ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58489— 2019/ IEC/TS 61508-3-1:2016

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ, ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Часть 3-1

Требования к программному обеспечению. Повторное использование уже существующих элементов программного обеспечения для реализации всей или части функции безопасности

(IEC/TS 61508-3-1:2016, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» совместно с ФГУП «СТАНДАРТИНФОРМ» на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 16 августа 2019 г. № 508-ст

4 Настоящий стандарт идентичен международному документу IEC/TS 61508-3-1:2016 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3-1. Требования к программному обеспечению. Повторное использование уже существующих элементов программного обеспечения для реализации всей или части функции безопасности (IEC/TS 61508-3-1:2016 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3-1: Software requirements — Reuse of pre-existing software elements to implement all or part of a safety function», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Требования 1
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 5
Библиография 6

Введение

Требования, установленные в настоящем стандарте, относятся к повторному использованию элементов программного обеспечения, предназначенных для реализации функции безопасности.

В настоящее время элементы программного обеспечения используются во множестве разных областей автоматизации для выполнения функции безопасности. Безусловно, подобные приложения будут и в дальнейшем разрабатываться и расширяться. Тем не менее разработчики программных средств не всегда хотят разрабатывать программное обеспечение для таких приложений «с нуля» и часто прибегают к использованию уже существующих программных средств, интегрируя их в новое приложение, которое может несколько отличаться от того, для которого данные программные средства предназначались.

В МЭК 61508-3:2010, подпункт 7.4.2.12, приведено требование, которое предлагает три способа достижения необходимой полноты безопасности уже существующего элемента программного обеспечения. Требования соответствия второму способу (Способ 2s) определены в МЭК 61508-2:2010, пункт 7.4.10.

Из этого следует, что МЭК 61508-3:2010, посвященный исключительно программному обеспечению, ссылается на требования МЭК 61508-2:2010, который рассматривает системы, включающие аппаратные средства, но исключающие программное обеспечение (см. МЭК 61508-2:2010, подраздел 1.1, перечисление е).

Настоящий стандарт устанавливает конкретные требования к элементам программного обеспечения, так как МЭК 61508-2:2010 не рассматривает программное обеспечение, а также предназначен заменить содержание второго способа (Способ 2s) в МЭК 61508-3:2010, подпункт 7.4.2.12, перечисление а) в будущем издании МЭК 61508-3.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ, ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Часть 3-1

Требования к программному обеспечению. Повторное использование уже существующих элементов программного обеспечения для реализации всей или части функции безопасности

Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3-1. Software requirements. Reuse of pre-existing software elements to implement all or part of a safety function

Дата введения — 2020—07—01

1 Область применения

Настоящий стандарт определяет требования, выполнение которых позволяет утверждать, что уже существующие элементы программного обеспечения прошли проверку эксплуатацией и могут использоваться для реализации всей(всех) или части(ей) функции(ий) безопасности с УПБ 1 или УПБ 2.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения к нему):

IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению)

3 Термины и определения

В настоящем стандарте не используются новые термины или определения.

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации по следующим адресам:

- IEC Electropedia доступна по адресу gost.e-ecolog.ru ;
- сайт ИСО доступен по адресу http://www.iso.org/obp.

4 Требования

4.1 Примечания 1—4, представленные ниже, относятся ко всему разделу 4.

Примечания

1 Любая документация, необходимая для данного раздела настоящего стандарта, может либо сопровождать уже существующее программное обеспечение, либо быть включена как часть документации функции, связанной с безопасностью.

2 Под функцией повторно используемого программного обеспечения в настоящем стандарте понимают функцию, определенную на уровне спецификации требований (см. МЭК 61508-3:2010, подраздел 7.2). В качестве функции повторно используемого программного обеспечения не рассматривают конструкцию языка программирования.

Издание официальное

3 В 4.2, перечисления b) и c), приведены условия для данных по истории уже существующего программного обеспечения. Выполнение этих условий не предполагает, что программное обеспечение является детерминированным: скрытые внутренние состояния программного обеспечения могут влиять на его выполнение даже, когда выполняются точно такие же условия, как указанные в 4.1, перечисления b) и c). Таким образом, использование существующего программного обеспечения ограничено требованиями 4.7.

4 В некоторых случаях (например, входные данные являются аналоговым или синхронизирующим сигналом) демонстрация того, что программное обеспечение было проверено в эксплуатации, может быть трудной задачей.

