УДК 681.51:629.78

ВИЗУАЛЬНЫЙ ПОДХОД К ВЕРИФИКАЦИИ УПРАВЛЯЮЩИХ ПРОГРАММ РЕАЛЬНОГО ВРЕМЕНИ

© 2012 А. А. Тюгашев, А. Ю. Богатов, А. В. Шулындин

Самарский государственный аэрокосмический университет
имени академика С. П. Королёва (национальный исследовательский университет)

Описывается подход и поддерживающие его инструментальные программы, позволяющие проводить визуальную верификацию корректности синхронизации процессов, выполнение которых координируется на борту космического аппарата с помощью программ комплексного функционирования, реализующих управляющие алгоритмы реального времени. Разработка дополняет и может использоваться совместно с ранее описанной средой проектирования и разработки управляющих алгоритмов ГРАФКОНТ.

Управляющий алгоритм реального времени, бортовое программное обеспечение, космический аппарат, верификация, визуализация.

Введение

ЭВМ широко применяются как главный компонент автоматизированных систем управления сложными техническими объектами, комплексами, технологическими процессами [5, 7, 8]. Как правило, реализация алгоритмов управления возлагается на специализированное программное обеспечение (ПО), функционирующее в режиме реального времени. Программы такого рода обычно относятся к критическим - ошибка в них может привести к катастрофе, весьма значительным материальным и финансовым потерям, человеческим жертвам. В сетевом графике работ по созданию ракетно-космических комплексов критическим путём иногда является именно разработка системы управления. При этом в разработку бортового ПО вовлечены десятки людей, включая специалистов по бортовым системам, алгоритмистов, программистов и пр. В связи с этим вопросам обеспечения их корректности и надёжности уделяется особое внимание [5, 7]. Для достижения надлежащего уровня качества и надёжности управляющего программного обеспечения оно проходит многоступенчатый процесс тестирования и отладки.

К сожалению, тестирование ПО не может гарантировать отсутствие ошибок, а лишь позволяет обнаружить их наличие, причём не всегда. Всё это делает актуальным разработку и применение иных методов верификации и валидации, к которым можно отнести: инспекции текстов программ; символьное (символическое) выполнение; различные методы формальной верификации, использующие логический вывод [5]; проверку моделей (model checking) [6]. Весьма перспективными представляются подходы с автоматической генерацией заведомо правильной программы по некоторой высокоуровневой спецификации [8, 9, 11].

Одним из перспективных направлений здесь является применение различных визуальных средств. Среди наиболее естественных форм представления (восприятия) информации для человека можно выделить графический образ – рисунок, чертёж, схема и т.д. [1, 8, 12]. К этой форме человек прибегает всякий раз (возможно неявно для себя), когда необходимо решать (описывать, формулировать) действительно сложные задачи. В качестве типичных эпитетов для графического представления используются "дружест-

венный", "интуитивный", "простой", "привычный" и др. Человек способен за доли секунды воспринимать визуальную сцену целиком (симультанное восприятие), с моментальной качественной оценкой ряда важных свойств изображения.

Для использования на различных стадиях проектирования и разработки ПО для космических аппаратов графических средств имеется ряд весомых предпосылок [5, 9, 12]. Среди них можно выделить:

- сложность строгой и непротиворечивой спецификации требований к управляющим алгоритмам и достижения взаимопонимания между проектировщиками бортовых систем, алгоритмистами и программистами;
- необходимость тщательного документирования ПО, незамедлительного и точного отражения в документации всех изменений, вносимых в программы (поддержание актуальности документации);
- вероятность использования различных бортовых цифровых вычислительных машин (БЦВМ) и программных платформ.

Заметим, что системы реального времени можно разделить на два больших класса: системы, управляемые событиями, и системы, управляемые временем. Для управляемых событиями систем не имеет первостепенного значения момент события, важно лишь время, затрачиваемое на реакцию на него (таким образом, они «асинхронны» в некотором смысле), в то время как в управляемых временем системах именно наступление заданного момента времени является «спусковым механизмом» выполнения действий. Главным при этом является реализация некоторого плана управления (расписания) с привязкой протекающих процессов ко времени и корректным их согласованием (синхронизацией) друг с другом. С подобной ситуацией сталкиваются, когда необходимо обеспечить реализацию управления сложным техническим комплексом, содержащим большое число агрегатов, приборов и систем, которые должны работать совместно при решении сложных задач, например, космическим аппаратом (КА) [5, 7]. Среди важнейших требований, которым должно удовлетворять управляющее ПО, можно выделить класс требований к правильной синхронизации параллельно протекающих процессов. Примерами могут служить: «Процессы П1 и П11 должны стартовать одновременно», «Процесс П12 начинается по окончании процесса П11», «Процессы П3, П4 и П5 завершаются до начала исполнения процесса П8».

К сожалению, несмотря на достаточно широкое распространение визуальных методов в современном программировании и Computer Science [1, 2, 3], в известных методологиях визуального моделирования, в частности UML, описание синхронизирующих свойств программ реального времени до недавнего времени не поддерживалось. Лишь начиная с версии UML 2.0 были сделаны некоторые шаги в данном направлении, всё ещё остающиеся недостаточными для практического использования при верификации программ. Анализ имеющихся отечественных и зарубежных источников [1, 2, 3, 4, 5] не позволяет говорить о применении метода визуальной верификации (контроля человеком, не говоря о системах визуальной отладки алгоритмов) для проверки управляющих программ реального времени, используемых в индустрии.

Настоящая статья посвящена описанию подхода к проверке (верификации) управляющих алгоритмов и программ для КА путём оценки (визуального контроля) человеком важнейших синхронизирующих свойств критических секций алгоритма (с последующим уточнением и детализацией) и поддерживающих данный подход инструментальных программных средств.

Визуальная верификация управляющих алгоритмов реального времени (УА РВ)

Как отмечено выше, при описании систем реального времени весьма важной становится корректность синхронизации параллельно протекающих процессов. Ключевыми связками здесь являются: совпадение по началу, следование, совпадение по концу. Для этих связок наиболее естественным является наглядное представление в виде циклограммы (диаграммы Ганта) (рис. 1).

А. А. Тюгашевым и А. А. Калентьевым была предложена соответствующая графическому представлению в виде циклограммы математическая модель семантики УА РВ на основе набора кортежей, описывающих выполнение управляющим алгоритмом различных функциональных задач в требуемые моменты времени в зависимости от истинности тех или иных логических условий [9, 10]. В этой модели семантика УА РВ может быть определена как набор кортежей (четвёрок):

$$УА\ РВ = \{ < f_i, t_i, t_i, \overline{l_i} > \}, i=\overline{1,N},$$

где f_i – функциональная задача (действие); t_i - момент начала выполнения действия (целое число); t_i - длительность действия (целое неотрицательное число); $\overline{l_i}$ - логический вектор, включающий набор значений условий в трёхзначной логике, определяющий исполнение действия. При определении семантики УА РВ происходит привязка выполнения функциональных задач к требуемым моментам времени и обусловливание их выполнения.

Пример. Фрагмент семантики УА РВ может выглядеть как : < {f_1, 0, 100, (α_1=Л, α_2=Л,)}, {f_2, 450, 20, (α_1=И, α_2=Л)}, {f_3, 210, 310, (α_1=Л, α_2=Л)}, {f_4, 0, 210, (α_1=И, α_2=И)}>.

В данной модели не задаётся явным образом передача управления от одной функциональной задачи к другой, что позволяет реализовывать одну и ту же семантику программами с различными управляющими графами (говоря более точно, логико-временными схемами – аналогами управляющих графов для программ реального времени [9, 11]).

