Николай Горбунов

Безопасность и сертификация программного обеспечения

Часть 4. Примеры и перспективы

В статье приводится обзор современной терминологической и нормативно-технической базы функциональной и информационной безопасности ПО, затрагивается ряд основополагающих вопросов качества ПО и их привязка к нормативной базе. Рассматриваются примеры программных продуктов, соответствующих современным требованиям сертификации, и практические подходы к подтверждению соответствия. В четвёртой, заключительной, части приводятся практические примеры на базе существующих коммерческих решений и затрагиваются возможные перспективы развития технологий безопасности ПО.

Чтобы не создавать впечатление аналитического паралича, самое время приостановить анализ и перейти к синтезу. Допустим, в ТЗ написано: подлежит сертификации по такому-то стандарту, уровень безопасности такой-то. Что можно с этим сделать, чтобы уложиться в сроки и бюджет?

Вспоминая приведённую в третьей части статьи структуру программного стека, проведём границу между ОС и прикладным ПО – это разделит вопрос на два, смысл такого разделения будет ясен чуть позже.

Подготовка к сертификации системной платформы

Первое, с чего следует начать на уровне системной платформы (то есть связки оборудования и ОС) – это понять, что в ней проще сделать своими силами, а что лучше купить (так называемая дилемма “Build vs. Buy”). При прочих равных условиях купить всегда проще, но с сертифицируемыми компонентами ситуация усложняется, так как они являются товаром скорее штучным, чем массовым, и найти подходящую комбинацию не всегда физически возможно.

К примеру, функционально безопасные многоплатформенные ОС могут быть реально доступны всего для единиц моделей процессоров (да ещё и не в любой версии), и если выбирать процессор без оглядки на ОС, то можно попасть в неловкую ситуацию, когда оборудование уже есть, а ОС для него нет и не предвидится. С BSP (board support package – пакет поддержки оборудования) похожая история: готовых сертифицируемых BSP не так много, и надо быть готовым к тому, что подходящая ОС будет поддерживать только сам процессор, а сертифицируемые драйверы периферийных устройств придётся разрабатывать самостоятельно. Аналогично с пакетами сертификационной документации: они могут быть доступны не для всех стандартов, не по всем возможным уровням безопасности и не для всех комбинаций версии ОС и процессора (высокие уровни безопасности могут требовать трассировки требований до объектного кода, а значит, сертификационные пакеты для ОС на разных процессорах могут отличаться). Это значит, что даже если сертификационный пакет доступен, он не обязательно будет пригоден «из коробки» – может потребоваться доработка.

Иными словами, зная стандарт, по которому будет проводиться сертификация, и требуемый уровень (уровни)

Таблица 1

Пример матрицы доступности (PAM)

ОС	Версия	Сертификационные пакеты	Уровни безопасности	Поддерживаемые процессоры	BSP	Примечания
ОС 1	1.2.3	DO-178C	A,B,C,D	Процессор 1	Плата 1	Отладочная
					Плата 2	
				Процессор 2	Плата 3	
		МЭК 61508	SIL 3, 4	Процессор 3	Плата 4	
	4.5.6	EN 50128	SIL 3	Процессор 4	–	
ОС 2	7.8.9	МЭК 60880	SIL 2, 3	Процессор 5	–	

безопасности, нужно тщательно подобрать подходящие комбинации конкретной модели процессора и конкретной версии поддерживающей его ОС и для каждого варианта оценить степень пригодности имеющихся BSP и сертификационных пакетов. Списки доступных версий ОС для поддерживаемых процессоров и соответствующих сертификационных пакетов (так называемые *матрицы доступности продуктов* – Product Availability Matrix, PAM, табл. 1) обычно являются конфиденциальными и предоставляются производителями по запросу. Перед более детальной проработкой проекта имеет смысл запросить и внимательно изучить эти документы – это сразу даст ответ на вопрос, какие есть готовые комбинации, а что в любом случае придётся делать самим.

