УДК 004.67

Н.А. ЗАХАРОВ, С.В. КАЛИН, В.И. КЛЕПИКОВ, Д.С. ПОДХВАТИЛИН

ФГУП ИТМиВТ им. С.А. Лебедева РАН, Россия

АРХИТЕКТУРА РАСПРЕДЕЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ ЖЕСТКОГО РЕАЛЬНОГО ВРЕМЕНИ

Для построения распределенных систем управления высокой надежности предлагается архитектура с жестким временным разделением доступа к шине (TTA – Time Triggered Architecture). Основой TTA архитектуры являются сетевые протоколы (TTP, FlexRay), обеспечивающие высокоскоростной резервированный сетевой обмен по принципу временного разделения ресурсов. Рассмотрены особенности протоколов и вопросы проектирования, моделирования, разработки, интеграции и верификации TTA систем.

распределенная САУ, x-by-wire, Time-Triggered Architecture, жесткое реальное время

Введение

В основе современных тенденций развития систем управления в автомобильной и авиационной отраслях лежит концепция «сухого» или «электрического» управления, в англоязычной литературе обозначаемая терминами «x-by-wire» (по проводам), например – flight-by-wire, brake-by-wire, steer-by-wire (управление полетом, тормозами, рулевым приводом по проводам) [1 – 2]. Сущность данного подхода состоит в замене механических, гидравлических и пневматических приводов на интеллектуальные электрические привода, содержащие в себе локальные управляющие контроллеры, объединенные в единую распределенную систему высоко скоростными цифровыми каналами информационного обмена [3]. Понятно, что основными требованиями к такой системе являются ее высокая надежность в жестких условиях внешних возмущающих факторов и способность функционировать при появлении отказов в отдельных элементах и подсистемах. Архитектура TTA (Time-Triggered Architecture – архитектура с временным переключением) разработана специально с целью удовлетворения приведенным требованиям. Кроме самой архитектуры, идеология TTA за 25 лет своего эволюционного развития пополнилась методиками, инструментарием и аппаратно-программными компонентами, обеспечивающими интегрированный подход ко всем этапам проектирования, начиная с декомпозиции системы, и заканчивая ее реализацией из специализированных и коммерчески доступных компонент.

Результаты исследований

В настоящее время технологический и коммерческий успех платформы TTA определяется следующими основными факторами:

Цена. Распределенная архитектура позволяет оптимальным образом разместить функции системы по процессорам сети, снижая тем самым общее количество процессоров и, соответственно, стоимость системы.

Стабильность и надежность. Отказы в аппаратуре и программном обеспечении являются основным источником нестабильности и ненадежности сложной распределенной системы. Платформа TTA на архитектурном уровне обеспечивает устойчивость работы всей системы даже при наличии ошибок и отказов отдельных ее компонент, что существенно снижает сроки и стоимость разработки.

Безопасность. В сложной системе функции различного уровня критичности совместно используют системные ресурсы. Поэтому при сертификации централизованной системы ко всем ее компонентам

необходимо применять процедуры обеспечения качества, определяемые компонентой наивысшего уровня ответственности. Платформа TTA обеспечивает архитектурную безопасность и позволяет для каждой функции выполнять лишь необходимые для нее процессы обеспечения качества, тестирования и верификации.

Резервирование датчиков. Возможность использования в различных подсистемах TTA системы информации сразу со всех доступных датчиков позволяет реализовать режим перекрестной проверки исправности датчиков, что повышает отказоустойчивость всей системы. Это свойство также позволяет минимизировать общее количество однотипных датчиков.

Перечисленные свойства архитектура TTA обеспечивают ей успех, как в коммерческих, так и в специализированных ответственных приложениях. В коммерческих приложениях TTA система наряду с хорошими ценовыми параметрами обеспечивает простую интеграцию уже наработанных аппаратных и программных компонент, позволяет проводить покомпонентный ремонт и модернизацию системы. Для критичных по надежности систем TTA платформа благодаря четкой стандартизации и документированности предоставляет возможность выполнять проектирование в соответствии с самыми жесткими требованиями, такими как DO-178B уровня A. В настоящее время TTA платформа получает развитие в авиационной и автомобильной электронике, в частности при построении систем управления ГТД с полной ответственностью (FADEC).