4.2 Элемент считается проверенным в эксплуатации исключительно тогда, когда:

a) его описание:

1) существует и доступно,

2) удовлетворяет требованиям МЭК 61508-3:2010, подраздел 7.2,

3) конкретизирует предыдущее использование;

и

b) документально оформлено выполнение программного обеспечения со всеми комбинациями всех заявленных:

- комбинаций входных данных,

- последовательностей выполнения функции(ий) повторно используемого программного обеспечения,

- временны́х отношений при последовательных выполнениях функции(ий) повторно используемого программного обеспечения, которые будут реализованы в предназначенном приложении;

и

c) удовлетворяют требованиям 4.8 комбинации всех:

- входных данных,

- последовательностей выполнения функции(ий) повторно используемого программного обеспечения,

- временны́х отношений при последовательных выполнениях функции(ий) повторно используемого программного обеспечения, о которых не заявлено, что они проверены в эксплуатации;

и

d) комбинации, описанные в перечислении b), которые будут использоваться в предназначенном приложении, встречались в предыдущем использовании с такой же относительной частотой. Эта будущая частота должна быть обоснована при сравнении с предыдущим использованием и документально оформлена;

и

e) имеются адекватные доказательства для демонстрации полноты документации;

и

f) для элемента совместно с аппаратными средствами, на которых он будет работать, будет выполнен и документально оформлен:

- анализ любого опыта выполнения интеграции аппаратных средств и элемента программного обеспечения,

- анализ пригодности аппаратных средств и элемента программного обеспечения,

- выполнено и документально оформлено испытание аппаратных средств и элемента программного обеспечения. Такая документация включает:

- спецификацию целей испытаний для свойств, документально представленных в перечислениях a), b) и d) данного подраздела,

- подробное описание испытания для каждой отдельной цели,

- оценку достоверности, с которой установлено испытание каждой отдельной цели,

- демонстрацию того, что оцененная достоверность подходит для цели и результатов испытаний.

Примечания

1 Анализ пригодности и испытание нацелены на демонстрацию оценки работы аппаратных средств и элемента программного обеспечения в рамках предназначенного приложения. Могут учитываться также результаты выполненных анализов и испытаний, например, функционального поведения, точности, поведения в случае сбоя, времени реакции, реакции на перегрузку, удобства и простоты использования (например, предотвращение ошибок человека) и способности к сопровождению.

2 Математическое разбиение входных данных может помочь идентифицировать все комбинации, проверенные в эксплуатации.

3 Под «входными данными» подразумеваются все данные, являющиеся входными для элемента программного обеспечения. Например, может быть так, что аппаратные средства, на которых выполняется элемент программного обеспечения, генерируют внутренние данные, являющиеся входными для программного обеспечения. Такими данными могут быть диагностические данные.

4 Временные отношения, чаще всего нуждающиеся в верификации, — это линейные временные отношения вида «наиболее короткое время ≤ время выполнения ≤ самое длительное время». Существуют практические методы верификации и проверки взаимной согласованности требований синхронизации такой формы.

4.3 Документально оформленные свидетельства, необходимые для выполнения условий 4.2, должны:

a) демонстрировать, что следующие функциональные возможности и явления предшествующего опыта, оцененные для заявления о том, что элемент прошел проверку в эксплуатации, идентичны в предназначенном приложении элемента:

- аппаратные средства (например, поведение процессора, памяти, таймера, шины) и профили запросов,
- конфигурация (например, параметры компилятора, используемые при компиляции исходного кода для предложенного применения, инициализация переменных и констант программы, конфигурирование аппаратных средств, на которых выполняется программное обеспечение),
- интерфейсы программного обеспечения,
- библиотеки (включая библиотеки исходного кода, а также библиотеки бинарного кода),
- операционная система, интерпретаторы (например, применяемые для эмуляции архитектур процессора на процессорах, не имеющих такую архитектуру),
- транслятор (компилятор), редактор связей, генераторы кода;

и

b) содержать полное описание условий использования уже существующего программного обеспечения.

Примечания

1 Условия использования (операционный профиль) включают все факторы, которые могут вызывать систематические сбои в аппаратных средствах и программном обеспечении элемента. Например, дополнительные режимы использования, выполняемые функции, человеческие факторы.

2 Большинство этой информации может быть размещено в руководстве по безопасности (см. МЭК 61508-3:2010, подпункт 7.4.2.12).

