Йенс Виганд, Марк Чамберс

Применение многоядерных процессоров и виртуализации в приложениях повышенной безопасности

Многоядерность и виртуализация позволяют увеличить производительность устройств, сократить себестоимость за счёт более высокой степени интеграции оборудования, а также более эффективно обновлять приложения на протяжении всего жизненного цикла устройства.

Бурное развитие рынка встраиваемых систем делает его всё более подверженным действию так называемых подрывных инноваций (инноваций, предполагающих не развитие существующих технологий, а их полную замену), благодаря которым производители устройств промышленного назначения получают значительные возможности по улучшению как самих устройств, так и бизнеса в целом. В частности, широкие возможности для достижения конкурентных преимуществ предоставляют такие технологические тенденции, как:

- развитие многоядерных процессоров,
- виртуализация вычислений,
- увеличение сложности устройств с повышенными требованиями к безопасности.

Широкая доступность **многоядерных процессоров** стала, пожалуй, наиболее подрывной и вместе с тем наиболее многообещающей инновацией на рынке встраиваемых систем за много лет. Новейшие многоядерные процессоры Intel демонстрируют значительное увеличение как общей производительности, так и производительности на ватт, по сравнению с одноядерными. Системы на базе многоядерных процессоров также обеспечивают бóльшую масштабируемость, позволяя наращивать вычислительную мощность увеличением количества ядер без вмешательства в программное обеспечение (ПО). Тенденция к сдвигу в сторону многоядерности набирает обороты, и то, что объёмы продаж 2- и 4-ядерных процессоров Intel уже превышают объёмы продаж одноядерных процессоров, – наглядное тому подтверждение.

Другая важная технологическая тенденция – это **виртуализация вычислений.** Она предоставляет возможность нескольким виртуальным машинам работать на одной физической плате, представляя нижележащие ядра процессора, память и периферийные устройства как уровень абстракции. Виртуализация позволяет использовать в одном и том же устройстве одновременно несколько операционных систем, например ОС реального времени VxWorks (или VxWorks Cert) и ОС общего назначения Wind River Linux (рис. 1).

Прирост производительности, обеспечиваемый комбинацией многоядерного процессора и технологии виртуализации, позволяет объединить в одном устройстве функции, ранее выполняемые несколькими отдельными устройствами. Такая интеграция уменьшает общий объём оборудования и снижает энергопотребление, что позволяет сократить количество необходимых компонентов и получить выигрыш в эксплуатационных расходах.

Виртуализация обеспечивается *гипервизором,* который выполняет функцию диспетчера, защищая операционные среды от взаимного воздействия и предоставляя необходимые механизмы изоляции, которые могут быть использованы для увеличения надёжности и безопасности системы. Это позволяет развёртывать каждое приложение независимо от остальных, снижая стоимость жизненного цикла системы.

Архитектуры с повышенными требованиями к безопасности становятся всё сложнее по мере появления новых функциональных требований и новых требований нормативного соответствия. Один из факторов, влияющих на рост сложности, – это необходимость интерфейса между промышленными устройствами и большим числом внешних систем и сетей, таких как Интернет, производственное оборудование, точки оказания услуг и корпоративные сети. В результате устройствам приходится поддерживать более широкий спектр прикладного и связующего ПО разной степени критичности.

По мере роста сложности регулирующие органы выпускают всё больше формальных методов и процессов сертифи-

Рис. 1. Виртуализация вычислений

кации, призванных защитить системы от нежелательных взаимодействий ПО и внешних атак. Также растёт нормативное давление со стороны стандартов на приложения повышенной безопасности (МЭК 61508, CENELEC EN 50128, ISO 26262, МЭК 60880/62138) и дополнительных отраслевых стандартов в энергетике, на транспорте и в сфере управления промышленными технологическими процессами.

Сочетание технологий многоядерности и виртуализации может помочь производителям устройств для промышленной автоматизации, энергетики и транспорта защитить свои инвестиции в разработку. Эти технологии позволяют вычислительным системам исполнять больше приложений одновременно в безопасной среде, что, в свою очередь, предоставляет существующей многоядерной платформе гибкую расширяемость для достижения большей производительности, безопасности, масштабируемости, сертифицируемости и удобства использования.

