# Подход к созданию программно-аппаратных комплексов для построения систем, важных для безопасности

**Мякишев Д.В., Тархов Ю.А., Столяров К.А., Наконечный С.В., Столяров С.А.**
**НПП "Комплексы и системы"**

*Рассматриваются общие требования при создании программно-аппаратных комплексов, важных для безопасности, и методы, направленные на их выполнение. Рассматривается применение этих методов на примере создания ПТК "Шкаф базовый сбора и обработки сигналов".*

Появление новых технологий изменило представление о системах, важных для безопасности. Желание повысить качество управления, снизить риск аварий, создать более экономичные режимы эксплуатации за счет совершенствования алгоритмов управления привело к тому, что в настоящее время существует потребность в различных ПТК, помогающих решать узкоспециализированные задачи. Применение новых средств вычислительной и электронной техники, сетевых средств, ПО позволяет повысить качество будущих систем и снизить их стоимость.

В силу особенностей выполняемых задач к системам, важным для безопасности, и их компонентам предъявляются определенные общие требования, характеризующие их технические и экономические качества. По мнению авторов, наиболее важными требованиями являются *информационная безопасность, технологическая независимость и лицензионная (патентная) чистота* (рис. 1).

При создании программно-аппаратных комплексов как компонентов будущих систем *информационную безопасность* следует рассматривать в аспекте обеспечения выполнения всех заложенных в них функций по сбору, обработке и обмену данными и отсутствия "недокументированного" поведения. В настоящее время существует несколько документов, описывающих более детально это требование. Так, например, в документе NUREG/CR-6463 [1] определены четыре основных атрибута качества ПО систем, важных для безопасности: надежность, отказоустойчивость, прослеживаемость и сопровождаемость. Эти общие требования приобретают более четкие очертания в стандартах IEC 60880 [2] и IEC 61508-3 [3]: повторное использование модулей, самоконтроль, обработка сбоев и т.д.

| Технологии / Требования | открытые стандарты и спецификации | открытые исходные коды ПО | методы разработки ПО |
|---|---|---|---|
| информационная безопасность | + | + | + |
| технологическая независимость | + | — | — |
| лицензионная (патентная) чистота | + | + | — |

*Рис. 1. Влияние используемых технологий на выполнение общих требований*

Необходимость поддержания работоспособности систем, важных для безопасности, в течение длительного времени приводит к еще одному требованию, которое нужно учитывать при разработке – *технологическая независимость*. На практике это означает отказ от использования импортных компонентов и ориентацию на отечественного производителя. Очевидно, что следование этому принципу экономически и политически целесообразно, особенно в такой ответственной области, как атомная энергетика. К сожалению в современных условиях при создании и модернизации автоматизированных систем, использующих средства вычислительной техники, полной технологической независимости достичь не удается. Реальным компромиссом в данной ситуации является применение, где это необходимо, импортной комплектации (микросхем, разъемов и т.д.), при этом сборочные единицы (электронные модули, приборы, устройства) изготавливаются исключительно на российских предприятиях.

Не менее важным фактором, позволяющим оценить разрабатываемый комплекс, является его *лицензионная чистота*. Она влияет не только на стоимость будущих изделий, но и на область возможного применения как комплекса, так и систем, в которые он входит.

Для выполнения вышеуказанных требований, предъявляемых при создании и модернизации программно-аппаратных комплексов, предлагаются следующие пути:

– применение открытых стандартов и спецификаций;

– использование открытых исходных кодов ПО;

– применение методов разработки ПО, направленных на достижение определенных качественных характеристик продукта.

Одним из способов уменьшения технологической зависимости является проектирование оборудования на основе открытых стандартов и спецификаций. Из-за своей доступности эти стандарты и спецификации прошли многолетнюю проверку и получили широкое распространение среди производителей. Такая ситуация позволяет иметь выбор между поставщиками, тем самым уменьшая зависимость от конкретного производителя.

*Человеку свойственно ошибаться, но производственным процессам не свойственно прощать эти ошибки...*
Журнал "Автоматизация в промышленности"

В то же время применение открытых стандартов при проектировании компонентов оборудования и организации взаимодействия между ними позволяет придать системе такое немаловажное свойство, как *масштабируемость*. Это позволит в будущем расширять состав компонентов и функций, используя имеющийся задел, таким образом сохраняя вложенные инвестиции.

Необходимым этапом создания системы, важной для безопасности, и ее отдельных компонент является *верификация* и *валидация*, подтверждающие соответствие ПО и системы в целом поставленным требованиям. Это возможно только при наличии исходных кодов программ, позволяющих провести их детальный анализ и подтвердить возможности системы.

