УДК 004.054

В.В. Скляр

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

МЕТОД СЕРТИФИКАЦИИ ИУС НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ К ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В статье представлены результаты разработки метода сертификации ИУС на соответствие требованиям к функциональной безопасности. Данный метод базируется на постановке и решении задачи выбора оптимальной стратегии сертификации по критерию "объем оборудования / затрачиваемые ресурсы".

Ключевые слова: *сертификация, информационно-управляющая система, функциональная безопасность.*

1. Анализ проблемы

Обеспечение функциональной безопасности (ФБ) информационно-управляющих систем (ИУС) проводятся в рамках концепции обеспечения техногенной безопасности. При этом возможны следующие типовые сценарии [1]:

– разработка ИУС для нового технического комплекса критического использования (ТККИ) – при этом основным критерием является требование, чтобы риск ТККИ соответствовал установленным требованиям для данного класса техногенных объектов; при этом риск должен быть оправдан экономической выгодой, получаемой обществом от эксплуатации потенциально опасного ТККИ; технический прогресс, в том числе и прогресс информационных технологий, приводит к тому, что требования к безопасности ТККИ постоянно пересматриваются и ужесточаются;

– модернизация ИУС в рамках модернизации ТККИ – при этом основным критерием является требование, чтобы суммарный риск ТККИ после модернизации не превышал риск ТККИ после модернизации; также, весьма обязательным иногда является требование, чтобы после модернизации риск ТККИ соответствовал установленным требованиям для данного класса объектов (например, после аварии на АЭС Фукусима были выдвинуты требования по переоценке безопасности существующих АЭС).

Сертификация является обязательным процессом для ИУС ТККИ. При этом под сертификацией понимается подтверждение соответствие продукта и процессов его создания установленным требованиям. Обычно сертификация завершает разработку ИУС, и без нее невозможно получение разрешения на ввод системы в эксплуатацию. При подготовке к сертификации важным этапом является определение общей стратегии сертификационных работ. В известных работах по ФБ [2, 3] данному вопросу не уделялось достаточно внимания.

На практике крайне важным является эффективное с точки зрения затрат проведение сертификации, которое позволило бы в кратчайшие сроки вывести на рынок максимальный объем оборудования. Например, стоимость сертификации на новом рынке цифровой платформы, на базе которой могут быть построены ИУС, важные для безопасности АЭС, оценивается в 1 млн. долларов.

Таким образом, эффект от оптимального выбора стратегии сертификации может быть весьма существенным.

В данной статье представлены результаты разработки метода сертификации ИУС на соответствие требованиям к ФБ.

2. Постановка и решение оптимизационных задач при сертификации ИУС

Рассматриваемый в статье метод базируется на постановке и решении задачи выбора оптимальной стратегии сертификации по критерию "объем оборудования / затрачиваемые ресурсы".

Рассмотрим исходные данные для постановки задачи выбора оптимальной стратегии сертификации [4, 5].

Обычно, исходя из маркетинговой стратегии предприятия, определяется время на сертификацию, которое соответствует времени вывода товара на рынок TTM (Time to Market – время до выхода на рынок). Если умножить параметр TTM на количество человек N, занятых в проекте по сертификации, то получим суммарное количество человеко-часов – $N \cdot TTM$. Однако это значение является теоретическим, поскольку персонал, занятый в проекте, как правило, не может 100% рабочего времени выполнять действия, связанные с сертификацией. Часть рабочего времени будет посвящена исполнению основных служебных обязанностей. Данный факт может быть учтен через так называемый фокус-фактор FF, который имеет значение от 0 до 1 и определяет, какую долю времени сотрудник выполняет работу по сертификации. Поскольку для каждого сотрудника фокус-фактор может иметь индивидуальное значение, целесообразно вводить оценку

временных ресурсов (человеко-часов) проекта основанную на интеграции индивидуальных оценок:

$$RT=\sum_{k=1}^{N} RT_k=\sum_{k=1}^{N} FF_k \cdot TTM \qquad (1)$$

где RT_k – временные ресурсы k-го сотрудника, вовлеченного в проект по сертификации; FF_k – фокус-фактор k-го сотрудника, вовлеченного в проект по сертификации; N – количество сотрудников, вовлеченных в проект по сертификации; TTM – календарное время, отводимое на сертификацию.

