НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

РУКОВОДСТВО ПО ПРИМЕНЕНИЮ ИСО 13849-1 И МЭК 62061 ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

ОКС 35.200*

_____

* В ИУС 9-2014 ГОСТ Р 55743-2013 приводится с ОКС 13.110. -
- Примечание изготовителя базы данных.

Дата введения 2014-09-01

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью "Корпоративные электронные системы" и Федеральным бюджетным учреждением "Консультационно-внедренческая фирма в области международной стандартизации и сертификации "Фирма "ИНТЕРСТАНДАРТ" на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 58 "Функциональная безопасность"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 08 ноября 2013 г. N 1464-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/ТО 23849:2010* "Руководство по применению ИСО 13849-1 и МЭК 62061 при проектировании систем управления оборудованием, связанных с безопасностью" (ISO/TR 23849:2010 "Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery", IDT)

_____

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0-2012 *(раздел 8). 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 национального органа Российской Федерации по стандартизации в сети Интернет (gost.ru)*

Введение

Настоящий стандарт подготовлен экспертами из МЭК/ТК 44/РГ 7 и ИСО/ТК 199/РГ 8 в ответ на возникшие в этих технических комитетах просьбы объяснить отношение между МЭК 62061 [1] и ИСО 13849-1 [2]. В частности, настоящий технический отчет призван помочь пользователям указанных стандартов и, насколько это возможно, связать их терминологически для обеспечения уверенности, что разработка систем, связанных с безопасностью, может выполняться в соответствии с любым из этих стандартов.

Предполагается, что настоящий технический отчет будет включен в МЭК 62061 и ИСО 13849-1 с помощью технической поправки, которая будет ссылаться на опубликованную версию настоящего стандарта. Этой поправкой также будет удалена приведенная в таблице 1 информация о рекомендуемом применении МЭК 62061 и ИСО 13849-1, представленная во введение обоих стандартов, которая сейчас признана устаревшей. Впоследствии предполагается объединить МЭК 62061 и ИСО 13849-1 усилиями рабочих групп ИСО/ТК 199 и МЭК/ТК 44.

1 Область применения

В настоящем стандарте объясняется, как необходимо применять МЭК 62061 и ИСО 13849-1[1)] при проектировании связанных с безопасностью систем управления для оборудования машин.

---

1) В настоящем стандарте рассматривается ИСО 13849-1:2006, а не ИСО 13849-1:1999, который был отменен.

2 Общие положения

2.1 МЭК 62061 и ИСО 13849-1 определяют требования к проектированию и реализации связанных с безопасностью систем управления оборудованием[1)]. Методы, разработанные в этих стандартах, различны, но при правильном их применении можно достичь сопоставимого уровня снижения риска.

[1)] Эти стандарты были приняты европейскими органами по стандартизации CEN и CENELEC как ИСО 13849-1 и ЕН 62061 соответственно, где они были опубликованы со статусом гармонизированных стандартов в соответствии с Директивами по машиностроению 98/37/ЕС и 2006/42/ЕС. В соответствии с условиями их публикации правильное применение любого из этих стандартов предполагает их соответствие основным требованиям безопасности Директив по машиностроению 98/37/ЕС и 2006/42/ЕС.

2.2 МЭК 62061 и ИСО 13849-1 классифицируют связанные с безопасностью системы управления, реализующие функции безопасности, по уровням, которые определяются различными значениями вероятности опасного отказа в час. ИСО 13849-1 вводит пять уровней безопасности (УБ), *a*, *b*, *c*, *d* и *e*, в то время как МЭК 62061 использует три уровня полноты безопасности (УПБ) 1, 2 и 3.

2.3 Так как в стандартах на продукцию (тип С) комитеты определяют требования к безопасности для связанных с безопасностью систем управления, то рекомендуется, чтобы эти комитеты классифицировали необходимые для них уровни в значениях УБ и УПБ.

2.4 Конструкторы оборудования могут использовать или МЭК 62061, или ИСО 13849-1 в зависимости от особенностей применения.

