СЕКЦИЯ 9: УПРАВЛЕНИЕ РАЗВИТИЕМ АВИАЦИОННО-КОСМИЧЕСКИХ И ДРУГИХ КРУПНОМАСШТАБНЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ КОМПЛЕКСОВ

ИСПОЛЬЗОВАНИЕ СРЕДСТВ МОДЕЛЕ-ОРИЕНТИРОВАННОЙ СИСТЕМНОЙ ИНЖЕНЕРИИ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ В ПРОЕКТАХ СОЗДАНИЯ СОВРЕМЕННЫХ АВИАЦИОННЫХ СИСТЕМ

Балашов Ю.В., Лобановский Ю.И.

ПАО «Корпорация «Иркут»,
Россия, г. Москва Российская Федерация, Ленинградский проспект, д. 68
balur@list.ru , streamphlow@gmail.com,

Батоврин В.К.

РТУ МИРЭА,
Россия, г. Москва Российская Федерация, проспект Вернадского, д. 78
batovrin@mirea.ru

Аннотация: рассмотрены возможности оценки безопасности, включая построение деревьев отказов с учетом эффектов межсистемного взаимодействия и каскадных отказов, на основе анализа функциональной архитектуры воздушного судна и его систем, который поддерживается средствами моделе-ориентированной системной инженерии.

Ключевые слова: моделе-ориентированная системная инженерия, функциональная архитектура, оценка безопасности, каскадный отказ.

Введение

Оценка безопасности является одной из ключевых составляющих в проектах создания современных авиационных систем. Необходимость подобной оценки применительно к самолетам и высокоинтегрированным системам самолетов, а также требования к ее содержанию закреплены, в частности, в общепризнанных стандартах ARP 4754A и ARP4761 [1, 2]. В контексте указанных стандартов, которые рекомендованы к использованию и в нашей стране, важнейшее значение приобретает определение функциональной архитектуры самолета и его систем, описание которой используется в качестве основы в процессе выявления и ранжирования функциональных угроз.

Отечественный опыт и рекомендации по построению и прикладному использованию функциональной архитектуры инженерных систем, включая авиационные системы, отсутствуют. С другой стороны, общепринятой практикой системной инженерии является согласованное применение подхода жизненного цикла и архитектурного подхода. Эта практика подразумевает использование модели жизненного цикла в качестве концептуальной основы процессов и действий, относящихся к развитию инженерных систем на протяжении их существования, в сочетании с формированием многоаспектного представления об объекте архитектуры в его окружающей среде, а также принципов реализации и эволюции этого объекта и связанных с ним процессов жизненного цикла [3 – 6]. Таким образом, стоит задача адаптации практик системной инженерии и требований стандартов ARP 4754A и ARP 4761 к условиям отечественных авиационных проектов. Причем, при решении задачи адаптации необходимо принимать во внимание, что зачастую в этих проектах построение функциональной архитектуры самолета подразумевает использование обратного инжиниринга.

Важной особенностью современных самолетов и их ключевых систем является то, что в процессе оценки безопасности приходится одновременно рассматривать многие сотни функций с учетом их взаимодействия. Практическое решение подобной задачи невозможно без формализованного применения системной инженерии в сочетании с компьютерным моделированием, поддерживающим на протяжении жизненного цикла авиационной системы выработку требований к системе, инженерию архитектуры, собственно системное проектирование, системный анализ и другие процессы. Такие возможности предоставляет моделе-ориентированная системная инженерия (Model-Based Systems Engineering, MBSE). Использование MBSE предполагает, что вся деятельность по созданию системы привязана к развитой совокупности моделей, а сами модели управляются, контролируются и интегрируются в увязке с другими методами и инструментами системной

инженерии, которые обеспечивают развитие системы на протяжении ее жизненного цикла [7, 8]. На практике MBSE опирается на определенный комплекс средств, включая метод моделирования, адаптированный к условиям проекта, определенный язык моделирования и специальные инструменты моделирования, разработанные и реализованные в соответствии с правилами принятого языка моделирования [9]. Таким образом, для практического решения задачи оценки безопасности современного самолета и его систем необходимо, чтобы средства MBSE обеспечивали комплексную поддержку инженерии архитектур технических систем.

