УДК 681.5.09
ББК 32.965

БЕЗОПАСНОЕ УПРАВЛЕНИЕ СЛОЖНЫМИ ТЕХНИЧЕСКИМИ СИСТЕМАМИ

Аншаков Г. П.[1]
(*Государственный научно производственный ракетно-космический центр ЦСКБ-ПРОГРЕСС, г. Самара*)
Мостовой Я. А.[2]
(*Самарский государственный аэрокосмический университет, г. Самара*)

Рассматриваются критические по безопасности сложные системы, состоящие из большого числа механических и электронных подсистем, чьей работой нужно взаимосвязанно управлять. Безопасное управление такими сложными техническими системами (*СТС*) *базируется на богатых возможностях встроенной вычислительной техники по контролю состояния подсистем и СТС в целом и принятию решений по управлению в нештатных ситуациях. Вопросы безопасного управления СТС рассмотрены исходя из опыта создания бортовых комплексов управления космическими аппаратами.*

Ключевые слова: сложные технические системы, информационная безопасность, управление, критические системы, программное обеспечение.

1. Введение

Прекращение нормального функционирования критических по безопасности эксплуатации сложных технических систем

[1] *Геннадий Петрович Аншаков, зам. генерального конструктора, член-корр. РАН, доктор технических наук, профессор* (*443009, г. Самара, ул. Земеца, 18, , тел.*(*8462*) *9926198, e-mail: csbd@mail.samtel.ru*).
[2] *Яков Анатольевич Мостовой, доктор технических наук, профессор* (*443086. Россия, Самара, Московское шоссе, 34,тел.* (*8462*) *3378084*).

(СТС) ведет к большим экономическим потерям, ущербу окружающей среде или гибели людей. Использование в СТС системной ЦВМ и аппаратуры со встроенными ЦВМ, образующими локальную сеть, позволяет реализовать при создании критических СТС эффективную стратегию безопасности.

Безопасность информационных взаимодействий определяется защищенностью информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, могущих принести ущерб субъектам информационных взаимодействий.

Без преувеличений можно сказать, что наибольший ущерб субъектам и объектам информационных отношений в СТС наносят сбои и отказы аппаратуры СТС и ошибки в программном обеспечении (ПО) системной и встроенных в аппаратуру ЦВМ [3, 4]. Практика показывает, что не редки также ошибки эксплуатирующего персонала при задании данных для работы ПО СТС, приводящие к тяжелым последствиям для СТС.

В связи с этим вопросы защиты от злоумышленных действий и внешних атак на СТС, в том числе и с применением вредоносного ПО, в данной статье не рассматриваются, поскольку авторы являются сторонниками изоляции критических СТС, обеспечивающей их информационную безопасность.

При выстраивании стратегии информационной безопасности критических систем прежде всего необходимо рассмотреть принципы создания безопасного ПО с учетом того, что системное свойство «безопасность» должно сохраняться и в том случае, когда свойство «безотказность» уже нарушено.

2. Принципы создания безопасного программного обеспечения критических СТС

В основе концепции обеспечения безопасности ПО лежат несколько базовых идей, которые уже используются и развиваются.

1. Повышение безотказности (безошибочности) ПО посредством

– уменьшения первичного потока ошибок за счет применения эффективных технологий проектирования ПО;

– конструирования толерантного (устойчивого) к ошибкам ПО. В настоящее время создание в полной мере толерантного ПО для практических применений представляется нереалистичным. Однако создание ПО, толерантного не в полной мере, но обеспечивающего «мягкий останов» ПО и СТС при проявлении ошибки в ПО или исходных данных, является задачей вполне выполнимой (см. ниже);

– проведения отладки ПО с четко сформулированными целями и критериями отлаженности, с использованием эффективных инструментальных средств, например, имитационной математической модели внешней среды – модели, позволяющей воспроизводить детали межпрограммных взаимодействий ПО во всех вариантах эксплуатации СТС.