Временные ресурсы проекта могут быть преобразованы в денежное измерение, если в выражение (1) ввести почасовую оплату для сотрудников:

$$RC=\sum_{k=1}^{N} RC_k=\sum_{k=1}^{N} FF_k \cdot SAL_k \cdot TTM\,, \qquad (2)$$

где RC_k – финансовые ресурсы, затрачиваемые на k-го сотрудника, вовлеченного в проект по сертификации; SAL_k – финансовое вознаграждение за 1 час работы для k-го сотрудника, вовлеченного в проект по сертификации.

Выражение (2) может учитывать как затраты на оплату труда сотрудников предприятия, так и затраты на оплату труда внешним консультантам, привлекаемым для выполнения технического консалтинга по сложным проектам.

Для постановки задачи оптимизации может быть использован как временной, так и денежный измерители, в зависимости от того, какой показатель для предприятия является более важным: время выхода на рынок или доступные для сертификации фонды. Кроме того, планирование сертификации требует выделения из общего процесса отдельных задач сертификации $Task_i$, которые характеризуются следующими параметрами:

– требуемыми ресурсами RT_i и RC_i;

– компонентами K_{ij}, j = 1,…,m, сертификация которых реализуется при выполнении i-й задачи;

– приоритетами Pr_i, которые расставляются, исходя из того, какие сертификацию каких компонентов затрагивает выполнение i-й задачи; приоритеты могут быть установлены, в том числе, и для задач, выполняемых в процессе сертификации ядра.

После получения описанных выше исходных данных может быть сформулирована и решена задача выбора стратегии сертификации, которая является оптимизационной и имеет следующую постановку: в рамках заданных ресурсов (т.е. за заданное время, либо, не превышая заданную стоимость) сертифицировать максимально возможное количество компонентов, согласно установленным для них приоритетам. Для общности введем для временных и денежных ресурсов обобщенное обозначение Resource. Данная оптимизационная задача является задачей динамического программирования, поскольку представление исходных данных подразумевает аддитивную целевую функцию и аддитивные ограничения [6].

Задача выбора стратегии сертификации. Найти совокупность сертифицируемых компонентов, для которых сумма приоритетов $Pr \to max$ при $Resource \le Resource_{заданное}$.

Целевой функцией является

$$f(Pr)=\sum_{i=1}^{M} Pr_i \cdot \frac{1}{Recource_i} \;\to\; max$$

при ограничениях

$$\sum_{i=1}^{M} Resource_i \le Resource_{ЗАДАННОЕ}\,.$$

Решение такой задачи включает следующую последовательность действий:

1. Присвоение суммарному ресурсу значения Resource = 0 и счетчику итераций значения s = 0.

2. Построение для задач сертификации кортежа

$$Pr^{(M-s)} / Resource^{(M-s)} \left\langle \frac{Pr_i}{Resource_i} \right\rangle .$$

3. Выбор максимального элемента кортежа

$$\frac{Pr_i}{Resource_i} = max\,.$$

4. Проверка условия существования нескольких элементов кортежа с одинаковым максимальным значением.

5. Если существует несколько элементов кортежа с одинаковым максимальным значением, то следует выбрать ту задачу сертификации, для которой $Resource_i = Resource_i\ min$.

6. Если условие 4 не выполняется, то суммарному ресурсу присваивается значение

$$Resource=Resource+Resource\left(\frac{Pr_i}{Resource_i}=max\right)$$

и счетчику значения s = s + 1. Выбор задачи сертификации Taski и включение ее в перечень работ по выполнению сертификации.

7. Проверка условия $Resource > Resource_{заданное}$. Если данное условие выполняется, то выполнение алгоритма заканчивается.

8. Если условие, указанное в действии 7 не выполняется, то из кортежа $Pr^{(M-s)}/Resource^{(M-s)}$ удаляется элемент, выбранный на шаге 3.

После этого снова выполняются шаги 2 – 8.

Решением задачи является множество задач сертификации $Task(Pr \to max) = \{Task_i\}$, для которого имеем значение приоритетов сертифицируемых компонентов

$$Pr=\sum_i Pr\left(\frac{Pr_i}{Resource_i}=max\right)$$

и значение требуемых ресурсов

$$\text{Resource}=\sum_i \text{Resource}\left(\frac{\text{Pr}_i}{\text{Reource}_i}=\max\right).$$

Обратная задача выбора стратегии сертификации. Найти совокупность сертифицируемых компонентов: Resource → min при Pr ≥ $\text{Pr}_{\text{заданное}}$.

Такая задача реже применяется на практике, поскольку сложно определить требуемое значение приоритета для множества компонентов платформы. Тем не менее, ниже приводится решение сформулированной задачи.

