УДК 004.42:006.063:629.73:338.45 **doi: 10.32620/aktt.2019.8.24**

А. Г. БУРЯЧЕНКО, В. В. НЕРУБАССКИЙ

АО «Элемент», Одесса, Украина

ВНЕДРЕНИЕ НОВОЙ ВЕРСИИ СТАНДАРТА DO-178C В ПРАКТИКУ СЕРТИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Приводится информация о том, что АО "Элемент", являясь разработчиком электронных систем авиационного назначения и встроенного программного обеспечения, большое внимание уделяет их надежности и безотказности, в том числе в полетных условиях. При этом используется общемировой принцип, предусматривающий сертификацию программного обеспечения как процесс документирования жизненного цикла этого программного обеспечения от момента выдачи технического задания до сопровождения в эксплуатации.

Фактическим стандартом, описывающим все этапы разработки, тестирования и внедрения безопасного программного обеспечения в авиационной отрасли на протяжении более 30 лет является RTCA DO-178 и его аналоги (ED-12, КТ-178). DO-178 прошел длительный путь развития и совершенствования. Различные его варианты в разные моменты времени наиболее полно соответствовали характеристикам аппаратуры, но, самое главное, возможностям средств разработки программного обеспечения.

В данной статье приводятся основные особенности и отличия текущего варианта DO-178C от предыдущего DO-178B. Эти отличия или, более точно, изменения, разделены на несущественные и существенные. Отмечается, что DO-178C мало отличается от DO-178B по объему текста, но главное отличие заключается в добавлении других документов. Эти документы в комплексе расширяют возможности DO-178, приближая его к самым современным технологиям разработки программного обеспечения. Такими технологиями являются объектно-ориентированное программирование и модельно-ориентированная разработка программного обеспечения. Указанные технологии должны быть отслеживаемыми, а их цели должны совпадать с целями базового документа.

Отмечается, что разработчики программного обеспечения авиационного применения должны предусмотреть не только выгоды от внедрения DO-178C, но и возможные задержки и дополнительные затраты, связанные с использованием дополнительных инструментов и технологий. В целом при надлежащем планировании DO-178C является ключом к сохранению конкурентоспособности в области разработки критического программного обеспечения для авиации.

Ключевые слова: *регулятор двигателя цифровой; программное обеспечение; модельно-ориентированная разработка; объектно-ориентированное программирование; сертификация программного обеспечения.*

Введение

В сентябре 2014 г. АО "Элемент" получило сертификат типа Р-72 АР МАК на регулятор двигателя цифровой РДЦ-450М. Этому предшествовала большая работа, связанная с проведением испытаний блока РДЦ-450М, включая летные в составе турбовального ГТД АИ-450М и вертолета Ми-2М, и оформлением необходимых справок и документов. В марте 2016 г. Госавиаслужба (Державіаслужба) Украины выдала ГП "Ивченко-Прогресс" сертификат типа TD0070 на ТВД АИ-450С, в состав которого входит модифицированный регулятор РДЦ-450М-С. В дальнейшем оба сертификата получили дополнения. Отмечается, что последний соответствует нормам летной годности EASA CS-E.

За "кадром" названий этих официальных документов осталась информация о том, что встроенное программное обеспечение (ПО) блоков РДЦ-450М и РДЦ-450М-С было сертифицировано в соответствии с Квалификационными требованиями КТ-178В "Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники" АР МАК. Необходимо заметить, что КТ-178В являются практически полным аналогом американо-европейскому стандарту RTCA DO-178B/ EUROCAE ED-12B "Software considerations in airborne systems and equipment certification".

АО "Элемент", являясь одним из немногих предприятий Украины с опытом сертификации ПО своих изделий по самой сложной категории А указанного стандарта, продолжает отслеживать изменения в общемировых тенденциях сертификации ПО авиационного применения. Данная статья, написанная по материалам зарубежной печати, призвана проинформировать всех заинтересованных о внед-

© А. Г. Буряченко, В. В. Нерубасский, 2019

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

рении нового стандарта КТ-178С (DO-178C, ED-12C) и особенностях его применения [1, 2].

