Защищённая операционная система реального времени

Сергей Зыль, Владимир Махилёв

Статья раскрывает секрет успеха защищённой операционной системы «жёсткого» реального времени QNX, рассказывает об истории её создания и сертификации на соответствие российским требованиям по информационной безопасности и технологической независимости.

Сегодня в российской оборонной промышленности среди специалистов по информационным технологиям сложно найти человека, который бы ни разу не слышал об изделии КПДА.00002-01. Что же это за продукт, и почему он так знаменит?

Чтобы ответить на этот вопрос, необходимо в первую очередь рассказать о QNX — знаменитом семействе операционных систем реального времени (ОС РВ). Создателей QNX Дэна Доджа и Гордона Белла в 2003 году журнал "Fortune" назвал героями промышленности. Действительно, разнообразие областей науки и техники, в которых нашла своё применение ОС РВ QNX, вызывает удивление даже у её разработчиков. Системные аналитики и главные конструкторы, не занимающиеся программированием непосредственно, в качестве основной причины применения QNX в своих проектах называют удивительно гибкую и элегантную архитектуру этих операционных систем. Отношение же программистов хорошо иллюстрирует известное высказывание: «QNX в мире операционных систем — это то же самое, что автомат Калашникова в мире стрелкового оружия».

История создания

Такая операционная система, как QNX, не могла не обратить на себя внимание и специалистов отечественного оборонно-промышленного комплекса (ОПК). Однако, несмотря на столь завидную репутацию, использовать её для внутреннего рынка они не имели права — в России действуют жёсткие требования технологической независимости и информационной безопасности. Проведение комплекса работ, необходимого для сертификации QNX на соответствие российским нормативным актам, было поручено компании «СВД Встраиваемые Системы». Эта компания была создана в 2002 году на базе технического отдела SWD Software Ltd. — официального дистрибьютора QNX в России и странах бывшего СССР, успешно работающего на рынке систем реального времени с 1991 года. Все помещения «СВД Встраиваемые Системы» разместились на закрытых территориях предприятий ОПК г. Санкт-Петербурга. Компания получила лицензии Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю РФ и Министерства обороны РФ, а также свидетельство о соответствии системы менеджмента качества компании требованиям ГОСТ РВ 15.002 и ГОСТ Р ИСО 9001. При этом каждый инженер компании имеет сертификат специалиста по ОС РВ QNX, выданный разработчиком — канадской компанией QNX Software Systems.

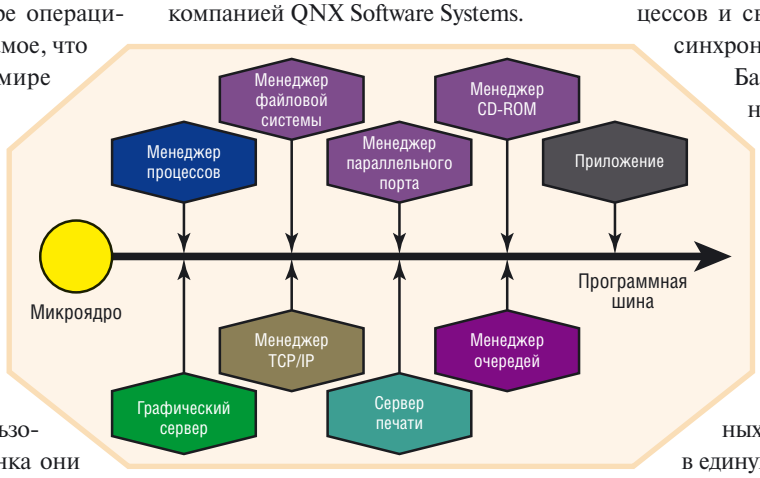

Рис. 1. Архитектура защищённой операционной системы реального времени

«СВД Встраиваемые Системы» получила от канадской компании QNX Software System исходные тексты ОС РВ QNX 4.25 на неограниченное время с правом модификации и в соответствии с требованиями ГОСТ РВ 15.203 разработала на их основе программный комплекс «Защищённая операционная система реального времени QNX» — изделие КПДА.00002-01. Изделие успешно прошло сертификацию по третьему уровню защиты от несанкционированного доступа (НСД) и второму уровню контроля отсутствия недекларированных возможностей (НДВ), что позволяет использовать его в автоматизированных системах (АС) класса защищённости до 1Б включительно. Особо стоит отметить, что в процессе сертификации была выполнена проверка технологии и оборудования, используемых в процессе производства программного обеспечения.

Особенности архитектуры

Визитной карточкой QNX являются микроядро, полная защита памяти процессов и связь между ними на основе синхронного обмена сообщениями.

