УДК 004.415: 004.412

В.В. СКЛЯР

Государственный НТЦ по ядерной и радиационной безопасности, Украина

ПРОЦЕСС УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ КРИТИЧЕСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: АНАЛИЗ И ПРИМЕНЕНИЕ ТРЕБОВАНИЙ

Процесс управления конфигурацией играет существенную роль в формировании жизненного цикла программного обеспечения (ПО). В статье проанализирована значимость данного процесса для качества критического ПО. На базе положений стандарта IEEE 828-1990 проанализированы требования к управлению конфигурацией ПО. Данные требования интерпретированы и реализованы в системе управления жизненным циклом ПО на Научно-производственном предприятии «Радий».

управление конфигурацией, жизненный цикл, критическое программное обеспечение

1. Анализ влияния процесса управления конфигурацией на качество ПО. Постановка задачи

При оценке программного обеспечения (ПО) систем критического применения (далее критического ПО) существенное внимание уделяется процессам жизненного цикла (ЖЦ), таким как разработка, сопровождение, управление конфигурацией, документирование, обеспечение качества, верификация и валидация, управление [1].

Одним из важных процессов ЖЦ ПО, которому, тем не менее, посвящено недостаточное количество публикаций (особенно в отечественных и русскоязычных изданиях), является управление конфигурацией. Под конфигурационным управлением подразумевается процесс, состоящий в применении на протяжении всего жизненного цикла ПО процедур идентификации, определения базового состава компонентов ПО, контроля модификаций и версий компонентов, фиксации и отчетности о состоянии компонентов, обеспечения полноты, непротиворечивости и корректности компонентов, хранения, обработки и предоставления компонентов [2].

В табл. 1 приведены результаты анализа причин аварий на предприятиях химической промышленности по данным публикации [3]. В табл. 2 приведены результаты анализа дефектов, выявленных при тестировании систем управления, предназначенных для функционирования на борту девяти наиболее известных космических аппаратов NASA, запущенных в 1990-х гг. [4].

Таблица 1

Результаты анализа причин аварий на предприятиях химической промышленности

Причина аварии	% от общего кол-ва аварий
Ошибки при выполнении работ по обеспечению безопасности	41,5
Ошибки операторов	18,3
Ошибки конфигурационного управления	13,4
Ошибки проектирования	8,5
Ошибки при выполнении технического обслуживания	8,5
Выход химической реакции из-под контроля	7,3
Другие причины	2,5

Рассмотренные примеры подчеркивают роль управления конфигурацией в обеспечении качества, надежности и безопасности критического ПО.

Требования к процессу конфигурационного управления содержатся в стандарте IEEE 828-1990 «Стандарт IEEE для планов управления конфигурацией программного обеспечения». Данный стандарт рекомендован в качестве базового национальными и международными нормативными документами по критической программной инженерии [5 – 7].

Таблица 2

Результаты анализа причин дефектов систем управления космическими аппаратами NASA

Причина внесения дефекта	% от общего кол-ва дефектов
Ошибки конфигурационного управления ПО	35
Ошибки конфигурационного управления техническими средствами (ТС)	24
Ошибки при проведении инспекций и обзоров	20
Ошибки при разработке логической структуры ПО	14
Ошибки при разработке процедур старта, рестарта и завершения работы	7

Целью данной статьи является анализ процедур процесса управления конфигурацией ПО, а также анализ их применимости в ЖЦ критического ПО.

2. Анализ процедур процесса управления конфигурацией

Согласно стандарту IEEE 828-1990 управление конфигурацией предусматривает:

– руководство процессом;

– непосредственную деятельность по управлению конфигурацией, включая идентификацию конфигурации, контроль конфигурации, учет статуса компонентов и аудиты управления конфигурацией (рис. 1);

– планирование процесса;

– определение ресурсов процесса;

– сопровождение процесса.

Ниже рассмотрены действия процесса управления конфигурацией, представленные на рис. 1.

