О РАЗВИТИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОНТРОЛЛЕРОВ

И.В. Петров (ООО «ПК Пролог»)

Сформулированы ключевые направления развития ПО контроллеров. В отдельную группу вынесены вопросы защиты и безопасности ПО контроллеров. Выявлен парадокс автоматизации: чем дешевле контроллер мы хотим изготовить, тем дороже его разработка и сопровождение.

Ключевые слова: ПО контроллеров, кибербезопасность, парадокс, средства коммуникации, Industry 4.0.

В последние 17 лет компания «ПК Пролог» сконцентрировала свои усилия на инструментальном программном обеспечении для ПЛК. Основной продукт — это комплекс программирования ПЛК CODESYS [1, 2]. Перед разработчиками контроллеров стоит задача установки CODESYS на вновь создаваемые линейки продукции, ориентированные на задачи завтрашнего дня. В эти проекты специалисты ООО «ПК Пролог» погружаются достаточно глубоко. В прошлом году проводились совместные работы с компаниями из России, Германии, Франции, Италии и Бразилии. В этих новых разработках прослеживаются общие тенденции развития ПЛК и, прежде всего, их программного обеспечения.

Очевидно, информационные технологии стали частью нашей повседневной жизни. Многие вещи стали привычными и обыденными. Естественно, люди хотят их использовать и в контроллерах. Наличие в ПЛК встроенной памяти, функции работы с файлами, многозадачность, работа по сети с верхним уровнем управления, удаленная настройка, графический интерфейс — эти характеристики даже не указываются в технических требованиях, они перешли в раздел «по умолчанию». При разработке контроллера обсуждаются только тонкости, например, какая визуализация нужна в типовых применениях (встраиваемая, Web, 3D анимация) (рис. 1). В настоящее время наблюдается активное применение Internet технологий в контроллерах.

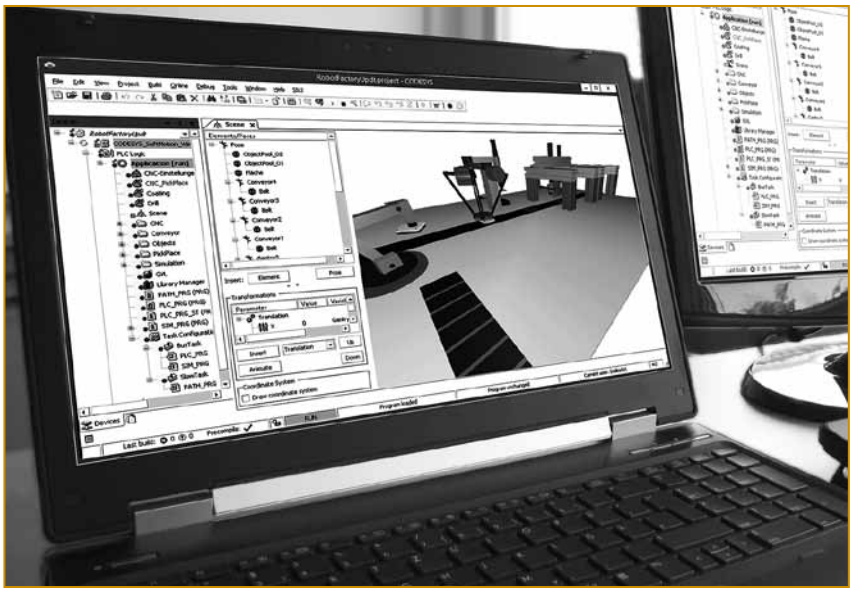

Рис. 1. 3D визуализация, реализованная в CODESYS

В целом, применение ИТ расширяет круг применений контроллеров, упрощает их обслуживание, снижает стоимость. Это происходит за счет применения массовых аппаратных, программных модулей и общедоступных коммуникационных устройств.