Повышенная производительность многоядерных процессоров Intel может также быть использована для объединения задач диспетчерского контроля и сбора данных, визуализации и сетевой безопасности в едином аппаратном блоке без модификации ПО. Более того, виртуализация помогает защитить инвестиции в разработку ПО путём уменьшения прямых зависимостей от применяемого оборудования – это упрощает разработчикам портирование и миграцию на новые архитектуры.

Далее описывается, как многоядерные технологии Intel в сочетании с технологиями виртуализации Wind River меняют подход разработчиков к промышленным приложениям и системам повышенной безопасности.

Масштабирование процессоров для промышленных решений

VxWorks, Wind River Linux и гипервизор Wind River могут выполняться на широком спектре процессоров Intel и поддерживаются мощным инструментарием на основе открытых стандартов, который привносит новую меру эффективности в процесс разработки систем, использующих многоядерные процессоры и несколько ОС одновременно. Эти возможности могут быть распространены на несколько типов промышленного оборудования, представленных различными уровнями «пирамиды автоматизации» (рис. 2).

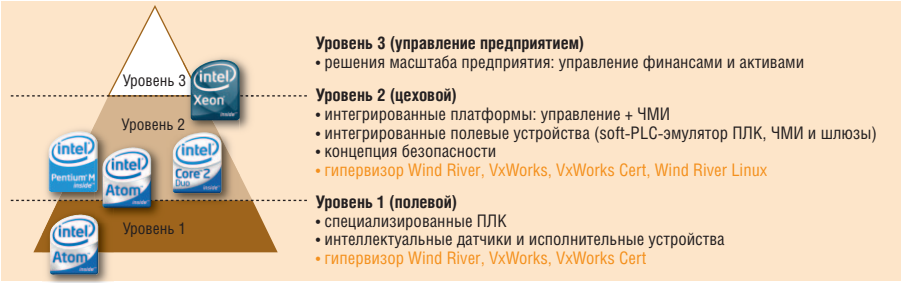

Рис. 2. «Пирамида автоматизации»

На серверах и рабочих станциях сети масштаба предприятия выполняются приложения коллективного управления производством (Collaborative Production Management – CPM), финансовые приложения, а также поддерживаются БД управления активами. Процессоры Intel Xeon предоставляют необходимую вычислительную мощность, чтобы бизнес-приложения работали бесперебойно и эффективно. Они могут выполнять большое число приложений масштаба предприятия за счёт поддержки конфигураций с 8 и более ядрами, а также за счёт увеличения эффективности параллельных вычислений (это достигается применением кэш-памяти большого объёма, что ускоряет переключение контекста).

Цеховой уровень содержит оборудование, которое сочетает в себе функции управления в реальном времени и человеко-машинного интерфейса (ЧМИ), обладающие разными степенями критичности. Эти устройства – идеальные кандидаты для гипервизора Wind River и многоядерных процессоров Intel, способных обеспечить одновременно и производительность вычислений, и разграничение программных модулей, и надёжность, требуемую для приложений повышенной безопасности. Процессор Intel Core 2 Duo, обладающий 2 ядрами, может реализовывать критичные по времени управляющие функции на выделенном ядре, и при этом выполнять остальные функции (например, отображение операторских панелей) на другом. Этот многоядерный процессор имеет рекордно высокую производительность на ватт, что позволяет размещать его в ограниченных пространствах.

Нижний (полевой) уровень непосредственно управляет производственным процессом, связывая датчики и исполнительные устройства с контроллерами и производственным оборудованием. Обычно здесь требуются устройства с очень низким энергопотреблением, поэтому сюда хорошо подходит Intel Atom серии Z5xx для встраиваемых применений. Данный процессор оптимизирован для минимизации выделяемой мощности, которая составляет всего 2 Вт, и обеспечивает преимущества архитектуры Intel для встраиваемых устройств управления, выполненных в компактном форм-факторе.