В докладе рассматриваются предварительные результаты использования MBSE в интересах оценки безопасности в рамках проектов создания авиационных систем.

1 Жизненный цикл самолета и оценка безопасности

При создании самолетов и его систем естественно использовать модель жизненного цикла, принятую в авиационной отрасли. Такую модель предоставляет стандарт ARP 4754A. Согласно его положениям в жизненном цикле самолета и его систем выделяются три укрупненные стадии – концептуальное проектирование, разработка, производство/ эксплуатация. Основное внимание уделяется стадии разработки, в составе которой выделяются этапы определения функций, разработки архитектуры, проектирования и реализации. Для наполнения этой модели используются процессы жизненного цикла с выделением трех групп: процесс разработки воздушного судна/ систем, общие процессы и процесс планирования разработки.

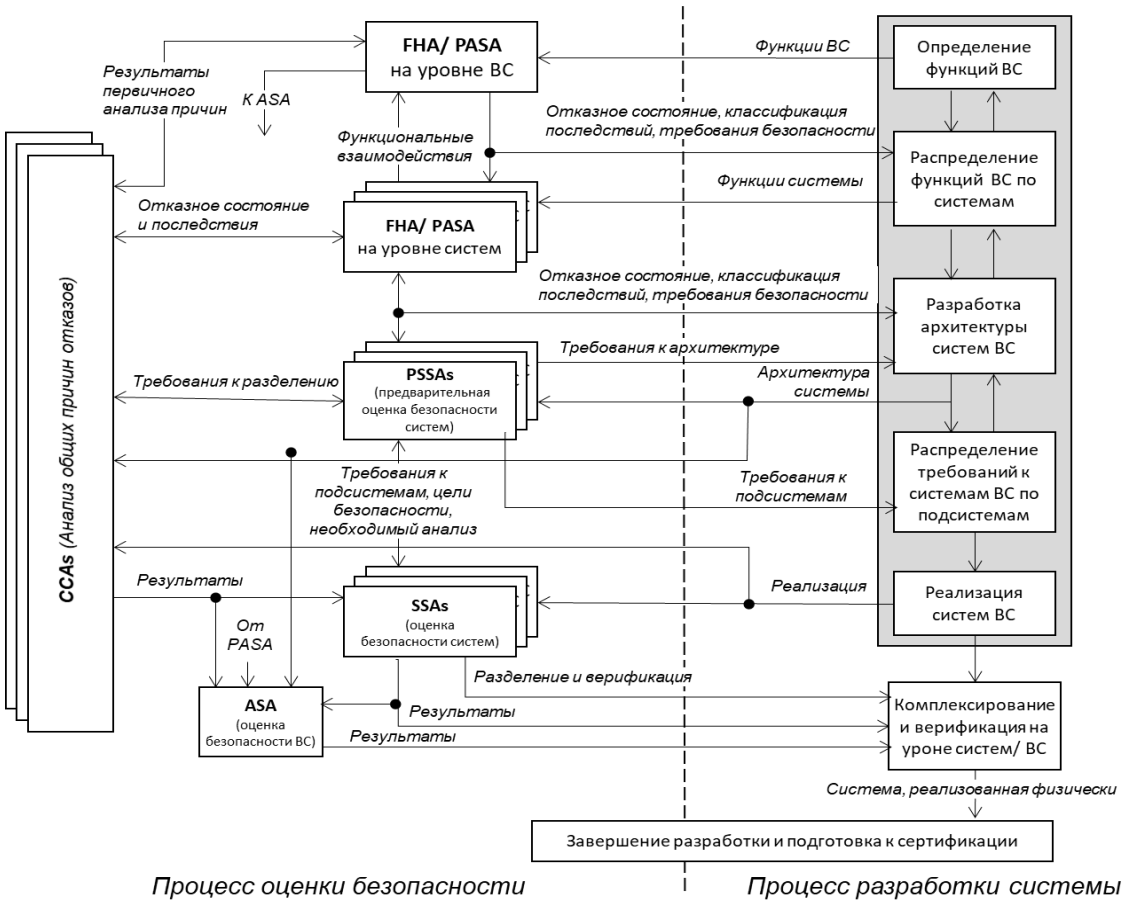

Рис. 1. Модель оценки безопасности согласно ARP 4754A (FHA – оценка функциональных угроз; PASA – предварительная оценка безопасности самолета, ВС – воздушное судно)

