УДК 629.039.58: 681.518.3

В. В. Скляр

ПАО «НПП “Радий”», г. Кировоград, Украина

Сертификация информационно-управляющей платформы на базе ПЛИС на соответствие требованиям по функциональной безопасности стандарта МЭК 61508

Рассмотрены основные положения стандарта МЭК 61508, проанализирован опыт по реализации процессов жизненного цикла в ходе сертификации информационно-управляющей платформы RadICS. Соблюдение положений МЭК 61508 является хорошей практикой, направленной на повышение безопасности ИУС АЭС, которую можно рекомендовать для внедрения в нормативную практику Украины.

Ключевые слова: информационные и управляющие системы, функциональная безопасность.

В. В. Скляр

Сертифікація інформаційно-керуючої платформи на базі ПЛІС на відповідність вимогам з функціональної безпеки стандарту МЕК 61508

Розглянуто основні положення стандарту МЕК 61508, проаналізовано досвід з реалізації процесів життєвого циклу в ході сертифікації інформаційно-керуючої платформи RadICS. Дотримання положень МЕК 61508 є хорошою практикою, що спрямована на підвищення безпеки інформаційних та керуючих систем АЕС і може бути рекомендована для впровадження в нормативну практику України.

Ключові слова: інформаційні та керуючі системи, функціональна безпека.

Стандарт МЭК 61508 «Функциональная безопасность электрических / электронных / электронных программируемых систем, относящихся к безопасности» применяется как основа регулирующих требований по безопасности, предъявляемых к ИУС АЭС в таких, например, странах, как Канада, Финляндия, Аргентина, Корея. В ряде других стран соответствие ИУС АЭС требованиям МЭК 61508 означает изначально высокий уровень доверия к таким системам, что существенно снижает усилия по лицензированию [1, 2].

В Украине требования стандарта МЭК 61508 обязательными не являются. Тем не менее, научно-производственным предприятием «Радий» начата в 2011 г. реализация проекта по сертификации новой информационно-управляющей платформы, называемой RadICS, на соответствие требованиям МЭК 61508. Данная платформа может применяться в системах безопасности класса 2 (категория безопасности А по классификации МЭК либо класс 1Е по классификации IEEE). Особенность платформы RadICS — применение программируемых логических интегральных схем (ПЛИС) в качестве программируемых компонентов вместо традиционных микропроцессоров.

Цель данной статьи — освещение особенностей проекта по сертификации платформы RadICS в части внедрения процессов безопасного жизненного цикла. Подобный опыт на данный момент уникален для Украины. Мотивацией сертификации послужили, во-первых, перспектива выхода на международные рынки с продуктом, который соответствует требованиям, признаваемым большинством национальных регулирующих органов; во-вторых, возможность с упреждением учесть новейшие требования международных стандартов, которые пока не внедрены в Украине, но могут быть учтены в дальнейшем; в-третьих, платформа, разработанная согласно требованиям МЭК 61508, поддерживает пригодность к долгосрочной эксплуатации и сопровождению на протяжении всего срока службы энергоблока [3].

Платформа RadICS включает в себя:

шасси для размещения модулей;

модули ввода и вывода для приема и выдачи дискретных и аналоговых сигналов различных номиналов;

логические модули для выполнения управляющих алгоритмов;

модули оптической связи для коммуникаций между шасси.

Платформа RadICS позволяет конфигурировать любые виды цифровых информационных и управляющих систем (ИУС) для АЭС, а также для других приложений, связанных с обеспечением безопасности.

Обзор требований стандарта МЭК 61508. Первая редакция МЭК 61508 была выпущена на протяжении 1998—2000 гг. и включала семь частей:

1. Общие требования.
2. Требования к электрическим / электронным / электронным программируемым системам, относящимся к безопасности.
3. Требования к программному обеспечению.
4. Определения и сокращения.
5. Примеры методов определения уровней интегрированности безопасности.
6. Руководство по применению МЭК 61508–2 и МЭК 61508–3.
7. Обзор методов и средств.

Вторая редакция МЭК 61508, включающая те же части, вышла в 2010 г. В ней усилен ряд требований по безопасности, в частности требования к квалификации

инструментальных средств, требования к трассировке требований к продукту, а также требования к наличию концепции продукта, которая должна предшествовать спецификации требований по безопасности.

В основе требований по функциональной безопасности лежит понятие уровня интегрированности (полноты, целостности) безопасности (Safety Integrity Level — SIL). Наивысший уровень безопасности соответствует SIL4. Системы безопасности АЭС должны соответствовать уровню SIL3. Для каждого из уровней SIL устанавливается перечень требований по безопасности, включая соответствующие значения показателей безопасности, а также перечень мероприятий, заключающихся в соблюдении требований к процессам жизненного цикла, направленным на достижение требований по безопасности (табл. 1).

