О НОВЫХ НАПРАВЛЕНИЯХ РАЗВИТИЯ СРЕДЫ ISaGRAF: КУРС НА ПОДДЕРЖКУ ФУНКЦИОНАЛЬНО БЕЗОПАСНЫХ СИСТЕМ

С.В. Золотарев, М.Е. Кудрявцева (Компания ФИОРД)

Обсуждаются некоторые аспекты решения задачи построения функционально безопасных систем (safety system, «систем, связанных с безопасностью») с помощью технологии программирования контроллеров ISaGRAF. Системы, связанные с безопасностью, в статье трактуются в соответствии со стандартом IEC 61508 («Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»). Основное внимание уделено подходу к обеспечению возможностей функциональной безопасности применительно к ПЛК, принятом в спецификации безопасных функциональных блоков организации PLCOpen и реализованном в среде ISaGRAF.

Ключевые слова: безопасность, программирование контроллеров, функциональные блоки, ПЛК, тип данных, сертификация.

Функциональная безопасность и программное обеспечение контроллеров

Прежде чем перейти к рассмотрению конкретного технического вопроса о возможностях технологии ISaGRAF как инструмента программирования ПЛК, применяемых в приложениях, удовлетворяющих требованиям функциональной безопасности, остановимся на самом понятии функциональной безопасности. Термины «функциональная безопасность», «связанный с безопасностью» относятся к любым техническим и/или программируемым системам, отказ в которых как одиночный, так и возникший в комбинации с другими отказами или ошибками, может привести к жертвам, травмам среди людей или к ущербу для окружающей среды. Важность решения проблемы функциональной безопасности систем была остро поставлена на повестку дня в середине 70-х гг. XX века после целого ряда крупных аварий на промышленных объектах в Европе и США [1], приведших к многочисленным жертвам среди людей. Для СССР и современной России примерами таких катастроф стали аварии на Чернобыльской АЭС и на Саяно-Шушенской ГЭС.

Подчеркнем, что функциональная безопасность не является синонимом надежности, хотя и тесно связана с ним. В некоторых случаях ненадежная система может быть абсолютно функционально безопасной. Например, частые сбои в работе игровой приставки не несут никакой серьезной опасности для жизни и здоровья человека (если, конечно, не учитывать ущерб психическому здоровью), и поэтому игровая приставка может считаться вполне функционально безопасной. Термин функциональная безопасность соотносится с надежностью оборудования, обеспечивающего безопасность, и коррелирует с вероятностью правильного функционирования такого оборудования. Примерами систем, связанных с безопасностью, являются системы аварийного останова технологического процесса, блокировки опасных механизмов, железнодорожная сигнализация, управление котлом и горелками, устройства обнаружения огня и утечек. Все перечисленные системы обычно строятся с использованием ПЛК, и поэтому задача создания «безопасных» ПЛК (то есть ПЛК, удовлетворяющих требованиям систем, связанных с безопасностью) или ПЛК, поддерживающих методы обеспечения функциональной безопасности, является весьма актуальной. Очевидно, что эта задача требует адекватного решения как на аппаратном, так и на программном уровне, обеспечивая такую работу ПЛК, что даже при наихудшем стечении обстоятельств отказ должен сказываться на процессе только предсказуемым, безопасным образом (http://www.exida.com/articles/cvsplc_rev1.pdf).

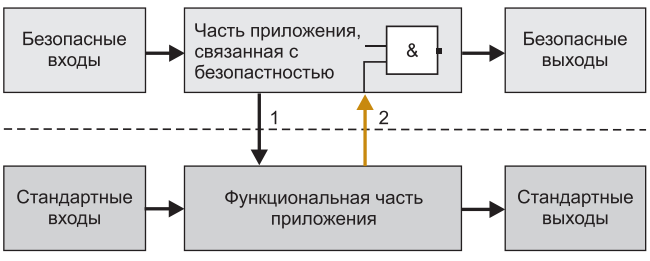
Осознание необходимости формальных требований к функциональной безопасности привели к разработке базового стандарта в рамках Международной электротехнической комиссии: IEC 61508 – «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». Соответствующая ему версия принята в России в качестве стандарта ГОСТ Р МЭК 61508. На базе IEC 61508 принят ряд отраслевых стандартов, наиболее известными из которых являются IEC 61511 «Функциональная безопасность. Безопасность приборных систем для промышленных процессов», IEC61513 «Атомные электростанции. Системы контроля и управления, важные для безопасности», IEC 62061 «Безопасность в машиностроении. Функциональная безопасность электронных и программируемых электронных систем управления машинами», IEC 60204–1 «Безопасность машин. Электрооборудование машин и механизмов», ISO 13849 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью», EN 50216