1. Развитие

Исходный вариант RTCA DO-178A был последний раз пересмотрен в 1992 г., что привело к появлению DO-178B. DO-178C - это последняя редакция руководящих принципов DO-178B, официально выпущенная в январе 2012 г., в которой описываются цели процессов жизненного цикла ПО, действия и аспекты проектирования для достижения целей и доказательства того, что цели были выполнены.

Большая часть DO-178B была посвящена описанию методологии последовательной разработки нового, специализированного ПО для авионики. Этот подход представляет собой методологию разработки и проверки, основанную на требованиях, которая включает ряд альтернативных методов для достижения этих целей. DO-178B не является строгим или подробным стандартом, это лишь общая среда документирования разработки высоконадежного ПО. Разработчики оборудования и ПО для авионики должны были соблюдать указания, изложенные в DO-178B. То же самое можно сказать и о DO-178C.

2. Незначительные изменения

Так называемые «незначительные изменения» в DO-178C включают устранение хорошо известных ошибок и несоответствий, а также добавление согласованной терминологии по всему документу. Также было проведено уточнение формулировок.

Согласованные системные / программные аспекты стали более понятными, предоставляя дополнительное обоснование общих целей разработки ПО и их оправдания.

1. Ошибки и несоответствия.

DO-178C избавился от ошибок DO-178B и устранил несоответствия в таблицах Приложения А. Чтобы устранить несоответствия в отношении стандартов ПО уровня D, цель A-9 DO-178B № 1, планы и стандарты были разделены на две цели в DO-178C, а именно:

- гарантия того, что разработка ПО и интегральные процессы соответствуют утвержденным программным планам (Таблица A-9 № 2);

- гарантия того, что разработка ПО и интегральные процессы соответствуют утвержденным стандартам ПО (Таблица A-9 № 3).

2. Согласованная терминология.

DO-178C решает проблемы DO-178B с использованием определенных терминов, таких как «руководство», «рекомендации», «назначение», «цель», «задача» и «деятельность». Это было достигнуто путем расширения глоссария и изменения соответствующим образом текста, чтобы использование этих конкретных терминов было единообразным во всем документе.

3. Усовершенствования в формулировках.

DO-178C улучшил формулировки по всему документу с целью сделать данный документ более точным, сохранив при этом первоначальную цель DO-178B.

4. Цели и действия.

DO-178C подтвердил, что для полного понимания рекомендаций необходимо рассмотреть весь текст документа. Например, Приложение А теперь включает ссылки на каждое действие, а также на каждую цель. Кроме того, в разделе 1.4, который теперь называется «Как использовать этот документ», подчеркивается, что действия являются основной частью общего руководства.

5. Скоординированные аспекты системы / ПО.

В разделе 2 DO-178B появились принципы разработки ПО, что позволило отразить текущую практику системы. Эти обновления были сделаны на основе координации с другими организациями по стандартам авионики, которые обновляли свои руководящие указания на системном уровне, в то время как документ SC-205 / WG-71 (EUROCAE) обновил руководящие указания на уровне программного обеспечения DO-178B.

6. Скрытые цели в DO-178B.

В Приложение А DO-178C добавлены так называемые «скрытые цели», включающие в себя:

- средства для обнаружения объектного кода, который непосредственно не прослеживается в исходном коде, и средства для обеспечения определения его области проверки (Таблица A-1 № 4);

- гарантию того, что планы и стандарты ПО разработаны и проверены на согласованность (Таблица A-9 № 1);

- явную цель - обеспечить непосредственное отслеживание объектного кода в исходном коде «Отслеживание исходного кода» (Таблица A-7 № 9).

7. Пропуски тем DO-178B.

DO-178C рассмотрел несколько общих тем, которые привели к изменениям в нескольких разделах документа, таких как надзор за поставщиками, элементы данных и отслеживаемость. При рассмотрении этих тем в Приложение А были добавлены две дополнительные цели:

- загружаемый файл элемента данных параметров (PDIF) соответствует требованиям низкого уровня (Таблица A-6 № 6);

- проверка покрытия элементов PDIF (Таблица A-7 № 9);