Применение открытых стандартов и спецификаций и наличие открытых программных кодов, не защищенных патентами и лицензиями отдельных фирм, обеспечивает *лицензионную чистоту* создаваемого программно-аппаратного комплекса.

Однако открытость исходных кодов – условие необходимое, но не достаточное для обеспечения информационной безопасности. Необходимо использовать современные методы разработки ПО, позволяющие придать определенные свойства конечному изделию. Следует отметить, что международные стандарты IEC 60880 [2] и IEC 61508-3 [3] предъявляют вполне определенные требования к методам создания ПО систем, важных для безопасности. В соответствии с этими стандартами метод проектирования должен способствовать модульности, инкапсуляции и детальной спецификации. На рис. 2 представлены взаимосвязи требований, предъявляемых по стандартам IEC 60880 [2] и IEC 61508-3 [3], и их влияние на свойства создаваемого ПО.

Очевидно, что на этапе проектирования комплексов общие подходы, направленные на выполнение предъявляемых требований, должны приобретать более четкие очертания в виде конкретных программных и аппаратных решений. При этом необходимо учитывать специфику применения комплексов.

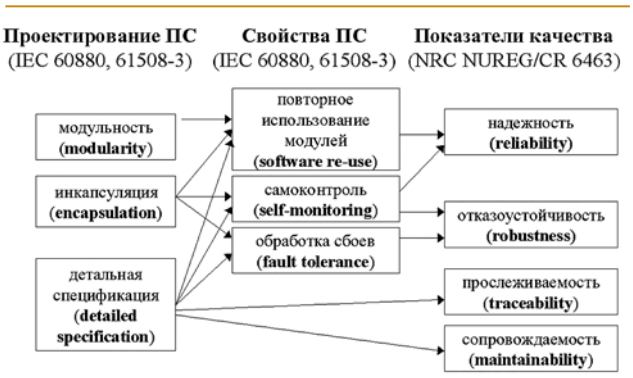


*Рис.2. Взаимосвязи требований, предъявляемых к ПО КСУ*

Одними из открытых стандартов, использование которых позволяет придать комплексу требуемые свойства, являются *системная шина VMEbus* (IEC 821) и "*Евромеханика*" (IEC 297). Их использование при создании комплексов позволяет организовать высоконадежный асинхронный протокол обмена данными, обеспечивающий работу в "жестком" РВ и обеспечить высокую степень механической прочности и возможность эксплуатации в жестких условиях (вибрация, удары и т.п.).

Следует отметить, что при непрерывном развитии стандарта IEC 821 в сторону улучшения производительности и других эксплуатационных характеристик сохраняется совместимость "снизу-вверх" для всех разработанных ранее изделий.

*Архитектура процессоров Intel 80×86/Pentium* также "де-факто" является открытым стандартом. Благодаря этому в настоящее время Intel-совместимые процессоры и компьютеры на их основе вот уже много лет лидируют на мировом рынке. Соответственно, по объему, разнообразию типов и степени отработанности ПО данный вид процессоров также не имеет себе равных. Это значительно повышает интегральную надежность компьютеров и систем, делает их эксплуатацию более простой и безопасной. Следует подчеркнуть, что с точки зрения технологической независимости применение процессоров данного вида является наименее рискованным, т.к. кроме самой фирмы Intel программно-совместимые процессоры выпускаются еще рядом производителей. То же можно сказать и о вспомогательных наборах микросхем, микросхемах памяти, других элементах, необходимых для создания законченных устройств. Это позволяет избежать зависимости от одного производителя (поставщика).

Очевидно, что при разработке ПО комплекса желательно использовать ранее созданный программный код, прошедший длительное тестирование в различных системах. Это способствует не только сокращению сроков разработки, но и повышению качества создаваемого продукта. При этом выборе необходимо учитывать открытость исходных кодов и их *лицензионную чистоту*. Примером таких программных средств является ядро ОС *Linux*. Следует отметить, что в настоящее время производители микросхем, как правило, сами выпускают драйвера для ядра *Linux*.

В то же время при создании ПО комплекса, как правило, необходимо разрабатывать новый программный код, обеспечивающий выполнение специфических задач, возлагаемых на комплекс. При этом необходимо учитывать требования стандартов IEC 60880 [2] и IEC 61508-3 [3]. Одними из таких


*Рис.3. Влияние предлагаемых методов на свойства ПО КСУ*

программных подходов, направленных на достижение требуемых свойств, являются *метод проектирования на основе базовых структур* [4] и *метод контрактного проектирования* [5]. Применение этих методов при создании нового ПО способствует улучшению таких характеристик, как надежность, отказоустойчивость, прослеживаемость и сопровождаемость [6] (рис. 3).