Процесс разработки воздушного судна/ систем (см. рис.1) включает пять действий – определение функций самолета, распределение функций самолета по системам, разработку архитектуры систем, распределение требований к системам самолета по подсистемам и реализацию систем самолета. Общие процессы жизненного цикла летательного аппарата и его основных систем включают: (а) оценку безопасности; (б) присвоение уровня гарантий проектирования; (в) определение требований; (г) валидацию требований; (д) управление конфигурацией; (е) гарантирование процессов, (ж) сертификацию и координацию деятельности с регулирующими органами. Процесс планирования

разработки нацелен на определение таких путей реализации летательного аппарата/систем, при которых будут удовлетворены требования, предъявляемые к летательному аппарату/системе и обеспечен необходимый уровень гарантий в отношении требований летной годности. Процесс планирования предполагает планирование жизненного цикла, взаимосвязей между процессами жизненного цикла, их последовательности, механизмов обратной связи и определение критериев перехода.

Модель оценки безопасности, рекомендованная ARP 4754A для проектов создания воздушных судов, показана на рис.1. Как видно, процесс оценки безопасности и процесс разработки неразрывно связаны между собой, причем эта связь определяется в привязке к функциональной и другим архитектурам самолета и его систем. Таким образом, использование архитектурного подхода является неотъемлемой частью рекомендованной модели оценки безопасности, причем, в этой модели архитектурный подход увязан с подходом жизненного цикла.

При практическом использовании модели оценки безопасности, рекомендованной стандартом ARP 4754A, сначала, в привязке к самолету в целом, проводится оценка функциональных угроз (Functional Hazard Assessment, FHA), при этом в качестве исходных данных используются сведения, полученные в результате определения функциональной архитектуры самолёта. Затем, после распределения функций самолета по его системам, FHA выполняется для каждой из этих систем, а в качестве исходных данных используются сведения, полученные в результате определения функциональной архитектуры систем более низкого иерархического уровня. По существу, FHA является методом прогнозирования, занятым исследованием последствий функциональных отказов отдельных систем или их частей. В основе FHA лежит рассмотрение гипотетических функциональных сбоев (потеря функции, некорректная реализация функции и т.п.) на основе анализа целей, для достижения которых реализуется функция, и поведения, связанного с реализацией этой функции, а в качестве основы всегда используются описания функциональной архитектуры на разных иерархических уровнях.

Как следует из сказанного для непосредственного использования рекомендованной ARP 4754A модели оценки безопасности в проектах создания авиационных систем предприятию следует наладить зрелый процесс системной инженерии, в основе которого должны лежать согласованные между собой подход жизненного цикла и архитектурный подход.

2 Разработка функциональной архитектуры

Функциональная архитектура отражает основные особенности и свойства системы, характеризующие ее функционирование в окружающей среде и воплощенные в функциональных элементах системы, отношениях между ними, а также в принципах проектирования и развития системы [4, 5]. Функциональная архитектура дает полное представление об упорядоченной совокупности функций (включая их составляющие) и интерфейсов (внутренних и внешних) и определяет последовательность выполнения функций, а также порядок и правила преобразования входных материальных, энергетических и информационных потоков в выходные потоки, осуществляемого системой в связи с выполнением своих задач. Кроме того, функциональная архитектура отражает сценарий функционирования системы, условия управления или обмена данными, а также помогает обосновать требования к функциональным характеристикам, необходимые для успешной реализации исходной совокупности требований. Для разработки функциональной архитектуры используется функциональный анализ. Функциональный анализ – это процесс системной инженерии, направленный на систематическое изучение функций существующей или создаваемой системы [10]. В процессе функционального анализа функции системы анализируются в контексте удовлетворения нужд и требований заинтересованных сторон с целью определения всех подфункций, необходимых для выполнения анализируемой функции; выявления функциональных взаимосвязей и интерфейсов (внутренних и внешних) и их отражения в функциональной архитектуре; определения требований к функциональным характеристикам на уровне системы в целом и отнесения этих требований к подфункциям более низкого уровня.

