DOI: 10.18137/RNU.V9187.22.01.P.104 УДК 004.054

А.П. Киреев, С.А. Шаров

СРЕДСТВА ВЕРИФИКАЦИИ ПРОТОКОЛА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВОЙ АППАРАТУРЫ КОСМИЧЕСКИХ АППАРАТОВ

Аннотация. Рассмотрен подход к разработке комплексов бортовой аппаратуры космических аппаратов на основе интегрированной модульной бортовой аппаратуры. Предложен набор инструментов для автоматизации процессов проектирования комплексов бортовой аппаратуры. Представлена модель верификации протокола информационно-логического взаимодействия программного обеспечения бортового комплекса управления и специальной аппаратуры космического аппарата с использованием метода формальной верификации моделей требований с помощью инструментального средства верификации SPIN.

Ключевые слова: специальное программное обеспечение, комплекс бортовой аппаратуры, космический аппарат, верификация программного обеспечения, линейная темпоральная логика.

A.P. Kireev, S.A. Sharov

MEANS OF VERIFICATION OF THE INFORMATION INTERACTION PROTOCOL SOFTWARE ON-BOARD EQUIPMENT OF SPACE VEHICLES

Abstract. The article presents the technology of formal proof of the presence of the specified properties of the software, the analysis for fault tolerance and preliminary assessment of the quality of the product before the appearance of the prototype.

Keywords: special software, onboard equipment, spacecraft, software verification.

Введение

Разработка современного специального программного обеспечения (далее – СПО) бортовой аппаратуры (далее – БА) космических аппаратов (далее – КА) представляет собой сложную и ресурсоемкую задачу, результат решения которой, к сожалению, не всегда удовлетворяет заданным требованиям и укладывается в рамки выделенных временных и финансовых ресурсов.

С целью сокращения времени проектирования и тестирования аппаратуры КА и уменьшения ошибок СПО в силу человеческого фактора на всех этапах ее создания, повышения надежности, отказоустойчивости, модульности и масштабируемости необходимо разработать и предоставить всем участникам процесса создания СПО единую модельно-языковую и информационно-программную среду, в которой реализовать последовательно-итерационный, программно-управляемый процесс разработки и контроля качества всех артефактов жизненного цикла создания системы, – комплекса требований, проектных решений и реализации.

В настоящее время основным подходом к проектированию и разработке комплексов бортового оборудования КА является подход интегрированной модульной бортовой ап-

Киреев Андрей Павлович
старший научный сотрудник Военного научно-исследовательского института. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: верификация программного обеспечения. Автор 5 опубликованных научных работ.
Электронный адрес: vka@mail.ru

Шаров Сергей Алексеевич
старший научный сотрудник, начальник лаборатории Военного научно-исследовательского института. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: верификация программного обеспечения. Автор более 30 опубликованных научных работ.
Электронный адрес: vka@mail.ru

паратуры. Согласно этому подходу специализированные контроллеры заменяются на процессорные модули общего назначения, на которых обеспечивается независимая работа различных космических систем; физические соединения каждой космической подсистемы заменяются на виртуальные внутри коммутируемой сетевой инфраструктуры, основанной на таких технологиях, как SpaceWire (сетевая архитектура КА на основе стандарта ECSS Standart-E-50-12C) [1; 3; 5; 6; 9]. Это позволяет снизить необоснованное дублирование аппаратного обеспечения, приводящее к неприемлемому уровню энергопотребления и сложности системы бортового оборудования. С другой стороны, такой подход в значительной мере усложняет процесс разработки программного и аппаратного обеспечения, ставит новые задачи проектирования и интеграции программного и аппаратного обеспечения КА.

Для решения задач системной интеграции требуется точное понимание всех деталей разрабатываемого комплекса, как на высоком, так и на низком уровне детализации, а также предельная внимательность при анализе последствий, в случае внесения изменений. При этом размер комплекса бортовой аппаратуры (далее – КБА) современных КА и количество существенных деталей таково, что невозможно выполнить проектирование небольшим коллективом. В таких условиях применение специалистами традиционных способов разработки, основанных на описании всех требований и архитектурных решений, в текстовых документах становится чрезмерно трудоемким и подверженным ошибкам.

Возможность подключить к разрешению данных проблем программные средства автоматизации наталкивается на разнородность и неструктурированность информации. Естественным шагом по преодолению указанной проблемы является формализация информации, переведение ее в унифицированный машинный вид, что позволяет автоматизировать ее обработку.