Целевой функцией является

$$\text{f(Resource)}=\sum_{i=1}^{M}\text{Resource}_i\cdot\frac{1}{\text{Pr}_i}\ \rightarrow\ \min$$

при ограничениях

$$\sum_{i=1}^{M}\text{Pr}_i \geq \text{Pr}_{\text{ЗАДАННОЕ}}.$$

Решение такой задачи включает следующую последовательность действий:

1. Присвоение суммарному приоритету Pr = 0 и счетчику итераций значения s = 0.

2. Построение кортежа

$$\text{Resource}^{(M-s)}/\text{Pr}^{(M-s)}=\left\langle\frac{\text{Resource}_i}{\text{Pr}_i}\right\rangle.$$

3. Выбор минимального кортежа

$$\frac{\text{Resource}_i}{\text{Pr}_i}=\min.$$

4. Проверка условия существования нескольких элементов кортежа с одинаковым минимальным значением.

5. Если существует несколько элементов кортежа с одинаковым минимальным значением, то следует выбрать ту задачу сертификации, для которой $\text{Pr}_i = \text{Pr}_i$ max.

6. Если условие 4 не выполняется, то суммарному значению приоритета присваивается

$$\text{Pr}=\text{Pr}+\text{Pr}\left(\frac{\text{Resourse}_i}{\text{Pr}_i}=\min\right)$$

и счетчику значения s = s + 1. Выбор задачи сертификации Task_i и включение ее в перечень работ по выполнению сертификации.

7. Проверка условия Pr ≥ $\text{Pr}_{\text{заданное}}$. Если данное условие выполняется, то выполнение алгоритма заканчивается.

8. Если условие, указанное в действии 7 не выполняется, то из кортежа $\text{Resource}^{(M-s)}/\text{Pr}^{(M-s)}$ удаляется элемент, выбранный на шаге 3.

После этого снова выполняются шаги 2 – 8.

Решением задачи является множество контрмер для снижения риска активов задач сертификации Task(Resource → min) = {Resource_i}, для которых имеем значение приоритета

$$\text{Pr}=\sum_i \text{Pr}\left(\frac{\text{Resource}_i}{\text{Pr}_i}=\min\right)$$

и значение ресурсов

$$\text{Resource}=\sum_i \text{Resource}\left(\frac{\text{Resource}_i}{\text{Pr}_i}=\min\right).$$

Вычислительная сложность алгоритмов определяется количеством итераций, соответствующих количеству задач сертификации. Точность решения алгоритмов определяется тем, что в соответствии с постановкой имеется единственное решение, поскольку выбирается уникальное множество элементов кортежа.

3. Этапы метода сертификации ИУС на соответствие требованиям к функциональной безопасности

Метод сертификации ИУС на соответствие требованиям к функциональной безопасности включает следующие этапы (рис. 1).

1. Определение расходов на сертификацию. Значение данного показателя необходимо определить в связи с его влиянием на выбор стратегии сертификации. Временные ресурсы RT определяем согласно формуле (1), а финансовые ресурсы RC определяем согласно формуле (2). В дальнейшем для решения оптимизационной задачи может быть использован только один из видов ресурсов. Кроме того, значения RT и RC могут быть назначены, исходя из стратегии развития предприятия, либо, исходя из имеющихся в наличии времени и средств.

2. Определение ядра сертификации. При планировании сертификации и расстановке приоритетов может быть выделено так называемое ядро сертификации с наивысшим приоритетом, на которое требуются ресурсы RTCORE или же RCCORE. Без выполнения работ по сертификации ядра не может быть выполнена сертификация остальных компонентов. Тогда фактически из ресурсов, доступных для сертификации остается: ΔRT = RT – RTCORE (ΔRC = RC – RCCORE). Ядро сертификации может быть зафиксировано либо же для него также могут быть определены задачи сертификации и установлены приоритеты (см. шаги 3,5).

3. Определение задач сертификации. Общий объем работ по проекту декомпозируется на ряд задач, которые могут, например, включать:

– организацию работ по выполнению проекта;

– документирование;

– реализацию процессов жизненного цикла компонентов;

– разработку компонентов;

– верификацию компонентов;

– оценку безопасности и т.д.