Таблица 1. Уровни полноты безопасности SIL

Уровень полноты безопасности SIL	Назначение	Фактор снижения риска	Интенсивность опасных отказов при высокой интенсивности запросов (опасных отказов в час)	Интенсивность опасных отказов при низкой интенсивности запросов (вероятность отказа)
4	Защита от общей катастрофы	от 100 тыс. до 10 тыс.	от 10^{-9} до 10^{-8}	от 10^{-5} до 10^{-4}
3	Защита обслуживающего персонала и населения	от 10 тыс. до 1 тыс.	от 10^{-8} до 10^{-7}	от 10^{-4} до 10^{-3}
2	Защита оборудования и продукции; защита от травматизма	от 1000 до 100	от 10^{-7} до 10^{-6}	от 10^{-3} до 10^{-2}
1	Защита оборудования и продукции	от 100 до 10	от 10^{-6} до 10^{-5}	от 10^{-2} до 10^{-1}

«Объекты железнодорожного транспорта. Требования и подтверждение надежности, безотказности, обслуживаемости и безопасности». Кроме того, приведем названия еще некоторых стандартов Международной организации по стандартизации ISO, IEC и EN (Европейские нормы), на которые есть ссылки в данной статье: EN 574 «Безопасность машин. Приспособления двуручного управления», ISO 12100–1 «Безопасность машин. Основные понятия, общие принципы конструирования», EN 954–1 «Техника безопасности по машинам. Элементы систем управления, обеспечивающие их безопасность. Часть 1. Общие принципы проектирования», EN 418 «Техника безопасности по машинам. Устройства аварийного отключения», IEC 61496–1 «Безопасность оборудования. Электрочувствительные защитные устройства. Часть 1: Общие требования и испытания», EN 953 «Безопасность машин. Ограждения. Общие требования к проектированию и конструированию неподвижных и перемещаемых ограждений», EN 1088 «Безопасность машин. Блокировочные устройства, связанные с защитными устройствами. Принципы конструирования и выбора», IEC 61800-5-2 «Системы силовых электрических приводов с регулируемой скоростью. Часть 5-2. Требования безопасности. Функциональная безопасность».

В стандарте IEC 61508 предложено разделять системы на четыре уровня полноты безопасности SIL (Safety Integrity Level) в зависимости от назначения и требований к приемлемому фактору снижения риска возникновения опасного отказа (таблица 1) с учетом интенсивности таких отказов. Полноту безопасности предлагается оценивать двумя способами: количественно и качественно. Качественные методы ориентированы на минимизацию так называемых «систематических» отказов (в том числе ошибок в программах) путем использования средств управления качеством, которые устанавливают требования и действия на всех стадиях жизненного цикла продукта, начиная от анализа возможных рисков, формулирования требований безопасности, и заканчивая стадией обслуживания финального продукта, его эксплуатацией и утилизацией.



Модель ПО для систем, связанных с безопасностью

В стандарте IEC 61508 определено 16 этапов жизненного цикла продуктов, связанных с безопасностью. С целью уменьшения трудозатрат на разработку и сертификацию ПО ПЛК организация PLCOpen (www.plcopen.org) предложила свой подход для одного из этих этапов – "Этап 9: Реализация. Жизненный цикл ПО, связанного с безопасностью 9.1.1. Спецификация требований к функциям, связанным с безопасностью". Таким образом, PLCOpen явным образом определила уровень своей компетенции в вопросе функциональной безопасности ПО ПЛК. Спецификация PLCOpen была реализованы в рамках технологии программирования ISaGRAF [2], а также некоторыми другими поставщиками средств программирования контроллеров.

Организация PLCOpen рассматривает ПО ПЛК, связанного с безопасностью, на системном и прикладном уровнях и выделяет адекватные им языки программирования.