Некоторые рекомендации по выполнению функционального анализа и синтезу функциональной архитектуры применительно к авиационным системам содержатся, например, в [11, 12]. Здесь мы отметим, что основными результатами функционального анализа при создании авиационных систем являются:

- *Выделение функциональных границ,* определенных в контексте ожидаемых поведения и свойств системы.
- *Документирование всех функций системы,* определенных в контексте назначения системы и реализации ожиданий заинтересованных сторон. Для определения этих функций могут быть задействованы различные уровни системной иерархии и использованы различные методы и инструменты, включая построение контекстных диаграмм, функциональной иерархии, диаграмм функциональных потоков и N^2 диаграмм.
- *Определение обязательных ограничений,* связанных с практической реализацией и обусловленных неизбежными ограничениями, а также ожиданиями заинтересованных сторон.
- *Выделение функциональных интерфейсов,* включая полное определение функциональных взаимодействий между функциями и подфункциями, а также с окружающей средой и внешними системами.
- *Верификация результатов* функционального анализа на основе концепции операций.
- *Валидация результатов* функционального анализа в контексте удовлетворения нужд и требований заинтересованных сторон.

Мы полагаем, что каждая функция, полученная в результате функционального анализа, должна обладать определенными характеристиками, среди которых:

- *Необходимость*, т.е. функция должна определять существенную задачу, операцию, действие или деятельность, которые должны быть осуществлены или выполнены для достижения желаемого результата. Если функция будет проигнорирована или устранена, то в поведении самолета возникнут недостатки, которые не смогут быть полностью устранены за счет других возможностей системы, продукции или процесса.
- *Независимость от реализации*, т.е. функция, определяя поведение, объективно присущее или характерное для системы или ее элемента, несет информацию о том, что требуется, а не о том, как это может или должно быть выполнено.
- *Недвусмысленность,* т.е. функция должна быть определена таким образом, чтобы она могла интерпретироваться только одним способом. Описание функции должно быть простым и легким для понимания.
- *Непротиворечивость,* т.е. функция не должна противоречить другим функциям.
- *Реализуемость,* т.е. функция с приемлемым риском может быть технически реализована с учетом ограничений, накладываемых со стороны системы (затраты, график, технические и технологические возможности, правовые и нормативные ограничения и т.п.).
- *Прослеживаемость,* т.е. функция должна быть прослеживаемой снизу-вверх к конкретной, документально зафиксированной потребности (потребностям) или требованиям заинтересованных сторон, а также прослеживаемой сверху-вниз к конкретным функциям, определенным в спецификациях более низкого уровня. Таким образом, все относящиеся к функции связи «порождающий/порожденный» определяются так, чтобы функция прослеживалась как к ее источнику, так и ко всем производным функциям.
- *Верифицируемость,* т.е. функция должна быть определена так, чтобы имелась возможность получения объективного свидетельства того, что она реализована в системе.

В работе [13] мы предложили методику построения функциональной архитектуры самолета и его систем. Анализ этой архитектуры, который выполнялся с использованием обратного инжиниринга, показал, что характеристики целого ряда задокументированных функций не отвечают указанным выше требованиям. Соответственно, такие функции не могут без внесения изменений участвовать в процессе анализа безопасности. Отметим также, что при использовании обратного инжиниринга результаты анализа функциональной архитектуры служат естественной основой для планирования и реализации подобных изменений.

3 Метод моделе-ориентированной системной инженерии ARCADIA, поддерживаемый языком концептуального моделирования Capella

Имеется единственное стандартизированное средство MBSE, доступное для использования в нашей стране и поддерживающее инженерию архитектур применительно к промышленной продукции.

Метод моделе-ориентированной системной инженерии ARCADIA (ARChitecture Analysis and Design Integrated Approach) может применяться для разработки архитектуры систем любого типа, включая аппаратные средства системы и ее программное обеспечение [14]. Метод ARCADIA

предназначен для формирования и анализа семейства связанных между собой моделей, отражающих различные аспекты архитектуры и условий применения системы. При моделировании систем по методу ARCADIA используется несколько точек зрения на архитектуру системы, причем, процедуры анализа потребностей заинтересованных сторон четко отделены от процедур определения системного решения, пригодного для удовлетворения этих потребностей. Для поддержки метода ARCADIA используется язык ArcML [15], а в качестве инструмента моделирования применяется Capella – программное средство с открытым исходным кодом [16].

Метод Arcadia определяет пять рабочих уровней на которых разрабатываются согласованные между собой модели, отражающие различные точки зрения на архитектуру системы, а именно:

1. Уровень операционного анализа (Operational analysis level);
2. Уровень анализа назначения системы (System needs analysis);
3. Уровень логической архитектуры системы (Logical architecture level);
4. Уровень физической архитектуры системы (Physical architecture level);
5. Уровень иерархической структуры конечной продукции и контрактов на комплексирование (End product breakdown structure and integration contracts, EPBS).

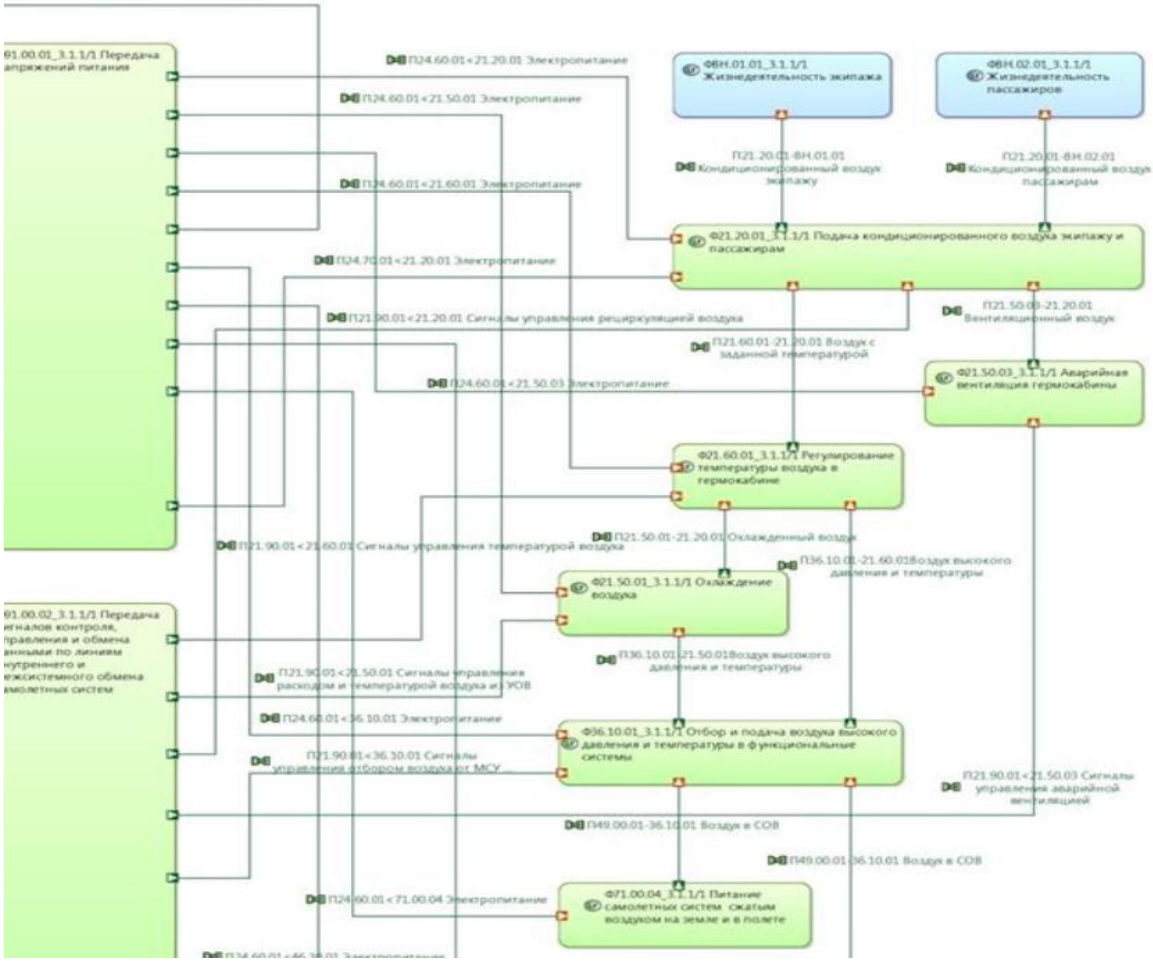

Рис. 2. Результаты моделирования функциональной архитектуры комплексной системы кондиционирования воздуха в среде Capella (фрагмент)

Модели, создаваемые на уровне операционного анализа, отражают представление заинтересованных сторон о том, чего хотят добиться пользователи создаваемой системы. Модели, создаваемые на уровне анализа назначения системы, отражают представление системных инженеров о том, какие возможности создаваемая система должна предоставить своим пользователям, причем внимание сосредоточено на анализе функционирования системы во взаимодействии с ее окружением. Модели, создаваемые на уровне логической архитектуры, отражают представление системных инженеров о том, как должна работать создаваемая система, для того чтобы соответствовать ожиданиям, зафиксированным на уровне системного анализа. Внимание на уровне логической архитектуры сосредоточено на анализе функционального взаимодействия между элементами системы, включая выделение подфункций, на выявлении связей между функциями и подфункциями

и на идентификации логических компонентов, которые реализуют эти подфункции. Модели, создаваемые на уровне физической архитектуры, отражают представление инженеров о предполагаемой конструкции и материальном воплощении создаваемой системы. Основное внимание на уровне физической архитектуры сосредоточено на выделении функций, обусловленных особенностями выбора и реализации так называемых поведенческих компонентов (например, компонентов программного обеспечения) которые выполняют эти функции, а также на реализации этих поведенческих компонентов в привязке к компонентам реализации (например, к процессору), которые предоставляют физические ресурсы, необходимые для реализации поведенческих компонентов. На уровне EPBS внимание инженеров сосредоточено на анализе физической архитектуры с целью определения требований, которым должен удовлетворять каждый из физических компонентов создаваемой системы, для того чтобы отвечать проектным ограничениям, налагаемым со стороны архитектуры системы, а также условиям и ограничениям, установленным на более высоких рабочих уровнях.

На текущем этапе работ внимание было сосредоточено на моделях, привязанных к уровню анализа назначения системы. Были построены модели функциональной архитектуры для ряда систем самолета. В качестве примера на рис. 2 частично показана построенная в среде Capella модель функциональной архитектуры комплексной системы кондиционирования воздуха в салоне самолета и кабине экипажа. Важным преимуществом метода ARCADIA является возможность построения и выделения функциональных цепочек, анализ которых в процессе оценки безопасности упрощает учет эффектов межсистемного взаимодействия и каскадных отказов. Однако в случае, когда количество анализируемых функций достигает нескольких десятков или, тем более, сотен, оценки безопасности на основе непосредственного анализа функциональных моделей, построенных в Capella, становится затруднительной. В этом случае может помочь использование метода ARCADIA и инструмента Capella в сочетании с Safety Architect [17].

Safety Architect представляет собой интегрированное с Capella программное средство, предназначенное для построения деревьев отказов отдельных систем и автоматической генерации на этой основе деревьев отказов для глобальной системы в целом. Алгоритмы, реализованные в Safety Architect, обеспечивают, в привязке к модели архитектуры, возможность анализа функциональных угроз и их оценки в соответствии с рекомендациями стандартов ARP 4761 и ISO 26262, а также построение моделей каскадных отказов.

В докладе будут прокомментированы первые результаты применения метода ARCADIA и инструмента Capella в сочетании с Safety Architect для оценки безопасности авиационных систем.

Заключение

Использование предприятием модели оценки безопасности, рекомендованной ARP 4754A для воздушных судов/ систем, требует обязательного налаживания зрелого процесса системной инженерии, в основе которого должны лежать согласованные между собой подход жизненного цикла и архитектурный подход.