4.4 Документально оформленные свидетельства, необходимые для выполнения условий 4.2, должны демонстрировать, что в период наблюдения было проведено исчерпывающее выявление отказов, то есть в промежуток времени, в ходе которого подверглось наблюдению поведение повторно используемого программного обеспечения для всех:

- проверенных в эксплуатации комбинаций входных данных,
- последовательностей выполнения функции(ий) повторно используемого программного обеспечения,
- временны́х отношений при последовательных выполнениях функции(ий) повторно используемого программного обеспечения.

Необходимо продемонстрировать, что любой отдельный отказ, вызванный программным обеспечением, был бы обнаружен и включен в отчет.

Для последовательностей сообщаемых отказов должна предоставляться документация, выполнен их анализ и оценка.

Примечания

1 Сбор свидетельств для элементов, проверенных в эксплуатации, требует наличия эффективной системы отчетов по отказам.

2 Настоящий стандарт для программного обеспечения не использует вероятностную концепцию интенсивности отказов.

4.5 Различия между предыдущими условиями использования (см. 4.2, примечание 1) и теми, которым подвергнется ПЭ (программируемая электронная) система, связанная с безопасностью, должны быть документально оформлены. Для этих различий должен быть выполнен и документально оформлен анализ их влияния с помощью комбинации надлежащих аналитических методов и конкретных испытаний, чтобы продемонстрировать, что вероятность систематических сбоев, способных привести к опасным отказам, настолько низка, что требуемый(ые) уровень(уровни) полноты безопасности функции(ий) безопасности, использующей(щих) этот элемент, был(и) достигнут(ы).

4.6 Обоснование безопасности элемента, проверенного в эксплуатации, должно документально оформляться на основе информации, доступной в 4.3. Это обоснование того, что элемент поддерживает требуемую функцию безопасности вместе с требуемым УПБ. Оно должно включать:

a) информацию из спецификации требований к безопасности программного обеспечения (см. МЭК 61508-3:2010, подраздел 7.2) ПЭ системы, связанной с безопасностью;

b) результаты тестирования элемента для предназначенного приложения;

c) документально оформленные доказательства, как они описаны в 4.2;

d) доказательства того, что элемент надлежащим образом использовался ранее.

4.7 Требования настоящего стандарта должны использоваться только при повторном использовании программного обеспечения для УПБ 1 и УПБ 2.

Примечание — Ограничение на использование программного обеспечения, проверенного в эксплуатации, для УПБ 1 и УПБ 2, связано с тем фактом, что методы, классифицированные как HR из таблиц в МЭК 61508-3:2010, приложения А и В, вплоть до УПБ 2 в основном рассматривают только аспекты поведения черного ящика.

4.8 Должны быть предоставлены доказательства того, что функции повторно используемого программного обеспечения уже существующего программного обеспечения, которые надлежащим образом (в соответствии с требованиями 4.1—4.3) не рассматривались при демонстрации проверки эксплуатацией, не оказывают никакого негативного влияния на полноту безопасности системы Э/Э/ПЭ (электрические/электронные/программируемые электронные), связанной с безопасностью.

Примечание — Данное требование может быть достигнуто за счет обеспечения физического или электрического отключения функций повторно используемого программного обеспечения или демонстрацией того, что входные данные для программного обеспечения ограничены таким образом, что эти функции исключены из рабочей конфигурации, или же с помощью иных доказательств и аргументов.

4.9 После внесения каких-либо модификаций в программное обеспечение, ранее проверенное в эксплуатации, оно более не должно восприниматься как проверенное в эксплуатации. Любые дальнейшие модификации программного обеспечения, проверенного в эксплуатации, должны соответствовать требованиям МЭК 61508-3:2010, подраздел 7.8.

Примечание — Модифицированное программное обеспечение более не является «проверенным в эксплуатации» и тем самым не входит в область применения настоящего стандарта.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
- IDT — идентичный стандарт.

Библиография

[1] IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 2. Требования к системам)

[2] IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 4: Definitions and abbreviations (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 4. Термины и определения)

УДК 62-783:614.8:331.454:006.354 ОКС 13.110

Ключевые слова: функциональная безопасность, программное обеспечение, уровень полноты безопасности, повторное использование программного обеспечения, уже существующее программное обеспечение

БЗ 8—2019/68

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 19.08.2019. Подписано в печать 02.09.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,12.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru