[S].瑞士：国际标准组织，2010.

[9] 许大禹，张本伟，刘婉婷，等.海上单元集成软件系统认证标准及其技术背景分析研究[J].海洋开发与管理.2015，32(12)：68－73.