Таким образом, возникает потребность в технологии для оптимизации разработки сложных программно-аппаратных комплексов КА, а также их верификации. Данная технология позволит провести предварительную оценку качества изделия до появления опытного образца, анализ на отказоустойчивость. Также будут сэкономлены временные и финансовые ресурсы, снижен риск появления ошибок и дефектов.

Для автоматизации процессов проектирования комплексов бортовой аппаратуры предназначаются автоматизированные рабочие места архитектора и интегратора модуль-

ной системы КБА КА. Набор инструментов должен позволять описывать модели комплекса бортовой аппаратуры КА, производить анализ моделей на соответствие требованиям, синтезировать подмодели системы, генерировать конфигурационные данные и бинарные образы программного кода на основе моделей.

Ориентировочный состав интегрированного инструментального комплекса модульной системы КБА КА представлен на Рисунке 1.

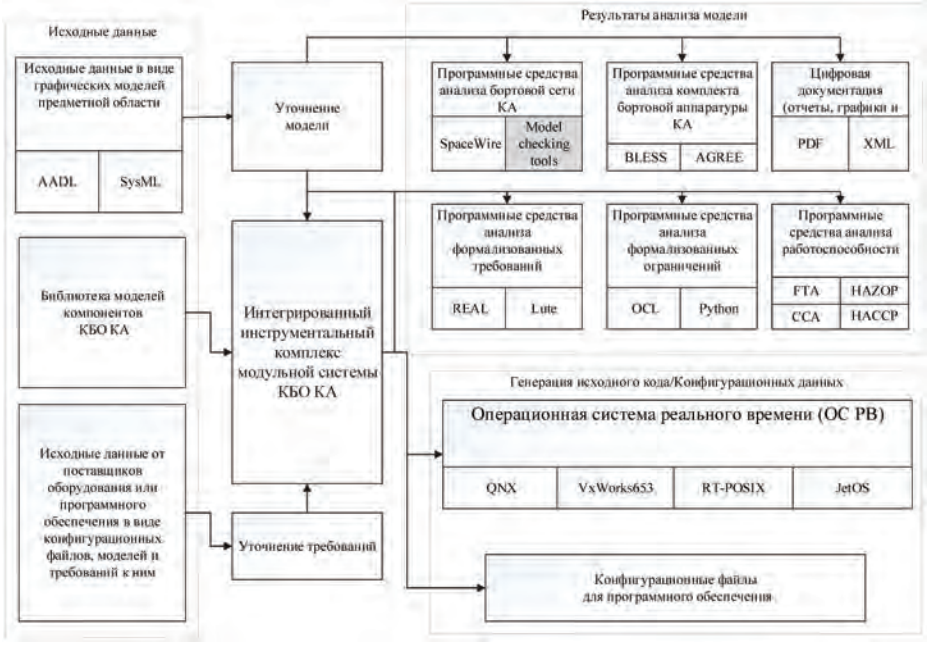

Рисунок 1. Интегрированный инструментальный комплексмодульной системы КБА КА

Данный программный комплекс включает в свой состав средства анализа и синтеза архитектурных моделей бортовой аппаратуры КА, программные средства анализа сетевой инфраструктуры и аппаратной конфигурации изделия, средства анализа отказоустойчивости БА КА, средства генерации и тестирования программного обеспечения под выбранную операционную систему реального времени.

Далее в статье рассматриваются средства верификации программного обеспечения бортовой сети КА с использованием одного из формальных методов – ModelChecking.

Методика и средства формальной верификации СПО БА КА

Помимо традиционных методов отработки комплектов бортового оборудования космических аппаратов на наземных эксплуатационных стендах, проведения программ тестирования специального программного обеспечения необходима верификация проектов СПО с использованием моделей проверки (Model Checking), основанная на различных спецификациях темпоральных логик (LTL, CTL, PCTL и др.). Инструмент SPIN (Simple Promela Interpreter) предназначен для анализа и формальной верификации PROMELA-моделей в соответствии с технологией Model Checking [7; 8].