С другой стороны, это вызывает некоторые новые проблемы, с которыми ранее специалисты по контроллерам не сталкивались. Прежде всего, это разделение ресурсов и обеспечение надежности управляющих программ ПЛК при сбоях встроенных ИТ-компонентов, технические и организационные вопросы кибербезопасности.

В новых российских контроллерах традиционный Modbus RTU присутствует, поскольку этот интерфейс практически доминирует в отечественных ключевых отраслях. В новейших зарубежных контроллерах наличие RS-485 — это уже опция. В каждом новом ПЛК обязательно есть один или несколько портов Ethernet. Он заменил собой последовательный порт при программировании контроллеров, при работе с HMI и SCADA. Ethernet сети реального времени (EtherCAT, Profinet, Powelink) упорно вытесняют последовательные интерфейсы на полевом уровне.

Ключевые направления развития ПО контроллеров

Первое — это обеспечение гибкости применения контроллеров. Как бы мы не старались, мы не можем сегодня заранее предусмотреть всю функциональность, которая может потребоваться конкретному заказчику. Например, ему может потребоваться подключить к ПЛК специализированный считыватель радиометок. Скорее всего, изготовитель такого устройства ориентируется на подключение его к компьютеру. Он снабжает его соответствующим интерфейсом и драйвером. При наличии в контроллере ОС можно использовать готовый драйвер. Поддержать же подобное устройство программно с нуля трудоемко и не всегда возможно, поскольку его изготовитель может просто закрыть свои ноу-хау.

Второе направление — это обеспечение удобных средств диагностики и обслуживания систем автоматики при их эксплуатации. Например, наладчик может работать с оператором SCADA-системы

по телефону или использовать локальный современный графический ЧМИ. Очевидно, что второй вариант гораздо эффективнее, быстрее и безопаснее. Все больше ПЛК имеют графический дисплей или оснащаются Web-интерфейсом.

Первое и второе направления привели к тому, что практически на всех новых контроллерах устанавливается полноценная ОС, наличие которой на порядок упрощает разработку и сопровождение всех уровней ПО контроллеров.

Третье направление развития — это средства качественной, удобной и надежной разработки прикладных программ для контроллеров. Безусловно, это направление включает средства диагностики, автоматического сканирования и настройки систем ввода/вывода. В программирование контроллеров приходят молодые ИТ специалисты. Они знакомы с технологией объектно-ориентированного программирования (ООП), современными системами управления версиями, командной работы, инструментами анализа и тестирования ПО. Поэтому разработчики CODESYS были вынуждены оснастить комплекс целым рядом дополнительных встроенных функций и отдельных специализированных инструментов, ориентированных на профессиональных программистов. Сюда же можно отнести дополнительный язык программирования, UML диаграммы состояний, диаграммы классов (ООП), средства интеграции с математическими пакетами.

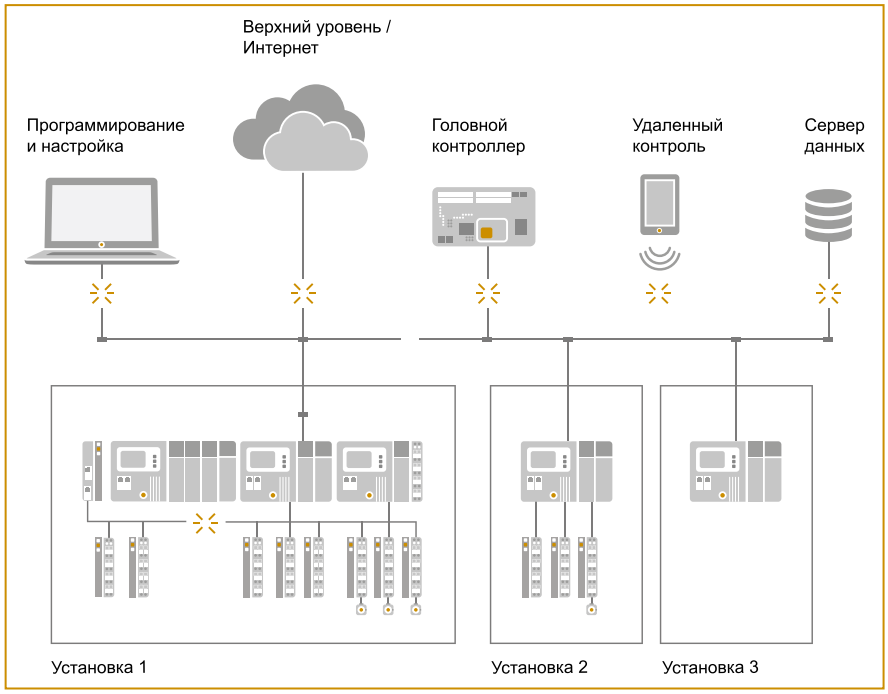

Рис. 2. Места уязвимости контроллеров

Четвертое направление — это средства быстрой разработки типовых проектов как для программистов, так и для технологов. Так в CODESYS появился Application Composer. Это инструмент, позволяющий составлять программы для типовых объектов без программирования вообще. Программа для контроллера генерируется автоматически. К этому направлению можно отнести обучающие модули, специализированные библиотеки и примеры прикладных программ. Многие пользователи CODESYS обладают уникальными знаниями и опытом. Они готовы ими поделиться бесплатно либо предложить готовые решения на коммерческой основе. Для этого был создан Internet магазин CODESYS Store. На сегодняшний день в нем уже доступны сотни полезных примеров и программных модулей, ускоряющих разработку прикладных приложений.

Пятое новое направление — это Industry 4.0. Пока нет четкого определения его границ. На практике, передовые изготовители контроллеров и ПО иногда придумывают совершенно новую функциональность, способы применения которой пока туманны и не подтверждены никакой практикой. Естественно, привередливый пользователь спрашивает: «Что это?». Менеджер по маркетингу поправляет галстук, делает умное лицо и отвечает: «Это Industry 4.0 — технологии будущего!». Если серьезно, то данное направление включает сегодня оснащение контроллеров новыми коммуникационными протоколами, например, OPC UA, интеграцию с Internet, средствами автоматического обслуживания оборудования и обновления ПО, интеграцию с CAD.

Средства безопасности и защиты

Далее прервем нумерацию, поскольку следующее направление является новым, но по актуальности его можно поставить на первое место. Это средства безопасности и защиты. Они делятся на две группы. Первая — это защита хорошего человека от опасной техники. На Европейских выставках на стендах любого изготовителя контроллеров обязательно присутствуют надписи «SIL2» или «SIL3» крупными буквами.

Вторая группа — это защита хорошей техники и процессов от опасных людей. Кибербезопасность контроллеров — сегодня горячая тема. Именно ей была посвящена российская конференция CODESYS в 2017 г. (рис. 2).

За последний год в CODESYS стали доступны некоторые компоненты для обеспечения безопасности. Их наличие само по себе не дает ничего. Их необходимо знать и использовать. Стандарты IEC 62443 вводят четыре уровня. Уровень 1 — это ошибки в работе оборудования и обслуживания. Уровень 2 — это угрозы внешних воздействий простыми средствами (например, подбор пароля). Уровень 3 — это угрозы внешних воздействий специальными инструментами (хакерскими). Уровень 4 — это применение ки-

бероружия, точно нацеленного на конкретный объект, на основе предварительно собранных данных. Новые программные компоненты CODESYS при их правильном применении закрывают второй и третий уровень. К ним относятся:

— кодирование исходных текстов прикладных программ и система их администрирования с парольной защитой;

— авторизация подключения к контроллеру;

— кодирование и цифровая подпись кода ПО контроллера;

— защита от изменения копирования кода прикладной программы аппаратным ключом;

— резервное копирование и восстановление ПО контроллера;

— защищенный протокол связи с контроллером для отладки и визуализации (на базе сертификатов X.509);

Еще один эффективный подход состоит в жестком контроле коммуникаций ПЛК и администрировании допустимых команд, которые контроллер будет выполнять в определенных режимах работы. Данный подход практически реализован в Kaspersky Security System (KSS) российской компании «Лаборатория Касперского». На его основе компанией BE.services GmbH (Германия) и при участи «ПК Пролог» разработан пакет Embedded Security Shield (ESS) для CODESYS. Он включает специальные компоненты ПО контроллера и конфигуратор, встраиваемый в среду программирования CODESYS. Пакет ESS уже успешно интегрирован в контроллере (RTU) компании Altus (Бразилия).

