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

УДК 621.45:681.527.7:004.415 **doi: 10.32620/aktt.2022.4sup2.12**

В. В. НЕРУБАСССКИЙ, Д. А. ЛАВРЕНЮК

АО «Элемент», Одесса, Украина

ВОПРОСЫ ВЫБОРА И КВАЛИФИКАЦИИ СРЕДСТВ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЭЛЕКТРОННЫХ СИСТЕМ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ АВИАЦИОННЫХ ДВИГАТЕЛЕЙ

Во вводной части статьи приводится информация о том, что АО "Элемент" является одним их ведущих предприятий Украины по научно-техническому направлению «Электронные системы измерения, контроля параметров и управления авиационными двигателями». В результате сотрудничества с ГП «Ивченко-Прогресс» и АО «Мотор Сич» АО «Элемент» к настоящему времени изготовило более 250 электронных регуляторов семейства РДЦ-450М для различных модификаций ТВД/ТВаД АИ-450. Программное обеспечение этих регуляторов сертифицировано в соответствии с руководством DO-178B/ED-12B. Программное обеспечение последующих регуляторов, находящихся в разработке, планируется сертифицировать по более современному руководству DO-178C/ED-12C, а также использовать при разработке квалифицированные по руководству DO-330/ED-215 инструменты разработки. Именно вопросам выбора и квалификации таких инструментов и посвящена данная статья. Приводится обзор и краткий анализ современных коммерческих средств разработки программного обеспечения встроенных систем, в том числе применительно к микроконтроллерам семейства STM32, которые широко используются в изделиях АО "Элемент". Указывается необходимая для эксплуатации этих средств разработки квалификация пользователя. Дается информация об инструментах верификации программного обеспечения, особенности интерпретации термина "верификация" в DO-178C/ED-12C. В качестве примера приводится средство СПИ, которое много лет с успехом применяется на АО "Элемент" для функциональной отработки электронных регуляторов. Описывается процесс определения уровня квалификации инструментов с использованием трех специальных критериев, дается алгоритм квалификации, приводятся примеры из практики АО "Элемент". Дается информация по недавно появившимся коммерческим пакетам поддержки разработчиков встраиваемого программного обеспечения при квалификации инструментов, приводится алгоритм работы, оцениваются недостатки и возможные проблемы. В заключении делается вывод о том, что процесс выбора и дальнейшей квалификации инструментов оказывает серьезное влияние на трудозатраты при проведении сертификации программного обеспечения встроенных систем авиационного применения.

Ключевые слова: *электронная система управления; электронный регулятор; программное обеспечение; DO-178C/ED-12C; DO-330/ED-215; квалификация инструментов.*

Введение

АО «Элемент» имеет более чем 20-летний опыт разработки электронных систем управления (ЭСУ) авиационных двигателей и является одним из ведущих предприятий Украины по научно-техническому направлению «Электронные системы измерения, контроля параметров и управления авиационными двигателями», имеет Сертификаты Разработчика и Изготовителя комплектующих изделий авиационной техники, выданные АР МАК и ГАСУ.

Активно сотрудничая с ГП «Ивченко-Прогресс» и АО «Мотор Сич», предприятие изготовило более 250 серийных электронных регуляторов семейства РДЦ-450М для различных модификаций

ТВД/ТВаД АИ-450 и выполняет разработку еще семи подобных изделий. В ряде случаев заказчиками выступают иностранные фирмы, такие как Diamond Aircraft (Австрия), TAI (Турция) и другие.

Для обеспечения безопасности бортовой аппаратуры авиационного применения все работы по программному обеспечению (ПО) регуляторов на АО «Элемент» ведутся в соответствии с рекомендациями DO-178C/ED-12C [1]. Необходимо отметить, что комплекс мероприятий и подготовка соответствующих документов по обеспечению доказательной базы для сертификации регуляторов по DO-178C/ED-12C является трудоемким и достаточно затратным процессом.

