Нормативные стандарты для встраиваемых систем, критичных к безопасности

Джон Карбоун (John Carbone), Express Logic

В статье описаны существующие стандарты и предписания для встраиваемых систем и приложений, в которых они используются.

Все мы наслышаны о страшных историях с автомобилями марки Toyota, терявших управление из-за проблем с управлением и тормозами. Как во всех современных автомобилях, в машинах Toyota используются микропроцессоры и соответствующее программное обеспечение для управления различными системами — от противоблокировочной тормозной системы (ABS) до систем впрыска топлива с электронным управлением и управления двигателем. Эти системы должны обеспечивать безопасность пассажиров и других транспортных средств, находящихся поблизости от автомашины. Несмотря на то, что в системах управления автомобилями Toyota не было обнаружено сбоев в аппаратном или программном обеспечении, некоторые эксперты полагают, что именно отказ систем управления привел к неисправному функционированию, с которым столкнулись многие водители. Но в любом случае от работы таких систем зависит наша жизнь.

Правительства многих стран мира приняли меры к тому, чтобы были тщательно разработаны стандарты для систем, критичных к безопасности. Эти стандарты должны примяться не только в отношении автомобилей, электронные системы которых подвергаются меньшему автоматическому регулированию, чем другие типы систем. Такие приложения как медицинская техника, авионика и промышленный контроль регулируются многими правилами, и разработчики должны представить доказательство совместимости новой продукции до того, как она появится на рынке.

Программное обеспечение критичных к безопасности систем является ключевым элементом, позволяющим им корректно работать. Как правило, это программное обеспечение представляет собой приложение, работающее поверх операционной системы. В некоторых случаях производители используют собственные ОС, в других — коммерческие ОСРВ. Так или иначе, система должна работать без сбоев, поскольку любая ошибка может привести к травме или смерти. В силу чрезвычайной важности мер по обеспечению безопасности функционирования систем управления в разработке правил, регулирующих применение соответствующего программного обеспечения, участвуют финансируемые государством агентства и независимые организации, к числу которых относятся следующие.

Промышленные системы. Международная электротехническая комиссия (МЭК) — всемирная организация, которая содействует развитию международного сотрудничества по всем вопросам, касающимся стандартизации в области электрических и электронных систем. IEC 61508 — международный стандарт под названием «Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью». Он определяет требования по проектированию, внедрению, функционированию и технической поддержке систем, обеспечивая необходимый уровень полноты безопасности (SIL). Стандарт IEC 61508 известен в Великобритании как BS EN 61508. К стандартам МЭК для совместного использования с IEC 61508 относятся: IEC 61511 (перерабатывающий сектор промышленности); IEC 61513 (атомные электростанции), IEC 62061 (механическое оборудование) и IEC 6180052 (системы силовых электрических приводов с регулируемой скоростью).

Авиационные системы. RTCA, Inc. является частной некоммерческой корпорацией США, которая занимается разработкой согласованных рекомендаций по вопросам, касающимся систем связи, навигации, контроля и управления воздушным движением (CNS/ATM). RTCA функционирует как федеральный консультативный комитет, чьими рекомендациями руководствуется Федеральная администрация по авиации США (FAA) в качестве основы для принятия разных решений, в т.ч. нормативного характера. RTCA DO-178B и его фактический европейский аналог EUROCAE ED12b определяют стандарт, в соответствии с которым FAA сертифицирует программное обеспечение для использования в авиационной технике. DO-178B определяет 5 уровней критичности: уровень A — неисправимая ошибка может привести к катастрофе; уровень B — опасная ошибка, которая ухудшает безопасность или рабочие характеристики системы, снижает способность экипажа управлять воздушным судном либо причиняет пассажирам серьезные повреждения или травмы со смертельным исходом; уровень C — значительная ошибка, но ее последствия менее серьезные, чем у ошибки предыдущего уровня; уровень D — заметная, но не существенная ошибка; уровень E — ошибка, которая не влияет на безопасность функционирования воздушного судна или на работу экипажа.

Медицинские системы. Центр по контролю над оборудованием и радиационной безопасностью (CDRH) при Управлении по контролю за пищевыми продуктами и лекарственными препаратами США (FDA) производит не только проверку безопасности и эффективности медицинских приборов перед их выходом на рынок, но также отзыв и проверку существующих устройств, подозревающихся в неисправной работе. В Великобритании проверку медицинского оборудования осуществляет агентство по регулированию медицинских продуктов (MHRA). Международный стандарт IEC 62304 определяет вопросы управления каче-

ством и общие требования в отношении медицинских приборов.

Индустрия встраиваемых медицинских устройств сталкивается со множеством противоречивых требований и проблем, главными из которых являются следующие: время выхода продукции на рынок, контроль за уровнем затрат, минимизация рисков, совместимость с текущими и будущими нормативными стандартами МЭК, увеличение сроков поддержки работающих устройств и инвестиции в средства и технологии, обеспечивающие долговременную ценность. Для снижения риска использования медицинских приложений в настоящее время утверждается законодательство, обязывающее руководящих сотрудников и директоров компаний, специализирующихся на производстве лекарственных препаратов и медицинских приборов, сертифицировать оборудование. Компания несет ответственность в виде штрафа за лжесвидетельство, если вся представленная ею информация для сертификации продукта оказывается неточной или не соответствует федеральным инструкциям. В случае если в процессе эксплуатации изделия выявляются ошибочные данные или информация, вводящая в заблуждение, изготовитель подвергается штрафу в размере до 5 млн долл. Кроме того, в этом случае в отношении руководящих сотрудников предусмотрено тюремное заключение сроком до 20 лет.