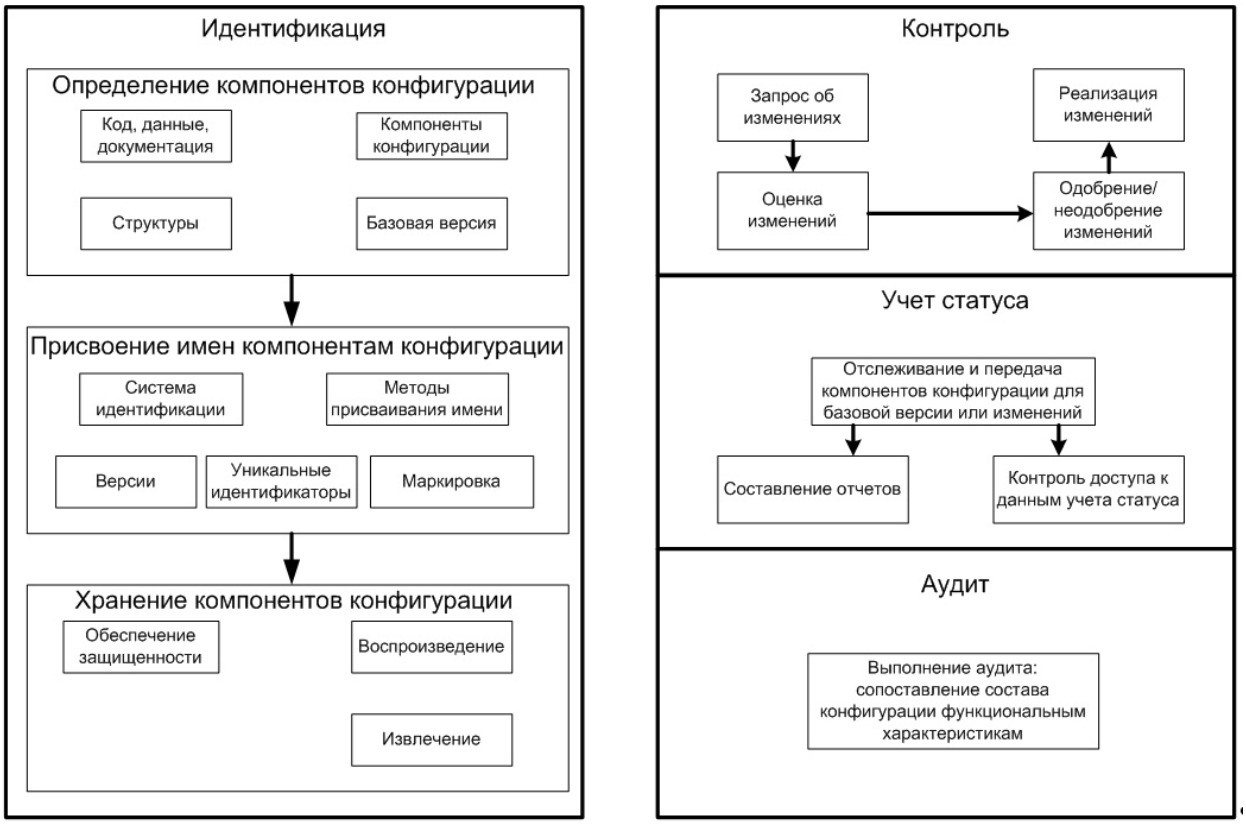

Рис. 1. Действия процесса управления конфигурацией

Определение компонентов конфигурации включает:

– определение момента фиксации согласованной конфигурации;

– определение контролируемых компонентов конфигурации;

– процедуры для изменения компонентов конфигурации, включая согласование изменений.

К контролируемым компонентам конфигурации относятся:

– компоненты ТС, включающие ПО;

– программируемые компоненты;

– программные модули;

– библиотечные компоненты;

– алгоритмы;

– операционные системы;

– инструментальные средства разработки и верификации;

– программная документация.

Присвоение имен компонентам конфигурации включает:

– систему идентификаторов компонентов и их версий, предусматривающую для каждого из компонентов уникальный идентификатор;

– систему маркировки компонентов и их версий.

Хранение компонентов конфигурации включает:

– обеспечение защищенности;

– извлечение;

– воспроизведение.

Для любого идентифицированного компонента должно обеспечиваться нахождение и тиражирование в любой из существующих конфигураций.

Действия по контролю конфигурации состоят в реализации изменений в скомпонованные элементы, включая запросы, оценку, одобрение/неодобрение и внедрение изменений. Изменения компонентов охватывают как исправления ошибок, так и расширение функциональности. Степень формализации, необходимая для внесения изменений, зависит от затрагиваемой базовой версии ПО и от воздействия изменений на ПО. Для каждого идентифицированного компонента конфигурации внесение изменений должно включать следующую последовательность шагов:

– идентификация и документирование необходимости изменения;

– анализ и оценка запроса на изменения;

– одобрение или не одобрение запроса на изменения;

– верификация, внедрение и выпуск изменения.