2. Принцип изоляции при создании ПО и СТС должен быть использован везде, где это возможно, и не только в части внешних связей СТС с окружающей средой, но и во внутренней среде – путем изоляции отдельных процессов управления СТС в рамках имеющихся функциональных возможностей.

Использование принципа изоляции позволяет сохранить «непотопляемость системы» при нарушении целостности ее «информационных отсеков», препятствуя распространению ошибочной информации и обеспечивая решение задач информационной устойчивости [1, 2]. При решении задачи изоляции необходимо, однако, обеспечить возможность реализации необходимых связей между структурными частями СТС, связей между СТС и системами более высокого уровня иерархии.

Поскольку связи подсистем в рассматриваемых СТС осуществляются на программном уровне системной ЦВМ, изоляцию и взаимодействие процессов необходимо обеспечивать соответствующим распределением памяти, защитой этого распределения средствами системной ЦВМ и ее операционной системы, реализацией межпроцессного обмена информацией только через операционную систему.

3. Невозможно создать на нынешнем технологическом уровне большое абсолютно защищенное ПО. Но возможно сформировать небольшое усиленно защищенное ядро безопасности, принимающее все решения, касающиеся защиты ПО. Таким

ядром для ПО является программа управления в нештатных ситуациях – программа «аварийной защиты». Всё остальное ПО будет действовать на менее защищенных уровнях.

4. Фиксированный набор задач, решаемых встроенными в системы ЦВМ, позволяет применить для хранения ПО и используемых констант постоянное запоминающее устройство (ПЗУ). При этом повышается защищенность ПО, так как изменение информации в ПЗУ связано с использованием специальных технических средств, санкционированное привлечение которых существенно ограничивается.

5. Для многих СТС условия их работы не позволяют оперативно проводить коррекцию ПО встроенных ЦВМ из-за отсутствия прямого физического доступа, а также из-за использования для хранения ПО ПЗУ. Однако доступность оперативной коррекции ПО может стать для таких систем важным преимуществом, влияющим на безопасность, например, в случаях устранения ошибок ПО или компенсации ошибок аппаратуры СТС путем изменения алгоритма обработки информации с нее. Применение технологий, позволяющих дистанционно и оперативно корректировать ПО, является еще одним способом обеспечения безопасности ПО СТС.

Эта корректировка должна проводиться либо без прекращения процесса функционирования СТС, либо с переводом СТС в запасное устойчивое состояние, в котором ее функционирование ограничено и безопасно.

3. Системные методы, реализующие безопасное управление СТС

В рамках рассматриваемой стратегии можно выделить ряд общесистемных методов по обеспечению информационной безопасности, которые лучше изложить на примере бортового комплекса управления космического аппарата (БКУ КА).

1. Составление при проектировании СТС перечня аварийных (нештатных ситуаций), выход из которых также прорабатывается на стадии проектирования СТС. Рассмотрение этого перечня, методов распознавания этих ситуаций и методов выхода из них приводит к созданию:

– ситуационных планов управления в нештатных ситуациях, которые в конечном итоге оформляются в виде инструкций по управлению в эксплуатационной документации;

– программ бортового ПО, обеспечивающих автономное управление в нештатных ситуациях и реализующих, в том числе, функцию «аварийной защиты» СТС.

Для реализации этой защиты в бортовое ПО вводится перечень возможных нештатных ситуаций и сценарии выхода из них, связанные с разной степенью вынужденного, но допустимого ухудшения качества функционирования СТС.

2. Создание методов встроенного контроля работоспособности подсистем СТС и бортового ПО, который осуществляется на многих уровнях:

– аппаратными средствами системной ЦВМ с выходом на внутренние прерывания в случае обнаружения аппаратурой ЦВМ нештатных ситуаций типа переполнения регистра результатов, нарушения распределения памяти, «зависания» и т.п.;

– средствами операционной системы бортовой ЦВМ обобщенно с выходом на программное прерывание в случае обнаружения нештатных ситуаций типа превышения допустимого времени занятости процессора одной задачей, занесения отрицательной уставки времени и т.п.;

– средствами бортового ПО, осуществляющими функциональный контроль типа выполнения заданной функции за заданное время и т.п. Эти средства распределены по функциональным алгоритмам бортового ПО.

3. Создание методов, обеспечивающих возможность оперативной и дистанционной коррекции по радиолинии «зашитого» в ПЗУ бортового программного обеспечения в процессе эксплуатации КА на орбите.

По мере развития электронных технологий последовательно разрабатывались различные варианты такой коррекции, причем все они сохранили свое значение и могут быть использованы совместно.

Технология коррекции программ ПЗУ в полете базировалась на предусмотренной при проектировании бортового ПО возможности обхода исполнения тех или иных участков про-

грамм в ПЗУ с заменой их на фрагменты программ, передаваемых на борт по радиолинии. После появления в бортовой ЦВМ флеш-памяти были созданы технологии коррекции содержимого флеш-памяти, в том числе без прекращения штатного функционирования БЦВМ.

4. Использование принципа изоляции СТС не должно препятствовать доступности операций ввода в ПО СТС необходимых для нее исходных данных и получения информации с результатами работы СТС. Поэтому внешние связи СТС с системами более высокого уровня иерархии должны быть реализованы с использованием пограничного контроля на межсетевых экранах, средств шифрования сообщений из систем более высокого уровня иерархии и т.п. [3]. Шифрование данных и формирование контрольной суммы ПО позволили решить проблему информационной безопасности достаточно эффективно. Это соответствует подходу, когда защищаются собственно данные, а не элементы информационной инфраструктуры, участвующие в получении, хранении, и передачи данных. Но при этом обязательна защита данных на всем пути их продвижения.

Также целесообразна сеансная работа канала связи с СТС, когда вне сеанса связи канал закрывается. Опыт эксплуатации КА подтверждает эффективность этих мероприятий.

5. Контроль за функционированием СТС посредством записи, сбора и передачи на Землю в виде телеметрической информации (ТМИ) всех событий на борту КА, а также дискретной записи состояний его внутренней среды. Назначаемый период дискретизации позволяет восстановить параметры всех физических процессов, протекающих на борту КА.

6. Создание резервов аппаратуры СТС, обеспечивающих выполнение целевой функции СТС с заданной вероятностью. Если для СТС методы обеспечения надежности, связанные с внесением избыточности в аппаратные средства, являются вполне достаточными для сохранения целостности и доступности информации, то для системной ЦВМ, реализующей функции аварийной защиты при возникновении в СТС нештатных ситуаций, требуется обеспечение отказосбоеустойчивости. Свойство отказосбоеустойчивости просто подключением резервной аппаратуры (вместо отказавшей) не обеспечивается даже при автомати-

ческом переходе на резерв по результатам работы встроенного контроля – необходимо сохранять также и информационную устойчивость.

Здесь под информационной устойчивостью понимается свойство восстановления информации после ее искажения вследствие сбоя, отказа или информационной атаки. Именно наличие организованной при проектировании СТС информационной устойчивости позволяет продолжить штатное функционирование СТС после подключения резервных устройств взамен отказавших. Методы обеспечения информационной устойчивости рассмотрены в [1, 2].

7. Проведение стендовых испытаний СТС, при которых используется реальное системное ПО, совместно с реальной системной ЦВМ. В составе стенда реальное ПО работает совместно с имитационной математической моделью внешней среды, структура и характеристики которой позволяют реализовать все варианты работы системы в штатных и нештатных ситуациях.

Задействование такого стенда позволяет предварительно моделировать и отрабатывать все управленческие решения в нештатных ситуациях перед тем как использовать их в реальной СТС.

Требование к имитационной математической модели внешней среды в этом случае такие же, как при отладке бортового ПО – полностью «подыгрывать» прохождению потоков данных в бортовом ПО для всех вариантов его использования. При отладке ПО используются специальные отладочные наборы входных данных, а для проверки управленческих решений – реальные данные СТС в конкретной ситуации.