Основным строительным блоком TTA системы является узел. Узел состоит из процессора с памятью, подсистемы ввода-вывода, коммуникационного TTP контроллера, операционной системы и соответствующего прикладного ПО. Все это реализуется в едином модуле, а в идеале – в едином кристалле. Дублированная TTP шина объединяет узлы в кластер. TTP шина вместе с коммуникационными контроллерами узлов образуют в кластере коммуникационную систему, которая функционирует автономно на основе заранее определенного периодического расписания в режиме множественного доступа с разделением времени (TDMA – Time Division Multiple Access). Коммуникационная подсистема читает сообщения (пакеты данных) сетевого коммуникационного интерфейса (CNI – communication network interface) узла в определенные расписанием моменты времени и отправляет их в CNI других узлов, обновляя записанную туда ранее информацию. Моменты времени чтения и записи сообщений содержатся в едином для всех узлов кластера расписании в виде описателя сообщений (MEDL – Message Descriptor List). Копии MEDL хранятся в каждом узле.

В настоящее время существуют две топологии TTA архитектур: шинная (TTA-Bus) и звездная (TTA-Star). В шинной топологии каждый узел содержит локальный блок шинной защиты (bus guardian), предотвращающий отказ узла типа «забивание» шины (babbling idiot faults). В звездной топологии присутствуют центральные блоки шинной защиты, которыми пользуются все узлы кластера.

Протокол TTP (Time Triggered Protocol) – коммуникационный протокол для высоконадежных приложений. TTP является основой архитектуры TTA (Time-Triggered Architecture).

Протокол TTP обеспечивает:

- автономную двухканальную отказоустойчивую передачу сообщений между CNI узлов кластера на основе технологии TDMA с гарантированными задержками и дрожанием фазы;
- отказоустойчивую синхронизацию таймеров узлов для обеспечения глобальной временной сетки без опорного временного сигнала;
- функцию определения принадлежности узла кластеру для исключения отказавших узлов;
- исключение повторов передач при отказах.

Протокол FlexRay – это стандарт безопасной и надежной шины, которая лежит в основе электрон-

ных (drive-by-wire) автомобилей. В электронных автомобилях механическая связь между водителем, двигателем, колесами и колодками тормозов заменяется на электронную. FlexRay благодаря применению архитектуры Byteflight, позволяет совместить в одной шине преимущества жесткого временного разделения (TTP) с событийным управлением, свойственным шине CAN. В настоящее время оба стандарта – и FlexRay и TTP используются конкурирующими группами, однако, учитывая преимущества FlexRay, TTAutomotive приняла решение о расширении TTA платформы, включив в неё спецификации этого протокола.

Синхронизация часов необходима для обеспечения всех узлов единой временной базой, на основе которой все узлы могут пользоваться единым расписанием обмена. Каждый узел на основе априорно известного ожидаемого времени прихода корректного сообщения и фактического времени его прихода вычисляет разницу хода часов передатчика и приемника. Отказоустойчивый усредняющий алгоритм вычисляет коррекцию локальных часов с тем, чтобы они находились в синхронизации со всеми остальными часами кластера. Распределенный алгоритм контроля целостности кластера в случае возникновения отказа выясняет место его возникновения – выходная цепь передатчика или входная цепь приемника. Базовые алгоритмы TTP протокола были формально верифицированы и успешно протестированы в условиях имитации миллионов отказов, при воздействии радиационного и электромагнитного излучений.

В TTP реализована **концепция парирования одиночных отказов**, основанная на том, что вероятность одновременного появления отказов в двух различных компонентах ничтожно мала. Для исключения блокирования или «забивания» шины отказавшим узлом TTP содержит блок защиты шины (bus guardian). Блок защиты шины гарантирует, что узел может выполнять передачу только один раз в течение TDMA раунда, исключая тем самым монополизацию шины отказавшим узлом. При появлении множественных отказов, которые не могут быть парированы самим протоколом, TTP информирует об этом прикладное приложение, которое в свою очередь может принять решение о прекращении своей работы или о переходе в режим безопасный режим.