При подготовке второй и последующих версий конфигурации ПО должна быть обеспечена обозримость связей по отношению к предыдущей версии. В любой момент времени должно обеспечиваться актуальное состояние конфигурации. Компоненты конфигурации рабочей версии должны быть идентичны используемым для разработки. Компоненты конфигурации базовых версий ПО, находящиеся на хранении, должны быть идентичны компонентам конфигурации, находящимся в эксплуатации.

При реализации процесса управления конфигурацией должны быть также реализованы действия по контролю интерфейсов.

Управление заменой морально устаревших компонентов подразумевает замену элементной базы снятой с производства и отсутствующей на рынке. Данные действия, хотя и относятся к ТС, однако могут привести к изменениям в ПО. Замена морально устаревших компонентов проводится следующим образом:

– анализ предложений на рынке элементной базы;

– выявление электронных элементов, применяемых в ТС, но отсутствующих в коммерческой продаже;

– поиск альтернатив отсутствующим элементам;

– анализ применимости новой элементной базы;

– проектирование ТС с использованием новой элементной базы;

– изготовление ТС с использованием новой элементной базы;

– определение необходимого объема квалификационных испытаний ТС;

– проведение квалификационных испытаний ТС;

– документирование внесенных изменений, включая внесение изменений в документацию.

Для программируемых компонентов, кроме того, выполняется анализ необходимых изменений и непосредственное изменение программного кода с последующей верификацией.

Действия по учету статуса конфигурации реализуются путем генерации соответствующих отчетов. Уровень требуемых деталей и специфических данных могут изменяться в соответствии с информационными потребностями проекта. При учете статуса конфигурации должна быть собрана следующая информация:

– какие из компонентов следует отслеживать и включать в состав версий конфигураций ПО и/или рабочих версий и в контроль изменений;

– с какой частотой и в какой форме следует генерировать отчеты об учете статуса конфигурации;

– какая информация должна собираться, сохраняться, обрабатываться и выводиться в отчетах об учете статуса конфигурации;

– как следует контролировать доступ к компонентам конфигурации в зависимости от их статуса.

Аудиты управления конфигурацией определяют, в какой степени действительные компоненты конфигурации соответствуют требуемым физическим и функциональным характеристикам.

Для каждого планируемого аудита управления конфигурацией должны быть определены:

– цель;

– компоненты конфигурации, подвергающиеся аудиту;

– расписание выполнения задач аудита;

– процедуры для проведения аудита;

– участники аудита;

– требуемая документация;

– процедуры фиксации и анализа выявленных недостатков, а также реализации корректирующих действий;

– критерии соответствия и специфические действия, которые следует выполнить после согласования результатов аудита.

При проведении аудита управления конфигурацией применяются следующие критерии оценки.

– документы по управлению конфигурацией должны включать информацию о всех составляющих процесса управления конфигурацией (руководство процессом, деятельность по управлению конфигурацией, планирование процесса, определение ресурсов процесса, сопровождение процесса);

– в документах по управлению конфигурацией для каждого из видов деятельности (идентификация, контроль, учет статуса, аудиты, а также контроль покупных компонентов и интерфейсов) должны быть установлены ответственные лица и необходимые ресурсы;

– для всех компонентов должен быть установлен порядок включения в конфигурацию, а также порядок контроля конфигурации.

3. Результаты применения процедур процесса управления конфигурацией

Рассмотрим результаты применения требований к процессу управления конфигурацией на примере Научно-производственного предприятия (НПП) «Радий», которое является разработчиком ПО для систем безопасности АЭС.

Единицей продукции НПП «Радий» для АЭС являются программно-технические комплексы (ПТК), представляющие собой совокупность ТС, поставляемых комплектно с ПО, необходимым сервисным оборудованием и эксплуатационной документацией. Особенностью разработки ПТК на НПП «Радий» является то, что сначала создается головной образец ПТК. Затем на базе головного образца разрабатываются поставочные комплекты ПТК, предназначенные для конкретных энергоблоков АЭС.