От уровня управления предприятием до уровня управления технологическими процессами разработчики могут строить различные платформы с разными уровнями производительности, используя один и тот же код и встраиваемые процессоры Intel с длительным жизненным циклом. В дополнение к этим преимуществам производители оборудования обычно находят, что поддержка программного кода для процессоров общего назначения (таких как процессоры архитектуры Intel) проще, чем для специализированных процессоров. Причиной тому служит наличие у процессоров Intel богатой экосистемы, предлагающей широкий спектр развитых средств разработки. Например, компания Wind River, являясь членом Сообщества встраиваемых и телекоммуникационных решений Intel (Intel Embedded and Communications Alliance), тесно работает с компанией Intel, реализуя в своей продукции поддержку преимуществ новейших процессоров, как только они появляются на рынке.

Виртуализация при помощи гипервизора Wind River

Гипервизор Wind River предоставляет возможность разбиения ресурсов одной физической платы на несколько виртуальных плат (рис. 3). Каждая виртуальная плата может либо работать под управлением операционной системы (ОС), называемой гостевой ОС (guest OS), либо выполнять минимальный бинарный модуль. Для распределения процессорных ядер, памяти и периферийных устройств по виртуальным платам гипервизором предоставляются средства конфигурации. Ядра процессора могут быть либо жёстко привязаны к

конкретной виртуальной плате либо разделяться между несколькими виртуальными платами на основе выбранной дисциплины планирования. Память выделяется так, чтобы каждая виртуальная плата располагала своим собственным уникальным адресным пространством и не могла влиять на другие виртуальные платы. Для высокоскоростного обмена данными между виртуальными платами могут быть использованы буферы разделяемой памяти. Периферийные устройства типа последовательного интерфейса или Ethernet могут использоваться виртуальными платами либо монопольно, либо в разделяемом режиме.

Механизм виртуальных плат обеспечивает портирование приложений с существующих специализированных ОС, которые при использовании гипервизора могут выполняться параллельно с коммерческими ОС. Это открывает путь последовательной миграции на готовые коммерческие (COTS) решения, а также упрощает переход на новое оборудование, включая передовые многоядерные платформы Intel. Дополнительным преимуществом является возможность использовать существующие приложения, которые могут быть хорошо отлажены и не требовать изменений, и одновременно реализовывать новую функциональность на более функционально богатых ОС типа Wind River Linux.

Традиционно во многих промышленных приложениях для реализации цельной системы требовались две или более вычислительные платформы одновременно. Причиной этому часто была разная природа объединяемых приложений: для задач управления требовалось приложение жёсткого реального времени, в то время как для взаимодействия с оператором был нужен продвинутый графический интерфейс. В ряде других случаев необходимость использовать разные аппаратные платформы была вызвана требованиями производительности. Улучшенная производительность многоядерных процессоров в сочетании с разделением ресурсов и защитой, предоставляемыми механизмом виртуальных плат, открывают новые возможности для интеграции промышленных систем.

Разделение ресурсов и защита виртуальных плат предотвращают влияние возможных сбоев в работе одной платы на работу других. Если возникает проблема в менее критичной задаче графического интерфейса, она не нарушит работу другой виртуальной платы, отвечающей за критичные системные задачи. В дополнение к этому диспетчерская функция гипервизора Wind River позволит отследить критичный сбой виртуальной платы и перезагрузить её, в то время как остальные платы будут продолжать работать в обычном режиме. Это помогает значительно увеличить надёжность промышленных приложений.

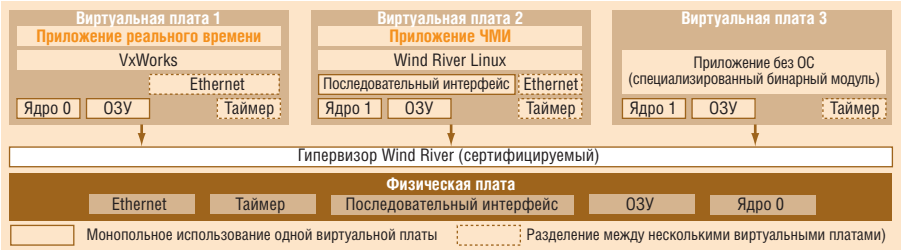

Рис. 3. Разбиение системы на несколько виртуальных плат

Гипервизор Wind River – только один из компонентов пакета поддержки многоядерных вычислений Wind River, в который входит множество технологий, необходимых производителям промышленных устройств, чтобы в полной мере воспользоваться возможностями многоядерных процессоров. Пакет поддержки многоядерных вычислений Wind River включает в себя:

- поддержку многоядерной конфигурации ПО и виртуализации;
- передовые ОС:
  - VxWorks, лидер рынка ОС реального времени,
  - VxWorks Cert (ОС реального времени, сертифицируемая для приложений повышенной безопасности по стандартам DO-178B и МЭК 61508 уровень 3),
  - Wind River Linux;
- среду разработки Wind River Workbench для проектирования, отладки и оптимизации многоядерных и виртуализированных систем.

Гипервизор Wind River можно использовать на одно- и многоядерных процессорах как высокопроизводительное средство интеграции оборудования при одновременном обеспечении необходимого разделения программных модулей.

Intel Virtualization Technology: новый уровень виртуализации

Компания Intel расширила возможности виртуализации, разработав дополнительную технологию Intel Virtualization Technology (Intel VT). Intel VT выполняет множество задач, связанных с виртуализацией (таких, например, как трансляция адресов), на аппаратном уровне, что уменьшает размер программного кода гипервизора и увеличивает его производительность.

Гипервизор Wind River использует технологию Intel VT, чтобы обеспечить максимум производительности и надёжности для виртуализированных приложений. Без этой технологии гипервизору пришлось бы делегировать бóльшую часть управляющих функций операционной системе, что потребовало бы сложных и ресурсоёмких вычислений. Технология Intel VT позволяет выполнять критичные операции аппаратно, что снижает вычислительную нагрузку на гипервизор и таким образом способствует увеличению производительности. К тому же без аппаратной поддержки гипервизор был бы единственным гарантом безопасности ключевой информации о процессоре и состоянии системы, расположенной в незащищённой области памяти. Intel VT предоставляет мощный уровень изоляции, предотвращающий доступ программных компонентов к ключевой системной информации, расположенной в незащищённой памяти.

Intel предоставляет три класса технологий виртуализации:

- Intel VT-x – Intel VT для архитектур IA-32 и Intel 64 обеспечивает базовый каркас, реализующий эффективную работу мониторов виртуальных машин (VMM);
- Intel VT-d – Intel VT для устройств ввода/вывода (directed I/O) обеспечивает виртуализацию ввода/вывода, например отображение запросов DMA в сегменты памяти, фильтрацию и отображение (remapping) прерываний;
- Intel VT-c – Intel VT для устройств сетевой совместимости (connectivity) работает в сочетании с Ethernet-контроллерами Intel, поддерживающими фильтрацию и распределение сетевого трафика по очередям, «принадлежащим» конкретным виртуальным машинам (VM).

Устройства, использующие гипервизор в сочетании с Intel VT, получают значительный выигрыш в надёжности и производительности своей виртуализированной среды.

Вопросы сертификации по безопасности

Серьёзным вопросом, встающим перед производителями устройств в процессе сертификации, является необходимость соответствия требованиям к критичному ПО, в частности, – изоляция/защита его от остальных компонентов системы. Если программное и аппаратное обеспечение системы полностью интегрированы, приложение с обычными требованиями к безопасности, выполняющееся операционной системой общего назначения, тоже должно быть безопасным. Реализация этого требования – очень сложная и затратная задача, поскольку объём кода ОС общего назначения очень велик. Кроме того, было бы полезно иметь возможность периодически пересматривать некритичную часть ПО, чтобы, например, усовершенствовать графический интерфейс или расширить совместимость без необходимости повторно сертифицировать всю систему много раз на протяжении её жизненного цикла, поскольку это влечёт за собой дополнительные расходы и задержки графика проектов.