Выше описанный подход к разработке комплексов, используемых при создании систем, важных для безопасности, был использован при создании ПТК "Шкаф базовый сбора и обработки сигналов" (ПТК ШБ СОС) в ОАО "Электромеханика" (г. Пенза).

Основу ПТК ШБ СОС представляет собой программируемый контроллер, выполняющий функции приема дискретных и аналоговых сигналов, обработки полученных данных, выдачи аналоговых и дискретных сигналов управления на исполнительные механизмы и обмена технологической информацией с другими комплексами по цифровым каналам связи.

Ядром контроллера является электронный модуль центрального процессора (ЭМЦП), осуществляющий взаимодействие с модулями ввода/вывода, обработку данных и обмен информацией по цифровым каналам связи. Обмен данными с модулями ввода/вывода организован по системной шине VMEbus. Это позволяет использовать в составе контроллера не только модули ввода/вывода, входящие в состав ПТК ШБ СОС, но и модули сторонних разработчиков, тем самым расширяя функциональные возможности.

Плата-носитель ЭМЦП с мостом PC/104↔VME является базовым устройством для построения процессорных модулей для разных условий эксплуатации. В настоящее время существует большое число производителей промышленных одноплатных компьютеров с архитектурой процессора Intel 80×86/Pentium и интерфейсом PC/104, регламентируемых открытой спецификацией. Это позволяет осуществлять не только выбор между поставщиками, но в зависимости от сложности требуемой обработки данных выбирать одноплатные компьютеры с соответствующей вычислительной мощностью.

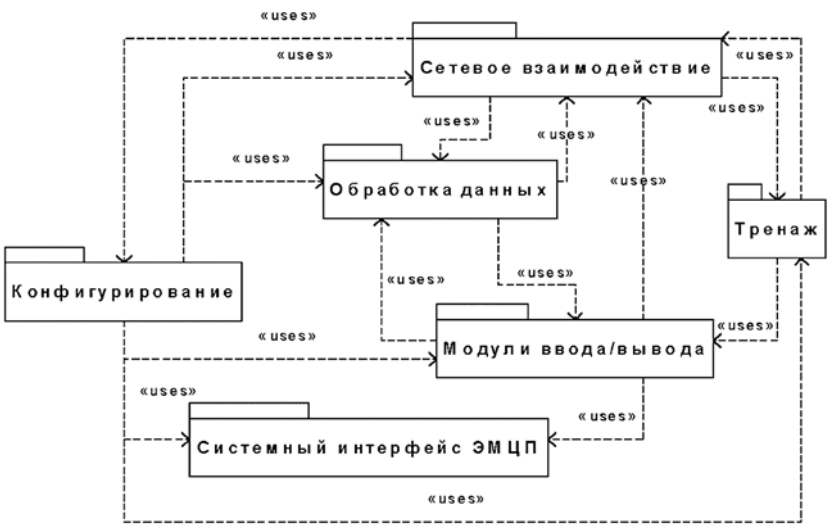


*Рис.4. Базовая структура ПО ПТК ШБ СОС*

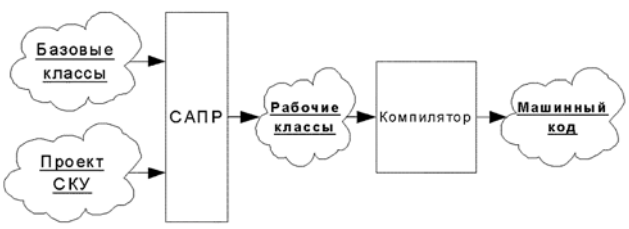


*Рис.5. Схема создания ПО конкретной системы*

ПО ПТК ШБ СОС представляет собой набор базовых программных элементов проектируемых систем. При создании ПТК была разработана базовая структура ПО контроллера, приведенная на рис. 4. Базовые элементы представляют собой программные артефакты обработки данных. В этом случае создание ПО разрабатываемых систем заключается в параметризации базовых элементов и добавлении информации о потоках данных внутри ПО. При этом возможно использование *системы автоматизированного проектирования* (САПР), позволяющей разработчику (проектанту) системы рассматривать создаваемое ПО не как текст на языке программирования, а как взаимодействие алгоритмов обработки данных, выраженных в виде удобных для восприятия и понимания разработчи-

ку понятий с определенными характеристиками. В свою очередь САПР на основе таких знаний, базовых элементов и принципов параметризации создает ПО в виде рабочих классов [7]. После компиляции этих рабочих классов разработчик получает машинный код. Схема создания ПО конкретной системы приведена на рис. 5.