Установлены следующие типы конфигурации для ПО, разработанного НПП «Радий»:

– ПО головного образца ПТК;

– ПО поставочного комплекта ПТК;

– рабочая версия – промежуточный результат разработки, основанный на компонентах ПО головного образца ПТК.

Совокупность компонентов ПО и ТС, входящих в состав согласованных конфигураций головных образцов ПТК и поставочных комплектов ПТК, образует программно-аппаратную платформу «Радий».

Процедуры для изменения компонентов конфигурации ПО (обозначены на рис. 2 соответствующими номерами) включают:

1) разработка поставочного комплекта ПТК на базе головного образца ПТК;

2) разработка нового головного образца ПТК;

3) модификации компонентов ПО поставочных комплектов ПТК;

4) изменение рабочей версии компонента конфигурации ПО;

5) включение измененных компонентов ПО в состав головного образца ПТК.

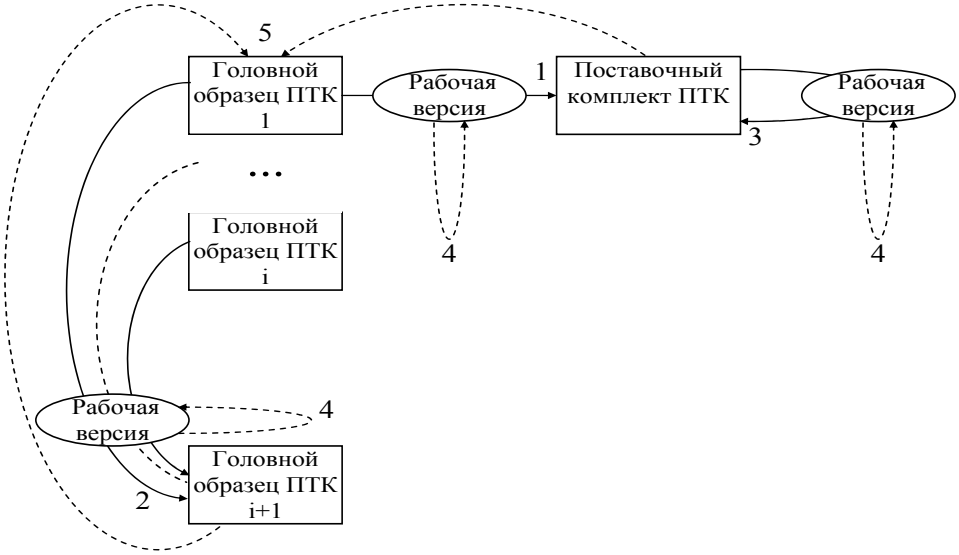

Рис. 2. Процедуры изменения компонентов конфигурации

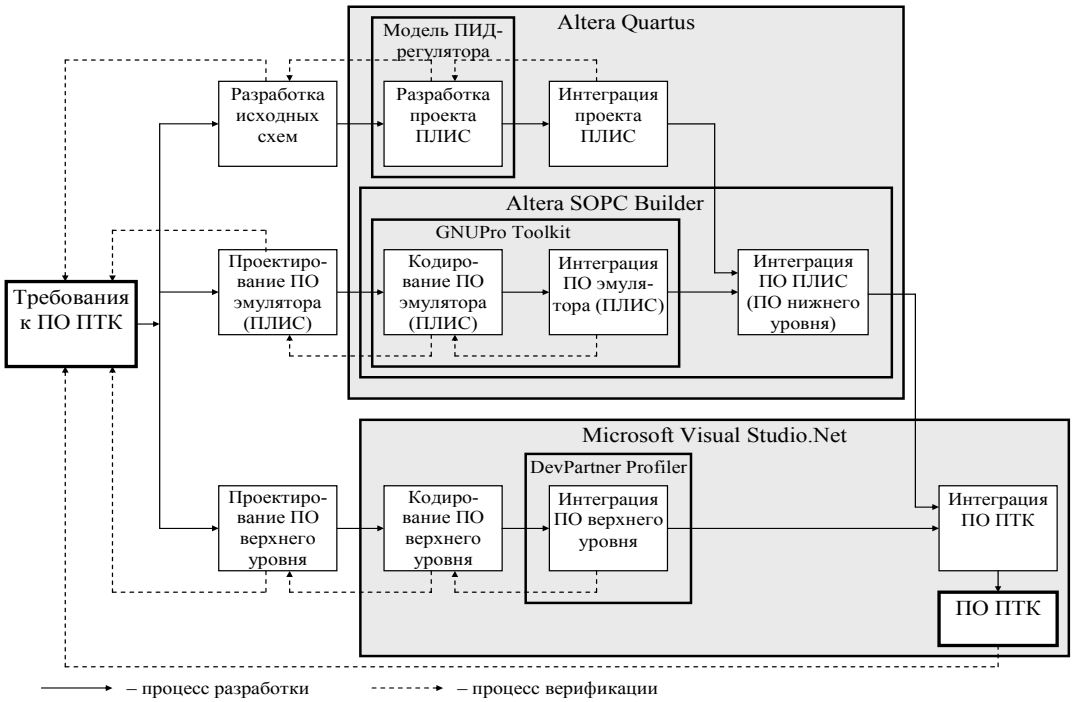

Рис. 3. Конфигурация инструментальных средств разработки и верификации ПО

В ходе выполнения процедур 1, 2, 3 генерируются рабочие версии. Компоненты рабочих версий также могут изменяться в процессе разработки, что демонстрируется наличием процедуры 4. Процедуры 3, 5 направлены на изменение компонентов утвержденных и одобренных версий головных образцов и поставочных комплектов. Процедура 1 (а в дальнейшем и процедура 3) может быть реализована для любого из головных образцов ПТК.

Важным фрагментом процесса управления конфигурацией является управление конфигурацией инструментальных средств (ИС) разработки и верификации ПО. На рис. 3 конфигурация ИС, применяемая на НПП «Радий», совмещена с процессами разработки и верификации, применяемыми для трех типов ПО, применяемых в ПТК для АЭС: 1) графические схемы алгоритмов в среде ПЛИС; 2) ПО эмуляторов в среде ПЛИС; 3) ПО рабочих станций верхнего уровня [7].

Выводы

Согласно проанализированным данным (см. таблицы 1, 2), ошибки управления конфигурацией занимают третье место среди причин аварий в химической отрасли и являются причиной более половины дефектов систем управления космическими аппаратами.

