УДК 004.052.2 DOI: 10.22184/NanoRus.2019.12.89.147.148

ОРГАНИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН КОСМИЧЕСКИХ АППАРАТОВ С ДЛИТЕЛЬНЫМ СРОКОМ ЭКСПЛУАТАЦИИ

LONG LIFE SPACECRAFT ONBOARD SOFTWARE DESIGN

ГУСЕВ ЕГОР ВЛАДИМИРОВИЧ
egusev@inbox.ru

ТИХОНОВ СЕРГЕЙ НИКОЛАЕВИЧ

АО «Научно-исследовательский институт «Субмикрон»
124460, г. Москва, г. Зеленоград,
Георгиевский просп., 5, стр. 2

GUSEV EGOR V.
egusev@inbox.ru

TIKHONOV SERGEY N.

Submicron Scientific Research Institute JSC
bld. 2, 5 Georgievsky Ave.,
Zelenograd, Moscow, 124460

В статье рассматриваются аспекты организации бортового программного обеспечения космических аппаратов с длительным сроком эксплуатации. Предлагаемые решения позволяют повысить живучесть бортовой вычислительной системы.

Ключевые слова: бортовое программное обеспечение; живучесть; диагностирование; восстановление; модификация.

The paper considers aspects of long life spacecraft onboard software design. Proposed solutions allow one to increase onboard computing system vitality.

Keywords: onboard software; vitality; control; repair; modification.

Многолетний опыт показывает, что в процессе длительной эксплуатации бортовая аппаратура (БА) космического аппарата (КА) под воздействием внешних и внутренних факторов деградирует, выявляются системные ошибки проектирования. Зачастую неисправности и непредусмотренные ситуации становятся непреодолимым препятствием для дальнейшей эксплуатации КА.

В этих условиях особенное значение приобретает живучесть бортовой вычислительной системы (БВС), т. е. способность адаптироваться к аппаратным неисправностям и ошибкам проектирования, проявляющимся в процессе эксплуатации.

Наиболее эффективный способ адаптации БВС к изменяющимся условиям функционирования — это коррекция бортового программного обеспечения (БПО).

БПО включает в себя общее программное обеспечение (ОПО) и специальное программное обеспечение (СПО). Задача ОПО состоит в обеспечении СПО всеми необходимыми средствами для решения целевой задачи.

Для парирования неисправностей или ошибок проектирования в ОПО, разрабатываемое АО «НИИ «Субмикрон», закладываются следующие средства:

- диагностирования — для своевременного обнаружения и идентификации сбоев и неисправностей;
- восстановления — для восстановления функционирования БПО;
- модификации — для изменения функционирования БПО.

Диагностирование неисправности аппаратных средств БВС выполняется с помощью бортового тестового программного обеспечения (БТПО), входящего в состав ОПО. Тесты БТПО запускаются при включении и по запросу СПО.

Для диагностирования сбоев в процессе функционирования СПО средствами ОПО выполняется контроль системных параметров и параметров вызова функций на допустимость.

При обнаружении сбоев или неисправностей формируется обобщенная и расширенная диагностическая информация. Обобщенная диагностическая информация отображает текущее состояние БВС и признаки готовности к выполнению целевой задачи. Расширенная диагностическая информация содержит данные о системе и БПО на момент обнаружения неисправности или сбоя, необходимые для последующей их идентификации. Например, при возникновении исключения в массив диагностической информации попадают вектор исключения и значения регистров процессора в момент исключения.

Вся диагностическая информация доступна для СПО и может быть передана по штатным каналам связи на наземный пункт управления.

Для восстановления и модификации в ОПО выделено ядро, которое включает в себя:

- предварительные тесты ядра аппаратных средств БВС;
- интеллектуальный загрузчик с функциями выгрузки БПО из ППЗУ в ОЗУ и запуска БПО из ОЗУ;
- безопасный «динамический останов» с функциями поддержки аварийных режимов работы БВС.

Для исключения искажения информации ядро ОПО размещается в масочном или однократно программируемом ПЗУ. Это позволяет восстановить функционирование БВС даже при полностью неработоспособном ППЗУ.

Все БПО делится на сегменты — функционально выделенные подпрограммы. В заголовке каждого сегмента содержится описатель со следующей информацией:

- тип;
- идентификатор;
- номер версии;
- контрольные суммы секций;
- адреса в ОЗУ;
- параметры загрузки и запуска;
- контрольная сумма описателя сегмента.

В зависимости от объема в ППЗУ может храниться несколько копий и версий каждого сегмента. Интеллектуальный загрузчик выполняет поиск исправной (по контрольной сумме) версии сегмента и выгрузку его в ОЗУ. При наличии в ППЗУ нескольких исправных версий сегмента с одним идентификатором предпочтение отдается копии со старшим номером версии.

При искажении сегмента в ППЗУ интеллектуальный загрузчик найдет исправную копию и автоматически восстановит функционирование БВС. Если потребуется модификация заданного сегмента целиком, то при помощи средств ОПО можно, не стирая текущей версии сегмента, записать в резервную область ППЗУ новую версию сегмента.