2.5 При выборе и применении любого из этих стандартов необходимо руководствоваться следующим:

- при наличии предшествующих знаний и опыта в проектировании связанных с безопасностью систем управления машин на основе концепции категорий, описанных в ИСО 13849-1:1999, может оказаться, что использование ИСО 13849-1:2006 является более подходящим;
- если связанные с безопасностью системы управления реализованы на основе неэлектрической технологии, то это может означать, что использование ИСО 13849-1 является более подходящим;
- если требования заказчика продемонстрировать полноту безопасности, связанной с безопасностью системы управления машины, заданы в значениях величины УПБ, то это может означать, что использование МЭК 62061 является более подходящим;

- для связанных с безопасностью систем управления машин, используемых например, в промышленных процессах, в которых другие связанные с безопасностью системы (например, приборные системы обеспечения безопасности, соответствующие [3]) характеризуются значениями величины УПБ, использование МЭК 62061 является более целесообразным.

3 Сравнение стандартов

3.1 Было выполнено сравнение технических требований ИСО 13849-1 и МЭК 62061 по следующим направлениям:

- терминология;
- оценка рисков и распределение характеристик безопасности;
- спецификация требований к безопасности;
- систематическая полнота;
- диагностические функции;
- безопасность программного обеспечения.

3.2 Кроме того, в соответствии с обоими стандартами была выполнена оценка использования упрощенных математических формул для определения вероятности опасных отказов (PFH_D) и $MTTF_d$.

3.3 В результате выполнения этой работы получены следующие выводы:

- связанные с безопасностью системы управления, достигающие приемлемого уровня функциональной безопасности, могут быть разработаны с использованием любого из этих стандартов путем интеграции несложных[1)] подсистем связанной с безопасностью электрической системы управления (СБЭСУ) или связанных с безопасностью элементов системы управления (СБЭ/СУ), разработанных в соответствии с МЭК 62061 или ИСО 13849-1 соответственно;

---

1) Термин "несложная" СБЭСУ или СБЭ/СУ должен рассматриваться как эквивалентный термину "низкая сложность", определенному в 3.2.7 МЭК 62061:2005.

- оба стандарта также могут быть использованы для выполнения проектных решений для сложных СБЭСУ и СБЭ/СУ за счет интеграции электрических / электронных / программируемых электронных подсистем, разработанных в соответствии с [4];
- оба стандарта в настоящее время представляют большую ценность для специалистов, использующих машины и оборудование, а также очень полезен опыт применения данных стандартов. Результаты практического применения стандартов МЭК 62061 и ИСО 13849-1, полученные в течение разумного периода времени, очень важны для поддержки любых дальнейших инициатив по созданию объединенного стандарта;
- в рассматриваемых стандартах существуют небольшие различия, а некоторые понятия (например, управление функциональной безопасностью) нуждаются в дальнейшей проработке с целью формирования эквивалентности между соответствующими методологиями разработки и некоторыми техническими требованиями.

4 Оценка риска и определение требуемых характеристик

4.1 Сравнение использования методов определения УПБ и (или) УБ для конкретной функции безопасности позволило установить, что существует хороший уровень соответствия между этими методами, представленными в приложении А каждого из соответствующих стандартов.

4.2 Независимо от того, какой метод используется, важно то, что уделяется особое внимание обеспечению соответствующего обоснования для параметров риска при определении УПБ и (или) УБ, которое, как правило, относится к конкретной функции безопасности. Эти обоснования могут быть более высокого качества, если они выполняются с участием ряда сотрудников (например, проектировщиков, специалистов по техническому обслуживанию, операторов), что обеспечивает правильность понимания опасностей, которые могут присутствовать в оборудовании.

4.3 Дополнительные сведения о процессе оценки риска и определении целевых показателей можно найти в [5] и [6].

5 Спецификация требований к системе безопасности

5.1 Первый этап соответствующей методики и в ИСО 13849-1, и в МЭК 62061 требует выполнение спецификации функции(й) безопасности, реализуемых связанной с безопасностью системой управления.

5.2 Должна быть выполнена оценка каждой функции безопасности, которая должна быть реализована схемой управления с использованием, например, либо приложения А ИСО 13849-1, либо приложения А МЭК 62061. Следует установить, какое необходимое снижение риска должно быть обеспечено каждой конкретной функцией безопасности в оборудовании и, в свою очередь, какой необходим уровень уверенности в том, что схемы управления смогут реализовать эту функцию безопасности.