В статье проанализированы положения стандарта IEEE 828-1990, который является базовым для реализации процесса управления конфигурацией в жизненном цикле критического ПО. Основой процесса управления конфигурацией является выполнение четырех действий: 1) идентификация конфигурации; 2) контроль конфигурации; 3) учет статуса компонентов; 4) аудиты управления конфигурацией.

Анализ положений стандарта IEEE 828-1990 позволил внедрить процесс управления конфигурацией в системе управления ЖЦ ПО на НПП «Радий».

Среди важнейших действий по внедрению процесса управления конфигурацией на предприятиях следует отметить идентификацию типов применяемых конфигураций и установление реализуемых процедур по изменению типовых конфигураций.

Дальнейшее исследование целесообразно направить на разработку формального описания процедур управления конфигурацией.

Литература

1. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. – Х.: Нац. аэрокосмический ун-т «Харьк. авиац. ин-т», 2004. – 159 с.

2. Kim J.H., Lee J., Kim K., Kim Y., Baek J. Development of Management of Change (MOC) Software for Small and Medium Sized Chemical Plants // Proceeding Conference “PSAM 7 – ESREL ´04”, Berlin, 2004. – P. 2687-2692.

3. Lutz R., Mikulski I. Empirical Analysis of Safety-Critical Anomalies During Operations // IEEE Transactions on Software Engineering. – 2004. – Vol. 30. – n 3. – P. 172-180.

4. Heland J., Albold A. Configuration Management of Railway Vehicles' Software for a Railway Operator // Proceeding Conference “PSAM 7 – ESREL ´04”, Berlin, 2004. – P. 2102-2106.

5. Voas J. Maintaining Component-Based Systems // IEEE Transactions on Software. – 1998. – V. 24, n 7. – P. 531-540.

6. Липаев В.В. Сопровождение и управление конфигурацией сложных программных средств. – М.: Синтег, 2006. – 372 с.

7. Бахмач Е.С., Сиора А.А., Скляр В.В., Токарев В.И., Харченко В.С. Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС // Радіоелектронні і комп’ютерні системи. – 2007. – №. 7(26). – С. 75-82.

Поступила в редакцию 12.02.2008

Рецензент: д-р техн. наук, проф. Г.Н. Жолткевич, Харьковский Национальный университет, им. В.Н. Каразина, Харьков.