Реализация перечисленных механизмов отказоустойчивости обеспечивается свойствами TTP протокола поддерживать **согласованность (consistency) данных**. В однопроцессорной системе согласованность гарантируется благодаря возможности всем компонентам ПО пользоваться одной копией данных, записанных в ОЗУ. Такой вид согласованности данных не работает в распределенной системе по следующим причинам. Во-первых, из-за задержек при передаче нет гарантии, что переданное сообщение будет принято всеми узлами-приемниками в одно и то же время. Во-вторых, некоторые узлы могут находиться в нерабочем состоянии, или сообщение из-за сбоя в коммуникационной системе может быть потеряно. Поддержка согласованности данных в TTP протоколе обеспечивается на уровне коммуникационного контроллера CNI путем реализации на аппаратном уровне функций контроля целостности кластера (Membership), подтверждений (Acknowledgment) и предотвращения сегментации (Clique Avoidance).

Контроль целостности кластера. Благодаря циклической (round-robin) схеме TDMA раундов, каждый узел ожидает и проверяет список членов кластера для всех узлов данного раунда. Каждый передатчик, не соответствующий списку членов, определяется как неисправный. Это обеспечивает согласованное взаимодействие группы узлов, каждый из которых видит других в своих списках членов кластера.

Подтверждения. Узел А после каждой своей передачи ожидает от других узлов подтверждения того, что его сообщение было принято на коммуникационном уровне. Это достигается проверкой в

списке членов кластера узла А первого и, возможно, второго подтвердившего узла. Если эти узлы находят узел А в своих списках членов кластера, они подтверждают, что передача узла А была успешно принята. В противном случае узел А извещается о неудачной передаче. В силу принципа временного разделения повторная передача выполняется в следующем цикле.

Предотвращение сегментации кластера. Перед выполнением каждой операции посылки узел проверяет – является ли он членом наибольшего сегмента (majority clique) кластера. Если узел находится в наименьшем сегменте, это означает, что вероятность необнаруженной ошибки велика и это может привести к несогласованности данных. Эта ситуация транслируется прикладному приложению, которое должно решить вопрос о переходе в состояние останова или в режим безопасного функционирования.

Комбинация этих алгоритмов наряду с общей временной базой, поддерживаемой алгоритмом синхронизации часов, обеспечивают согласованность коммуникационного канала. Это гарантирует, что все корректно работающие узлы получают одинаковую информацию в одинаковые моменты времени. TTA платформа, таким образом, обеспечивает приложения мощной программной моделью, которая позволяет эффективно работать со сложными распределенными системами.

Проектирование TTA системы выполняется в два этапа, или на двух уровнях – кластерном и узловом. На кластерном уровне проектируются топология сети и интерфейсы узлов. Далее каждый узел проектируется на основе функциональных спецификаций и спецификаций сетевого интерфейса.

Двухуровневый подход к проектированию TTA архитектуры позволяет реализовать важное свойство **компонуемости** (Composability) системы. Система, обладающая свойством компонуемости, позволяет декомпозировать ее на отдельные модули, которые могут быть разработаны и протестированы независимо друг от друга и затем проинтегрированы без учета их взаимного влияния. При интеграции в единый кластер модули не оказывают влияния на работу друг друга, т.к. каждый из них взаимодействует только со своим блоком CNI. Блоки CNI в свою очередь работают под управлением статически сформированного расписания, не зависящего от того какие модули присутствуют в кластере.

Проектирование кластера TTA системы вручную – достаточно трудоемкий процесс. Разработка сетевого протокола (циклического расписания) требует синхронизации сотен данных между десятками задач, выполняемых на разных узлах. Компания TTAutomotive поставляет набор инструментальных пакетов ^{TTX}Tools, позволяющих автоматизировать все этапы проектирования, как на кластером, так и на узловом уровнях. Моделирующий пакет ^{TTX}Matlink, реализованный в среде Matlab/Simulink, позволяет с использованием графических средств создать модель будущей TTA системы, проверить ее функционирование и в принципе, получить исполняемый код посредством пакета Real-Time Embedded Workshop.