Базовые функции операционной системы вынесены в особый системный модуль, включающий микроядро и менеджер процессов. Микроядро является, по сути дела, лишь коммутирующим элементом, своего рода программной шиной (рис. 1), обеспечивающей интеграцию других изолированных программных компонентов в единую систему. К задачам, решаемым микроядром, относятся:

- диспетчеризация процессов;

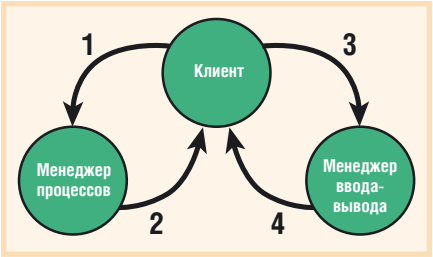

Рис. 2. Установление соединения клиента с менеджером ввода-вывода

- первичная обработка прерываний;
- первичная маршрутизация сетевых сообщений;
- обеспечение безопасного взаимодействия между процессами на основе синхронных сообщений и асинхронных уведомлений.

За годы разработки небольшое (менее десяти килобайтов) микроядро было тщательно отлажено. Маленький размер микроядра и чётко ограниченный список выполняемых им функций обеспечивают надёжность и защищённость операционной системы в целом.

Менеджер процессов, вместе с микроядром входящий в единый системный модуль, гарантирует, что ни один процесс в системе не может вторгаться в адресное пространство другого процесса, а также предоставляет уникальную по эффективности и простоте использования службу пространства имён, которая позволяет процессам быстро находить друг друга.

Однако сам по себе системный модуль никому не нужен. Для решения прикладных задач нужны файловые системы, сетевые протоколы, доступ к устройствам и т.д. И здесь скрыта важная особенность ОС РВ QNX — возможность динамически добавлять/удалять любой сервис или аппаратный драйвер. Это даёт операционной системе уникальную модульность и наращиваемость, позволяет построить как компактную встраиваемую, так и сложную распределённую систему. Компоненты, расширяющие сервисы ОС, называют менеджерами ввода-вывода. Менеджер ввода-вывода — это прикладная программа, которая при запуске регистрируется в пространстве имён менеджера процессов и умеет обрабатывать запросы клиентских приложений. Если менеджер ввода-вывода работает с каким-либо аппаратным устройством, то его называют драйвером. Взаимодействие клиентских приложений с менеджерами ввода-вывода организовано так, как показано на рис. 2.

1. Клиент вызывает библиотечную функцию open(), указывая в аргументах функции имя, зарегистрированное менеджером ввода-вывода в пространстве имён. При этом менеджеру процессов будет послано синхронное сообщение-запрос, содержащее заданное имя.
2. Менеджер процессов в сообщении-ответе передаёт клиенту параметры доступа к соответствующему менеджеру ввода-вывода. Этот ответ содержит, например, идентификатор процесса менеджера ввода-вывода.
3. Функция open(), используя полученные параметры доступа, посылает сообщение-запрос менеджеру ввода-вывода.
4. Менеджер ввода-вывода, исходя из приоритета клиента, текущей загрузки, мандатных правил разграничения доступа или исходя из иных критериев, принимает решение о том, стоит ли взаимодействовать с данным клиентом, возвращает статус (удачно/неудачно), и функция open() завершается. Дальнейшее взаимодействие между клиентом и менеджером ввода-вывода осуществляется уже напрямую.

Разработка менеджеров ввода-вывода — как чисто программных компонентов, так и драйверов — это хорошо налаженная технология. По сути дела, большую часть драйвера программист пишет на основе хорошо документированного шаблона или каркаса, поэтому основные усилия разработчик может сконцентрировать на аппаратно-зависимой части драйвера.

Внедрения

Рассказывая про ОС QNX, сложнее всего, пожалуй, говорить о внедрениях, и в первую очередь это касается изделия КПДА.00002-01. С одной стороны, посещая любую выставку, связанную с передовыми технологиями автоматизации, вы можете по характерным признакам узнать эту операционную систему на многих стендах, представляющих самое разнообразное оборудование и программное обеспечение. С другой стороны, факт использования той или иной операционной системы часто является коммерческой тайной производителей конечных изделий — и не только исходя из соображений безопасности, но и в целях сохранения конкурентных преимуществ. Однако мировой опыт достаточно богат примерами построения решений на основе QNX, и среди них немало таких, которые связаны с ответственными или мобильными применениями, с системами двойного назначения, с использованием в условиях космоса, моря и т.д., то есть решений, которые можно рассматривать в качестве открытых аналогов многих военных применений. Приведём некоторые из них:

- система высокоточной обработки трёхмерных видеоизображений ASVS, разрабатываемая компанией Neptec и предназначенная для удалённого управления стыковкой космических аппаратов;
- система наблюдения и сигнализации Senstar-100 компании Senstar-Stellar, решающая задачи периметровой охраны важных объектов;

Рис. 3. Управление бортовым манипулятором космического корабля «Шаттл» реализовано на основе QNX

Фото предоставлено ИПМТ ДВО РАН

Рис. 4. Автономно-привязной подводный аппарат TSL

- радионуклидный анализатор RASA компании Pacific Northwest National Laboratory для идентификации ядерных объектов и мониторинга окружающей среды;
- система управления бортовым манипулятором космического корабля «Шаттл» (рис. 3);
- многоцелевые автономные подводные роботы (MT-98, TSL и др.) разработки Института проблем морских технологий ДВО РАН (рис. 4) [1, 2].