5.3 Такой уровень уверенности, определяемый как УБ в ИСО 13849-1 и (или) УПБ в МЭК 62061, связан с конкретной функцией безопасности.

5.4 Ниже перечислена информация, которая должна быть предоставлена для функций безопасности в стандарте (типа С) на изделие.

Для функции(й) безопасности, реализуемой(ых) схемой управления:

- имя функции безопасности;
- описание функции безопасности;
- требуемый уровень безопасности в соответствии с ИСО 13849-1 ($УБ_т$ от *а* до *е*) и (или) требуемый уровень полноты безопасности в соответствии с МЭК 62061 (УПБ от 1 до 3).

6 Определение целевых характеристик для УБ и УПБ

В таблице 1 представлено соотношение между УБ и УПБ, основанное на средней вероятности опасного отказа в час. Однако оба стандарта содержат дополнительные требования (например, к систематической полноте безопасности) к этим вероятностным целям, которые также должны быть применены к связанной с безопасностью системе управления. Строгость этих требований связана с соответствующими УБ и УПБ.

Таблица 1 - Соотношение между УБ и УПБ, основанное на средней вероятности опасного отказа в час

Уровень безопасности (УБ)	Средняя вероятность опасного отказа в час (1/ч)	Уровень полноты безопасности (УПБ)
a	$\geq 10^{-5}$ до $< 10^{-4}$	Специальные требования к безопасности отсутствуют
b	$\geq 3x10^{-6}$ до $< 10^{-5}$	1
c	$\geq 10^{-6}$ до $< 3x10^{-6}$	1
d	$\geq 10^{-7}$ до $< 10^{-6}$	2
e	$\geq 10^{-8}$ до $< 10^{-7}$	3

7 Проектирование системы

7.1 Общие требования, применяемые МЭК 62061 и ИСО 13849-1, к проектированию системы

При разработке СБЭСУ или СБЭ/СУ должны быть учтены следующие аспекты:

- любой из двух стандартов в рамках ограничений их соответствующих областей применения может быть использован для разработки связанных с безопасностью систем управления с приемлемой функциональной безопасностью, которая указана для достигаемых УПБ или УБ;

- связанные с безопасностью несложные элементы, которые разработаны для соответствующих УБ согласно ИСО 13849-1, могут быть интегрированы как подсистемы в связанную с безопасностью электрическую систему управления (СБЭСУ), разработанную в соответствии с МЭК 62061. Любые сложные связанные с безопасностью элементы, которые разработаны для соответствующих УБ согласно ИСО 13849-1, могут быть интегрированы в связанные с безопасностью элементы системы управления (СБЭ/СУ), разработанные в соответствии с ИСО 13849-1;

- любая несложная подсистема, которая разработана согласно МЭК 62061 для соответствующих УПБ, может быть интегрирована как связанный с безопасностью элемент в любую комбинацию СБЭ/СУ, разработанную согласно ИСО 13849-1;

- любая сложная подсистема, которая разработана согласно [4] для соответствующих УПБ, может быть интегрирована как связанный с безопасностью элемент в любую комбинацию СБЭ/СУ, разработанную согласно ИСО 13849-1 или в качестве подсистемы в СБЭСУ, разработанную согласно МЭК 62061.

7.2 Оценка PFH_D и $MTTF_d$ и использование исключения сбоев

7.2.1 Оценка PFH_D и $MTTF_d$

7.2.1.1 Значение $MTTF_d$ в контексте ИСО 13849-1 относится к одному каналу СБЭ/СУ без диагностики и только в этом случае является величиной, обратной величине PFH_D, рассматриваемой в МЭК 62061.

7.2.1.2 $MTTF_d$ является параметром компонента(ов) и (или) отдельного канала без учета таких факторов, как диагностика и архитектура, в то время как PFH_D является параметром подсистемы, который учитывает вклад факторов, таких как диагностика и архитектура в зависимости от структуры проекта.

7.2.1.3 В ИСО 13849-1, приложение К, представлены соотношения между $MTTF_d$ и PFH_D для СБЭ/СУ для различных архитектур, которые определены для различных категорий и значений диагностического охвата (DC).