Компоненты повышенной безопасности требуют временно́й и пространственной изоляции от остальных компонентов с меньшей степенью критичности. Сегодняшние концепции изоляции больше рассчитаны на реализацию каждой функции независимой подсистемой, но этот подход аппаратно избыточен и увеличивает стоимость. Более того, сложившиеся зависимости между компонентами, вызванные использованием технологий полностью или частично собственной разработки, обычно вызывают дополнительные трудности при миграции на коммерческие (COTS) программные и аппаратные решения. Однако разработчики, проектировавшие свои системы с расчётом на гибкую миграцию, находятся в выигрышном положении и могут легко воспользоваться всеми преимуществами новых технологий, такими как многоядерность и виртуализация.

Снижение риска

Если отставить в сторону авиацию, космонавтику и военные приложения, где регулирование осуществляется устоявшимся стандартом ARINC 653, большинство отраслей испытывает недостаток в унифицированном подходе к функциональной безопасности. Это оставляет пространство для свободной трактовки стандартов и может выразиться для производителей устройств в дополнительной непредсказуемости и неопределённости. В большинстве случаев производители устройств сталкиваются с растущим объёмом требований по реализации различных степеней критичности и всё более строгих ограничений. В ARINC 653 полезным подходом является разделение ПО на отдельные модули, которые можно сертифицировать независимо друг от друга.

Компания Wind River, признанный эксперт в технологиях безопасности ARINC 653, удовлетворяющих требованиям DO-178B, использует свои наработки на промышленном рынке, чтобы снизить риски и помочь инженерам разрабатывать безопасные и предсказуемые приложения. Защита памяти, предоставляемая гипервизором Wind River, может быть использована для обеспечения пространственного разделения приложений на виртуальных платах (рис. 4*). Такая конфигурация предоставляет приложениям выделенные защищённые контексты, что является принципиально важным для гарантирования целостности и безопасности независимых программных модулей. Пространственное разделение позволяет приложениям работать независимо друг от друга, что создаёт возможность производителям сертифицировать их по отдельности как более простые независимые компоненты. Плюс назначение разных виртуальных плат различным ядрам и/или применение соответствующей дисциплины планирования (если несколько виртуальных плат делят ядро между собой) поможет получить необходимое разделение во времени.

Оптимизированный для процессоров Intel гипервизор Wind River предоставляет:

- механизм реализации пространственного и временного разделения приложений;
- возможность изоляции критичных функций (например, soft-PLC-эмулятора ПЛК) от всех остальных (например, графического интерфейса);

Рис. 4. Виртуализация в приложениях с повышенными требованиями к безопасности

- открытый модульный подход, потенциально обеспечивающий безопасность при одновременном сокращении затрат.

Перспективы соответствия будущим требованиям безопасности и производительности

Сочетание многоядерности и технологии виртуализации открывает путь к реализации будущих требований к безопасности и производительности в промышленных и транспортных приложениях. По сути, программные и аппаратные технологии от Intel и Wind River могут помочь разработчикам своим единым стандартизированным подходом к пространственному и временно́му разделению. Высокая производительность многоядерных процессоров Intel с технологией Intel VT позволяет приложениям безопасно выполняться в виртуализированной среде. Wind River, в свою очередь, предоставляет программный каркас, включающий в себя ОС VxWorks Cert, сертифицируемый по стандартам МЭК 61508 и DO-178B, и сертифицируемый гипервизор.

Производители, сертифицирующие приложения повышенной безопасности по МЭК 61508 уровень 3 или другим отраслевым стандартам, производным от МЭК 61508, могут получить значительный выигрыш от использования продуктов Wind River на процессорах архитектуры Intel, увеличивающих безопасность и надёжность в виртуализированной среде реального времени. ●

Авторы – Йенс Виганд (Jens Wiegand), руководитель направления промышленных и медицинских приложений компании Wind River, Марк Чамберс (Mark Chambers), менеджер по маркетингу направления программных продуктов корпорации Intel. Перевод Николая Горбунова, сотрудника фирмы ПРОСОФТ Телефон: (495) 234-0636 E-mail: info@prosoft.ru

*Данная диаграмма носит исключительно иллюстративный характер и показывает общее направление развития продуктов Wind River. Она не может быть включена ни в какие контракты или использована при принятии решений о закупках. Разработка, выпуск и обеспечение характеристик любой заявленной функциональности продуктов Wind River остаётся на усмотрение Wind River.