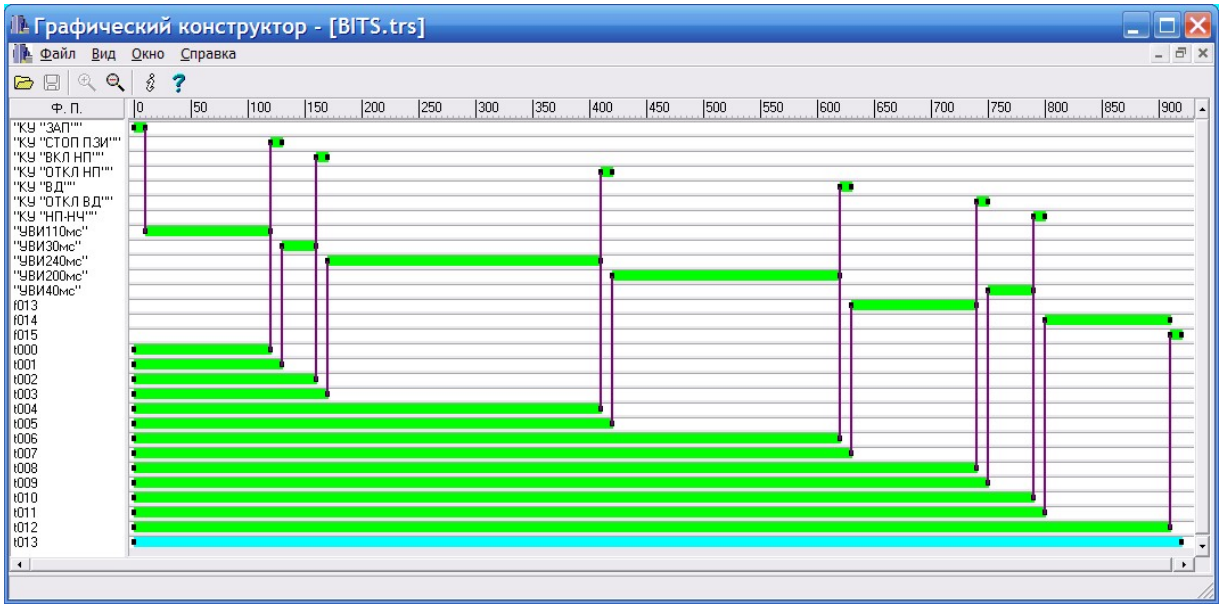

Рис. 1. Визуальная верификация циклограммы управляющего алгоритма

Заметим, что это открывает возможность проведения оптимизирующих преобразований управляющих программ. Ситуация здесь аналогична той, которая возникает в случае вычислительных алгоритмов, когда могут быть написаны несколько вариантов программы, осуществляющей одно и то же функциональное преобразование входных данных в выходные.

При анализе циклограммы управляющего алгоритма программиста могут интересовать ответы на вопросы вида: «Завершается ли выполнение функциональной задачи f_1 до начала выполнения функциональной задачи f_2?», «Одновременно ли начинается выполнение функциональных задач f_1 и f_5?», «Возможно ли при какой-то комбинации логических условий наложение выполнения функциональных задач f_5 и f_3 во времени?», «Заканчивается ли выполнение функциональной задачи f_3 к моменту времени $t=500$?» и т.д. Подобные вопросы возникают при контроле выполнения важнейших свойств управляющих алгоритмов, задаваемых в спецификациях. Визуальное представление позволяет разработчику быстро оценить выполнение необходимых свойств и затем, при необходимости, использовать для уточнения специальный инструментарий.

В разработанной авторами ранее системе информационной поддержки жизненного цикла ПО КА - ГРАФКОНТ [9, 11] используются связки проблемно-ориентированного языка описания управляющих алгоритмов реального времени [9, 10], отражающие согласование выполнения отдельных функциональных задач во времени и в логическом пространстве. Например, запись $f_1 \rightarrow f_2$ означает, что выполнение функциональных задач f_1 и f_2 связано непосредственным следованием во времени, f_1 СН f_2 – что они должны начаться одновременно, $(\sim\alpha_3) \Rightarrow f_7$ - что выполнение ФЗ f_7 обусловливается ложностью условия α_3. Каким образом можно проконтролировать выполнение управляющей программой на практике спецификаций, построенных подобным образом? В системе ГРАФКОНТ для обратного инжиниринга (*reverse engineering*) бортовых программ управления используется простой алгоритм, позволяющий по имеющейся программе построить на первом шаге ее логико-временную схему, а затем - семантику в приведённом выше смысле (реализуемое расписание).

В соответствии с этим внутренние структуры данных системы ГРАФКОНТ пригодны для формирования визуальных представлений семантики (циклограммы) алгоритма, на основе чего становится возможным проводить их визуальную верификацию. Однако в описанной в [9-11] системе ГРАФКОНТ, несмотря на достаточно богатое использование визуальных средств, данная возможность не была в полной мере реализована. В результате проведённых авторами работ в дополнение системы ГРАФКОНТ были созданы и испытаны специальные инструменты визуализации. Данные инструменты позволяют проводить автоматизированную верификацию выполнения временных ограничений и требований необходимой синхронизации процессов. При этом с помощью дополнительной несложной алгоритмической обработки помимо наглядного изображения, используемого для визуального контроля выполнения целевых свойств человеком (рис. 2), может быть автоматически построен набор формул исчисления УА РВ, истинных на данной семантической модели (рис. 3).