Использование этого стенда в контуре управления СТС для контроля правильности подготовленных исходных данных перед их вводом в СТС представляется важным и полезным, так как объем и структура исходных данных для работы СТС могут быть весьма значительными и, как показывает опыт, их подготовка сопровождается частыми ошибками.

Принцип изоляции процессов управления в СТС (см. раздел 2, п. 2) доставляет весьма эффективное средство обеспечения информационной безопасности. Так, итальянская

научная аппаратура «Памела», установленная на КА «Ресурс–ДК» [2], имела выход на бортовую локальную сеть по ГОСТ 26765.52–87 (1553В), по которой она управлялась со стороны БКУ КА и по которой она передавала полученную ею научную информацию в радиолинию БКУ для передачи на Землю.

Наличие «чужой» активной аппаратуры иностранного производства в одной локальной сети шинной топологии с целевой аппаратурой, аппаратурой системы угловой ориентации и стабилизации и т.п. КА создавало дополнительную проблему безопасности, так как работа в сети в принципе могла быть нарушена при отказах аппаратуры «Памела», качество разработки и изготовления которой нами не контролировалось. Задача обеспечения безопасности была решена путем изоляции аппаратуры «Памела» на специально выделенной для нее локальной бортовой сети. При этом в системной бортовой ЦВМ БКУ пришлось установить второй сетевой адаптер, специально выделенный под аппаратуру «Памела», благо что техническая возможность этого имелась.

Рассмотренные методы обеспечения информационной безопасности для КА имеют общенаучное и общетехническое значение и могут быть применены для любой сложной технической системы, использующей в своем составе ЦВМ или сеть ЦВМ.

Литература

1. АНШАКОВ Г.П., МОСТОВОЙ Я.А., СОЛЛОГУБ А.В. *Устойчивость информационных взаимодействий в сложных технических системах //* Труды VI международной конференции по проблемам управления и моделирования в сложных системах, Самарский НЦ РАН, ИПУСС РАН, г. Самара, 2004. – С. 425–430.
2. АХМЕТОВ Р.Н., МОСТОВОЙ Я.А., СОЛЛОГУБ А.В. *Информационная устойчивость управления сложными техническими системами* // Труды IX международной конференции по проблемам управления и моделирования в сложных системах, Самарский НЦ РАН, ИПУСС РАН, г. Самара, 2007. – С. 264–272.

3. ГАЛАТЕНКО В.А. *Основы информационной безопасности*. – М.: Интернет-Университет Информационных Технологий. Бином. Лаборатория знаний, 2008. – С. 205.
4. КОЗЛОВ Д.И., АНШАКОВ Г.П., МОСТОВОЙ Я.А., СОЛЛОГУБ А.В. *Управление космическими аппаратами зондирования земли: Компьютерные технологии.* – М.: Машиностроение, 1998. – 386 с.

SAFE CONTROL IN COMPLEX TECHNICAL SYSTEMS

Gennadiy Anshakov, CSBD–PROGRESS, Samara, Deputy the General constructor, member of the cortexes RAS, doctor of technical sciences, professor (443009, Samara, Zemeca str., 18, e-mail: csbd@mail.samtel.ru, tel.(8462) 9926198).
Jakob Mostovoi, SSAU, Samara, doctor of technical sciences, professor (443086, Russia, Samara, Moscow freeway, 34, tel. (8462) 3378084).

Abstract: We consider safety-critical complex systems consisting of a large number of mechanical and electronic subsystems to be controlled and coordinated. Safe control in such complex technical systems (CTS) is based on the capabilities of the built-in computing machinery to monitor states of the subsystems and the CTS as a whole and to make control actions in contingency situations. The problems of safe control in CTS are considered on the basis of authors' experience of on-board complexes control systems development for space vehicles.

Keywords: complex technical systems, information safety, control, critical systems, software.

Статья представлена к публикации
членом редакционной коллегии Д. А. Новиковым