На начальном этапе планирования разработки критического ПО для ЭСУ большое значение имеет выбор программных инструментов (средств разработки, верификации, тестирования, документирования). В соответствии с DO-330/ED-215 [2] эти инструменты должны быть квалифицированы.

Специалисты АО «Элемент» оперативно знакомятся с современными тенденциями в области сертификации ПО для электронных систем автома-

тического управления (САУ) авиационных двигателей [3] и готовы поделиться своим опытом и взглядами по данному вопросу.

1. Термины и понятия

Прежде чем приступись к изложению, необходимо определить ряд базовых понятий и терминов, необходимых для дельнейшего понимания материала статьи.

Уровень ПО основан на вкладе ПО в возможные отказные состояния, определяемые в процессе оценки безопасности системы (FAR 23/25, 27/29 и др.). Уровень ПО предполагает, что объем работ, выполнение которых необходимо для доказательства соответствия сертификационным требованиям, изменяется в зависимости от категории отказного состояния [1]. Предусмотрено пять уровней ПО: A (катастрофическое), B (аварийное), C (сложное), D (усложнение условий полета) и E (без последствий).

В процессе оценки безопасности системы для регуляторов семейства РДЦ-450М был принят уровень ПО А.

Инструмент (Tool) – компьютерная программа или функциональная часть таковой, используемая для осуществления помощи в разработке, проверке, анализе создании или модификации другой программы, данных или ее документации. Синонимом является термин **средство разработки**.

Вычислительным ядром для регуляторов семейства РДЦ-450М являются микроконтроллеры семейства STM32 (ядро ARM Cortex). Поэтому инструменты будем рассматривать в контексте их применения для STM32.

2. Выбор средств разработки

Условно средства (инструменты) разработки ПО для ЭСУ можно разделить на две большие категории:

1. Коммерческие программные пакеты с ручным написанием кода – Microsoft Visual Studio, IAR Embedded Workbench и другие.

2. Коммерческие модельно-ориентированные пакеты с возможностью генерации кода – Matlab/Simulink, SCADE и другие.

Кратко рассмотрим особенности вышеперечисленных категорий средств.

Microsoft Visual Studio – один из наиболее распространенных пакетов, однако для разработки встроенного ПО к нему требуется инструмент VisualGDB и конфигуратор микроконтроллера (в нашем случае - CubeMX). Такая комбинация имеет все положительные особенности базовой IDE для работы с кодом, развитые средства отладки и написания тестов, универсальность и невысокую стоимость. Однако Visual Studio не квалифицирована для авиационного применения. Для работы нужны высококвалифицированные программисты.

CubeIDE (вариант STM32CubeIDE) – многофункциональный интегрированный инструмент разработки, поддерживающий микроконтроллеры семейства STM32. Однако для, например, тестирования, необходимо устанавливать внешние компоненты: Cygwin 3.0.7 x86 и Google Test Framework, что не совсем удобно и трудоемко. Инструменты условно бесплатны, но также не квалифицированы для авиационного применения. Требуются высококвалифицированные программисты.

IAR Embedded Workbench – интегрированная среда, которая является профессиональным набором инструментов для разработки и отладки приложений для микроконтроллеров с ядром ARM. Распространяется на коммерческой основе, имеет ограниченный функционал тестирования и не квалифицирована для авиационного применения. Для программистов.

Matlab (в комбинации с **Simulink**) – это среда и язык технических расчетов, предназначенный для решения широкого спектра инженерных и научных задач любой сложности в том числе для авиации. Обеспечивает проектирование встраиваемых алгоритмов посредством моделирования и автоматической генерации кода для систем управления и обработки сигналов.

Для квалификации инструментов, поддерживающих верификацию по DO-178C, предлагается инструмент **DO Qualification Kit**. Этот набор включает необходимые документы, тестовые модели и код, процедуры тестирования и ожидаемые результаты. Как недостатки – высокая стоимость полного пакета, а также необходимость «ручной» привязки к микроконтроллеру. Matlab предназначен для инженерных специалистов.