Например, при разработке функционально безопасной IMA-платформы, подлежащей сертификации по DO-178C до уровня B включительно, выбор процессора QorIQ P4080 в сочетании с ОС VxWorks 653 версии 2.4 даст готовый сертификационный пакет для ОС (включая сетевой стек) и BSP для отладочной платы (на его основе можно будет создать BSP для разрабатываемого вычислительного устройства). Аналогично в качестве основы для железнодорожной вычислительной платформы, сертифицируемой по EN 50128 SIL 3, может быть использовано сочетание процессора PowerPC MPC8548 и ОС VxWorks Cert версии 6.6 – для этой комбинации доступна сертификационная документация по МЭК 61508 SIL 3 и BSP для отладочной платы. Поскольку стандарт EN 50128 является производным от МЭК 61508, их требования схожи, и доработки сертификационного пакета для ОС будут минимальными.

В случае платформ смешанной безопасности, не подпадающих под спецификацию ARINC 653 (хотя ОС, совместимые с ARINC 653, например VxWorks 653, используются для построения систем смешанной безопасности не только в авиации), дополнительно встаёт вопрос выбора сертифицируемого гипервизора. В настоящее время почти все производители безопасных ОС, включая компанию-пионера в этой области Wind River, обладают гипервизорами собственной разработки, но на рынке присутствуют также и независимые производители гипервизоров. Как и следует ожидать, в первом случае имеется выигрыш по производительности, зато во втором существует более широкий выбор поддерживаемых гостевых ОС.

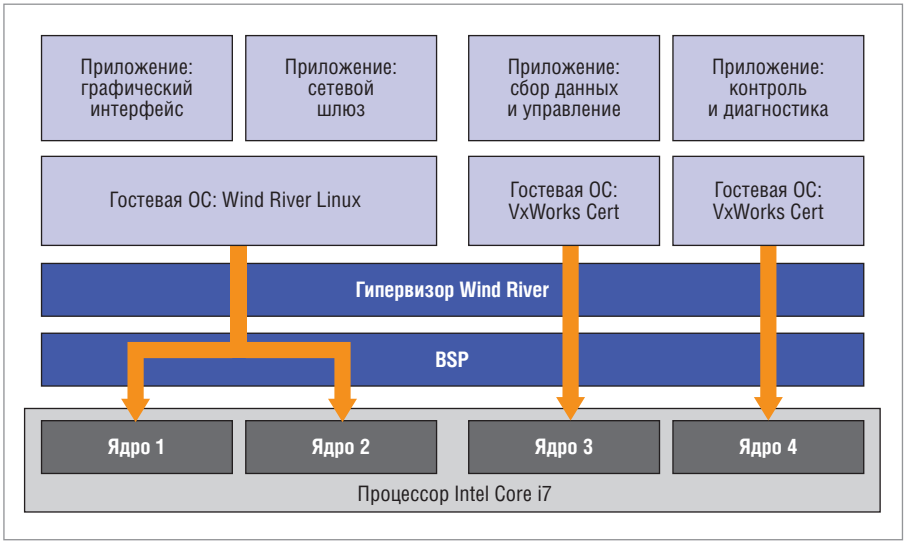

Рис. 1. Пример системы смешанной безопасности на базе платформы Intel System Consolidation Series

ОС, сертифицируемые по стандартам функциональной безопасности, обычно являются встраиваемыми ОС реального времени (ОС РВ), поэтому вопрос: «Использовать ОС РВ или нет?» для функционально безопасных систем чаще всего не стоит (как известно, свобода – это отсутствие выбора). В случае информационной безопасности все немного сложнее, так как по стандартам информационной безопасности сертифицируются не только ОС РВ, но и ОС общего назначения, поэтому при выборе защищённой ОС нужно учитывать ещё и природу решаемой задачи. Например, при прочих равных условиях для разработки защищённого АРМ более подходящим решением может оказаться ОС общего назначения (например, Astra Linux SE), в то время как защищённые системы управления будут требовать применения ОС РВ (например, ЗОСРВ «Нейтрино»). Выбор конкретной версии опять же будет определяться составом защищённого дистрибутива (то есть в основном набором драйверов и BSP, так как наличие драйвера в природе и включение его в состав сертифицированного дистрибутива – разные вещи).

Некоторые производители идут ещё дальше и предоставляют сертифицированные (или сертифицируемые) системные платформы *целиком*, то есть безопасное оборудование, безопасную ОС вместе с BSP и полный пакет необходимой сертификационной документации в едином комплекте. Примером такого решения является функционально безопасный вычислитель для железнодорожных применений от немецкой компании MEN на базе процессорной платы MEN F75P [1] и ОС QNX Safe Kernel, сертифицированный по EN 5012x SIL 4; доступность данной платформы для заказчиков ожидается в 2015 году. Аналогичным примером по части информационной безопасности может служить недавно анонсированная российская вычислительная платформа «Грифон-К» на базе процессорной платы FASTWEL CPC512 [2] и защищённой ОС Astra Linux SE «Смоленск». Очевидный плюс таких решений – вопрос сертификации системной платформы отпадает сразу, и можно сразу заниматься разработкой и подготовкой к сертификации прикладного ПО.