Инструмент Spin поддерживает разработку и анализ корректности параллельных и распределенных систем с конечным числом состояний, спецификация свойств которых

представлена формулами LTL. Основная цель использования пакета Spin – это проверка корректности взаимодействующих параллельных асинхронных процессов. Spin фокусируется именно на асинхронной модели, которая естественна для программных систем. Система Spin предоставляет пользователю [4]:

• язык Promela (Protocol Meta Language) – С-подобный язык для спецификации моделей;

• удобные средства для выражения требований корректности формулами линейной темпоральной логики (без оператора X (Next Time)).

Цель языка Promela – дать возможность пользователю построить модель параллельной системы для последующей проверки в ее поведении аспектов координации и взаимодействия параллельных процессов. Поэтому в языке только три типа объектов спецификации:

• процессы;

• каналы, по которым процессы взаимодействуют;

• переменные простых типов [2].

Ниже рассмотрен протокол информационно-логического взаимодействия бортовой аппаратуры, состоящей из бортового комплекса управления (далее – БКУ) и радиолокатора с синтезированием апертуры (далее – РСА). Данный протокол может функционировать на прикладном уровне сетевой модели Space Wire и включать в свой состав множество узлов. При этом в данном примере используется модель информационно-логического протокола с двумя узлами (БКУ и РСА).

Для проверки исполнения принятых свойств протокола информационного взаимодействия бортовой аппаратуры задаются формулы линейной темпоральной логики LTL. В случае проверки режима работы РСА необходимо убедится, что РСА начнет работать в заданном режиме только после получения управляющей команды от БКУ.

Например, формула проверки на базе темпоральной логики LTL может быть представлена выражением

$$!G\left(P \to \left(P \times U \times Q\right)\right), \tag{1}$$

где – $!G$ модальный оператор «глобально, все время»; P – РСА функционирует в заданном режиме наблюдения; U – модальный оператор «с тех пор, как»; Q – БКУ выдал команду на начало радиолокационного наблюдения.

Логический инвариант проверки выполнения ограничения функционирования системы перед условием R может быть определен в виде

$$FR \to \left(!W \times U \times R\right). \tag{2}$$

Логический инвариант проверки ограничения функционирования системы между двумя условиями D и V может быть представлен выражением

$$G\left(\left(D \wedge !V \wedge FV\right) \to \left(!C \times U \times V\right)\right), \tag{3}$$

где D – БКУ провел тестирование; C – РСА прошел режим тестирования аппаратуры; V – БКУ выдал команду на установку режима радиолокационного наблюдения.

Формула проверки ограничения функционирования системы после условия A и до выполнимости условия B может быть определена в виде

$$G\left(A \wedge !B \to \left(!K \times U \times B\right)\right), \tag{4}$$

где A – БКУ провел тестирование; K – РСА прошел режим тестирования аппаратуры; B – БКУ выдал команду на установку режима радиолокационного наблюдения.

Типы сообщений между СПО БА КА зависят типа информационного взаимодействия и предназначены для проверки состояния аппаратуры; спецификации режима работы РСА (например, детального или обзорного режима, возможного разрешения при съемке поверхности Земли); определения формата выходных данных РСА.

Модель верификации протокола информационного взаимодействия СПО БА КА представлена на Рисунке 2.