Таблица 1. Значения показателей безопасности для различных уровней SIL и режимов функционирования системы

Уровень интегрированности безопасности	**PFD_{avg} _ средняя вероятность опасного отказа на запрос функции безопасности (для режима с низкой частотой запросов)**	**PFH — средняя частота отказов функции безопасности, 1/ч (для режима с высокой частотой запросов и для непрерывного режима)**
SIL4	$10^{-5} \geq PFD_{avg} > 10^{-4}$	$10^{-9} \geq PFH > 10^{-8}$
SIL3	$10^{-4} \geq PFD_{avg} > 10^{-3}$	$10^{-8} \geq PFH > 10^{-7}$
SIL2	$10^{-3} \geq PFD_{avg} > 10^{-2}$	$10^{-7} \geq PFH > 10^{-6}$
SIL1	$10^{-2} \geq PFD_{avg} > 10^{-1}$	$10^{-6} \geq PFH > 10^{-5}$

Такой подход к оцениванию и обеспечению безопасности является риск-ориентированным и базируется на принципе ALARA (ALARP) (as low as reasonably applicable / practicable), который подразумевает максимально возможное снижение риска, достигаемое за счет реально имеющихся (ограниченных) ресурсов [4].

Отметим, что для систем, важных для безопасности, рассматриваются три режима функционирования: с низкой частотой запросов (запросы на выполнение функции происходят реже, чем один раз в год), с высокой частотой запросов (запросы на выполнение функции происходят чаще, чем один раз в год) и непрерывный режим.

Повышение уровня SIL (т. е. повышение на порядок значений показателей безопасности) может быть достигнуто резервированием. Например, для обеспечения безопасности ИУС АЭС достаточна сертификация программно-технических средств в нерезервированной конфигурации на соответствие SIL2. Тогда резервирование по схеме «1 из 2» либо «2 из 3» позволяет достичь уровня SIL3. Процессы жизненного цикла при этом, однако, должны соответствовать SIL3.

Кроме того, отказы системы делятся на группы. С точки зрения влияния на безопасность системы, различают опасные отказы (такие отказы, которые приводят к отказу функции безопасности либо снижают вероятность корректного выполнения функции безопасности по запросу) и безопасные отказы (такие отказы, которые приводят к ложному срабатыванию функций безопасности, переводящему систему в безопасное состояние, либо повышают вероятность ложного срабатывания функций безопасности). С точки зрения детектирования отказов средствами самодиагностики, различают выявленные и скрытые отказы. Таким образом, имеем четыре группы отказов: опасные скрытые, опасные выявленные, безопасные скрытые и безопасные выявленные. Очевидно, что первая группа отказов представляет собой наибольшую опасность. Именно с наличием этой группы отказов связано понятие доли (фракции) безопасных отказов (Safe Failure Fraction — SFF), под которой понимают отношение суммы интенсивностей всех безопасных отказов и опасных выявленных отказов к общей интенсивности отказов (т. е. в числителе отсутствует интенсивность опасных скрытых отказов).

SFF относится к важным показателям безопасности, который влияет на достижение того или иного уровня SIL (табл. 2). SFF зависит от полноты диагностического покрытия, которое должно снижать долю опасных скрытых отказов до требуемого уровня. Для упрощенных расчетов можно принять SFF равным полноте диагностического покрытия. Самодиагностика реализуется для всех компонентов ИУС: технических средств (ТС), программного обеспечения, а также линий коммуникации. SFF зависит также от степени резервирования системы, которая в МЭК 61508 трактуется как устойчивость ТС к отказам (Hardware Fault Tolerance — HFT).

Таблица 2. Значения SFF для различных уровней SIL в зависимости от степени резервирования системы

SFF	**Нерезервированная система (HFT = 0)**	**Резервированная система «1 из 2», «2 из 3» (HFT = 1)**	**Резервированная система «1 из 3», «2 из 3» с переходом в «1 из 2» или «1 из 1» (HFT = 1)**
> 60 %	–	SIL1	SIL2
60 % — < 90 %	SIL1	SIL2	SIL3
90 % — < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Особые требования выдвигает МЭК 61508 к процессам разработки ИУС, включая компоненты программного обеспечения (ПО) и ТС. К таким процессам относятся:

управление функциональной безопасностью;
управление проектом;
управление персоналом и обучение;
управление конфигурацией и контроль изменений;
управление документацией;
квалификация инструментальных средств;
поэтапная разработка с поэтапной верификацией и валидацией (так называемый безопасный жизненный цикл, имеющий V-образную форму).