SCADE – семейство продуктов компании ANSIS для проектирования критических по безопасности систем и встраиваемого ПО – от анализа и определения требований до тестирования и интеграции. Это наиболее дорогостоящий пакет, но квалифицированный для авиационного применения. В качестве недостатка можно отметить, что SCADE - аппаратно-независимый пакет, в нем нет средств поддержки микроконтроллеров. SCADE предназначен для инженерных специалистов.

Естественно это далеко не полный список средств разработки встраиваемого ПО. Существуют даже многофункциональные инструменты «внутреннего употребления» (на фирмах Turbomeca, Honeywell и др.), которые не продаются!

Анализ показывает, что выбор инструмента –

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

нетривиальная задача. Первоначально при разработке ПО АО «Элемент» использовал комбинацию средств: IAR Embedded Workbench как генератор кода, инструмент верификации ПО gcov, инструмент тестирования ПО CUnit (последние два - свободно распространяемые). Такой набор разнородных средств несколько усложнял процесс, но удешевлял разработку в конечном итоге.

В настоящее время считаем целесообразным использовать два универсальных инструмента, например, Matlab/Simulink для перспективных разработок и Microsoft Visual Studio/VisualGDB/ CubeMX для сопровождения существующих проектов, для которых уже написано более 20 тыс. строк оттестированного и верифицированного кода.

Читатель вправе выбрать свой набор инструментов, наиболее соответствующий его опыту и потребностям.

3. Об инструментах верификации

DO-178C/ED-12C не делает различия между инструментами разработки и инструментами верификации ПО. Это было сделано намеренно, т.к. появились новые типы инструментов, которые не подходили под вышеуказанные категории [2].

Например, АО «Элемент» много лет использует стенд для проверки и испытаний (СПИ) семейства регуляторов РДЦ-450М. СПИ предназначен для:

- интеграции ПО и аппаратной части регулятора;
- отработки интерфейса регулятора с взаимодействующими системами;
- отработки алгоритмов управления двигателем;
- динамической отработки ПО регулятора в контуре управления совместно с математической моделью силовой установки (двигатель, гидромеханическая часть, трансмиссия, несущий винт);
- проведения квалификационных испытаний ПО регулятора.

СПИ по набору своих функций действительно сложно однозначно отнести к инструментам разработки или инструментам верификации ПО.

4. Процесс квалификации инструментов

DO-330/ED-215 определяет три критерия (таблица 1), которые определяют применимый уровень квалификации инструмента (TQL) в отношении уровня ПО (таблица 2) [2, 4].

Таблица 1

Критерии определения инструмента DO-178C

	Описание
a	Критерий 1. Инструмент, выходные данные которого являются частью создаваемого ПО, и поэтому он может быть источником ошибок
b	Критерий 2. Инструмент, который автоматизирует процесс(ы) верификации ПО и поэтому может не обнаружить ошибку, и выходные данные которого используются для обоснования исключения и упрощения: - процесса(ов) верификации, отличного от тех, который автоматизируется данным инструментом, или - процесса(ов) разработки, который может влиять на ПО “нелетающих” систем.
c	Критерий 3. Инструмент, который в рамках предлагаемого его использования, может не обнаружить ошибку.

Таблица 2

Определение уровня квалификации инструмента TQL (Tool Qualification Level)

Уровень ПО	Критерии		
	1	2	3
A	TQL1	TQL4	TQL5
B	TQL2	TQL4	TQL5
C	TQL3	TQL5	TQL5
D	TQL4	TQL5	TQL5
E	TQL4	TQL5	TQL5

Критерий 1 включает в себя то, что в DO-178B/ED-12B называлось «инструментами разработки», в то время как два других критерия разделяют бывшие «инструменты проверки» в зависимости от сертификационного кредита, требуемого квалификацией инструмента.

Критерий 3 – это «классическое» использование средства верификации: целью средства является создание или проверка артефакта, а заявление о сертификации относится только к целям, применимым к этому артефакту.