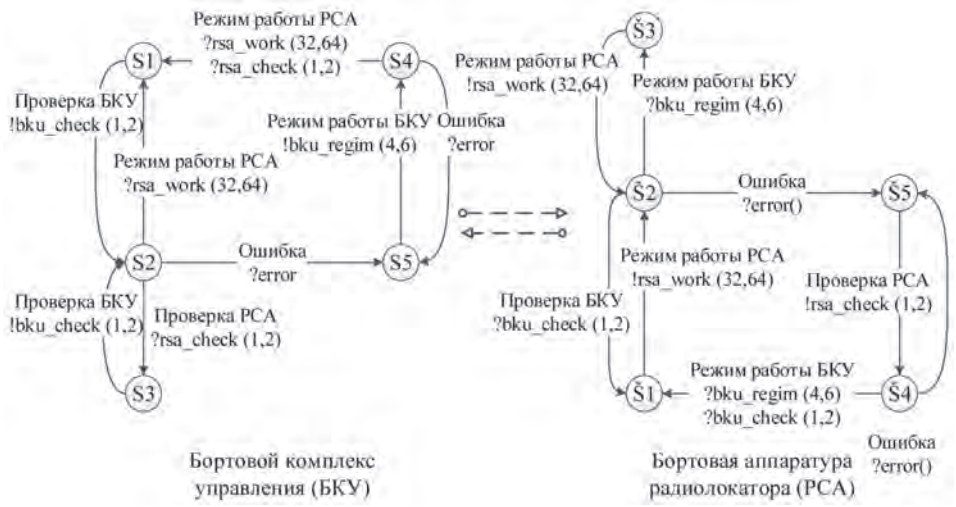

Рисунок 2. Модель верификации протокола информационного взаимодействия СПО БА КА

Проверка свойств работы протокола информационного взаимодействия осуществляется с помощью программных средств верификации (с учетом формул LTL). Программные средства верификации поддерживают несколько режимов проведения анализа: случайный, управляемый и интерактивный режимы.

В случайном режиме все недетерминированные решения выбираются случайным образом. В интерактивном режиме все недетерминированные решения задает пользователь. В управляемом режиме проводится управляемый выбор недетерминированных решений.

Далее программные средства производят верификацию с помощью разработанной модели, а в окне вывода отображаются все события модели, произошедшие с начала работы.

На Рисунке 3 представлен фрагмент ошибочной трассы протокола информационного взаимодействия БКУ и РСА в виде диаграммы взаимодействия процессов. Процесс БКУ отправляет управляющие команды процессу РСА, в зависимости от которых меняется его состояние.

Логический инвариант оказывается нарушенным при возникновении ошибочной ситуации при переходе БКУ и РСА в рабочий режим (ошибочная трасса функционирования) с выявлением недетектированной ошибки в комплекте БКУ, что наглядно демонстрирует эффективность применения методов модельной верификации при разработке бортовой аппаратуры.

Таким образом, для проведения качественной диагностики неисправностей протоколов информационного взаимодействия, возникающих при функционировании ПО бортовой аппаратуры, необходимо применение современных методов выявления его ошибок. Помимо традиционных методов тестирования как бортового оборудования космических

аппаратов на наземных эксплуатационных стендах, так и специального программного обеспечения, требуется верификация проектов СПО с использование моделей проверки (Model Checking), основанных на современных спецификациях темпоральных логик.

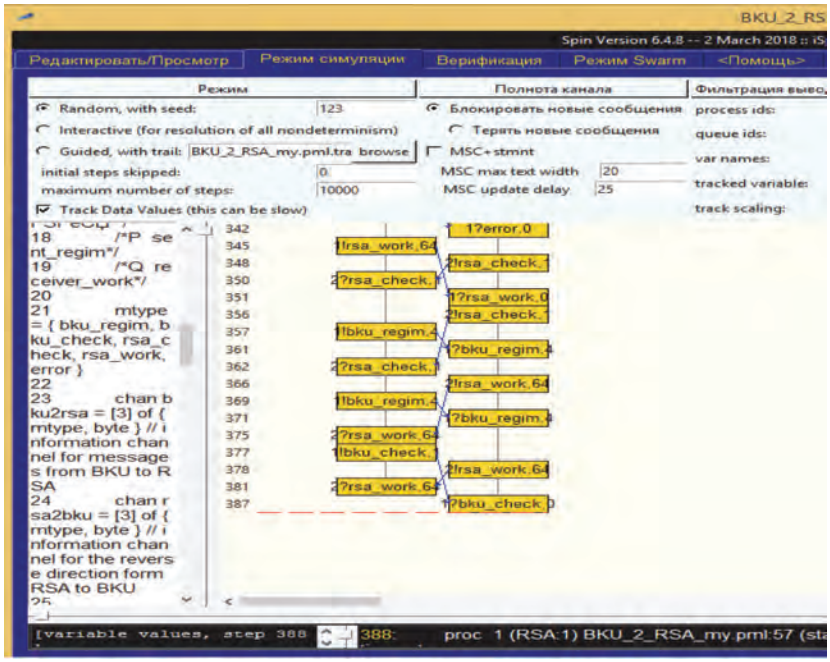

Рисунок 3. Фрагмент ошибочной трассы протокола информационного взаимодействия БКУ и РСА

Заключение

Для реализации методов формальной верификации моделей требований, проектных решений и реализации СПО БА КА можно использовать математический аппарат темпоральных логик (LTL и CTL), математические модели (Крипке и др.), алгоритмы автомата Бюхи и инструментальное средство верификации SPIN.

