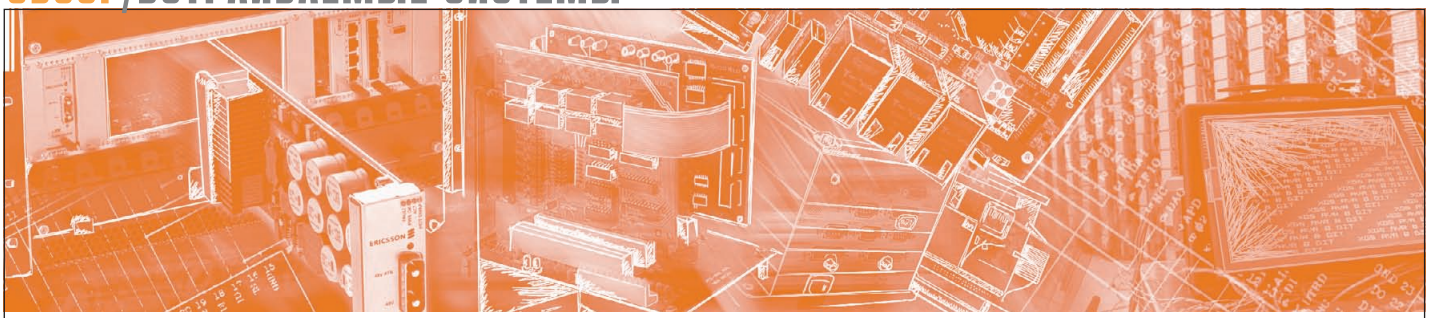

Йенс Виганд

Функциональная безопасность: как сделать ПО частью решения

Сложность ПО и связанная с ней стоимость работ по обеспечению необходимого уровня функциональной безопасности продолжают неуклонно расти. Список нормативных документов, стандартов и правительственных предписаний, устанавливающих требования к функциональной безопасности, постоянно расширяется, усиливая давление на и без того жёсткие сроки и бюджеты проектов и оставляя всё меньше времени на реализацию необходимой функциональности. В настоящей статье описываются три шага, которые производители систем автоматизации и управления могут предпринять, чтобы обратить в свою пользу современные технологии встраиваемого ПО.

Значимость функциональной безопасности как ключевой характеристики систем автоматизации и управления будет велика всегда по объективным причинам. Кроме морально-этических императивов, существуют ещё сухие нормативные и экономические аспекты – несоответствие нормам выливается как в упущенные возможности, так и в штрафы и судебные иски. В ряде известных случаев дело доходило до вмешательства регулирующих органов и отзыва целых линеек продукции, нанося серьёзный удар по прибыли и имиджу производителя.

По мере того как всё большее число функций, связанных с безопасностью в управляющих системах, отдаётся на откуп программному обеспечению (ПО), возникает всё больший соблазн считать процесс разработки ПО частью проблемы, то есть ещё одним сложным фактором, с которым приходится бороться. Однако дальновидным этот подход не назовешь. В сегодняшнем мире правильно выбранные и корректно используемые программная платформа, технологическая база и инструментарий способны обеспечить солидную базу для приложений, к которым предъявляются самые строгие требования по функциональной безопасности, при этом в срок и в рамках отпущенного бюджета.

В настоящей статье описываются три шага, которые производители систем автоматизации и управления могут предпринять, чтобы обратить в свою пользу передовые технологии встраиваемого ПО, снизив издержки, получив новый источник конкурентных преимуществ и при этом прочно оставаясь в рамках современных стандартов функциональной безопасности.

Шаг 1: интеграция оборудования с применением многоядерных процессоров и виртуализации

В задачах сокращения издержек интеграция является традиционным подходом. Однако для производителей систем автоматизации и управления в этом вопросе не всё так гладко, как может показаться.