1. Системное ПО ПЛК, связанное с безопасностью: встраиваемое ПО, микропрограммы или ОС. Используемые языки: C, C++, ассемблер. Это уровень языков с полной вариативностью: независимые от приложения языки, используемые для реализации микропрограмм функций безопасности, операционных систем или средств разработки. Эти языки обычно используют поставщики системного ПО и редко для реализации функций безопасности в прикладных программах. Обратим еще внимание на то, что для системного уровня приложений, связанных с безопасностью, как правило, требуется использование ОС РВ (VxWorks, Integrity, QNX Neutrino и др.), которые гарантируют детерминированное время реакции на события [3]. Системный уровень де-

тально не рассматривается в спецификации PLCOpen, а лишь выделяется.

2. Прикладное ПО ПЛК («приложение»), связанное с безопасностью. PLCopen пре длагает использовать на данном уровне усеченные версии языков программирования (с ограниченной вариативностью), инструкции и сертифицированные функциональные блоки (ФБ), например, ориентированные на целевые рынки в соответствии со стандартами IEC 62061 и ISO 13849-1. Это значительно упрощает разработку ПО и его сертификацию. Заметим, что PLCOpen не допускает включение в рассмотрение аппаратные средства, обеспечивающие функциональность подсистемы безопасности.

Модель прикладного ПО для систем, связанных с безопасностью

PLCopen предлагает собственную модель прикладного ПО для систем, связанных с безопасностью, которая базируется на описании типовой взаимосвязи ФБ. В модели (рисунок) предлагается разделять прикладное ПО ПЛК («приложение») на функциональную часть приложения и часть приложения, связанную с безопасностью. Эти части приложения могут выполняться на одном вычислительном устройстве или на двух или более отдельных, но взаимосвязанных устройствах. Обмен данными между этими частями приложения, представленный пунктирной линией, может быть реализован по сети, через систему ввода/вывода или разделяемую память, если приложения выполняются на одном устройстве. Важным требованием является отсутствие любого нежелательного влияния на часть приложения, связанную с безопасностью, со стороны функциональной части приложения. Исходя из этого требования на рисунке в левой части модели изображены два множества входов (стандартные и безопасные), в правой части – два множества выходов (стандартные и безопасные). Средние блоки символизируют две отдельные среды исполнения. Обмен разрешенными данными между частью приложения, связанной с безопасностью, и функциональной частью приложения отображается стрелками. Функциональная часть приложения имеет доступ к безопасным входам только по чтению (вертикальная стрелка 1 на рис. 1) и глобальным переменным. Небезопасные сигналы входа не могут быть подключены непосредственно к безопасным выходам (вертикальная стрелка 2 и оператор AND на рис. 1), однако они могут также подаваться на вход ФБ в части приложения, связанной с безопасностью (на рис. 1 не показано).

В целях четкого разграничения между безопасными и стандартными сигналами организацией PLCOpen предложено использовать специальный префикс – «безопасный» (SAFE) для данных, связанных с безопасностью. В частности, вводится специальный тип данных SAFEBOOL, применимый для входов/выходов внутри ПО и используемый только в части приложения, связанной с безопасностью. Выделение явным образом «безопасных» типов данных подразумевает признание того, что сигналы влияют на безопасность системы и должны рассматриваться с особой осторожностью. Исходя из этого предположения, связи между данными могут быть автоматически проверены на предмет выявления любых недопустимых связей между стандартными и безопасными сигналами. Хотя «безопасный» тип данных не может гарантировать, что действие сигнала является реально безопасным (например, в случае их неправильного подсоединения к периферии), однако этот организационный инструмент может использоваться для сведения к минимуму ошибок в приложениях. Кроме того, такой подход упрощает и сокращает верификацию потока сигналов и сертификацию продукта. Возможными средствами поддержки «безопасных» типов данных могут быть различные средства их отображения/представления (например, специальным цветом или специальным типом данных) и фактическая поддержка компилятором.