На подходе также сертифицируемые коммерческие системные платформы смешанной критичности – первой ласточкой стала презентованная в 2014 году линейка System Consolidation Series от Intel, сочетающая многоядерные процессоры Intel с поддержкой виртуализации (VT), сертифицируемый гипервизор от Wind River и комбинацию безопасной ОС РВ VxWorks Cert и ОС общего назначения Wind River Linux (рис. 1). Платформа позволяет разделить многоядерный процессор между несколькими ОС, выполняющими задачи разной степени критичности, например, запустить на двух ядрах безопасные (читай – требующие сертификации) приложения под управлением независимых копий VxWorks Cert, а оставшиеся два ядра задействовать под Linux в режиме SMP, например для задач графического интерфейса.

Подготовка к сертификации прикладного ПО

Для сертификации прикладного ПО (связующее ПО мы здесь не рассматриваем – его можно считать частью системной платформы, о которой говорилось ранее), вопрос: «Что можно купить?» не актуален: прикладной код в любом случае придётся частично унаследовать, а частично разработать. Поэтому общий список задач всегда выглядит одинаково.

1. Если разрабатываемая система является системой смешанной критичности, то определить требуемое количество разделов безопасности, разбить функции по уровням безопасности и на основе этого определить наполнение разделов.
2. Разработать собственно код согласно требованиям стандарта.
3. Провести предписываемые применимым стандартом процедуры контроля качества кода (в системах смешанной критичности они могут быть разными для разных разделов).
4. На базе результатов выполнения процедур контроля качества сформировать пакет сертификационной документации.

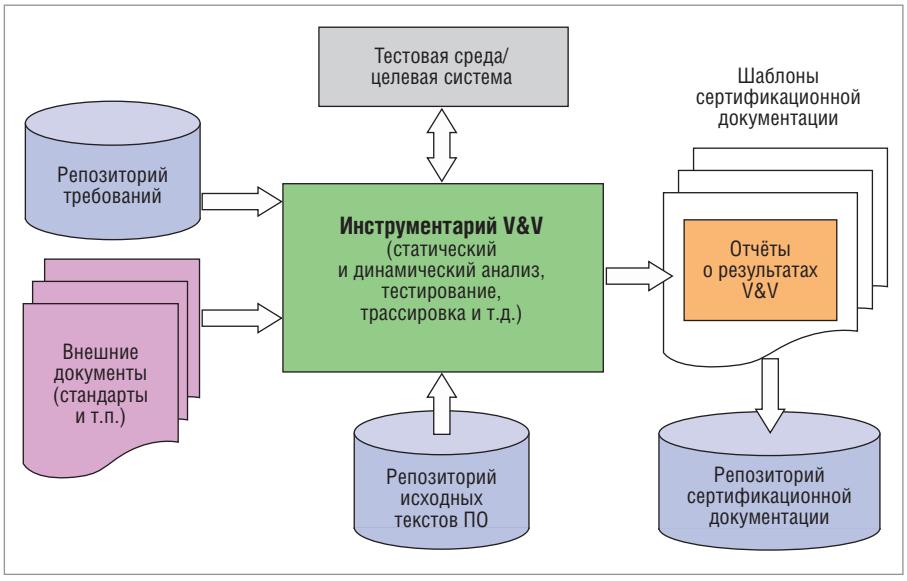

Рис. 2. Построение и поддержание целостности сертификационной документации с использованием инструментария V&V

5. Обеспечить целостность сертификационного пакета на протяжении всего жизненного цикла проекта.