Далее дана краткая характеристика каждого из процессов.

Управление функциональной безопасностью. Процесс управления функциональной безопасностью является основополагающим. Для его реализации рекомендуется разработать соответствующий план управления функциональной безопасностью (Functional Safety Management Plan — FSMP). Данный план определяет:

организационную структуру проекта и распределение ролей, требуемый уровень компетенций и степень независимости персонала;

документирование проекта и структуру проектной документации;

общее и детальное описание безопасного жизненного цикла (рис. 1); детальное описание каждого из этапов должно включать полный перечень разрабатываемых документов с указанием для каждого из документов идентификационного номера, наименования, метода верификации, а также вовлеченных участников проекта (автор, верификатор и лицо, утверждающее документ);

стратегию выполнения проекта, включая подход к составлению графика выполнения, распределению ресурсов и контролю выполнения действий и задач;

описание общего подхода к работе с требованиями к продукту, включая сбор и утверждение требований, их распределение между компонентами продукта (аллокацию), а также трассировку;

политику проведения периодических аудитов;

подход к обеспечению информационной безопасности;

процедуру контроля изменений;

подход к квалификации инструментальных средств;

планирование верификации и валидации.

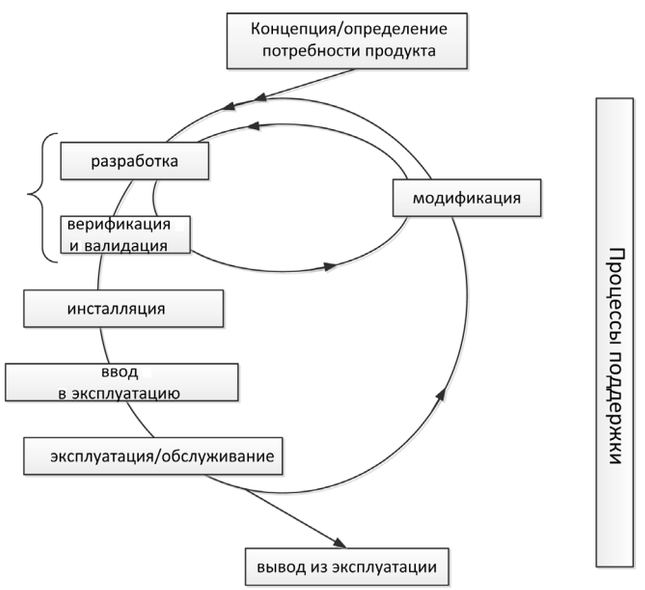

Рис. 1. Концепция безопасного жизненного цикла

Управление проектом. Методология управления проектами разработана американским институтом проектного менеджмента (Project Management Institute — PMI) и заложена в фундаментальном руководстве [5]. Полный объем деятельности по управлению проектами включает управление интеграцией, содержанием, сроками, стоимостью, качеством, персоналом, коммуникациями, рисками, закупками.

МЭК 61508 требует внедрения управления проектами как процесса, необходимого для соответствия любому из уровней SIL. На практике реализация сложных проектов невозможна без систематического и качественного управления. Однако руководство [5] позволяет из всего вышеперечисленного объема выбрать только те виды деятельности, которые являются наиболее адекватными для того или иного проекта. Некоторые из процессов, рассмотренных ниже, а именно: управление персоналом, управление конфигурацией, а также управление документацией — ничто иное, как области знаний дисциплины управления проектами.

Управление персоналом и обучение. Человеческий фактор — залог успеха либо неудачи проекта. Поэтому подбор и расстановка персонала играют решающую роль в реализации проектов сертификации сложных продуктов, и МЭК 61508 учитывает это положение.

Организационная структура проекта и распределение ролей, которые в общих чертах должны быть отражены в FSMP (см. выше), детализируются в плане управления персоналом (Personnel Plan). Этот план должен быть разработан при поддержке службой управления персоналом. Организационная структура проекта, как правило, описывается организационной диаграммой (рис. 2).

Кроме того, план управления персоналом должен содержать:

основные должностные обязанности каждого из участников проекта;

полный перечень сотрудников, назначенных для работы над проектом, с указанием их ролей и степени независимости проектных команд (например, независимость группы верификации и валидации от группы разработки);

подход к ведению записей о тренингах;

план проведения тренингов, направленных на развитие и поддержание требуемых компетенций персонала;

матрицу компетенций, показывающую связь между требуемыми и реальными компетенциями каждого из участников проекта;

краткие резюме ключевых должностных лиц проекта.

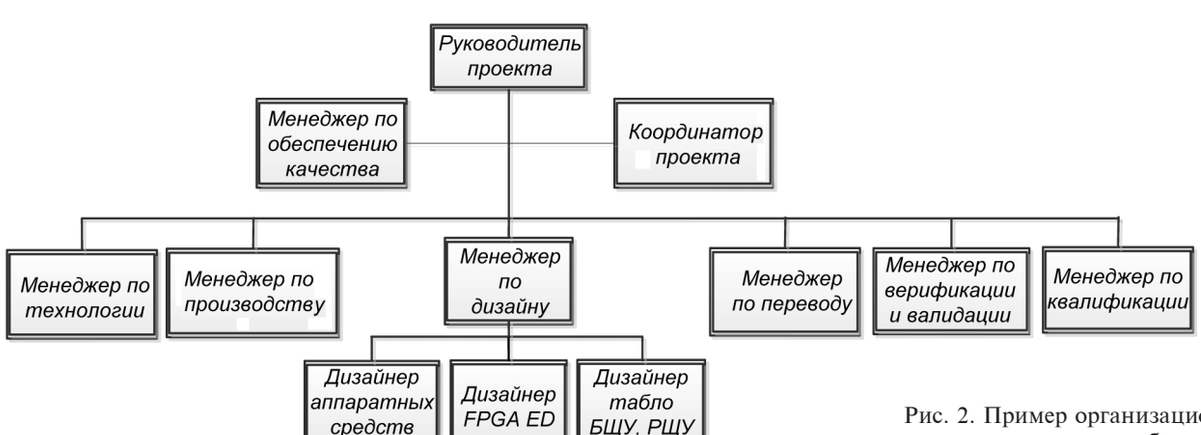

Рис. 2. Пример организационной структуры проекта по разработке ИУС АЭС

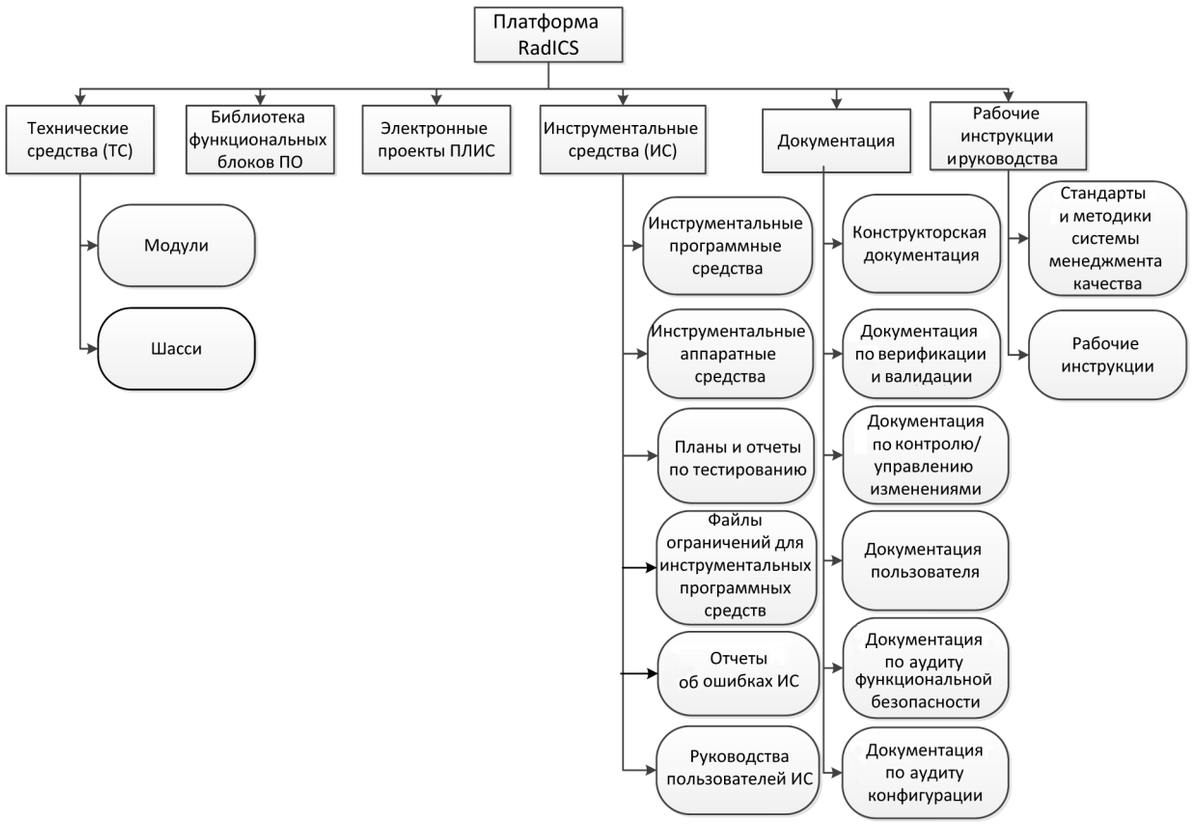

Рис. 3. Пример структуры компонентов конфигурации

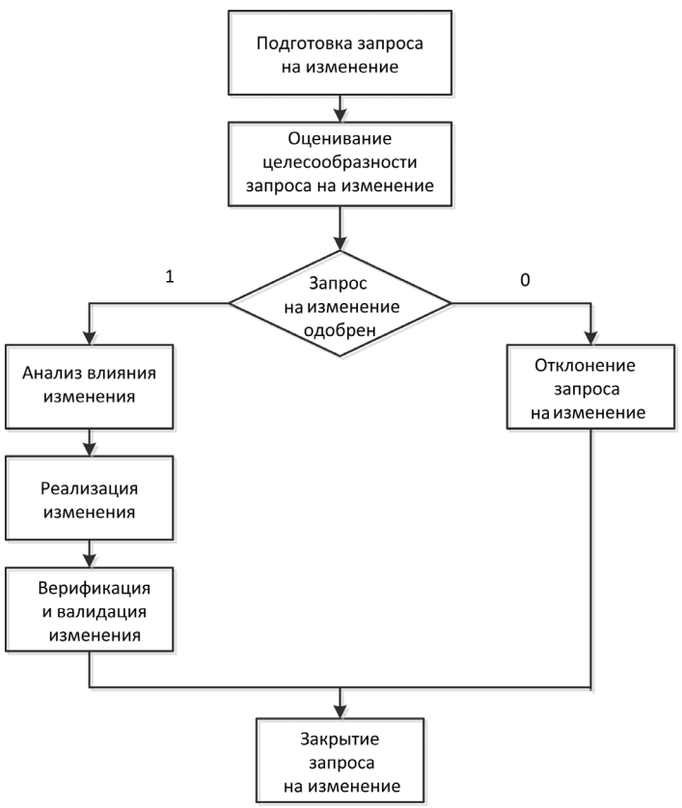

Рис. 4. Алгоритм реализации процедуры контроля изменений

Управление конфигурацией и контроль изменений. Процесс управления конфигурацией направлен на выполнение процедур по идентификации, контролю и трассируемости версий каждого из компонентов продукта на протяжении всего жизненного цикла. Типовыми компонентами ИУС, подлежащими управлению конфигурацией, являются ТС и ПО, включая библиотечные компоненты, инструментальные средства и документы, в том числе рабочие руководства и инструкции (рис. 3).

Для планирования данного процесса должен быть разработан план управления конфигурацией (Configuration Management Plan — CMP), включающий в себя:

распределение ролей и ответственности для данного процесса; для этого в проекте, как правило, назначается группа, выполняющая действия по управлению конфигурацией и контролю изменений;

ресурсы процесса (персонал, инструментальные средства, утвержденные процедуры и инструкции);

перечень компонентов конфигурации;

подход к наименованию компонентов конфигурации, который может заключаться, например, в генерации для каждого из компонентов буквенно-цифрового идентификатора;

подход к созданию и хранению компонентов конфигурации;

перечень базовых конфигураций (для различных этапов жизненного цикла) и их состав;

процедуру контроля конфигурации;

процедуру контроля изменений (рис. 4);

учет статуса компонентов конфигурации;

процедуру аудита компонентов базовых конфигураций.

Управление документацией. Документы являются компонентами конфигурации, однако их специфика требует