В контексте оценки безопасности важнейшим результатом этого процесса является построение функциональной архитектуры самолета/ систем самолета. Возможная методика построения функциональной архитектуры самолета/ систем самолета предложена нами в [13]. В отечественных условиях эту методику приходится сочетать с обратным инжинирингом. В последнем случае результаты функционального анализа позволяют быстро выделять функции, которые не обладают характеристиками, указанными нами во втором разделе доклада, и планировать на этой основе необходимые изменения.

В процессе оценки безопасности авиационных систем приходится одновременно рассматривать многие сотни функций с учетом их взаимодействия. В этих условиях удобным средством борьбы со сложностью становится моделе-ориентированная системная инженерия. Выбор средств MBSE для использования в отечественных проектах авиационных систем сегодня ограничен. Тем не менее, первый опыт использования для оценки безопасности метода моделе-ориентированной системной инженерии ARCADIA и инструмента Capella в сочетании с Safety Architect показывает, что удается не только строить деревья отказов с учетом эффектов межсистемного взаимодействия, но и оценивать безопасность систем в случае наличия рисков каскадных отказов.

Литература

1. SAE ARP 4754A. Aerospace recommended practice. Guidelines for development civil aircraft and systems. 2010. https://www.sae.org/standards/content/arp4754a/
2. SAE ARP 4761. Aerospace recommended practice. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. 1996. https://www.sae.org/standards/content/arp4761/
3. *Blanchard B. S., Blyler J. E.* System engineering management. – Wiley, 2016. – 569 p.
4. *Buede D. M., Miller W. D.* The Engineering Design of Systems: Models and Methods. 3rd Edition. – Wiley, 2016. – 581 p.
5. ISO/IEC/IEEE 42010:2011. Systems and software engineering. Architecture description. https://www.iso.org/ru/standard/50508.html
6. ISO/IEC/IEEE 24748-1:2018 Systems and software engineering. Life cycle management. Part 1: Guidelines for life cycle management. https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
7. Systems Engineering Handbook. A guide for system life cycle processes and activities. 4th Edition. INCOSE-TP-2003-002-04-2015. – Wiley, 2015. – 305p.
8. *Holt J., Perry S., Brownsword M*. Foundations for Model-based Systems Engineering. From Patterns to Models. – The Institution of Engineering and Technology, London, UK, 2016. – 417 p.
9. *Delligatti L.* SysML Distilled. A Brief Guide to the Systems Modeling Language. – Addison-Wesley, 2014. – 301 p.
10. ISO/IEC/IEEE 24765:2017 Systems and software engineering-Vocabulary https://www.iso.org/standard/71952.html
11. *Jackson S*. Systems Engineering for Commercial Aircraft: A Domain-Specific Adaptation. 2nd Edition. – Ashgate, 2015. – 316 p.
12. FAA Systems Engineering Manual. – Version 1.0.1., 2014. http://everyspec.com/FAA/FAA-General/FAA_SEM_V1x0_19JUN2014_52250/
13. *Balashov Y., Batovrin V., Lobanovsky Y.* Methodology of functional architecture assembly of complex systems on airliner example. Proceedings of 2019 Actual Problems of Systems and Software Engineering (APSSE), 2019, p.p. 35-41.
14. *Voirin J.-L.* Model-based System and Architecture Engineering with the Arcadia Method. – Elsevier, 2018. – 388 p.
15. XP Z67-140:2018-03 Technologies de l'information - ARCADIA - Méthode pour l'ingénierie des systems soutenue par son langage de modélisation conceptuel - Description Générale - Spécification de la méthode de définition de l'ingénierie et du langage de modélisation. https://www.boutique.afnor.org/xml-en/1953115/false
16. *Roques P*. Systems Architecture Modeling with the Arcadia Method. A Practical Guide to Capella. – Elsevier, 2018. – 292 p.
17. Safety Architect. Model based safety assessment software. https://www.all4tec.com/en/safety-architect-fmeca-fta-sofware/
18. ISO 26262-3:2018 Road vehicles. Functional safety. Part 3: Concept phase. https://www.iso.org/standard/68385.html