Дальше начинаются нюансы, так как чёрт, как известно, кроется в деталях. В частности, сертификация по функциональной безопасности предполагает, что контроль качества и создание сертификационной документации производятся на стороне разработчика, а оценщик только подтверждает, что всё сделано правильно и требования стандарта выполнены. Отечественная практика сертификации по информационной безопасности, напротив, подразумевает, что контроль качества выполняется на стороне оценщика, поэтому наличие полного сертификационного пакета может облегчить процедуру оценки, но с норма-

ПРОИЗВОДСТВО ЭЛЕКТРОНИКИ ЛЮБОЙ СТЕПЕНИ СЛОЖНОСТИ

Доломант
ЗАО «НАУЧНО-ПРОИЗВОДСТВЕННАЯ ФИРМА «ДОЛОМАНТ»

КОНТРАКТНОЕ ПРОИЗВОДСТВО

Контрактная сборка электронного оборудования

- ОКР, технологические консультации
- Макеты, установочные партии
- Полное комплектование производства, поддержание складов
- Серийное плановое производство
- Гарантийный и постгарантийный сервис

ЗАКАЗНЫЕ РАЗРАБОТКИ

Разработка электронного оборудования по ТЗ заказчика в кратчайшие сроки

- Модификация КД существующего изделия
- Разработка спецвычислителя на базе COM-модуля
- Конфигурирование модульного корпусированного изделия
- Сборка магистрально-модульной системы по спецификации заказчика
- Разработка изделия с нуля

ТЕЛ.: (495) 739-0775 / PRODUCT@DOLOMANT.RU / WWW.DOLOMANT.RU

Реклама

тивной точки зрения обязательным не является – формально достаточно исходных текстов, документации, ЗБ (заданий по безопасности) и применимых ПЗ (профилей защиты), всё остальное оценщик делает сам. Поэтому вопрос использования инструментария верификации и валидации (V&V) более актуален для разработчиков функционально безопасных систем – там у разработчика есть больше возможностей для самостоятельного управления стоимостью сертификации. Впрочем, разработчики информационно безопасных систем тоже могут почерпнуть из использования инструментария V&V много полезного, особенно если используемый разработчиком и оценщиком инструментарий совпадает или хотя бы совместим.

Формирование пакета сертификационной документации выделено в отдельный пункт не случайно, так как здесь тоже есть нюансы. Основная проблема в том, что в стандартах хоть и приводится состав и структура соответствующих сертификационных пакетов, но зачастую содержится недостаточно подробностей о том, что конкретно каждый документ должен содержать и в каком виде. Поэтому даже при полном соблюдении «буквы» стандарта разное оформление сертификационных документов может дать разное (читай – очень разное) время прохождения процедуры подтверждения соответствия. Чтобы сократить потери времени в процессе оценки, ряд компаний (например, упомянутая LDRA) предоставляет не только инструментарий V&V, но и, во-первых, *шаблоны сертификационной документации*, а во-вторых, *системы управления взаимодействием с оценщиком* (Certification Liaison Management System, или просто Certification Management System; соответствующий продукт от LDRA так и называется – LDRA Certification Management System, сокращённо LCMS). Это позволяет, во-первых, сразу оформить документы «правильно» (а значит, сократить количество итераций аудита), а во-вторых, демонстрировать их оценщику и получать обратную связь по чётко формализованному процессу.

Таким образом, идеальная картина может выглядеть примерно так, как показано на рис. 2. (Предполагается, что на предприятии-разработчике развёрнуты и используются система управления требованиями, системы управления версиями для кода и документов, квалифицированный по требуемому стандарту инструментарий V&V и система управления взаимодействием с оценщиком.)

1. Требования стандарта и их производные требования (например, связанные стандарты) импортируются в инструментарий V&V (зачастую этот шаг сводится к простому выбору шаблона проекта). Это даёт перечень конкретных действий, которые нужно будет выполнить.
2. Требования проекта импортируются в инструментарий V&V либо из системы управления требованиями, либо (если требования хранятся в виде документов) из хранилища системы контроля версий. Это даёт отправную точку для трассировки требований.
3. Исходные тексты из хранилища системы контроля версий импортируются в инструментарий V&V и привязываются к требованиям.
4. В инструментарии V&V различным программным модулям в соответствии с требуемым уровнем безопасности назначаются соответствующие процедуры контроля качества (статический анализ, ревью, анализ покрытия, тестирование и т.п.) и назначаются исполнители.

WIND RIVER

VxWorks: 20 лет в космосе – полет нормальный!

