Научная статья
Original article
УДК 004.424

# ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

FUNCTIONAL SAFETY ASSESSMENTS

**Аверкиев Александр Александрович,** магистр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), aaverkiev07@icloud.com
**Камбулов Данил Александрович,** магистр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kambulov18@yandex.ru

**Averkiev Alexander Alexandrovich**, Master, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), aaverkiev07@icloud.com
**Kambulov Danil Alexandrovich**, Master, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kambulov18@yandex.ru

**Аннотация.** В статье предлагается методика оценки функциональной безопасности автоматизированных систем на основе метода морфологического анализа. Основное внимание в работе уделяется анализу метода для оценки функциональной безопасности автоматизированных систем в целом.

**Abstract.**The article proposes a method for assessing the functional safety of automated systems based on the method of morphological analysis. The main attention is paid to the analysis of the method for assessing the functional safety of automated systems as a whole.

**Ключевые слова**: и фразы: безопасность, отказ, морфологический анализ, морфологический ящик, функциональная безопасность, автоматизация, автоматизация производства, анализ отказов, оценка безопасности.

**Key words:** and phrases: safety, failure, morphological analysis, morphological box, functional safety, automation, production automation, failure analysis, safety assessment.

Важнейшие функции дорожных транспортных средств все чаще реализуются с использованием электрических и/или электронных систем. Неисправности этих систем могут создавать угрозу безопасности пассажиров и/или других участников дорожного движения. Таким образом, необходимо обеспечить уверенность в том, что удалось избежать необоснованных остаточных рисков. Стандарт безопасности ISO 26262 был разработан, чтобы удовлетворить эту потребность, предоставляя руководство в форме требований и процессов для предотвращения необоснованного остаточного риска, вызванного неправильным поведением систем [1]. Как и многие стандарты безопасности, которые охватывают сложные программные системы, ISO 26262 определяет требования к созданию рабочих продуктов, т. е. результатов жизненного цикла безопасности, и оставляет разработчикам возможность интерпретировать эти требования в контексте своих продуктов [2]. Чтобы предоставить обоснование для конкретного продукта, соответствие стандарту ISO 26262 требует разработки и оценки обоснования безопасности для элементов, связанных с безопасностью. Стандарт определяет элемент как «систему или набор систем для реализации функции на уровне транспортного средства» [1]. Чтобы оправдать свободу от необоснованного риска, следует разработать обоснование безопасности, в котором требования безопасности показаны как полные и удовлетворяемые доказательствами, полученными из рабочих продуктов ISO 26262. Однако стандарт не содержит практических указаний по разработке и анализу аргументов безопасности, а также не описывает, как следует оценивать аргументы безопасности в процессе оценки

функциональной безопасности. В этой статье мы основываемся на опыте авторов в разработке и оценке обоснований безопасности в контексте ISO 26262. Мы исследуем значение и природу обоснования безопасности, основанного на продукте, в аргументации, а также роль, которую это обоснование должно играть в оценке. функциональная безопасность. Документ также основан на существующей работе по случаям безопасности в различных областях [3-4] и в автомобильной промышленности, в частности, принимая во внимание вопросы, связанные с обеспечением безопасности на основе продуктов и процессов процесс соблюдения и оценка достоверности. Этот подход оценивается в отраслевом тематическом исследовании.