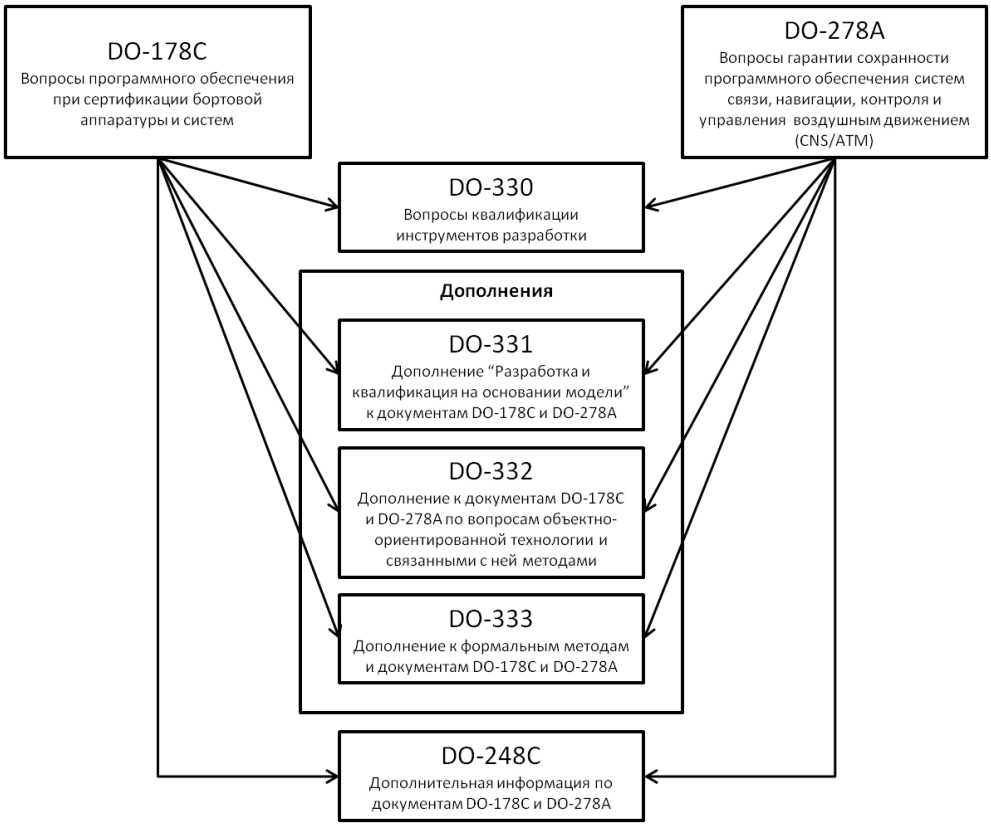

Рис. 1. Взаимосвязь стандартов ПО для авионики

- добавлены данные трассировки;

- данные жизненного цикла должны быть предоставлены и проверены (Раздел 11.21).

8. Пропуски и уточнения DO-178B.

DO-178C рассмотрены несколько конкретных вопросов, которые привели к изменениям только одного или двух абзацев. Каждое такое изменение может оказать влияние на конечный результат.

Например, дополнение к уровню А, в котором говорится, что «если компилятор, компоновщик или другие средства генерируют дополнительный код, который не прослеживается напрямую в исходном коде, то должна быть выполнена дополнительная проверка, чтобы установить правильность такого сгенерированного кода» (6.4.4.2.b).

3. Существенные изменения

Так называемые «существенные изменения» включают в себя дополнения, связанные с технологическими средствами, выделенными в отдельные документы и призванными сохранить ядро DO-178 в будущем. Квалификация инструментов помогает обеспечить отделение бортового ПО от этих самых инструментов, которые не используются в полете.

1. Технологические добавки. DO-178C предполагает, что новые методологии разработки ПО могут привести к новым проблемам.

Раздел 12 посвящен квалификации именно инструментов. Технологические добавки включают в себя следующее:

- разработка и проверка на основе моделей как дополнения к DO-178C и DO-278A (DO- 331);

- объектно-ориентированные технологии и связанные с ними техники как дополнения к DO-178C и DO-278A (DO-332);

- дополнение к формальным методам DO-178C и DO-278A (DO-333);

- вопросы квалификации программного инструмента (DO-330).

Эти новые добавки обеспечивают общность руководств и целей для DO-178C и DO-278A (рис. 1). Вместо того, чтобы расширять текст DO-178B, каждое дополнение описывает какие цели DO-178C пересмотрены для конкретных методов.

Каждое дополнение дает описание специфической технологии и вспомогательную информацию для уточнения этих используемых технологий. Каждое дополнение определяет объем дополнения и цели, которые он содержит. Таблицы целей в приложениях имеют ту же структуру, что и соответствующая таблица целей в DO-178C.

2. Разработка и верификация на основе моделей – дополнение к DO-178C и DO-278A.

Это дополнение содержит модификации и дополнения к целям DO-178C и DO-278A, поясни-

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

тельный текст и описание данных жизненного цикла ПО, которые следует учитывать при разработке и проверке на основе моделей. Это дополнение также применяется к моделям, разработанным в процессе разработки требований к ПО или архитектуре ПО.

Модель – это абстрактное представление множества программных аспектов системы, которая используется для поддержки процесса разработки ПО или процесса проверки ПО.

3. Объектно-ориентированные технологии и связанное с ними дополнение к DO-178C и DO-278A. Это дополнение определяет дополнения, модификации и исключения в целях DO-178C и DO-278A, если они используются как часть методики разработки ПО, а корректировка жизненного цикла и дополнительные указания не требуется.

4. Формальные методы – дополнение к DO-178C и DO-278A. Это дополнение определяет дополнения, модификации и исключения в целях DO-178C и DO-278A когда формальные методы используются как часть ПО, а корректировка жизненного цикла и дополнительные указания не требуется.

5. Квалификация инструментального ПО (DO-178B Раздел 12.2): термины «инструмент разработки» и «инструмент проверки» заменены тремя квалификационными критериями, которые определяют применимый уровень квалификации инструмента (TQL) относительно уровня ПО.

4. Краткие итоги

В целом DO-178C снизил уровень субъективности для многих видов деятельности при разработке ПО. Без сомнения, новое руководство DO-178C, принятое авиационной промышленностью, повлияет на процессы сертификации и разработки ПО. Разработчики ПО и производители аппаратуры должны тщательно учитывать как краткосрочные, так и долгосрочные затраты и выгоды.. Как избежать дорогостоящих переделок, но при этом эффективно использовать новые технологии – вот ключ к сохранению конкурентоспособности продукции. Ошибки при первоначальном планировании могут дорого обойтись позднее при возникновении задержек.

Заключение

Очевидно, что вопрос внедрения нового стандарта DO-178C непростой даже для тех, кто имеет опыт сертификации ПО авиационного применения по DO-178B. Однако на Украине государство в лице Госавиаслужбы не оказывает разработчикам никакой помощи. В прежние времена (до 2014 г.), когда приходилось сотрудничать с АР МАК, ситуация была гораздо лучше.

Здесь видится два выхода.

Первый – Украина законодательно присоединяется к Евросоюзу в области авиации и тогда автоматически на ее территории будут действовать соответствующие авиационные правила, в том числе DO-178C.

Второй – DO-178C переводится на украинский язык и Госавиаслужба Украины берет на себя хотя бы консультативные функции. В любом случае надо что-то делать и есть надежда, что новый президент и его команда уделят должное внимание развитию национальной авиации.

Литература

1. RTCA DO-178C: Software Considerations in Airborne Systems and Equipment Certification. RTCA, Inc.: USA, Issued 12-13-11.

2. EASA Software Aspects of Certification. [Электронный ресурс]. – Режим доступа: http://www.easa.eu.int/certification/docs/certification-memorandum/EASA%20Proposed_CM_SWCEH-002.pdf. – 2.03.2018.

References

1. *RTCA DO-178C: Software Considerations in Airborne Systems and Equipment Certification*. RTCA, Inc.: USA, Issued 12-13-11.

2. *EASA Software Aspects of Certification.* Available at: http://www.easa.eu.int/certification/docs/certification-memorandum/EASA%20Proposed_CM_SWCEH-002.pdf. (accessed 2.03.2018).

Поступила в редакцию 25.05.2019, рассмотрена на редколлегии 7.08.2019

ВПРОВАДЖЕННЯ НОВОЇ ВЕРСІЇ СТАНДАРТУ DO-178C В ПРАКТИКУ СЕРТИФІКАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

А. Г. Буряченко, В. В. Нерубаський

Наводиться інформація про те, що АТ "Елемент", що є розробником електронних систем авіаційного призначення та програмно-апаратних засобів, велику увагу приділяє їх надійності та безвідмовності, в тому числі в польотних умовах. При цьому використовується загальносвітовий принцип, який передбачає серти-

фікацію програмного забезпечення як процес документування життєвого циклу цього програмного забезпечення від моменту видачі технічного завдання до супроводу в експлуатації.

Фактичним стандартом, що описує всі етапи розробки, тестування та впровадження безпечного програмного забезпечення в авіаційній галузі протягом більше ніж 30 років є RTCA DO-178 та його аналоги (ED-12, КТ-178). DO-178 пройшов тривалий шлях розвитку та вдосконалення. Різні його варіанти в різні часи повною мірою відповідали характеристикам апаратури, але, найголовніше, можливостям засобів розробки програмного забезпечення.

У даній статті наводяться основні особливості і відмінності поточного варіанту DO-178C від попереднього DO-178B. Ці відмінності або, точніше, зміни, розділені на несуттєві і суттєві. Відзначається, що DO-178C мало відрізняється від DO-178B за обсягом тексту, але головна відмінність полягає в додаванні інших документів. Ці документи в комплексі розширюють можливості DO-178, наближаючи його до найсучасніших технологій розробки програмного забезпечення. Такими технологіями є об'єктно-орієнтоване програмування та модельно-орієнтована розробка програмного забезпечення. Зазначені технології повинні бути відстежуваними, а їхні цілі повинні збігатися з цілями базового документа.

Відзначається, що розробники програмного забезпечення авіаційного застосування повинні передбачити не тільки вигоди від впровадження DO-178C, а й можливі затримки і додаткові витрати, пов'язані з використанням додаткових інструментів і технологій. В цілому при належному плануванні DO-178C є ключем до збереження конкурентоспроможності в області розробки критичного програмного забезпечення для авіації.

Ключові слова: регулятор двигуна цифровий; програмне забезпечення; модельно-орієнтована розробка; об'єктно-орієнтоване програмування; сертифікація програмного забезпечення.

INTRODUCTION OF NEW VERSION DO-178C STANDARD TO PRACTICE OF SOFTWARE CERTIFICATION

A. H. Burjachenko, V. V. Nerubaskiy

The information is given that JSC “Element”, being a developer of electronic systems for aviation purposes and embedded software, pays great attention to their reliability and dependability, including in-flight conditions. It uses the global principle, which provides for certification of software as a process of documenting the life cycle of this software from the moment of issuance of technical specifications to maintenance in operation.

The actual standard describing all stages of the development, testing, and implementation of safe software in the aviation industry for over 30 years has been RTCA DO-178 and its analogs (ED-12, KT-178). DO-178 has come a long way of development and improvement. Its various options at different points in time most closely corresponded to the characteristics of the equipment, but, most importantly, to the capabilities of the software development tools.

This article presents the main features and differences of the current version of DO-178C from the previous DO-178B. These differences, or, more precisely, the changes, are divided into non-essential and significant. It is noted that DO-178C differs little from DO-178B in text volume, but the main difference is the addition of other documents. These documents in the complex extend the capabilities of DO-178, bringing it closer to the most modern software development technologies. Such technologies are object-oriented programming and model-oriented software development. The specified technologies should be traceable, and their goals should coincide with the goals of the base document.

It is noted that aviation application software developers should consider not only the benefits of implementing the DO-178C but also possible delays and additional costs associated with the use of additional tools and technologies. In general, with proper planning, the DO-178C is key to maintaining competitiveness in the development of critical software for aviation.

The State Aviation Administration of Ukraine does not provide adequate support to developers and manufacturers of aviation software. We hope that this situation will improve.

Keywords: digital engine regulator; software; model-oriented development; object-oriented programming; software certification.

Буряченко Анна Григорьевна – главный метролог, АО «Элемент, Одесса, Украина.

Нерубасский Вадим Владимирович – ст. науч. сотр. бюро разработки программного обеспечения АО «Элемент, Одесса, Украина.

Burjachenko Anna Hryhorievna – Chief Metrologist, JSC “Element”, Odessa, Ukraine, e-mail: annaodessa55@gmail.com, ORCID Author ID: 0000-0003-4480-6965.

Nerubaskiy Vadym Vladimirovich – senior scientist, software development bureau JSC «Element», Odessa, Ukraine, e-mail: odessa@element.od.ua, ORCID Author ID: 0000-0002-7145-5753.