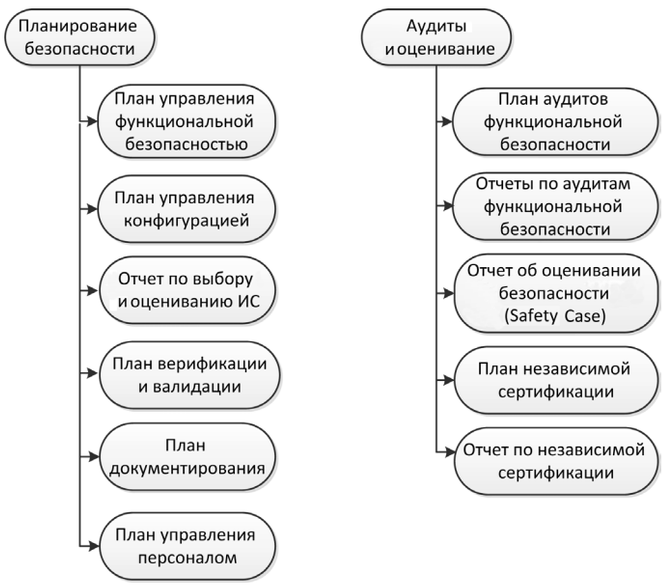

Рис. 5. Пример структуры репозитория для документов по планированию и оцениванию функциональной безопасности

реализации отдельной процедуры. Для этого применяются специальные системы управления электронным документооборотом. В такой системе под каждый из проектов создается структура, называемая репозиторием, которая отражает структуру компонентов конфигурации (рис. 5).

Для реализации процесса разрабатывается план документирования (Document Plan), который должен определять:

применяемые в проекте форматы и шаблоны;

идентификацию документов;

используемые в проекте иностранные языки и подход к переводу документов;

требования к идентификации версий документов;

требования к выполнению рецензирования документов с применением средств разметки и трассировки;

политику предоставления доступа к документам.

Кроме того, в плане документирования для каждого из проектных документов должны быть определены идентификатор, наименование, а также лица, вовлеченные в процесс разработки (автор, верификатор и лицо, утверждающее документ).

Квалификация инструментальных средств. МЭК 61508 уделяет особое внимание инструментальным средствам (ИС), применяемым для разработки ИУС. В МЭК 61508–3 приведена классификация ИС по степени влияния на безопасность ИУС, которая определяет три категории ИС:

к категории Т1 относятся ИС, которые не влияют на исполняемый код ИУС; примером таких ИС являются текстовые редакторы, системы электронного документооборота, электронные таблицы;

к категории Т2 относятся ИС, которые поддерживают тестирование или другие методы верификации исполняемого кода ИУС (поэтому ошибка ИС может привести к необнаружению дефекта в ИУС, но не может непосредственно привести к появлению дефекта); примером таких ИС являются тестовые генераторы, ИС статического анализа, ИС оценивания полноты тестового покрытия;

к категории Т3 относятся ИС, которые непосредственно генерируют исполняемый код ИУС; примером таких ИС являются компиляторы кода, инструменты сборки кода, интегрированные среды разработки.

Перед началом разработки ИУС должны быть выполнены действия по квалификации (оцениванию) ИС, применяемых в проекте. Полученные результаты излагаются в отчете о выборе и оценивании ИС (Tool Selection and Evaluation Report).

Объем оценивания зависит от категории ИС. Для ИС категории Т3 применяется максимальный объем критериев оценивания. Такие критерии включают:

идентификацию ИС, включая назначение, наименование, производителя и номер версии;

обоснование выбора ИС с точки зрения выполняемого функционала;

содержание руководства пользователя, которое для ИС категории Т3 должно содержать аспекты безопасного применения; руководство пользователя также должно включать информацию по применению опций и установок ИС для генерации различных компонентов конфигурации;

опыт применения ИС как в компании, выполняющей проект, так и в других компаниях с учетом поддержки сопровождения и переходами между используемыми версиями;

информацию о процедурах тестирования и конфигурационного управления, применяемых разработчиком ИС;

информацию об известных дефектах ИС и методах избежания влияния этих дефектов на разрабатываемую ИУС;

подтверждение того, что ИС выполняет функции согласно спецификации; в качестве такого подтверждения для ИС категории Т3 может быть рассмотрен сертификат соответствия МЭК 61508; если такой сертификат отсутствует, требуется выполнение валидации ИС;

анализ механизмов отказов и стратегий их избежания.

Безопасный жизненный цикл. Безопасный жизненный цикл включает последовательность этапов, после каждого из которых выполняются действия по верификации и валидации (ВиВ). В МЭК 61508 рассматриваются следующие этапы [2]:

– А1: Разработка концепции продукта, основанной на маркетинговых исследованиях. Результат данного этапа — документ, описывающий концепцию продукта; ВиВ выполняют методом обзора;

– А2: Планирование безопасности. Результат этапа — планирующие документы, перечень которых приведен в левой части рис. 5. ВиВ выполняют методом обзора;

– А3: Разработка требований безопасности. Результат этапа — спецификация требований безопасности, которая описывает требования к продукту, как к «черному ящику», без привязки к компонентам; данные требования являются непосредственным входом для разработки продукта и должны далее трассироваться во все проектные документы, а затем покрываться тестами. ВиВ выполняют методом обзора;