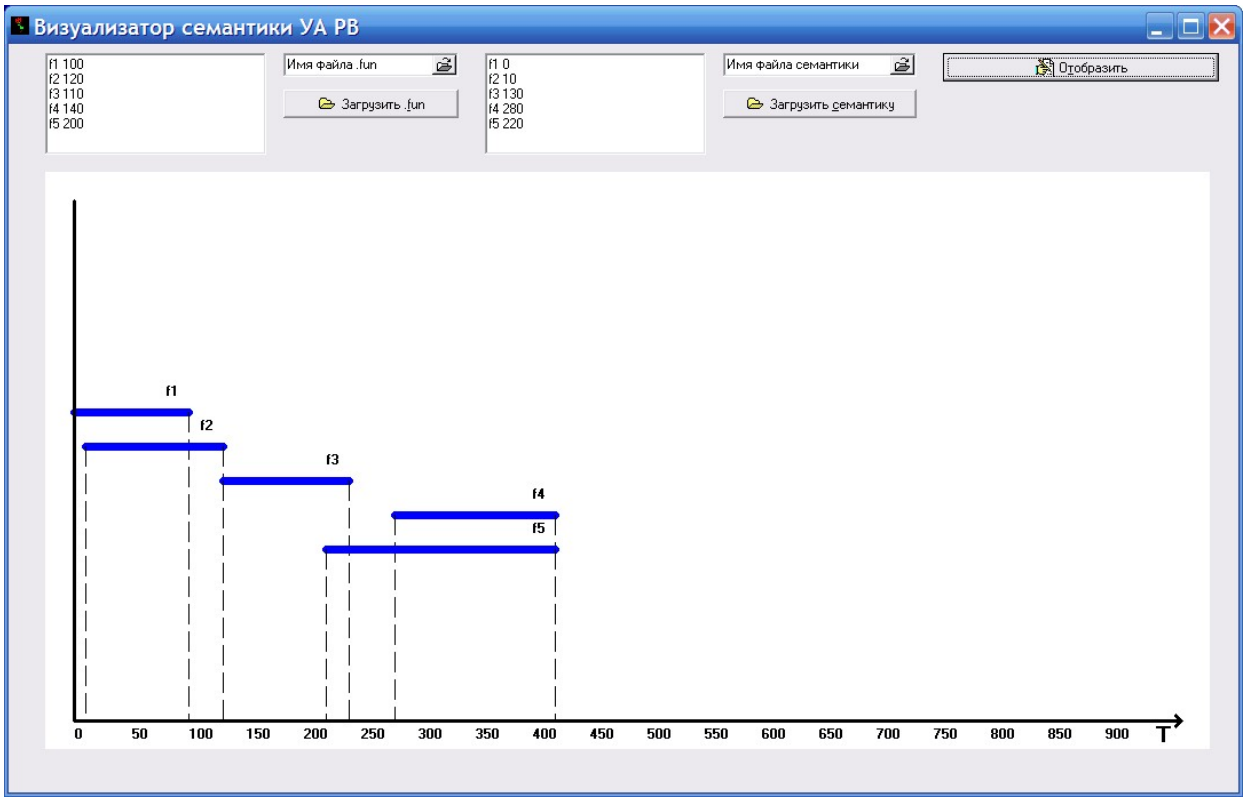

Рис. 2. Визуальный контроль семантики по системной таблице

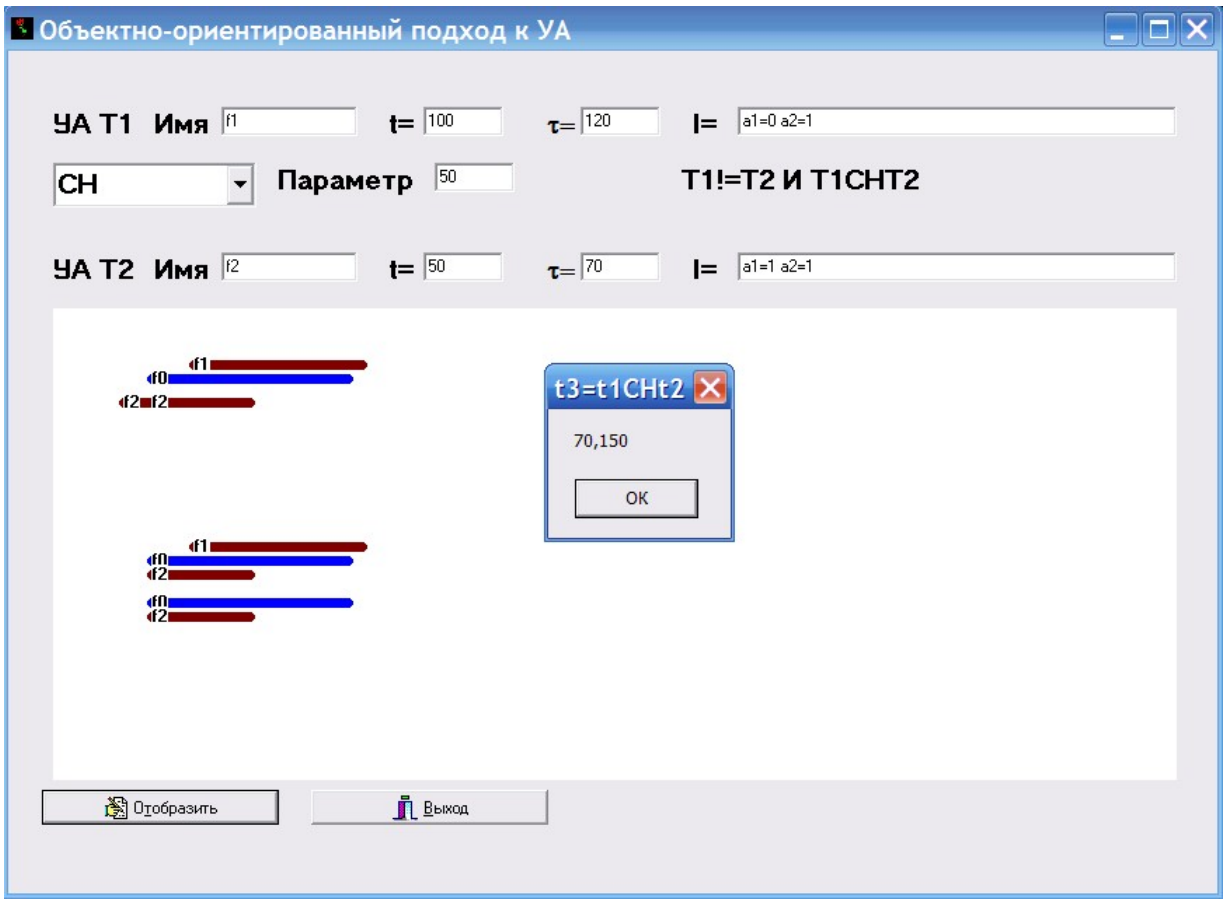

Рис. 3. Автоматическое выявление стандартных временных связок

Таким образом, используемая модель семантики позволяет производить проверку (верификацию) необходимых свойств на семантической модели, т.е. использовать некий аналог метода model checking.

Заметим, что исчисление УА РВ [10, 11] за счёт наличия в нём набора правил вывода даёт возможность проводить и формальную дедуктивную верификацию выполнения временных спецификаций.

Заключение

С использованием инструментальных программных средств визуализации семантики управляющих алгоритмов реального времени возможна визуальная проверка свойств УА РВ, связанных с синхронизацией выполняемых функциональных задач. Данные средства являются дополнением и дальнейшим развитием инструментального программного комплекса ГРАФКОНТ/ГЕОЗ, разработанного по заказу ГНПРКЦ «ЦСКБ-Прогресс» в СГАУ с целью сокращения затрат времени и труда при разработке управляющих бортовых программ, повысить надёжность и качество бортового ПО, снизить зависимость от опыта и искусства отдельно взятого проектанта или программиста.

Библиографический список

1. Parker, D. A. Survey of Visual Programming Tools / D. Parker - Technical Report, University of Alberta, Canada, 2003.

2. Boshernitsan, M. Visual Programming Languages: A Survey / M. Boshernitsan, M. S. Downes. - Technical Report No. UCB/CSD-04-1368 Computer Science Division, EECS University of California, 2004.

3. Glinert, E. P. Visual Programming Environments: Paradigms and Systems, 1990.

4. Авербух, В. Л. Современные тенденции в разработке средств визуализации программного обеспечения параллельных вычислений [Текст] / В. Л. Авербух, М. О. Бахтерев, П. А. Васёв и др. // Международный семинар «Супервычисления и математическое моделирование»: тез. докл. – Саров: ФГУП «РФЯЦ ВНИИЭФ», 2011. С. 18-19.

5. Jia, Xu. On Inspection and Verification of Software with Timing Requirements / Xu Jia // IEEE transactions on software engineering. Vol. 29, No. 8, august 2003.

6. Кларк, Э. Верификация моделей программ: Model checking [Текст] / Э. Кларк. Грумберг, Пелед. - МЦНМО, 2002.

7. Управление космическими аппаратами зондирования Земли [Текст]: Компьютерные технологии / Д. И. Козлов, Г. П. Аншаков, Я. А. Мостовой, и др. – М.: Машиностроение,1998.

8. Зюбин, В. Е. Графические и текстовые формы спецификации сложных управляющих алгоритмов: непримиримая оппозиция или кооперация? [Текст] / В. Е. Зюбин // сб. тр. VII Международ. конф. по электрон. публикациям "EL-Pub2002" - Новосибирск, 2003.

9. Тюгашев А. А. Интегрированная среда для проектирования управляющих алгоритмов реального времени [Текст] / А. А. Тюгашев // Изв. РАН. Теория и процессы управления. - 2006. - № 2. - С. 128-141.

10. Калентьев, А. А. ИПИ/CALS технологии в жизненном цикле комплексных программ управления [Текст] / А. А. Калентьев, А. А. Тюгашев. – Самара: Изд-во Самар. науч. цента РАН. - 2006.

11. Тюгашев, А. А. Автоматизация спецификации, верификации и синтеза управляющих программ реального времени с применением логического и алгебраического подходов. [Текст] / А. А. Тюгашев // Мехатроника, автоматизация, управление. - 2007. -№ 7. - С. 46-51.

12. Тюгашев, А. А. Графические языки программирования и их применение в системах управления реального времени [Текст] / А. А. Тюгашев; Рос. акад. наук, Самар. науч. центр. - Самара: Изд-во Самар. науч. центра РАН, 2009.

VISUAL APPROACH TO VERIFICTAION OF REAL-TIME CONTROL SOFTWARE

© 2012 A. A. Tyugashev, A. Yu. Bogatov, A. V. Shulyndin

Samara State Aerospace University
named after academician S. P. Korolyov (National Research University)

The paper is devoted to the problem of verification of critical real-time control programs, for example, verification of spacecraft onboard software. A special software complex supporting visual verification of correct synchronization between the controlled processes is described in the paper. A semantic model of real-time control algorithm is also provided.

Real-time control algorithm, onboard software, space vehicle, verification, visualization.

Информация об авторах

Тюгашев Андрей Александрович, доктор технических наук, профессор кафедры программных систем, Самарский государственный аэрокосмический университет имени академика С. П. Королёва (национальный исследовательский университет). E-mail: tau797@mail.ru. Область научных интересов: автоматизация процессов жизненного цикла, методы спецификации, синтеза и верификации управляющего программного обеспечения реального времени.

Богатов Артем Юрьевич, аспирант кафедры программных систем, Самарский государственный аэрокосмический университет имени академика С. П. Королёва (национальный исследовательский университет). E-mail: artmbogatov@yandex.ru. Область научных интересов: автоматизация проектирования, оптимизация управляющих программ.

Шулындин Александр Вадимович, аспирант кафедры программных систем, Самарский государственный аэрокосмический университет имени академика С. П. Королёва (национальный исследовательский университет). E-mail: sasha2410@mail.ru. Область научных интересов: верификация управляющих программ, верификация спецификаций программ.

Tyugashev Andrey Alexandrovich, doctor of sciences, professor of the program systems department, Samara State Aerospace University named after academician S. P. Korolyov (National Research University). E-mail: tau797@mail.ru. Area of research: automation of life-cycle processes, methods of synthesis, specification and verification of real-time control software.

Bogatov Artyom Yuryevich, post-graduate student, Samara State Aerospace University named after academician S. P. Korolyov (National Research University). E-mail: artmbogatov@yandex.ru. Area of research: automation of software design, optimization of control software.

Shulyndin Alexander Vadimovich, post-graduate student, Samara State Aerospace University named after academician S. P. Korolyov (National Research University). E-mail: sasha2410@mail.ru. Area of research: specification and verification of real-time control software.