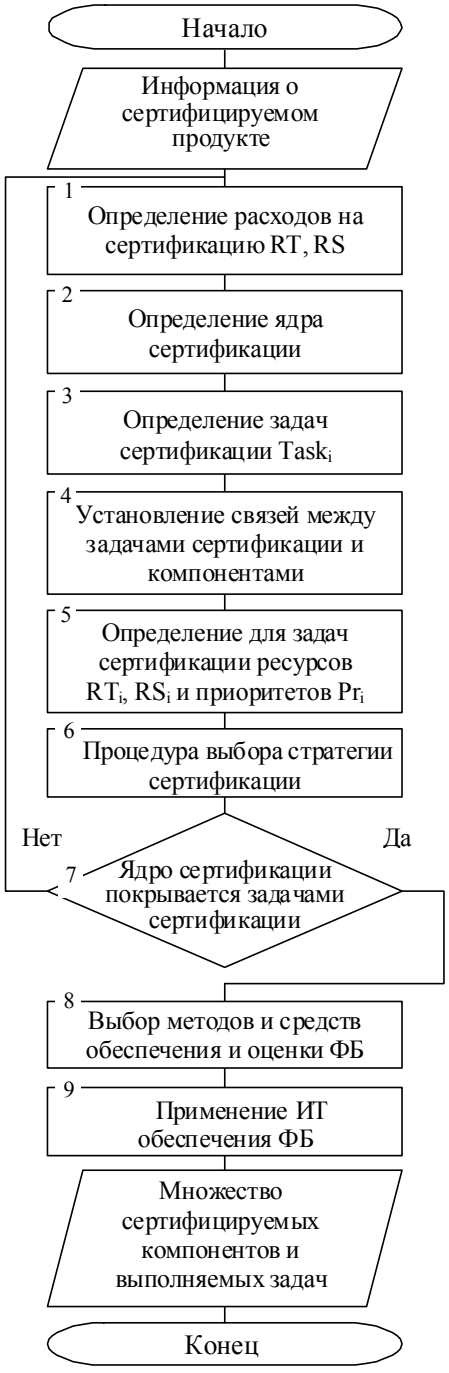

Рис. 1. Этапы метода сертификации ИУС на соответствие требованиям к ФБ

4. Установление связей между задачами сертификации и компонентами. Задачи сертификации могут относиться ко всем, к одному или к нескольким компонентам. Для последующей объективной установки приоритетов должны быть установлены связи между задачами сертификации и сертифицируемыми компонентами. Связи могут иметь один из следующих типов:

– "один-к-одному" – единственная задача сертификации выполняется только для одного компонента;

– "один-ко-многим" – единственная задача сертификации выполняется для нескольких компонентов;

– "многие-к-одному" – несколько задач сертификации выполняется для одного компонента;

– "многие-ко-многим" – несколько задач сертификации выполняется для нескольких компонентов.

5. Определение для задач сертификации ресурсов и приоритетов.

Осуществляется оценка трудоемкости задач сертификации, в соответствии с которой для задач $Task_i$, определяются по формулам (6.1) и (6.2) необходимые временные и финансовые ресурсы RT_i и RC_i. Соответственно для задач сертификации устанавливаются приоритеты Pr_i.

Задача определения приоритетов в данной работе не рассматривается. На практике для этого могут быть применены стандартные методы взвешивания или ранжирования [7, 8].

6. Процедура выбора стратегии сертификации. Для этого решается оптимизационная задача которая, имеет следующую постановку: в рамках заданных ресурсов (т.е. за заданное время, либо, не превышая заданную стоимость) сертифицировать максимально возможное количество компонентов, согласно установленным для них приоритетам.

7. Если ядро сертификации покрывается задачами сертификации, то на этом задача выбора стратегии верификации считается завершенным, и может быть осуществлен переход к оценке ФБ ИУС и ее компонентов.

В противном случае ресурсов, выделенных на сертификацию, оказывается недостаточным для сертификации ядра.

Тогда объем ресурсов должен быть пересмотрен, после чего повторяются шаги 1-7.

8. Выбор методов и средств обеспечения и оценки ФБ. При сертификации происходит выполнение обеспечения и оценки ФБ ИУС и сертифицированных компонентов. Для этого в полном объеме или частично может быть использована информационная технология (ИТ) обеспечения и оценки ФБ.

Таким образом, необходимо определить, какой объем таких методов и средств будет задействован для реализации целей и задач сертификации.

9. После выбора методов и средств обеспечения и оценки ФБ осуществляется их применение в составе информационной технологии обеспечения и оценки ФБ.

Выводы и направления дальнейших исследований

Для поддержки существующих методов и моделей обеспечения и оценивания ФБ ИУС [1 – 3] требуется их внедрение в процессы жизненного цикла системы. Такое внедрение может быть обеспечено в рамках сертификации ИУС и ее компонентов на соответствие требованиям по безопасности. В области важных для безопасности ИУС сертификация также заключается в обеспечении и оценивании ФБ ИУС.