Вместе с остальными сегментами в ОЗУ выгружается специальный сегмент — таблица описателей сегментов (ТОПСЕГ). ТОПСЕГ содержит указатели на сегменты, составляющие текущую конфигурацию БПО. После выгрузки исправных сегментов в ОЗУ загрузчик проходит по ТОПСЕГ и выполняет контроль, инициализацию и запуск перечисленных там сегментов. Порядок расположения указателей на сегменты в ТОПСЕГ определяет последовательность их запуска. Внося изменения в ТОПСЕГ или записывая новую версию ТОПСЕГ, можно переопределить последовательность запуска БПО, добавить или удалить сегменты, установить «заплатки» на сегменты, требующие локальной модификации.

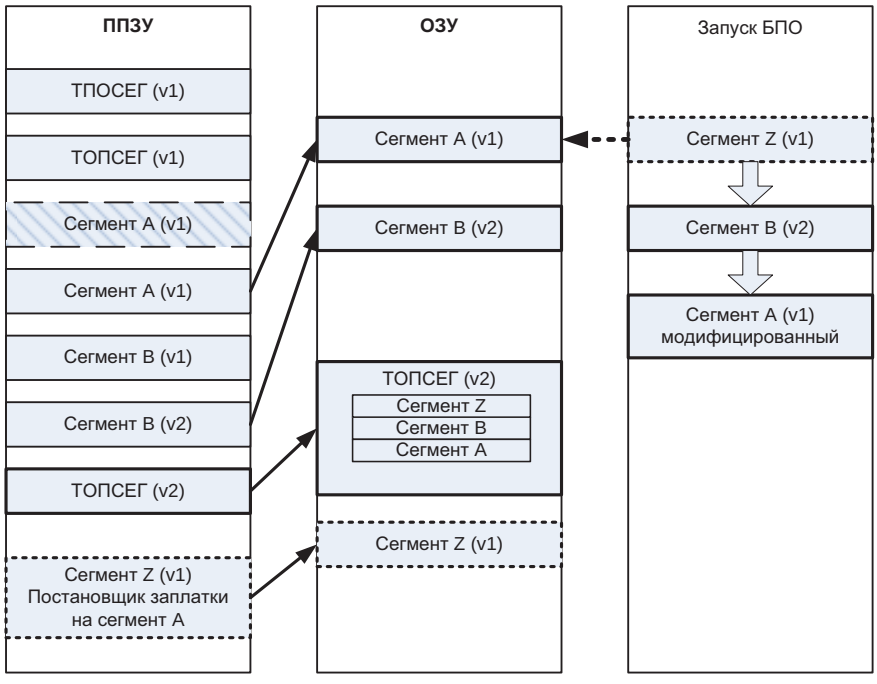

Рис. 1. Работа интеллектуального загрузчика

Для локальной модификации сегмента в ППЗУ записывается специальный сегмент «постановщик заплатки», а в ТОПСЕГ добавляется указатель на него. Сегмент «постановщик заплатки» содержит программный код, при запуске которого выполняется подмена фрагмента кода модифицируемого сегмента в ОЗУ. При постановке «заплатки» также подменяются значения контрольных сумм в описателе модифицируемого сегмента. Таким образом, после выполнения сегмента «постановщика заплатки» в ОЗУ остается модифицированный сегмент, который затем запускается загрузчиком.

Для безопасности предусмотрена модификация ТПОСЕГ в два этапа: прием и отработка в ОЗУ, запись отработанного ТПОСЕГ в ППЗУ.

При невозможности сформировать рабочую конфигурацию БПО или при возникновении исключения в процессе работы ядро ОПО запускает безопасный «динамический останов» (ДОС). В этом режиме ОПО ожидает прихода директив по штатным каналам связи (МКИО, RS, SpaceWire и т. п.). С помощью директив ДОС обеспечивается считывание диагностической информации, запись информации в ОЗУ и ППЗУ БВС, передача управления на заданный адрес. При наличии скоростного канала связи в режиме ДОС можно выполнить прием, запись в ОЗУ и запуск БПО.

Средства повышения живучести БВС, реализованные в ОПО АО «НИИ «Субмикрон», позволяют:

1) своевременно диагностировать неисправности и сбои;
2) передавать информацию о них по каналу связи для последующего анализа;
3) восстановить или модифицировать БПО для возобновления штатного функционирования вычислительной системы.

В части диагностирования и модификации элементы предлагаемых средств были успешно опробованы в БВС реальных КА.

Авторы считают, что в данной работе новыми являются следующие положения и результаты: внедрение ТОПСЕГ и интеллектуального загрузчика с функциями восстановления и модификации БПО для повышения живучести БВС КА.

ЛИТЕРАТУРА

1. Микрин Е. А. Бортовые комплексы управления космическими аппаратами и проектирование их программного обеспечения. — М.: МГТУ им. Н. Э. Баумана, 2003. — 336 с.
2. Липаев В. В. Надежность и функциональная безопасность комплексов программ реального времени. — М.: ЗАО «Светлица», 2013. — 192 с.