Особенности и преимущества VxWorks:

- Настраиваемые домены защиты памяти
- «Жесткое» реальное время: переключение контекста/реакция на прерывание – единицы микросекунд
- Поддержка POSIX API
- Ресурсоемкость: ОЗУ/ПЗУ – сотни килобайт
- Поддержка многопроцессорности (SMP/AMP) и многоядерных процессоров
- Расширенная поддержка сетей TCP/IP (IPv4, IPv6)
- Функции управления энергопотреблением
- Мощный графический пакет Tilcon Graphics Suite
- Мощная интегрированная среда разработки на базе Eclipse
- Поддерживаемые процессоры: x86, ARM, MIPS, PowerPC, ColdFire
- Сертификация МЭК 15408 («Общие критерии») EAL 4/4+/6+, DO-178B уровень A, МЭК 61508 SIL 3, CENELEC EN 50128 и FDA 510(k)
- Открытый исходный текст, возможность построения ОС из исходных текстов

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР WIND RIVER

ProSoft®

Москва Тел.: (495) 234-0636 • Факс: (495) 234-0640 • info@prosoft.ru • www.prosoft.ru
С.-Петербург Тел.: (812) 448-0444 • Факс: (812) 448-0339 • info@spb.prosoft.ru • www.prosoft.ru

Реклама

5. По мере разработки тестовых сценариев они привязываются к требованиям, реализацию которых призваны демонстрировать, и коду, который их реализует. Это формирует матрицу трассировки.
6. Результаты выполнения процедур контроля качества и матрица трассировки экспортируются в форматированный отчёт.
7. Отчёт вставляется в шаблон соответствующего сертификационного документа.
8. Заполненные шаблоны сертификационной документации сохраняются в системе контроля версий, откуда их впоследствии сможет забрать система управления взаимодействием с оценщиком.

В роли системы управления требованиями может выступать, например, DOORS, в роли системы контроля версий – Perforce или Subversion (SVN), в роли инструментария V&V – LDRA Tool Suite, а в роли системы управления взаимодействием с оценщиком – LDRA Certification Management System (LCMS). Шаблоны сертификационной документации входят в поставку LCMS, поэтому вопрос в этом случае решается автоматически. Требуемая конфигурация LDRA Tool Suite будет определяться тем, по какому стандарту и на какой уровень проводится сертификация.

В реальном мире начальные условия могут, мягко выражаясь, отличаться от представленных (всем, наверное, доводилось восстанавливать спецификации по коду), как результат, первой реакцией на план работ по сертификации часто является безотчётное желание один раз сделать всё вручную и забыть, как страшный сон. Однако первые две-три ручные итерации, как правило, ставят всё на свои места и убеждают в том, что принятая методология разработки безопасного ПО – не прихоть полубога, а ценный способ при внесении очередного изменения не забыть одну какую-нибудь небольшую, но критическую деталь.

Что дальше?

Инновационность и безопасность всегда находятся в противовесе – без инноваций невозможно двигаться вперёд, но без безопасности инновации были бы колоссом на глиняных ногах. За последние годы маятник технического прогресса ощутимо качнулся в сторону инноваций, и технологии безопасности изо всех сил стараются не отставать, чтобы сохранить баланс. Попробуем, суммировав всё сказанное, вкратце обрисовать текущее положение и возможную перспективу.

Во-первых, то, что требования современных стандартов функциональной и информационной безопасности к качеству ПО на текущий момент фактически аналогичны и привязаны к управлению рисками, говорит о том, что методики контроля качества наконец-то не только устоялись, но и вышли на системный уровень. Одновременно с этим развитие сетевых технологий и увеличение степени связности устройств (в том числе составляющих элементы критической инфраструктуры) привело к тому, что задачи функциональной и информационной безопасности перестали рассматриваться по отдельности. Таким образом, сейчас уже есть все предпосылки для выработки единой системы приоритетов между задачами функциональной и информационной безопасности и создания объединённого подхода к управлению рисками. На базе этого подхода может быть разработана единая нормативно-техническая база, которая бы позволила производить интегральную оценку функциональной и информационной безопасности по единой системе методик и в рамках единой системы профилей.