Наилучшая стратегия, которой может воспользоваться производитель медицинских приборов, заключается в использовании самой передовой технологии, которую может предложить отрасль. Эта технология обеспечивает определение требований к приложению и его управлению; управление изменениями и конфигурацией; управление качеством и тестирование; моделирование и архитектуру; управление версиями и сотрудничество коллективов.

Технологии, которые обеспечивают наилучшую рентабельность инвестиций, характеризуются:

- историей об успешном применении (например, ОС, которые успешно работали в сотнях миллионов приложений);
- операционной системой (и процессором), которая отвечает требованиям приложения по стоимости, энергопотреблению, занимаемой площади и не содержит дополнительных неиспользуемых функций;
- сертифицированными операционными системами;
- точной статистикой относительно времени выхода продукции на рынок и суммарной стоимости разработки.

Железнодорожные перевозки. Европейский комитет по стандартизации в области электротехники и электроники (CENELEC) отвечает за стандарты для европейских железных дорог. Эти стандарты получают распространение в Сев. Америке и на рынке общественного транспорта. Такие стандарты CENELEC как EN 50126, EN 50128 и EN 50129, как правило, считаются приемлемыми при проведении анализа безопасности системы. EN 50126 часто называют стандартом RAMS (reliability, availability, maintain¬ability and safety — надежность, доступность, удобство обслуживания и безопасность) для железнодорожной сети. EN 50129 применяется для систем безопасности, обеспечивающих электронный контроль и защиту. EN 50128 отвечает за безопасную работу программного обеспечения в системах контроля и защиты. Стандарты EN 50128 и EN 50129 представляют собой интерпретацию серии международных стандартов IEC 61508 для указанных приложений.

Все международные стандарты программного обеспечения с особыми требованиями к безопасности включают общие элементы, применимые ко всем системам ПО независимо от конечных приложений. При всем индивидуальном отличии друг от друга все стандарты, как правило, требуют, чтобы программное обеспечение сопровождалось точным описанием планирования, проектирования, разработки, требований, верификации, управления конфигурацией и соответствия техническим условиям.

Кодом называется исходная программа, составленная разработчиком и включающая все исходные тексты приложений и системы, методику испытаний, скрипты и объектный код. Тестирование подразумевает проверку правильности функционирования кода, а также его способности выполнять поставленные задачи и удовлетворять требованиям системы. Тестирование включает покрытие кода и анализ, позволяющие убедиться в том, что все инструкции программы проверены. Наконец, также проводятся структурное, функциональное тестирование и приемосдаточные испытания. В акт испытаний входят результаты всех тестов.

Отделы разработки производителей медицинской, авиационной и промышленной техники составляют полный комплект документации для согласования со стандартами, критичными к безопасности. По сути, отделы проектирования занимаются этой работой многие годы. Однако некоторыми ее аспектами инженеры пренебрегают или затрудняются ими заниматься. Прежде всего, критичное к безопасности программное обеспечение, как правило, использует ОСРВ для контроля и управления приложением данного процессора. Вообще говоря, такие приложения выполняют несколько задач, или потоков, имеют ОСРВ с приоритетным планированием и прерыванием в реальном времени. Коммерческая ОСРВ обеспечивает эти функции с помощью интерфейса API, позволяющего сэкономить значительное время на разработку изделия.

При использовании коммерческой ОСРВ разработчику приходится удовлетворять нормативные требования к документации и тестированию программного обеспечения, созданного независимой организацией. Время, требуемое для составления всей документации по ОСРВ, может занимать существенную часть от полного процесса подготовки проекта. Более того, некоторые коммерческие ОСРВ не имеют полного исходного текста, что дополнительно затрудняет работу по составлению документации.

Заказчики компании Express Logic успешно составляют всю необходимую документацию в соответствии с требованиями государственных агентств в отношении ОСРВ ThreadX, которая применяется во многих медицинских, промышленных и авиационных приложениях. Однако этот процесс требует дополнительного времени и затрат. Для многих компаний в такой ситуации намного проще получить готовое решение, соответствующее нормативным документам. Новый пакет сертификации от Express Logic включает все проектирование ОСРВ, код, тестирование и полностью подготовленную документацию в соответствии с существующими стандартами, которая гарантированно будет утверждена управляющим агентством. Такое готовое решение снимает с разработчиков огромное бремя, позволяя им заняться собственно проектом.

По мере дальнейшего развития технологий можно ожидать, что количество критичных к безопасности требований увеличится, позволив уменьшить вероятность системных ошибок, которые могут привести к тяжелым последствиям. Вероятно, решения «под ключ» станут нормой и позволят значительно увеличить качество встраиваемого программного обеспечения.