Парадокс современной автоматизации

Бурное развитие ПО контроллеров привело к интересному парадоксу. Допустим, требуется создать максимально дешевый контроллер. Логично выбрать самое дешевое и простое процессорное ядро, например, на базе ARM Cortex M3 с минимальным объемом памяти. Возникает задача установить на него нужное ПО. Полноценная ОС на него не встанет. Поставить систему МЭК программирования можно. Однако необходимо будет очень тщательно изучить задачи потенциальных заказчиков, отсечь «лишнее», определить четко нужную функциональность, написать под нее «нижний» уровень и втиснуть в имеющиеся аппаратные ресурсы. На практике это выливается в длительную работу (год и более). Последующее сопровождение такого контроллера требует постоянной работы команды специалистов, которым нужно постоянно платить зарплату. Если же мы поставим более мощный процессорный модуль, оснащенный достаточным объемом памяти и ОС, например Linux, то установка CODESYS Control выполняется за пару дней. Мы, не задумываясь, разрешаем всю существующую в CODESYS Control функциональность по умолчанию. Последующее обновление системного ПО в этом случае производится очень просто. Аппаратно более мощный контроллер оказывается дешевле при объемах производства до нескольких тысяч единиц.

Дорога к истине вымощена парадоксами.
Оскар Уайльд

Получаем парадокс: чем дешевле контроллер мы хотим изготовить, тем дороже его разработка и сопровождение.

Современный контроллер на 80% — это программный продукт. Поэтому, говоря о развитии контроллеров, мы в первую очередь говорим о его программном обеспечении.

Список литературы

1. *Петров И.В.* Упрощенные инструменты МЭК программирования – удел пользователя ПЛК? // Автоматизация в промышленности. 2006. №4.
2. *Петров И.В.* CoDeSys – повседневный инструмент программиста ПЛК // Автоматизация в промышленности. 2012. №8.

Петров Игорь Викторович *– ООО «ПК Пролог».*
Контактный телефон (481-2) 38-29-31.
E-mail:info@prolog-plc.ru
Http://www.prolog-plc.ru

Евразийский инжиниринговый центр по станкостроению будет создан на площадке МГТУ "СТАНКИН" в Москве

По решению стран Евразийского экономического союза (ЕАЭС) Евразийский инжиниринговый центр по станкостроению (ЕИЦС) — совместный центр государств-членов — будет располагаться на площадке МГТУ "СТАНКИН" в Москве. Учредителями ЕИЦС выступят организации четырех стран Евразийского экономического союза — Армении, Беларуси, Казахстана и России. ЕИЦС станет центром развития станкоинструментальной отрасли в Союзе. Его деятельность будет направлена на формирование и внедрение инновационных решений в промышленное производство для содействия переходу стран ЕАЭС к новому технологическому укладу.

Предполагаемая функциональность центра позволит решать целый ряд вопросов отрасли в рамках Союза: сформировать долгосрочный прогноз развития отрасли станкостроения, обеспечить прозрачность закупок станочного оборудования путем подготовки заключений о наличии производства его аналогов на территории ЕАЭС, повысить качество выпускаемого оборудования путем содействия созданию испытательных лабораторий и сертификационных центров в Союзе. Работа центра также нацелена на внедрение современных инновационных технологий мирового уровня в производственные процессы машиностроительных предприятий государств-членов, что обеспечит повышение конкурентоспособности этого сектора промышленности.

Http://www.eurasiancommission.org