– А4: Валидация, целью которой является подтверждение соответствия финального продукта спецификации требований безопасности; в жизненном цикле данный этап делится на две составляющие: сначала, по окончании этапа А3, разрабатывают план валидации, а финальным этапом разработки продукта является выполнение валидационного тестирования;

– А5: Разработка системного проекта (дизайна). Результат этапа — документ, описывающий архитектуру продукта с учетом распределения функций между компонентами ПО и ТС, а также взаимосвязей между

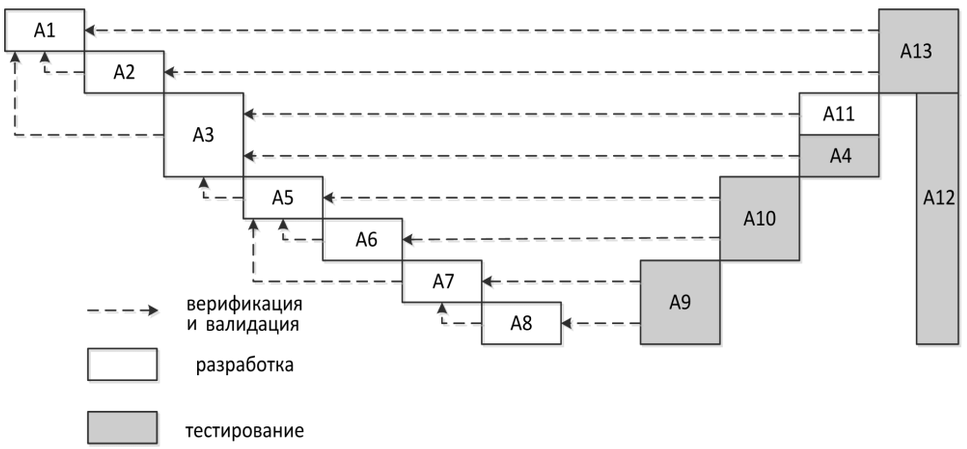

Рис. 6. Структура безопасного жизненного цикла

этими компонентами. ВиВ выполняют методом обзора. Требования системного проекта являются входом для интеграционного тестирования продукта (см. этап А10);

– А6: Проект ТС. Результат этапа — конструкторская документация (КД), позволяющая выпускать ТС на производственных мощностях. КД включает в себя спецификации компонентов, сборочные и монтажные чертежи, схемы электрические принципиальные, схемы печатных плат и т. п. ВиВ КД выполняют методом обзора. Для проекта ТС выполняют анализ надежности, а также анализ видов и последствий отказов (Failure Mode and Effect Analysis — FMEA). МЭК 61508 требует проведения по результатам FMEA так называемого тестирования с «засевом» дефектов (Fault Insertion Tests — FIT), когда в узлы ТС, а также в код ПО вносятся дефекты, а цель тестирования — демонстрация обнаружения внесенных дефектов средствами встроенного диагностирования; такие тесты проводят как часть интеграционного тестирования (см. этап А10);

– А7: Архитектурный проект ПО (для продуктов на базе ПЛИС применяется термин «электронный проект»). Результат этапа — документ, описывающий проект ПО верхнего уровня с учетом компонентов и интерфейсов между ними. ВиВ выполняют методом обзора. Требования системного проекта являются входом для интеграционного тестирования ПО (см. этап А9);

– А8: Детальный проект ПО и кодирование. В жизненном цикле данный этап делится на две части: сначала разрабатывают документ, описывающий детальный проект ПО для всех компонентов, определенных на этапе А7, а затем кодируют эти компоненты. ВиВ для детального проекта ПО выполняют методом обзора, ВиВ для кода — методом статического анализа;

– А9: Функциональное тестирование ПО. В жизненном цикле данный этап делится на две части: сначала тестируют отдельные компоненты ПО на соответствие требованиям детального проекта (см. этап А8), а затем интегрируют ПО и выполняют интеграционное тестирование ПО на соответствие требованиям архитектурного проекта (см. этап А7); для электронных проектов ПЛИС, кроме того, выполняют специфические виды тестирования, такие как логическое и временное моделирование, а также статический временной анализ [5];

– А10: Системная интеграция. На этом этапе интегрируют компоненты ТС и ПО, затем выполняют тестирование с «засевом» дефектов (см. этап А6), после чего — интеграционное тестирование продукта на соответствие требованиям системного проекта (см. этап А5);

– А11: Разработка руководства по безопасности. Результат этапа — документ, представляющий собой руководство пользователя продукта с учетом требований по безопасности. ВиВ выполняют методом обзора;

– А12: Аудиты функциональной безопасности. Данный этап реализуется периодически в процессе выполнения проекта. Его результат — оценка соответствия реализуемых процессов и полученных документов требованиям МЭК 61508 (см. рис. 5);

– А13: Независимая сертификация функциональной безопасности. В отличие от предыдущего этапа, данный этап выполняет независимый сертификационный орган после окончания выполнения проекта. Результат этапа — сертификат о соответствии продукта и процессов его разработки требованиям МЭК 61508 (см. рис. 5).