Наиболее эффективное использование TTA архитектуры достигается при применении **операционной системы жесткого реального времени,** такой как QNX или TTP-OS, специально предназначенной для приложений, основанных на использовании TTP протокола. Данные системы занимают исключительно малые вычислительные ресурсы, и обеспечивает быстрое переключение задач. TTP-OS разработана в соответствии с требованиями стандарта сертификации авиационных систем DO-178B Level A.

TTA подход принят за основу построения распределенной **аппаратно-программной платформы САУ перспективных двигателей** авиационного и наземного применения. Для реализации проекта создания перспективной платформы под руководством НПО «Сатурн» и ОАО «НПП «Темп» им. Ф. Короткова» на базе Института точной меха-

ники и вычислительной техники РАН создан координационный совет, в который вошли представители ведущих предприятий отрасли, такие как ОКБ «Сухой», ФГУП ЦИАМ, АО «Завод им. Климова» и др.

Применение платформенного подхода предполагает тесную взаимную увязку элементной базы, функциональных модулей, архитектурных решений, системного и прикладного программного обеспечения, инструментальных средств проектирования аппаратного и программного обеспечения, технологической и производственной подготовки, сопровождения САУ в эксплуатации.

TTA система состоит из набора типовых модулей, связанных по дублированному каналу TTP, поддерживается также дублированный CAN протокол. Типовые модули размещаются в корпусе системы или непосредственно на датчиках и исполнительных механизмах. В набор типовых модулей входит модуль вычислителя (МВ), коммуникационный модуль (МК), модуль дискретных сигналов (МДС), модуль следящей системы (МСС), модуль вторичного источника питания (МВИП) и еще около 30 модулей.

Согласно сформулированным требованиям, перспективная платформа должна строиться на отечественной элементной базе, для чего будут разработаны ряд универсальных и специализированных микросхем, удовлетворяющих требованиям повышенной температурной, вибрационной и спецстойкости. Планируется разработка микросхем микроконтроллера, межмодульного обмена, коммуникационного контроллера (MIL-1553, ARINC, Ethernet), следящей системы, силовой ИМС системы зажигания и ряда других.

Выводы

Использование платформенного подхода позволит:

– сократить сроки и трудозатраты на проектирование и освоение производства;

– обеспечить комплексное выполнение требований стандартов DO-254 и DO-178B на архитектурном, аппаратном и программном уровнях;

– унифицировать элементную базу и отказаться от импортной комплектации;

– повысить надежность САУ за счет применения типовых модулей;

– унифицировать состав бортовой и наземной аппаратуры (включая стендовую) и ПО;

– унифицировать системные решения на уровне смежных конструкторских бюро;

– выполнять модернизацию САУ максимально использую предшествующие наработки;

Применение единого подхода построения бортовой и наземной аппаратуры позволяет решить двоякую задачу – повысить качество и надежность наземных систем до уровня бортовых и снизить стоимость бортовых систем за счет большого тиража наземных установок.

Первым в семействе унифицированных модулей перспективной распределенной архитектуры бортовых систем управления является процессорный модуль, разработанный в ИТМиВТ по заказу ОАО «НПП «Темп».

Литература

1. TTA-Group Steer-by-Wire [Электронный ресурс]. – Режим доступа: http://www.ttagroup.org.

2. Time-Triggered Protocol TTP/C, High-Level Specification Document, Protocol Version 1.1 [Электронный ресурс]. – Режим доступа: http://www.-tttech.com/technology/specification.htm.

3. Синхронизация и декодирование протокола FlexRay [Электронный ресурс]. – Режим доступа: http://www.prist.ru/info.php/articles/lecroy_flexray.htm.

Поступила в редакцию 18.02.2008

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.