Пример разработки ПТК ШБ СОС показывает, что предлагаемый подход к созданию комплексов для построения систем, важных для безопасности, способствует выполнению соответствующих требований. В настоящее время ПТК ШБ СОС успешно прошел приемочные испытания. Комиссия рекомендовала использование ПТК ШБ СОС для построения систем нормальной эксплуатации, важных для безопасности. В ближайшее время планируется доработать его технические и программные средства с целью выполнения требований, предъявляемых к управляющим системам безопасности.

**Список литературы**


1. *NUREG/CR-6463*, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems", U. S. Nuclear Regulatory Commission.
2. *IEC 60880,* "Software for Computers in the Safety Systems of Nuclear Power Stations".
3. *IEC 61508-3,* "Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements".
4. *Мякишев Д.В.* Объектно-ориентированное проектирование на основе эталонных моделей// "Открытые системы", 1998, №3, с. 64-66.
5. *Бертран Мейер.* Построение надежного объектно-ориентированного программного обеспечения: введение в контрактное проектирование// "Открытые Системы", 1998, №6, с. 34-38.
6. *Мякишев Д.В., Наконечный С.В.* Применение объектно-ориентированного подхода для повышения качества программных средств систем контроля и управления// Сборник докладов на второй научно-технической конференции "Системы контроля и управления. Их роль в обеспечении безопасности. Нормы, практика и тенденции развития". М.: ИД "Технологии", 2002, с. 37-42.
7. *Мякишев Д.В., Балашов А.И., Наконечный С.В и др.* Метод эталонных моделей как основа проектирования программного обеспечения комплексов управления технологическими процессами// "Приборы и системы. Управление, контроль, диагностика", 2002, №9, с. 1-5.



***Мякишев Дмитрий Владимирович** – канд. техн. наук, генеральный директор, **Тархов Юрий Андреевич** – технический директор, **Столяров Константин Алексеевич** – директор по проектам, **Наконечный Сергей Владимирович** – ведущий специалист-программист, **Столяров Сергей Алексеевич** – ведущий специалист-программист НПП "Комплексы и системы". Контактный телефон (8412) 45-59-98. E-mail: copm_sys@tl.ru*


## НОВОСТИ

### Датчики давления "Метран-100"

ГРУППА ПРЕДПРИЯТИЙ МЕТРАН ТРАДИЦИИ ТОЧНОСТИ

Новый комплекс интеллектуальных датчиков давления "Метран-100" вобрал в себя самые надежные и лучшие модели ранее выпускаемых датчиков. Датчики "Метран-100" полностью заменяют известные семейства датчиков "Метран-22", –43, –45, –49, "Сапфир-22М" и др., а также обеспечивают возможность замещения импортных датчиков аналогичного назначения.

Основой всех сенсорных блоков датчиков семейства "Метран-100" является чувствительный элемент с монокристаллической структурой кремния на сапфире.

В памяти сенсорного блока хранятся результаты предварительных измерений выходных сигналов сенсора во всем рабочем диапазоне давлений и температур. Эти данные используются микропроцессором для расчета коэффициентов коррекции выходного сигнала при работе датчика.

Цифровой сигнал сенсорного блока вместе с коэффициентами коррекции поступает на вход электронного преобразователя, микропроцессор которого корректирует этот сигнал по температуре и линеаризует его. На выходе электронного блока формируется стандартный выходной сигнал и цифровой сигнал в стандарте протокола HART.

Энергонезависимая память сенсорного блока, в случае отказа электронной части датчика, упрощает устранение неполадок в приборе: ремонт сводится лишь к замене его микропроцессорной платы.

В датчиках "Метран-100" реализовано 25 универсальных команд HART-протокола. К ним относятся: перенастройка диапазона измерения; смена единиц измерения; установка нуля; две команды калибровки – верхний и нижний предел измерений; команда расширенной диагностики состояния датчика.

"Метран-100" тестируется по ряду параметров (ПЗУ, микропроцессор, обрыв сенсора и др.), результаты диагностики выводятся на экран компьютера или на HART-коммуникатор.

Предусмотрена установка нуля датчика простым нажатием кнопки без разгерметизации оболочки электронного блока и без нарушения требований взрывозащиты.

Датчики давления "Метран-100" имеют встроенный фильтр радиопомех.

Помимо исполнения датчика "Метран-100" с поддержкой по HART-протоколу имеется исполнение с обычным аналоговым выходным сигналом, тем не менее, "Метран-100" может быть легко, сменой всего одной платы (операция может быть выполнена потребителем), превращен в интеллектуальный с поддержкой HAR-протокола.

Перенастройка диапазонов в пределах одной модели датчика – 25:1.

Погрешность – до 0,1 % от калиброванного диапазона измерений, включая погрешность нелинейности, гистерезис и повторяемость.

**E-mail: metran@metran.ru**
**Http:// www.metran.ru**