Новый тип «безопасных» данных SAFEBOOL – это тип данных, который применяется в средах, связанных с безопасностью. SAFEBOOL представляет собой более высокий уровень с точки зрения полноты (целостности) безопасности и вводит различие между переменными, связанными и не связанными с безопасностью. SAFEBOOL действует как BOOL в рамках системы, но может содержать дополнительную информацию (атрибуты), необходимую для задания состояния и уровня безопасности (например, может включать уровень производительности PL, вероятность отказа при запросе PFD, вероятность отказа в час PFH). Такая информация может использоваться для вычисления полноты безопасности SIL с помощью инструментов программирования. Существует, по крайней мере, два способа формирования переменной SAFEBOOL на уровне приложений:

1) данные предоставляются самим устройством, ОС или микропрограммой;

2) данные предоставляются путем сочетания безопасных входов в самом приложении (например, как двухканальный безопасный вход).

Системы, связанные с безопасностью, должны основываться на «негативный» логике: безопасное значение SAFEBOOL должно быть по умолчанию FALSE. Разработчики приложений должны обеспечить, чтобы все переменные SAFEBOOL приводились по умолчанию к значению FALSE, а также в значение FALSE при инициализации и после любой ошибки.

Организация PLCOpen сформулировала следующие общие рекомендации и ограничения, действующие при разработке ПО ПЛК, связанного с безопасностью:

• часть приложения, связанная с безопасностью, выполняется как единая задача, однако функциональная (не связанная с безопасностью) часть приложения может состоять из нескольких задач и выполняться на отдельном процессоре или устройстве;

Таблица 2. ФБ, связанные с безопасностью, реализованные в ISaGRAF

ФБ	Описание / (Ссылочные стандарты)
SF_Antivalent	Преобразование двух безопасных несовпадающих входов в один безопасный выход с контролем времени несовпадения (EN 954-1)
SF_EDM	Управление безопасными выходами и мониторинг контролируемых исполнительных механизмов: контролируемая остановка с сохранением подвода питания к исполнительным механизмам (IEC 60204-1, EN 954-1, ISO 12100-2)
SF_EmergencyStop	Мониторинг кнопки аварийной остановки и запуска аварийной остановки (EN 418, EN 954-1, ISO 12100-2, EN 60204-1)
SF_EnableSwitch	Оценка сигналов от трехпозиционного переключателя (IEC 60204-1, EN 954-1, ISO 12100-2)
SF_Equivalent	Преобразование двух безопасных эквивалентных входов в один безопасный выход с контролем времени несовпадения (EN 954-1)
SF_ESPE	Мониторинг электрочувствительного защитного устройства (IEC 61496-1, EN 954-1, ISO 12100-2)
SF_GuardLocking	Управление блокирующим защитным ограждением с четырьмя состояниями защитного ограждения (EN 953, EN 1088, EN 954-1, SO 12100-2)
SF_GuardMonitoring	Мониторинг блокирующего защитного ограждения с двумя переключателями и контролем времени (EN 953, EN 1088, EN 954-1, ISO 12100-2)
SF_ModeSelector	Выбор режима работы системы (ручного, автоматического и др.) (MRL 98/37/EC, Annex I, EN ISO 12100-2, IEC 60204-1, EN 954-1, ISO 12100-2)
SF_MutingPar	Управление функциями безопасности с использованием параллельного отключения с четырьмя датчиками отключения (IEC 61496-1, IEC 62046, EN 954-1, ISO 12100-2)
SF_MutingPar_2Sensor	Управление функциями безопасности с использованием параллельного отключения с двумя датчиками отключения (IEC 61496-1, IEC 62046, EN 954-1, ISO 12100-2)
SF_MutingSeq	Управление функциями безопасности с использованием последовательного отключения с четырьмя датчиками отключения (IEC 61496-1, IEC 62046, EN 954-1, ISO 12100-2)
SF_OutControl	Контроль безопасного выхода с помощью сигналов безопасности и сигнала прикладной части приложения (EN 954-1, ISO 12100-2, EN 60204-1)
SF_SafelyLimitedSpeed	Активация мониторинга безопасного уменьшения скорости (IEC 61800-5-2, EN 954-1, ISO 12100-2, EN 60204-1)
SF_SafeStop1	Начало контролируемой остановки (IEC 60204-1, Категория 1)
SF_SafeStop2	Начало контролируемой остановки (IEC 60204-1, Категория 2)
SF_SafetyRequest	Установка привода в безопасное состояние (EN 954-1, ISO 12100-2, EN 60204-1)
SF_TestableSafetySensor	Обнаружение сигналов потери значения датчика, превышения времени отклика или статического «ВКЛ» (IEC 61496-1, EN 954-1, ISO 12100-2)
SF_TwoHandControlTypeII	Функциональность двуручного управляющего устройства (EN 574, Section 4, Type II).
SF_TwoHandControlTypeIII	Функциональность двуручного управляющего устройством (EN 574, Section 4, Type III).

• часть приложения, связанная с безопасностью, не должна прерываться функциональной частью приложения;

• после запуска цикла приложения, связанного с безопасностью, все значения соответствующих входных данных должны быть актуальными и стабильными в течение всего цикла.

• выходы, связанные с безопасностью, не могут быть напрямую изменены функциональной частью приложения;

• в программе, связанной с безопасностью, рекомендуется использовать сертифицированные ФБ, например, как определено в спецификации PLCOpen. Пользователь, таким образом, может добиться более высокого уровня защиты (предотвращения) от ошибок;

• ФБ, связанные с безопасностью, должны реализовываться на языке функциональных блоковых диаграмм FBD и лестничных диаграмм LD стандарта IEC 61131–3, в то время как содержимое функциональной части приложения (в том числе ФБ) может реализовываться на любом другом языке программирования (например, ST стандарта МЭК 61131–3, C) или даже в микропрограммах, или аппаратном обеспечении;

• каждый ФБ в части приложения, связанной с безопасностью, должен включать общедоступную информацию: автор, дата создания и выпуска, версия, история версий и функциональное описание (включая параметры вывода). Эта информация отображается во время сертификации, разработки и изменении программы и может быть частью ФБ или указываться, например, в виде гиперссылки.

Кроме общих рекомендаций, относящихся ко всем программным приложениям, PLCOpen выделяет три уровня приложений и соответствующие им рекомендации и ограничения с точки зрения сертификации на соответствие требованиям функциональной безопасности: базовый, расширенный и системный уровень. Для базового уровня фундаментальный подход заключается в том, что программа, связанная с безопасностью, состоит только из сертифицированных ФБ, которые могут «соединяться» друг с другом в графической форме. Программы, составленные из этих ФБ, имеют четкую структуру и легко читаются. Кроме того, время вывода на рынок таких программ значительно сокращается, так как они состоят из блоков, сертифицированных заранее. Рас-

ширенный уровень требуется в случае осуществления проектов, для которых текущий набор сертифицированных ФБ недостаточен, и пользователь может сам создавать требуемые блоки (или даже программы). Для этого ему предоставляется диапазон расширенных команд. Однако валидация функциональности для этих блоков и программ может быть значительно более сложной и потребует больше времени, так как в основе этого лежит трудоемкая сертификация всего процесса. Системный уровень должен использоваться поставщиками средств контроля безопасности. Системный уровень, как правило, реализуется специальными средствами на базе ОС РВ, однако он не является частью спецификации PLCOpen (а лишь выделяется как отдельный уровень).

Стандарт IEC 61508, часть 7 определяет ограничения в предпочтительных языках программирования для различных уровней полноты безопасности SIL (в терминах "Весьма рекомендованные", «Рекомендованные» или «Не рекомендованные»). Рекомендованные PLCOpen графические языки FBD и LD обеспечивают четкое представление о самой программе, связанной с безопасностью, и инструментальные средства с их использованием могут обеспечивать гораздо более высокий уровень поддержки и сопровождения для пользователей. Они формируют основу для упрощенной эксплуатации программ, связанных с безопасностью. Структурированный текст (ST), список инструкций (IL) и язык последовательных функциональных схем (SFC) не рассматриваются PLCOpen на данный момент, так как они требуют более высоких затрат на поддержку в процессе жизненного цикла. Говоря более конкретно, тестирование и валидация приложений, написанных на ST или IL, является более сложной задачей, чем для приложений на графических языках. Эта рекомендация относится к базовому и расширенному уровню. Для системного уровня рекомендации для языков, функций и типов данных отсутствуют.

PLCOpen предлагает ввести ограничения на типы данных в зависимости от уровня приложения для базового и расширенного уровней. Имеется поле, указывающее на то, разрешен элемент или не разрешен (http://www.plcopen.org/pages/tc5_safety/specifications).

Типы данных, отличные от SAFEBOOL, могут, кроме того, иметь атрибут "safe", например, SAFEINT, для того чтобы разрешить автоматически отслеживать безопасные данные.