Для критерия 2 заявленный сертификат сертификации распространяется на цели, которые выходят за рамки данных, непосредственно проверенных инструментом.

TQL, применимый для критерия 1, заменяет средство разработки DO-178B/ED-12B для каждого уровня ПО, а TQL-5 для критерия 3 заменяет средство проверки DO-178B/ED-12B.

В нашем случае Microsoft Visual Studio/VisualGDB/CubeMX будет квалифицироваться как TQL-1, а СПИ – как TQL-5.

Как видим, большинство разработчиков ПО предпочитают использовать покупные инструменты (COTS). Тем не менее, квалификация этих инструментов проводится не разработчиком инструмента, а непосредственно разработчиком ПО, причем квалификация должна проводиться для каждого проекта!

В простейшем случае при квалификации инструментов выполняются следующие действия:

- сертифицирующему органу предоставляется план квалификации инструмента;
- документируются эксплуатационные требования инструмента;
- демонстрируется, что инструмент удовлетворяет эксплуатационным требованиям, определяются ограничения инструмента;
- Сертифицирующему органу предоставляются результаты квалификации инструмента, включая ограничения.

В целом придется подготовить как минимум 14 документов, описывающих процессы жизненного цикла инструмента. Названия и содержание этих документов примерно соответствует тем, которые создаются при сертификации ПО по DO-178C/ED-12C.

5. Готовые пакеты квалификации инструментов (COTS)

В последние годы появилась группа коммерческих пакетов, обеспечивающих поддержку разработчиков встраиваемого ПО при квалификации инструментов. Характерные примеры таких пакетов - LDRA Tool Suite и Parasoft C/C++test. Все эти пакеты работают примерно одинаково:

- разработчик пакета поставляет набор шаблонов документов, нормативных документов и опорных тестов для инструмента и их эталонные результаты;
- вы заполняете шаблоны документов и запускаете предоставленные тесты в своем окружении;
- результаты тестов, запущенных вами, сравниваются с эталонами, и при расхождении результатов вы устраняете расхождение;
- Сертифицирующему органу предоставляются результаты квалификации инструмента.

Согласитесь, технология на первый взгляд удобная. Однако излишнее доверие к COTS-пакету квалификации инструментов может вызвать ряд проблем. В большинстве случаев вам придется проделать некоторые дополнительные операции, такие как проведение квалификационных испытаний и оценка их результатов. Такие добавочные задачи могут отнять достаточно много времени. Более того, пакет квалификации инструментов может потребовать предварительных условий, которые ваша целевая система не сможет обеспечить. Например, может понадобиться файловая система на целевом объекте для хранения промежуточных данных и результатов, либо возможность пошаговой отладки. При планировании использования инструмента примите во внимание дополнительные трудозатраты по квалификации, а также ограничения пакета [6].

Заключение

Не стоит думать, что если следовать всем вышеописанным правилам, то создание встроенного ПО превратится в бюрократический ад, который будет длиться вечно. Но и относиться к процессу квалификации инструментов без должного внимания не нужно. Ведь уровень квалификации напрямую влияет на трудозатраты. Так, для авиации, для квалификации инструмента по наивысшему уровню A DO-178C/ED-12C, требуется выполнение 76 контрольных мероприятий [5]!

Большое значение имеет тесное взаимодействие с Сертифицирующим органом. Причем это взаимодействие выполняется не обособленно, а в рамках процесса взаимодействия для сертификации целевого ПО.

И главное – всегда помните, что использование инструментов, квалифицированных по требованиям DO-178C/DO-330, уменьшает количество необнаруженных ошибок, но не обеспечивает абсолютную безопасность ПО или аппаратуры!

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

Литература

1. RTCA: DO-178C Software Considerations in Airborne Systems and Equipment Certification. Radio Technical Commission for Aeronautics, 2011.