Во-вторых, растущий объём кодовой базы критичных систем заставляет искать способы снижения трудозатрат на обеспечение качества кода, в частности, разделять приложения по уровням безопасности и вкладывать усилия пропорционально жёсткости требований. Это невозможно сделать без соответствующей поддержки со стороны ОС, и производители ОС отвечают на этот вызов: число проектов интегрированной модульной авионики на базе совместимых с ARINC 653 ОС сегодня в мире исчисляется сотнями, и проекты MILS-систем на базе соответствующих ОС тоже набирают обороты. По мере того как требования функциональной и информационной безопасности будут объединяться, следует ожидать появления ОС для систем смешанной критичности, способных удовлетворить объединённым требованиям. Пол Паркинсон [3] считает, что в борьбе за это место у ОС с MILS-архитектурой шансов больше, так как совместимые с ARINC 653 IMA-ориентированные ОС допускают реализацию драйверов в пространстве ядра, да и размер кода их ядра слишком велик. В подтверждение этих слов, кстати, компания Wind River недавно анонсировала для своей ОС VxWorks MILS 3.0.0.1 сертификационные пакеты по МЭК 15408 (профиль защиты SKPP [4] и DO-178C одновременно).

В-третьих, в то время как наступление многоядерных процессоров уже происходит по всем фронтам, не все аспекты их безопасности на настоящий момент достаточно изучены (как результат, все существующие на текущий момент безопасные проекты на базе многоядерных процессоров либо содержат существенные оговорки, либо используют только одно ядро). Исследования на эту тему активно ведутся, и по мере получения результатов будут появляться нормативно закреплённые рекомендации по архитектуре как самих многоядерных процессоров для безопасных применений, так и ОС для них. Тот же Пол Паркинсон считает, что с точки зрения ОС наибольшим потенциалом для развития в этом направлении обладают MILS-ориентированные архитектуры на основе гипервизора, использующие вычислительные ядра в режиме AMP. Это, в свою очередь, откроет путь для активного развития масштабируемых систем смешанной критичности с объединёнными требованиями к функциональной и информационной безопасности.

Заключение

Фантасты не ошибаются. В то время как мы смотрим в кино «Терминатора» и «Матрицу» и думаем, что это не про нас, количество программного обеспечения, которое ведёт себя не совсем так, как от него ожидается, непрерывно растёт, в том числе и в ответственных приложениях. По мере того как вычислительные технологии всё глубже проникают в нашу повседневную жизнь, всё больше когда-то простых и понятных вещей начинают зависеть от качества программного кода. Учитывая, какими темпами в последние десятилетия растёт объем этого кода [5], не стоит удивляться, что твоему сотовому телефону однажды могут понадобиться твоя одежда и мотоцикл.

Шутки шутками, но в упомянутой статье Нэнси Левесон [6] есть одна тревожная фраза: «Программные технологии открывают путь к созданию систем настолько сложных, что их поведение становится невозможно контролировать». Это было написано в 2004 году; за прошедшее с того момента время объём кода встраиваемых приложе-

ний – в том числе критичных – вырос в *десятки раз*. Кроме того, в последние годы к взрывному росту объёмов кода добавилось ещё одно измерение сложности, вызванное нарастающим переходом на многоядерные процессоры. Рост сложности увеличивает число неизвестных, а значит, растёт и потенциальное количество системных ошибок; противостоять же системным ошибкам можно только системными мерами. Программное обеспечение разрабатывается людьми, а человек несовершенен, и сделать его совершенным невозможно. Однако, накапливая знания об этом несовершенстве и собирая и внедряя лучшие практики, его влияние на качество ПО можно минимизировать. Именно стандартизация (как накопление знаний и практик) и сертификация ПО (как гарантия использования этих знаний и практик) в конечном счёте позволяют сохранять шаткий баланс между инновационностью и безопасностью.

Приятного полёта.

Литература

1. MEN F75P – Safe Computer [Электронный ресурс] // Режим доступа : http://www.men.de/products/safe-board-level-products/f75p/.
2. Процессорная плата CompactPCI 3U (CPCI-S.0 D0.70) на базе процессоров семейства Intel Ivy Bridge [Электронный ресурс] // Режим доступа : http://www.fastwel.ru/products/vstraivaemye-sistemy/compactpci/3u/506780.html
3. Паркинсон Пол. Многоядерные вычислительные среды и безопасность ПО. Часть 2 // Современная электроника. – 2013. – № 9.
4. U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness [Электронный ресурс] // Режим доступа : http://www.commoncriteriaportal.org/files/ppfiles/pp_skpp_hr_v1.03.pdf.
5. P. Judas and L.E. Prokop. A historical compilation of software metrics with applicability to NASA's Orion spacecraft flight software sizing // Innovations in Systems and Software Engineering. – September 2011. – Vol. 7. – Issue 3. – P. 161–170.
6. Leveson Nancy G. The Role of Software in Spacecraft Accidents [Электронный ресурс] // Journal of Spacecraft and Rockets. – 2004. – № 41. – Режим доступа : http://sunnyday.mit.edu/papers/jsr.pdf

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Отечественные производители электроники объединяют усилия

Процессорные модули FASTWEL в формате CompactPCI успешно прошли тестирование на совместимость с платами компании «Инструментальные Системы» (ЗАО «ИнСис»).