Укрупненная структура безопасного жизненного цикла с учетом последовательности этапов и выполнения ВиВ приведена на рис. 6. Номера этапов соответствуют их приведенному описанию.

Выводы

МЭК 61508 — современный стандарт, учитывающий передовой опыт в области оценивания и обеспечения функциональной безопасности ИУС. Процессы реализации безопасного жизненного цикла рассмотрены на основе опыта, полученного сотрудниками НПП «Радий» в ходе выполнения проекта по сертификации информационно-управляющей платформы RadICS на базе ПЛИС на соответствие требованиям стандарта МЭК 61508 (уровень интегрированности безопасности SIL3).

Завершение процесса сертификации и получение сертификата ожидается в 2014 г. Наличие сертификата значительно снижает риски лицензирования ИУС АЭС на базе платформы RadICS на различных международных рынках с использованием различной нормативной базы по безопасности. В 2013 г. «Радий» заключил контракт на поставку ИУС на базе платформы RadICS на канадский рынок. Данный проект является пилотным и должен быть выполнен в течение 2013 г.

Проект по сертификации ресурсоемкий, в настоящее момент затраты на проект составляют около 50 чел.-лет.

Применение требований МЭК 61508 повышает культуру разработки ИУС АЭС и их компонентов, вносит вклад в повышение культуры безопасности компании. Важны также внедрение в компании процедур проектного менеджмента [5], изучение международных требований и практик, усиление командной работы и профессиональный рост сотрудников.

Таким образом, соблюдение положений МЭК 61508 является хорошей практикой, направленной на повышение безопасности ИУС АЭС, которую можно рекомендовать для внедрения в нормативную практику Украины.

Список использованной литературы

1. *Smith D., Simpson K.* Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards. — Elsevier Butterworth-Heinemann, Oxford, UK, 2004. — 263 p.

2. *Medoff M., Faller R.* Functional Safety — An IEC 61508 SIL 3 Compatible Development Process — exida.com L.L.C., Sellersville, PA, USA, 2010. — 281 p.

3. Системы управления и защиты ядерных реакторов / [М. А. Ястребенецкий, Ю. В. Розен, С. В. Виноградская, Г. Джонсон, В. В. Елисеев, А. А. Сиора, В. В. Скляр, Л. И. Спектор, В. С. Харченко]; под. ред. М. А. Ястребенецкого. — К: Основа-Принт, 2011. — 768 с.

4. A Guide to the Project Management Body of Knowledge (PMBOK Guide). Fourth Edition. — Project Management Institute, 2008. — 467 p.

5. *Скляр В. В.* Качество программно-технических комплексов: процессный подход. Лекционный матеріал / Под ред. Харченко В. С. — Харьков: Нац. аэрокосмический университет им. Н. Е. Жуковского «ХАИ», 2013. — 133 с.

References

1. *Smith D., Simpson K.* Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards. — Elsevier Butterworth-Heinemann, Oxford, UK, 2004. — 263 p.

2. *Medoff M., Faller R.* Functional Safety — An IEC 61508 SIL 3 Compatible Development Process — exida.com L.L.C., Sellersville, PA, USA, 2010. — 281 p.

3. Nuclear Reactors Safety Control Systems / [M. A. Yastrebenetsky, Yu. V. Rozen, S. V. Vinogradskaya, G. Jonson, V. V. Eliseev, A. A. Siora, V. V. Sklyar, L. I. Spektor, V. S. Kharchenko]; Yastrebenetsky M. A. (edit.) — Kyiv: Osnova-Print, 2011. — 768 p.

4. A Guide to the Project Management Body of Knowledge (PMBOK Guide). Fourth Edition. — Project Management Institute, 2008. — 467 p.

5. *Sklyar V. V.* Quality of Instrumentation and Control Systems: a Process Approach. Lectures / Kharchenko V. S. (edit.) — Kharkiv: National aerospace university named after N. Zhukovsky “KhAI”, 2013. — 133 p.

Получено16.09.2013.