Основным преимуществом использования данных средств является возможность формального доказательства наличия у программы заданных свойств, которые необходимо описать соответствующим образом. Благодаря этому будет достигнут более высокий уровень качества процессов, результатов проектирования и разработки программных комплексов бортового оборудования КА в целом.

Применение средств верификации на основе темпоральной логики позволит получить высокий уровень надежности и совместимости программного обеспечения бортовой аппаратуры, снизить временные и финансовые издержки на различных этапах ее жизненного цикла за счет раннего обнаружения ошибок СПО бортовой аппаратуры.

Литература

1. *Голубев Е.Н., Тимофеев А.С.* Проблемы и методы испытаний бортовых комплексов управления с сетевой архитектурой // Сборник XVIII Всероссийской научно-практической конференции «Решетневские чтения». 2014. С. 224–226.

2. *Карпов Ю.Г.* Modelchecking. Верификация параллельных и распределенных программных систем. СПб.: БХВ-Петербург, 2010. 560 с.
3. *Шейнин Ю., Солохина Т., Петричкович Я.* Технология SpaceWire для параллельных систем и бортовых распределенных комплексов. Ч.2 // Электроника: НТБ. 2007. № 1. С. 38–49.
4. *Gerard J. Holzmann* (2014) Communications of the ACM, vol. 57, No. 2, pp. 64–73. Available at: https://dl.acm.org/doi/10.1145/2560217.2560218.html
5. ECSS Standart ECSS-E-ST-50-12C. SpaceWire, Links, Nodes, Routers and Networks. European Cooperation for Data Standardization, November, 2014.
6. *Selby R.W.* (2007) Software Engineering: Barry W. Boehm's Lifetime Contributions to Soft-ware Development, Management, and Research. Wiley- IEEE Computer Society Press.
7. Spin Model Checker. The Primer and Reference Manual by Gerard J. Holzmann, Addison Wesley 04.09.2003, 608 p. ISBN: 0-321-22862-6.
8. Spin Online References. Available at: http://spinroot.com/spin/Man/index.html (date of the application: 22.09.2021).
9. The Standish Group report. Available at: https://www.standishgroup.com /store/services/10-chaos-report-decision-latency-theory-2018-package.html (date of the application: 21.09.2019).

Referenses

1. Golubev E.N., Timofeev A.S. (2014) *Problemy i metody ispytanii bortovykh kompleksov upravleniya s setevoi arkhitekturoi* [Problems and methods of testing on-board control systems with network architecture]. *Sbornik XVIII Vserossiiskoi nauchno-prakticheskoi konferentsii "Reshetnevskie chteniya"* [Collection of KhVIII All-Russian Scientific and Practical Conference "Reshetnev Readings"], pp. 224–226 (in Russian).
2. Karpov Yu.G. (2010) *Model checking. Verifikatsiya parallel'nykh i raspredelennykh programmnykh system* [Checking model.Verification of parallel and distributed software systems]. St. Petersburg, BKhV-Peterburg Publishing, 560 p. (in Russian).
3. Sheinin Yu., Solokhina T., Petrichkovich Ya. (2007) *Tekhnologiya Space Wire dlya parallel'nykh system i bortovykh raspredelennykh kompleksov* [Spase Vire technology for parallel systems and onboard distributed systems]. *Elektronika. NTB*, No. 1, pp. 38–49 (in Russian).
4. Gerard J. Holzmann (2014) Communications of the ACM, vol. 57, No. 2, pp. 64–73. Available at: https://dl.acm.org/doi/10.1145/2560217.2560218.html
5. ECSS Standart ECSS-E-ST-50-12C. SpaceWire, Links, Nodes, Routers and Networks. European Cooperation for Data Standardization, November, 2014.
6. Selby R.W. (2007) Software Engineering: Barry W. Boehm's Lifetime Contributions to Soft-ware Development, Management, and Research. Wiley- IEEE Computer Society Press.
7. Spin Model Checker. The Primer and Reference Manual by Gerard J. Holzmann, Addison Wesley 04.09.2003, 608 p. ISBN: 0-321-22862-6.
8. Spin Online References. Available at: http://spinroot.com/spin/Man/index.html (date of the application: 22.09.2021).
9. The Standish Group report. Available at: https://www.standishgroup.com /store/services/10-chaos-report-decision-latency-theory-2018-package.html (date of the application: 21.09.2019).