- Для продуктов, требующих совместимости с МЭК 61508 (или с производными от него стандартами. – *Прим. пер.*), интеграция может вылиться в необходимость повторной сертификации. Это, в свою очередь, увеличит затраты и отсрочит выход обновлённого продукта на рынок.
- Растущие требования к информационной совместимости, как проводной (Ethernet, промышленные шины), так и беспроводной (Bluetooth, WLAN), создают проблемы своевременной доступности соответствующих протокольных стеков.
- У многих производителей наработана огромная база существующих инсталляций продуктов предыдущих поколений, и нужно найти способ внедрения инноваций, не ставя при этом работающие инвестиции под удар.

Для тех, кто хочет воспользоваться всеми преимуществами интеграции, не жертвуя при этом соответствием стандартам функциональной безопасности, современные технологии встраиваемых вычислений предлагают два решения: многоядерные процессоры и виртуализацию.

Сегодняшние многоядерные процессоры существенно превосходят одно-

ядерные как по общей производительности, так и по производительности на ватт. Они также упрощают масштабируемость приложений, позволяя впоследствии применять процессоры с бóльшим числом ядер без необходимости внесения изменений в ПО. Тенденция к переходу на многоядерные процессоры в настоящий момент набирает всё бóльшие обороты, и уже доступны операционные системы (ОС), связующее ПО и инструментарий, оптимизированные для работы в многоядерной среде. Использование современных многоядерных архитектур и технологии гипервизора позволяет сочетать в единой аппаратной платформе несколько операционных систем, сокращая затраты на оборудование и одновременно предоставляя широкие возможности по расширению функций с сохранением соответствия стандартам функциональной безопасности.

Второе решение, виртуализация, позволяет раздельно выполнять несколько операционных сред на одном и том же физическом устройстве, скажем, ОС реального времени (например, VxWorks) и ОС общего назначения (например, Windows или Linux). Разбиение системы на разделы (partitions) упрощает распределение ресурсов, в частности, вычислительные ядра могут быть как жёстко назначены конкретной виртуальной плате, так и разделяться между несколькими, а ОЗУ может быть разбито на непересекающиеся пространства, выделенные виртуальным платам для монопольного доступа. Виртуализация также позволяет изолировать функциональные блоки повышенной функциональной безопасности (например, блок эмуляции ПЛК – soft-PLC) от всех остальных.

Возможность использования нескольких ОС параллельно позволяет выбирать разные ОС для реализации отдельных функциональных блоков. ОС реального времени предпочтительны там, где необходимо обеспечить временной детерминизм; в дополнение к этому они гораздо более просты и легковесны, чем ОС общего назначения наподобие Linux – это делает их подходящими кандидатами на сертификацию. Linux, с другой стороны, выигрывает с точки зрения быстрой адаптации постоянно развивающихся стандартов в области коммуникаций и пользовательского интерфейса. Таким образом, сочетание обеих ОС в одной системе позволит взять от каждой из них сильные стороны – технология гипервизора делает этот подход осуществимым.

Сочетание технологий многоядерности и виртуализации несёт в себе богатый потенциал для увеличения производительности и надёжности промышленных приложений. Чистая выгода здесь заключается в том, что производители систем автоматизации и управления могут «упаковать» больше функций в одно физическое устройство, одновременно снизив затраты и сложность, и при этом упростить решение задач сертификации по современным стандартам функциональной безопасности.

Шаг 2: ставка на открытые платформы

Благодаря растущей роли ПО как фактора дифференциации продуктов способность добавлять функции, связанные с информационной и функциональной безопасностью, на программном уровне при использовании стандартной аппаратной платформы стала ключевым моментом.

Например, использование программных ядер реального времени в контроллерах с программируемой логикой (PLC) сейчас является обычной практикой, однако по мере продвижения по производственной цепочке необходимость в конвергенции технологий и интеграции растет. Производители устройств всё более полагаются на ПО как средство обеспечения безопасности и совместимости продукции; чтобы делать это эффективно, нужна подходящая программная платформа. Всё больше стратегических альянсов заключается с производителями инструментария разработки ПО, ОС и связующего ПО, и чем более стандартизованными становятся результирующие программные платформы, тем больше возможностей появляется для снижения издержек и сложности за счёт интеграции всевозможных подсистем.

Данные тенденции также несут в себе богатый потенциал для решения проблем жизненного цикла изделий. Типовой цикл разработки длится 1–3 года при цикле поставки до 8 лет и 10-летнем цикле поддержки. Результирующий жизненный цикл, который и так в ряде случаев достигает 20 лет, часто необходимо дополнительно продлевать при помощи обновлений, что требует соответствующей поддержки производителей.

Разработчики ПО встраиваемых систем могут помочь своим клиентам решить проблемы сохранения доли на рынке, защиты интеллектуальной собственности, сокращения сроков выхода на рынок и снижения стоимости жизненного цикла. Модульный подход к построению ПО помогает сократить сроки разработки, но сертификацию каждого модуля (например UDP-стека) всё равно каждый раз придётся проводить заново; в рамках подхода модульной сертификации стандартные программные компоненты могут поставляться как доверенные (trusted) в составе сертификационного пакета. Клиенты в свою очередь могут использовать этот пакет для сертификации по МЭК 61508, не только сокращая сертификационную процедуру, но и получая бóльшую гибкость на стадии разработки и, как результат, бóльшую стабильность бизнеса.

Многие производители устройств сейчас склоняются к использованию Linux, и здесь нельзя не упомянуть о связанной с этим проблеме поддержки. Linux как открытая платформа предоставляет богатейшую площадку для консолидации технологий, но рынок программных решений для Linux сильно фрагментирован. Часто, вместо того чтобы опираться на проверенный и поддерживаемый коммерческий дистрибутив, производители стремятся сделать собственную сборку Linux на основе одного из некоммерческих; сложность задачи и степень её влияния на процесс разработки при этом сильно недооцениваются. Использование коммерческого дистрибутива Linux обеспечивает как минимум такие преимущества, как стабильность кода, соответствие открытым стандартам (например, соответствие спецификации CGL проверяется на уровне дистрибутива – по данным Linux Foundation на 2009 год, спецификации CGL 5.0 соответствуют только MontaVista Linux Carrier Grade Edition v6.0, Wind River Linux v4.0 и Fujitsu Computer Technologies Limited ubinux v12. – *Прим. пер.*), доступность обучения и поддержки и гарантии возмещения ущерба – эти факторы обязательно нужно учитывать при принятии решения.

Открытые технологии в сочетании с описанными здесь концепциями многоядерности и виртуализации предоставляют широкий спектр новых возможностей. В частности, важным аспектом использования Linux в системах автоматизации и управления является возможность отделения «критических» функций

(с повышенными требованиями к безопасности) от «некритических» на единой аппаратной платформе. Будучи открытой ОС, Linux предоставляет высокий потенциал для реализации инновационного связующего ПО, но это сильно усложняет процесс сертификации по безопасности (из-за большой сложности и объёмов кода ОС общего назначения. – *Прим. пер.*). Технология гипервизора способна объединить Linux и ОС реального времени на программном уровне, позволяя «критическим» и «некритическим» приложениям выполняться на одной и той же аппаратной платформе. Многоядерные процессоры, в свою очередь, в сочетании с гипервизорами позволяют нескольким ОС выполняться на единой аппаратной платформе в раздельных защищённых пространствах.

Шаг 3: устойчивость к изменениям

Одна из основных причин, по которым процесс разработки ПО традиционно воспринимается как часть проблемы, а не часть решения, состоит в том, что процесс этот часто строится по принципу лоскутного одеяла из инструментов и технологий, оказавшихся под рукой. В результате процесс получается чересчур сложным, непредсказуемым и неповоротливым. Использование открытых программных платформ помогает сделать процесс разработки ПО более гибким и адаптируемым, но также важно иметь возможность поддерживать сложные структуры с изменяющимися требованиями, в том числе и со стороны нормативной базы.