В целях детализации возможностей базового уровня приложений организацией PLCOpen было предложено 19 «безопасных» ФБ, которые в полном объеме реализованы в ISaGRAF (табл. 2). Для каждого из «безопасных» ФБ в спецификации PLCOpen приводится подробное и краткое описание интерфейса, перечень ссылочных стандартов, описание функционирования в текстовой и графической форме (детальный граф состояний), временные диаграммы, включая стадии нормальной работы и поведения в начальной стадии, описание ошибок и способы их выявления, работу ФБ при возникновении ошибок, коды состояний и диагностики ФБ.

Организация PLCOpen предложила такую концепцию диагностических кодов, которая является универсальной для всех ФБ, связанных с безопасностью, Детальная информация о внутренней или внешней ошибке ФБ может быть получена с помощью значений DiagCode, которые образуют единую систему диагностики вне зависимости от поставщика ПО. Кроме того, разрешено добавлять собственные дополнительные сведения в значение выхода DiagCode. Например, значение DiagCode 8002hex означает, что ФБ активирован, зафиксирован запрос к функции безопасности и в результате выполнения ФБ безопасный выход будет установлен в значение TRUE.

В ISaGRAF полностью реализована концепция диагностических кодов.

Перспективы расширения поддержки технологии ISaGRAF в области систем, связанных с безопасностью

В целях расширения поддержки технологии ISaGRAF в области систем, связанных с безопасностью, в декабре 2011 г. компания ISaGRAF Inc. анонсировала вывод на рынок платформы FlexiSafe на основе технологии ISaGRAF и стандартов IEC 61508 и ISO 13849. Платформа FlexiSafe предназначена для облегчения сертификации OEM-производителями средств промышленной автоматизации в соответствии со стандартами IEC 61508 на уровне SIL3 или ISO 13849 на уровне PLe. Платформа FlexiSafe ориентирована на разработку систем, которые поддерживают распределенные приложения, совмещающие безопасную и небезопасную функциональность, расширенное управление безопасностью и средства управления жизненным циклом приложений. (http://www.fiord.com/images/industry_avt/soft/isagraf/FlexiSafe-flyer.pdf). FlexiSafe обеспечит основные элементы, необходимые для сертификации: сертификат SC3 (Systematic Capability уровня 3) стандарта IEC 61508 в редакции 2010 г., технологию встраиваемого ПО, которая может быть перенесена на любую «безопасную» ОС, включающую набор инструментов валидации и верификации, 100% тестовые отчеты по различным инструкциям TIC-кода, выполненные независимыми организациями, средства верификации кода приложения (разнообразные компиляторы), другие инструменты, помогающие сертификации конечным пользователем функций безопасности, зависящие от концепции безопасности приложений (PLCopen Safety Function Blocks, Cause and Effect Diagram, Static Checker, Version Source Control, Cross-Reference Browser, Dependency Tree,..)

С точки зрения безопасности платформа FlexiSafe позволяет многократно использовать результаты сертификации применительно к различным аппаратным платформам, упрощает разработку и сер-

тификацию приложений конечного пользователя, допускает сертификацию резервированных конфигураций. FlexiSafe предлагает следующий подход к сертификации:

• портирование сертифицированной исполнительной среды на целевую аппаратную платформу и ОС (принимая во внимание FlexiSafe и руководство по безопасности ОС);

• некоторые средства оценки мер безопасности, включенные в исполнительную среду;

• сервисы проверки портирования, использующие «строгий» системный слой и всеобъемлющий набор тестового покрытия;

• не требуется 100% тестирование приложения конечного пользователя (только функциональные тесты);

• приложения конечного пользователя могут использовать преимущества всех языков стандарта IEC 61131–3, включая SFC;

• отсутствие ограничений на использование ФБ;

• интегрированное управление безопасностью и средствами жизненного цикла приложений, соответствующее стандартам IEC 61508 и ISO 13849.