2. RTCA: DO-330 Software Tool Qualification and Considerations. Radio Technical Commission for Aeronautics, 2011.

3. Буряченко, А. Г. Внедрение новой версии стандарта DO-178C в практику сертификации программного обеспечения [Текст] / А. Г. Буряченко, В. В. Нерубасский // Авіаційно-космічна техніка і технологія. – 2019. – №8 (160), – С. 163-167. DOI: 10.32620/aktt.2019.8.24.

4. Mohamad Ibrahim, Umut Durak. State of the Art in Software Tool Qualification with DO-330: A Survey [Text] / Software Engineering 2021 Satellite Events, Lecture Notes in Informatics (LNI). – Gesellschaft fur Informatik, Bonn, 2021. – P. 1 - 23.

5. Квалификация инструментов для разработки встраиваемого ПО [Электронный ресурс] / Блог компании ЦИТМ Экспонента. – Режим доступа: https://habr.com/ru/company/etmc_exponenta/blog/534906/. – 25.12.2020.

6. Субдин, М. 7 советов и рецепт успешной квалификации инструментального программного средства [Электронный ресурс]. – Режим доступа: https://advalange.ru/tpost/frj8rs8fkl-7-sovetov-i-retsept-uspeshnoi-kvalifikat. – 20.07.2015.

References

1. *RTCA: DO-178C Software Considerations in Airborne Systems and Equipment Certification*. Radio Technical Commission for Aeronautics, 2011.

2. *RTCA: DO-330 Software Tool Qualification and Considerations*. Radio Technical Commission for Aeronautics, 2011.

3. Buryachenko, A.G., Nerubasskiy, V.V. Vnedrenie novoy versii standarta DO-178S v praktiku sertifikatsii programmnogo obespecheniya [Introduction of the new version DO-178C standard to practice of software certification]. *Aviacijno-kosmicna tehnika i tehnologia – Aerospace technic and technolog*, 2019, no. 8(160), pp. 163-167. DOI: 10.32620/aktt.2019.8.24.

4. Mohamad Ibrahim, Umut Durak. State of the Art in Software Tool Qualification with DO-330: A Survey. *Software Engineering 2021 Satellite Events, Lecture Notes in Informatics (LNI)*, Gesellschaft fur Informatik, Bonn, 2021, pp. 1-23.

5. *Kvalifikatsiya instrumentov dlya razrabotki vstraivaemogo PO* [Tools qualification for embedded software developments]. Blog kompanii TsITM Eksponenta. Available at: https://habr.com/ru/company/etmc_exponenta/blog/534906/ (accessed 25.12.2020).

6. Subdin, M. *7 sovetov i retsept uspeshnoy kvalifikatsii instrumental'nogo programmnogo sredstva* [7 tips and a recipe for successful tool qualification]. Available at: https://advalange.ru/tpost/frj8rs8fkl-7-sovetov-i-retsept-uspeshnoi-kvalifikat (accessed 20.07.2015).

Надійшла до редакції 10.06.2022, розглянута на редколегії 8.08.2022

ПИТАННЯ ВИБОРУ І КВАЛІФІКАЦІЇ ЗАСОБІВ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЕЛЕКТРОННИХ СИСТЕМ АВТОМАТИЧНОГО КЕРУВАННЯ АВІАЦІЙНИХ ДВИГУНІВ