В ISO 26262 обоснование безопасности определяется как «аргумент о том, что требования безопасности к элементу полны и удовлетворяются доказательствами, собранными на основе результатов деятельности по обеспечению безопасности во время разработки» [1]. То есть аргумент должен играть центральную роль в обосновании того, почему имеющиеся данные в форме рабочих продуктов (например, артефакты проектирования и анализа) соответствуют набору требований безопасности и, следовательно, почему был достигнут приемлемый уровень безопасности. достигнуто. Соответствие ISO 26262, основанное на нормативных частях стандарта, требует достижения определенного набора целей путем создания конкретного набора рабочих продуктов. В результате все системы, соответствующие стандарту, имеют общую структуру аргументов безопасности, связывающую требования безопасности высшего уровня с имеющимися доказательствами. К сожалению, эта общая структура аргументов является неявной и не задокументирована в стандарте. Неявный аргумент безопасности в ISO 26262 основан на следующей цепочке рассуждений. Достаточный и приемлемый уровень безопасности системы достигается демонстрацией отсутствия необоснованного риска, связанного с каждым опасным событием, вызванным неправильным поведением объекта (другие причины опасности не входят в область применения стандарта). Это достигается путем определения целей

безопасности, чтобы избежать необоснованного риска путем предотвращения или смягчения последствий выявленных опасных событий. Опасное событие – это возникновение опасности в определенных эксплуатационных ситуациях. Каждому опасному событию присваивается уровень полноты безопасности автомобилей (ASIL), основанный на сочетании трех параметров: серьезности (степени человеческого вреда), вероятности воздействия (эксплуатационных ситуаций) и управляемости (способности лиц, подвергающихся риску, принять меры). действие, чтобы избежать вреда). Затем утверждается, что каждой цели безопасности соответствует разработка концепции функциональной безопасности. Концепция функциональной безопасности определяет меры безопасности в контексте архитектуры транспортного средства, включая обнаружение неисправностей и механизмы смягчения последствий сбоев, для достижения целей безопасности.

Две дополнительные иерархии утверждений определены для подтверждения того, насколько концепция функциональной безопасности адекватно уточняется и удовлетворяется технической концепцией безопасности и аппаратными и программными компонентами (опять же в соответствии с требуемым УПБА).

Соответствие стандарту ISO 26262 и оценка приведенного выше неявного аргумента частично демонстрируются с использованием двух типов мер подтверждения: аудит функциональной безопасности и оценка функциональной безопасности.

**Литература**

1. ISO: ISO 26262 Дорожные транспортные средства. Функциональная безопасность. Стандарт ИСО (2011 г.)
2. Грейдон, П., Хабли, И., Хокинс, Р., Келли, Т., Найт.: Аргументация соответствия. Программное обеспечение IEEE, том. 29, выпуск 3 (2012)
3. Бишоп П., Блумфилд Р.: Методология разработки обоснования безопасности. В: Учеб. 6-я критически важная для безопасности система. Симп. (1998)

4. Келли, Т.: Системный подход к управлению случаем безопасности. В: Учеб. Всемирный конгресс Общества автомобильных инженеров (SAE) (2004 г.)
5. Фонд здравоохранения, Использование случаев безопасности в промышленности и здравоохранении. ISBN: 978-1-906461-43-0, (2012)
6. Диттель, Т., Арюс, Х.: Как «пережить» безопасность в соответствии с ISO 26262. SAFECOMP 2010, Вена, Австрия, (2010)

**References**

1. ISO: ISO 26262 Road Vehicles -- Functional Safety. ISO Standard (2011)
2. Graydon, P., Habli, I., Hawkins, R., Kelly, T., Knight.: Arguing conformance. IEEE Soft-ware, vol. 29, issue 3 (2012)
3. Bishop, P., Bloomfield, R.: A methodology for safety case development. In: Proc. 6th Safety-critical Sys. Symp. (1998)
4. Kelly, T.: A systematic approach to safety case management. In: Proc. Society of Automo-tive Engineers (SAE) World Congress (2004)
5. The Health Foundation, Using Safety Cases in Industry and Healthcare. ISBN: 978-1-906461-43-0, (2012)
6. Dittel, T., Aryus, H.: How to “Survive” a safety case according to ISO 26262. SAFECOMP 2010, Vienna, Austria, (2010)

*© Аверкиев А.А., Камбулов Д. А., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.*

**Для цитирования:** Аверкиев А.А., Камбулов Д. А. ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.