Тестирование проводилось сотрудниками компании «Инструментальные Системы». Проверялись совместимость базовых модулей «ИнСис» **FMC112cP, FMC115cP, FMC117cP** с процессорными x86-модулями различных производителей, в том числе с модулем **FASTWEL CPC503-02.** Целью испытаний было формирование пула совместимых комплектующих для серийного выпуска устройств сбора и цифровой обработки сигналов (ЦОС).

В случае тестирования с модулями FASTWEL всё заработало с первого раза. Тестирование проводилось под управлением операционных систем: Astra Linux, Windows XP/7/8.

Объединение усилий FASTWEL и «ИнСис» даёт возможность в сжатые сроки создавать сложнейшие высокопроизводительные комплексы ЦОС. Выбирая эту продукцию, клиенты получают оперативную техническую поддержку, а также возможность приобретения заказных и модификации серийных изделий (изменение BIOS, схемотехнических решений, проведение дополнительных испытаний и т.п.).

Модуль CPC503 в конструктиве CompactPCI 6U ориентирован на использование в АСУ промышленного и транспортного назначения. Поддержка спецификации PICMG 2.16 позволяет строить на базе CPC503-02 высоконадёжные многопроцессорные вычислительные комплексы. При использовании дополнительных графических ускорителей в формате XMC (в модуле предусмотрен соответствующий слот) вычислительная мощность такого комплекса может доходить до нескольких терафлопс, что является отличным показателем для встраиваемых систем. Модуль построен на базе процессоров Intel Core, поддерживающих спецификации DirectX 11, Open GL 3.1 и Open CL 1.1

Базовые модули (несущие платы) FMC112cP, FMC115cP, FMC117cP ЗАО «ИнСис» предназначены для создания систем сбора и цифровой обработки сигналов на базе промышленных компьютеров, соответствующих спецификации PICMG 2.0 R3.0 CompactPCI. Они используются совместно с мезонинными модулями стандарта FMC в системах с прямой передачей данных в память ПК либо с выполнением цифровой обработки сигналов в программируемых логических схемах (ПЛИС) и многоядерных процессорах цифровой обработки сигналов.

Модуль FASTWEL CPC503

На каждом модуле размещены разъёмы для установки двух мезонинных модулей FPGA Mezzanine Card (FMC) VITA 57.1-2008 (R2010). Каждый мезонин поддерживается отдельной ПЛИС.

Гарантийный срок на сетевое оборудование SCALANCE теперь составляет 5 лет

Компания SIEMENS увеличила гарантийный срок обслуживания промышленного сетевого оборудования серии SCALANCE до 5 лет.

Коммуникационные устройства SIEMENS SCALANCE созданы с учётом всех требований к промышленному оборудованию, в числе которых – работа в расширенном диапазоне температур, в условиях повышенной влажности, вибронагрузки и высокого уровня электромагнитного излучения, а также повышенный показатель наработки на отказ и удобство эксплуатации.

Кроме того, устройства поддерживают ряд разработанных компанией SIEMENS технологий, обеспечивающих резервирование и бесперебойную работу промышленных сетей.

Устройства SCALANCE широко применяются в России и за рубежом для обеспечения надёжной и высокоэффективной проводной и беспроводной передачи данных на любых промышленных объектах: в нефтегазовом секторе, энергетике, на транспорте и т.д.

Линейка SCALANCE включает коммутаторы, маршрутизирующие коммутаторы, медиаконвертеры, точки доступа Wi-Fi со специальными функциями для АСУ ТП, промышленные устройства сетевой безопасности, GSM-маршрутизаторы и модемы.

Увеличенным до 5 лет гарантийным сроком обеспечиваются устройства SCALANCE, поставленные после 1 января 2015 г. Продукция доступна для заказа у дистрибьютора SIEMENS на территории России – компании ПРОСОФТ.