Основой полученного метода сертификации ИУС на соответствие требованиям к функциональной безопасности является задача выбора стратегии сертификации, которая является оптимизационной и имеет следующую постановку: в рамках заданных ресурсов (т.е. за заданное время, либо, не превышая заданную стоимость) сертифицировать максимально возможное количество компонентов, согласно установленным для них приоритетам. Данная оптимизационная задача является задачей динамического программирования, поскольку представление исходных данных подразумевает аддитивную целевую функцию и аддитивные ограничения.

Теоретический аспект разработанного метода сертификации заключается в том, что он базируется на действенном критерии оптимизации "объем оборудования / затрачиваемые ресурсы". Данный критерий имеет также практическую ценность, поскольку позволяет планировать и оптимизировать ресурсы на обеспечение и оценивание ФБ ИУС. В комплексе с оптимизацией расходов на сертификацию и лицензирование такой подход позволяет повысить эффективность затрат по разработке оборудования.

Разработанный метод сертификации может быть положен в основу соответствующей информационной технологии.

Список литературы

1. Скляр, В.В. Методология риск-анализа функциональной безопасности информационно-управляющих систем [Текст] / В.В. Скляр // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения. – Х.: Нац. аэрокосмический ун-т «ХАИ», 2011. – Раздел 12. – С. 360-408.

2. Безопасность атомных станций: Информационные и управляющие системы [Текст] / М.А. Ястребенецкий, В.Н. Васильченко, и др.; под ред. М.А. Ястребенецкого. – К.: Техніка, 2004. – 472 с.

3. Ястребенецкий, М.А. Автоматика АЭС Украины после Чернобыльской аварии [Текст] / М.А. Ястребенецкий // Ядерна та радіаційна безпека. – 2011. – Т. 14, № 1. – С. 47–52.

4. Требования к разработке, верификации, сертификации и сопровождению программного обеспечения бортовой авиационной техники: опыт создания и использования стандарта предприятия [Текст] / В.В. Скляр, В.Б. Остроумов, Н.Ф. Сидоренко, В.С. Харченко // Авиационно–космическая техника и технология. – 2007. – № 6(42). – С. 94–99.

5. Andrashov, A. Certification of FPGA–based Safety Instrumentation and Control Platform in Accordance with IEC 61508 [Text] / A. Andrashov, V. Kharchenko, A. Siora, V. Sklyar, A. Volkoviy // Critical Infrastructure Safety and Security (CrlSS–DESSERT 2011): proceedings of the First International Workshop. – Kharkiv, 2011. – V. 1. – P.148 – 152.

6. Петров, Э.Г. Методы и средства принятия решений в социально-экономических и технических системах [Текст] / Э.Г. Петров, М.В. Новожилова, И.В. Гребенник, Н.А. Соколова. – Херсон: ОЛДИ-плюс, 2003. – 380 с.

7. Надежность технических системы: Справочник [Текст] / Ю.К. Беляев, В.А. Богатырев, В.В. Болотин и др.; под ред. И.А.Ушакова. – М. Радио и связь, 1985. – 608 с.

8. Корн, Г. Справочник по математике для научных работников и инженеров [Текст] / Г. Корн, Т. Корн. – М.: Наука, 1970. – 720 с.

Поступила в редколлегию 29.01.2014

Рецензент: д-р техн. наук проф. В.А. Краснобаев, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава.

МЕТОД СЕРТИФІКАЦІЇ ІУС НА ВІДПОВІДНІСТЬ ВИМОГАМ ДО ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ

В.В. Скляр

У статті представлені результати розробки методу сертифікації інформаційно-управляючих систем (ІУС) на відповідність вимогам до функціональної безпеки. Даний метод базується на постановці та вирішенні задачі вибору оптимальної стратегії сертифікації за критерієм "обсяг обладнання / витрачаємі ресурси".

Ключові слова: *сертифікація, інформаційно-управляюча система, функціональна безпека.*

CERTIFICATION METHOD OF I&C SYSTEMS COMPLIANCE WITH FUNCTIONAL SAFETY REQUIREMENTS

V.V. Sklyar

The article presents the development results of the certification method of Instrumentation and Control (I&C) systems i compliance with functional safety requirements. This method is based on the solution of the task of choosing the optimal strategy certification by criterion "a scope of equipment / resources spent."

Key words: *certification, Instrumentation and Control system, functional safety.*