С точки зрения требований стандарта IEC 61508, верификация и валидация ядра ISaGRAF в рамках FlexiSafe основана на допустимом в IEC 61505 подходе – «доказано практикой». ISaGRAF используется в условиях реальной эксплуатации в течение 14 лет в составе 850 тыс. исполнительных систем в ответственных промышленных приложениях, требующих обеспечения безопасности. Обеспечена инкапсуляция функций безопасности: оболочка ISaGRAF строится вокруг функциональности, которая проверяет правильность и безопасность функционирования. Портируемое тестовое окружение обеспечивает корректную функциональность и отсутствие побочных эффектов, сочетает Black-box и White-box испытания, покрывающие все операции ядра (I/O, обновления, и т.д.) и каждую инструкцию TIC-кода.

Отметим еще тот факт, что компания ISaGRAF Inc. в конце 2011 г. стала участником программы Wind River Partner Validation Program. Компании Wind River и ISaGRAF Inc. будут сотрудничать на рынках энергетики, транспорта и управления процессами с помощью решения для систем, связанных с безопасностью, и состоящего из платформы Wind River VxWorks Cert и ISaGRAF FlexiSafe. Wind River – это первый поставщик сертифицированной ОС, который предлагает решение на уровне SIL3. В соответствии с соглашением ISaGRAF Inc. будет интегрировать и сертифицировать FlexiSafe в среде платформы Wind River VxWorks Cert, являющейся коммерческой ОС РВ для критически важных приложений, связанных с безопасностью, и которые должны быть сертифицированы по строгим требованиям IEC 61508 и другим стандартам ПО. В частности, комбинация платформы VxWorks Cert и среды ISaGRAF будет сертифицированной по уровню SIL3 стандарта IEC 61508, предлагая промышленным компаниям проверенные и испытанные решения, обеспечивая сокращение времени вывода на рынок их собственных продуктов, а также снижение расходов на разработку и техническое обслуживание.

Список литературы

1. *Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон.* Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 с связанных с ним стандартов. М.: Издательский дом «Технологии». 2004.
2. *Колтунцев А.В., Золотарев С.В.* Стандарт IEC 61499 и система программирования контроллеров ISaGRAF 5: от теории к практике//Rational Enterprise Management. 2009. № 2.
3. *Синенко О.В., Золотарев С.В.* Современные ОС РВ для перспективной авионики//Военный парад. 2006. № 6.

Золотарев Сергей Викторович *– канд. техн. наук, ведущий эксперт,*
Кудрявцева Марина Евгеньевна *– менеджер направления программных средств компании ФИОРД.*
Контактный телефон (812) 323-62-12.
E-mail: info@fiord.com
http://www.fiord.com, www.isagraf.ru, www.fit-pc.ru

Оборудование Schneider Electric обеспечивает автоматизацию и электроснабжение знаменитой "Россиянки"

Компания Schneider Electric – мировой эксперт в области управления электроэнергией и промышленной автоматизации – поставила оборудование для автоматизированной системы управления ТП и систем распределения электроэнергии 0,4 кВ и 6 кВ доменной печи (ДП) № 7 Новолипецкого металлургического комбината (г. Липецк). Пусконаладочные работы успешно завершены. Оборудование Schneider Electric применяется на всех объектах комплекса доменной печи "Россиянка" для реализации задач АСУТП и позволяет обрабатывать до 50 тыс. технологических параметров всего комплекса печи.

"Россиянка" – первая доменная печь, построенная в нашей стране за последние 25 лет, а также наиболее важный объект Программы технического перевооружения НЛМК на период до 2012 г. После ввода в эксплуатацию ДП-7 даст самый значительный со времен СССР разовый прирост по выплавке чугуна в стране на отдельном предприятии – на 30%, что также обеспечит рост выпуска стали на НЛМК на 36%, до 12,4 млн. т/г.

На объектах ДП "Россиянка" установлено следующее оборудование Schneider Electric:

– ПЛК Quantum (в том числе с горячим резервированием), Premium (в том числе с функциями весоизмерения и весодозирования), M340 и Advantys STB;

– ПО: Unity Pro, Vijeo Citect, Vijeo Designer;

– промышленные компьютеры, панели оператора Magelis;

– сетевое оборудование ConneXium и др.;

– преобразователи частоты Altivar, устройства плавного пуска Altistart;

– коммутационная и пускорегулирующая аппаратура: Masterpact, Compact NSX, Multi (Acti) 9, Tesys U, Tesys T и др.;

– оболочки и шкафы Prisma+ и Sarel.

Http://schneider-electric.ru