Рис. 5. Робот PocketDelta компании CSEM предназначен для сборки сложных миниатюрных устройств и построен на основе QNX

Кроме того, можно упомянуть такие сферы применения, как сталелитейная промышленность, добыча, транспортировка и переработка нефти и газа, атомная энергетика, авиационные и морские тренажёры и симуляторы, автоматические телефонные станции и телекоммуникационное оборудование, робототехника (рис. 5) и управление беспилотными аппаратами, медицинские приборы и многое другое.

В настоящее время в различных отраслях широкое распространение получили системы управления, разработанные с использованием SCADA-пакетов, инструментальные средства которых позволяют силами специалистов-технологов, досконально знающих предметную область, в относительно короткие сроки создавать, разворачивать на объектах применения и эксплуатировать сложные автоматизированные системы управления без привлечения программистов. Специально для QNX разработан целый ряд SCADA-систем, среди которых наиболее распространёнными являются RealFlex, «СТАТУС» (рис. 6), RTWin. Каждая такая SCADA содержит готовые наборы тщательно протестированных компонентов АСУ для определённой отрасли промышленности, а также поддерживает специализированные технологические языки, например LCON 4.

Однако все области применения QNX, несмотря на разнообразие, предъявляют два важных требования, в конечном итоге определивших решение разработчиков при выборе операционной системы, — детерминированность и надёжность. Ведь многие изделия должны годами работать без обслуживания человеком и при этом должны гарантированно обрабатывать значительные объёмы информации, поступающей с различных датчиков.

Следует заметить, что вокруг изделия КПДА.00002-01 сложилась достаточно интересная ситуация: изначально предназначенный для ОПК, этот продукт оказался востребованным и при создании ответственных систем коммерческого учёта в добывающей промышленности, энергетике, а также в различных системах, применяемых на транспорте.

Особенности области применения

Предприятия ОПК традиционно уделяют особое внимание вопросам создания новых видов устройств, а в последние годы в связи с активным развитием отечественной микроэлектроники — даже новых ЦПУ (в том числе многоядерных) и процессорных модулей (в том числе прототипных плат) на их основе. Для разработчика аппаратуры одной из наиболее ответственных и проблемных задач является обеспечение поддержки созданного оборудования в операционных средах. Фактически речь идёт об обеспечении программно-аппаратной совместимости.

Рис. 6. Экранная форма SCADA «СТАТУС-4» (НПП «Автоматика-С») для QNX

В этом отношении изделие КПДА.00002-01 предоставляет разработчикам важное преимущество: интерфейсы и методика расширения хорошо документированы и при необходимости могут использоваться разработчиком самостоятельно. Область применения изделия простирается от создания драйверов устройств до реализации собственных системных сервисов, например поддержки особых протоколов обмена данными.

Однако не на всех предприятиях такие задачи возникают настолько часто, чтобы для их решения держать собственный штат квалифицированных системных программистов — представителей очень редкой и высокооплачиваемой специальности. Для решения такого рода проблем своих заказчиков руководство компании «СВД Встраиваемые Системы» приняло решение выйти за рамки традиционных форм технического сопровождения, применяемых коммерческими поставщиками программного обеспечения, и создать Центр разработок системного программного обеспечения QNX. Интересно, что этот Центр оказался востребованным и конкурентоспособным не только на российском рынке.

Заключение

Изделие КПДА.00002-01 по сути дела представляет собой конструктор, состоящий из легко модифицируемых системных компонентов-«кирпичиков» для современных АСУ, которые заказчик может с уверенностью в их качестве интегрировать с помощью предоставляемых ему инструментов и методов в создаваемое им комплексное решение. При этом каждый заказчик имеет возможность на любом этапе жизненного цикла создать и встроить в архитектуру АСУ практически любой новый системный «кирпичик» как своими силами, так и в партнерстве с «СВД Встраиваемые Системы». ●

Литература

1. Ваулин Ю., Инзарцев А. Применение ОС QNX в подводной робототехнике // Современные технологии автоматизации. 2002. № 3. С. 66-71.
2. Инзарцев А., Львов О. Бортовые вычислительные сети автономных подводных роботов // Современные технологии автоматизации. 2005. № 2. С. 68-74.

Авторы — сотрудники ООО «СВД Встраиваемые Системы»
Телефон/факс: (812) 373-1907