Компания Wind River является единственным на сегодняшний день производителем, предлагающим цельное решение, основанное на открытых платформах, – здесь можно назвать как средства разработки для полного цикла, так и операционные среды, позволяющие одновременно интегрировать функции, управлять сложностью и снижать риски. Сочетание универсального набора ОС, решений в области функциональной и информационной безопасности и вертикально-ориентированных технологических платформ, содержащих богатый выбор связующего ПО, и широкой партнёрской экосистемы создаёт прочный фундамент, позволяющий производителям работать более эффективно, гибко и стабильно.

К примеру, платформа Wind River VxWorks Cert позволяет разрабатывать приложения, сертифицируемые по МЭК 61508 и производным стандартам (например, МЭК 62304 для медицинского приборостроения или CENELEC 50126 в области железнодорожного транспорта), а также RTCA DO-178B/C и EUROCAE ED-12. Используя платформу VxWorks Cert в качестве основы для своих приложений, разработчики могут в полной мере использовать преимущества многоядерных процессоров и при этом эффективно решать вопросы соответствия стандартам функциональной безопасности. При этом, добавив к платформе VxWorks Cert технологию гипервизора, можно сосредоточиться на выполнении «критических» задач под управлением ОС VxWorks, а выполнение коммуникационных протоколов или приложений пользовательского интерфейса перенести, например, на ОС Linux (или другую ОС общего назначения).

Использование гипервизора также упрощает миграцию унаследованного (legacy) кода (гипервизор Wind River позволяет выполнять в выделенном разделе любые приложения, в том числе разработанные без использования ОС. – *Прим. пер.*). Услуги Wind River в области интеграции помогают избежать рисков и выйти из данной задачи кратчайшим путём, гарантируя предсказуемый график выпуска, а интегрированный инструментарий на основе Eclipse с поддержкой параллельной разработки для нескольких ОС и открытость платформы Eclipse, благодаря которой в неё можно легко интегрировать инструменты сторонних производителей, позволяют использовать для всех задач единую инструментальную среду. Для рабочих коллективов это сулит огромный выигрыш в производительности.

Заключение

Экосистема разработки систем автоматизации и управления в настоящий момент переживает технологическую революцию. В отличие от классического развития событий, когда инновационность, эффективность и оперативность зависели исключительно от технологий, сейчас всё большее значение приобретают такие факторы, как функциональная и информационная безопасность. Учитывая набирающую обороты тенденцию к использованию многоядерных процессоров и снижению издержек за счёт интеграции функций на единых аппаратных платформах, мы видим, что растут требования к программному обеспечению; обеспечить соответствие этим требованиям пользователям помогут программные платформы компании Wind River.

За более подробной информацией о решениях Wind River для производителей современных приложений повышенной функциональной безопасности обращайтесь к официальному дистрибьютору Wind River в России и СНГ – компании ПРОСОФТ. ●

Автор – руководитель направления промышленных и медицинских приложений компании Wind River
Перевод Николая Горбунова, сотрудника фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Продукция VIPA допущена к использованию на опасных производственных объектах

Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор) выдала разрешение на применение оборудования компании VIPA на поднадзорных службе производствах и объектах.

Разрешение, полученное официальным дистрибьютором компании VIPA – компанией ПРОСОФТ – распространяется практически на всю продукцию VIPA, предназначенную для использования в системах промышленной автоматизации: программируемые логические контроллеры серий System 200V и System 300S, систему удалённого ввода-вывода серии SLIO, а также на панели


ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ
РАЗРЕШЕНИЕ
№ РРС 00-046389
На применение
Оборудование (техническое устройство, материал):
Программно-технические комплексы VIPA SYSTEM 200, 300, SLIO
с панелью оператора Touch Panel.

оператора серии Touch Panel. Документ действует до конца 2016 года.

Безусловно, наличие такого разрешения позволит существенно расширить сферу применения оборудования немецкой компании. Теперь оно может быть использовано в системах автоматизации объектов нефтяной и газовой промышленности, химического производства, металлургической промышленности, железнодорожного транспорта и других отраслей. ●