В. В. Нерубаський, Д. О. Лавренюк

У вступній частині статті наводиться інформація про те, що АТ “Елемент” є одним з провідних підприємств України за науково-технічним напрямом «Електронні системи вимірювання, контролю параметрів та управління авіаційними двигунами». В результаті співпраці з ДП «Івченко-Прогрес» та АТ «Мотор Січ» АТ «Елемент» на сьогоднішній день виготовило понад 250 електронних регуляторів сімейства РДЦ-450М для різних модифікацій ТГД/ТВаД АІ-450. Програмне забезпечення цих регуляторів сертифіковано відповідно до керівництва DO-178B/ED-12B. Програмне забезпечення наступних регуляторів, що у розробці, планується сертифікувати по сучасному керівництву DO-178C/ED-12C, і навіть використовувати під час розробки кваліфіковані з керівництву DO-330/ED-215 інструменти розробки. Саме питанням вибору та кваліфікації таких інструментів і присвячено цю статтю. Наводиться огляд та стислий аналіз сучасних комерційних засобів розробки програмного забезпечення вбудованих систем, у тому числі стосовно мікроконтролерів сімейства STM32, які широко використовуються у виробах АТ “Елемент”. Вказується необхідна для експлуатації цих засобів розробки кваліфікація користувача. Надається інформація про інструменти верифікації програмного забезпечення, особливості інтерпретації терміну “верифікація” за DO-178C/ED-12C. Як приклад наводиться засіб СПІ, який багато років успішно застосовується на АТ “Елемент” для функціонального відпрацювання електронних регуляторів. Описується процес визначення рівня кваліфікації інструментів з використанням

трьох спеціальних критеріїв, дається алгоритм кваліфікації, наводяться приклади з практики АТ "Елемент". Надається інформація по комерційних пакетах, що недавно з'явилися, підтримки розробників вбудованого програмного забезпечення при кваліфікації інструментів, наводиться алгоритм роботи, оцінюються недоліки і можливі проблеми. У висновку робиться висновок про те, що процес вибору та подальшої кваліфікації інструментів надає серйозний вплив на трудовитрати при проведенні сертифікації програмного забезпечення вбудованих систем авіаційного застосування.

Ключові слова: електронна система керування; електронний регулятор; програмне забезпечення; DO-178C/ED-12C; DO-330/ED-215; кваліфікація інструментів.

ISSUES OF SELECTION AND QUALIFICATION OF SOFTWARE DEVELOPMENT TOOLS FOR AIRCRAFT ENGINES ELECTRONIC CONTROL SYSTEM

Vadym Nerubaskyi, Denys Lavreniuk

The introductory part of the article provides information that Element JSC is one of the leading enterprises in Ukraine in the scientific and technical direction "Electronic systems for measuring, parameters monitoring and controlling aircraft engines". Because of cooperation with Ivchenko-Progress SE and Motor Sich JSC, Element JSC has manufactured more than 250 EEC units of the RDC-450M family for various modifications of the AI-450 Turboshaft/Turboprop engines. The software of these EEC units is certified according to the DO-178B/ED-12B. The software of subsequent EEC units under development is planned to be certified according to the state-of-the-art DO-178C/ED-12C guideline, and development tools qualified according to the DO-330/ED-215 guideline will also be used in development. This article is devoted to the issues of selection and qualification of such tools. A review and brief analysis of modern commercial software development tools for embedded systems, including those applied to the STM32 family microcontrollers, which are widely used in the JSC Element products, is given. The qualification of the user required for operating these development tools is indicated. Information is given on software verification tools, features of the interpretation of the “verification” term in DO-178C/ED-12C. As an example, the SPI tool is given, which has been successfully used for many years at Element JSC for the functional development of EEC units. The process of determining the level of qualification of instruments using three special criteria is described, an algorithm for qualification is given, and examples from the practice of Element JSC are given. Information is given on recently appearing commercial DO-178 support packages for embedded software developers in the qualification of tools, an algorithm of operation is given, shortcomings and possible problems are assessed. Finally, it is concluded that the process of selecting and further qualification of tools has a serious impact on labor costs in the certification of software for embedded systems for aviation applications.

Keywords: electronic control system; electronic regulator; software; DO-178C/ED-12C; DO-330/ED-215; tool qualification.

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

Лавренюк Денис Александрович – инженер-программист бюро разработки программного обеспечения, АО «Элемент, Одесса, Украина.

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

Denys Lavreniuk – engineer-programmer, software development bureau, JSC «Element», Odesa, Ukraine, e-mail: odessa@element.od.ua, ORCID: 0000-0003-4741-3964.