7.2.1.4 Оценка PFH_D для последовательно соединенных СБЭ/СУ в соответствии с ИСО 13849-1 также может быть выполнена путем сложения значений PFH_D (например, полученных из ИСО 13849-1, приложение К) каждого СБЭ/СУ аналогично тому, как это выполняется для подсистем в МЭК 62061.

7.2.2 Использование исключения сбоев

7.2.2.1 Оба стандарта разрешают использование исключения сбоя, см. 6.7.7 МЭК 62061 и 7.3 ИСО 13849-1. МЭК 62061 не допускает использования исключения сбоя для СБЭСУ, необходимой для достижения УПБ 3, без аппаратной отказоустойчивости.

7.2.2.2 Важно, чтобы использование исключения сбоя было должным образом обосновано и соответствовало предполагаемому сроку жизни СБЭ/СУ или СБЭСУ.

7.2.2.3 В случае, если для функции безопасности, реализуемой СБЭ/СУ или СБЭСУ, указано УБ *e* или УПБ 3, неправильно полагаться только на исключение сбоя для достижения такого уровня безопасности. Это зависит от используемой технологии и предполагаемой внешней среды эксплуатации. Поэтому от разработчика требуется дополнительная осторожность в использовании исключения сбоя при увеличении УБ или УПБ.

7.2.2.4 В общем случае использование исключения сбоя не применимо к механическим аспектам электромеханических позиционных переключателей и ручных переключателей (например, устройство аварийной остановки) для достижения УБ *e* или УПБ 3 при разработке соответственно СБЭ/СУ или СБЭСУ. Исключения сбоев, которые могут быть применены к механическим неисправностям в конкретных условиях (например, износ/ коррозия, трещины), описаны в [7].

7.2.2.5 Например, в систему блокировки двери, которая должна быть способна обеспечить УБ *e* или УПБ 3, необходимо будет включить минимальную отказоустойчивость равную 1 (например, два обычных механических выключателя) для того, чтобы достичь указанного уровня безопасности, так как не принято исключать такие сбои, как сломанный переключатель привода. Однако возможно исключать сбои, такие как короткое замыкание проводников в панели управления, разработанной в соответствии с соответствующими стандартами.

7.2.2.6 Дополнительная информация по использованию исключения сбоя должна быть предоставлена в стандарте [7], который в настоящее время разрабатывается ИСО/ТК 199/РГ 8.

7.3 Проект системы, использующей подсистемы или СБЭ/СУ, соответствующие требованиям или МЭК 62061, или ИСО 13849-1

7.3.1 Во всех случаях, если подсистемы или связанные с безопасностью элементы систем управления разработаны в соответствии или с ИСО 13849-1, или с МЭК 62061, необходимо обеспечить соответствие стандарту всей системы, если выполнены все соответствующие требования такого стандарта.

7.3.2 При проектировании подсистема или элемент из связанных с безопасностью элементов систем управления должны удовлетворять или МЭК 62061, или ИСО 13849-1 соответственно. Допустимо, чтобы они удовлетворяли обоим из этих стандартов при условии, что требования этих используемых стандартов полностью соблюдаются.

7.3.3 Не допускается смешивать требования стандартов к проектированию подсистемы и элементов из связанных с безопасностью элементов систем управления.

7.4 Проект системы, использующей подсистемы или СБЭ/СУ, разработанные с применением других стандартов МЭК или ИСО

7.4.1 В проекте возможно применение готовых подсистем, например электрочувствительного защитного устройства, которые отвечают соответствующим стандартам МЭК или ИСО на изделие или [4], или МЭК 62061, или ИСО 13849-1. Поставщики таких подсистем должны предоставлять необходимую информацию для обеспечения их интеграции в связанную с безопасностью систему управления в соответствии с любым из МЭК 62061 и ИСО 13849-1.

7.4.2 Подсистемы, например системы регулирования скорости электрического привода, которые были разработаны с использованием стандартов на изделие, таких как [8], который реализует требования [4], могут использоваться в связанных с безопасностью системах управления в соответствии с МЭК 62061 (см. также 6.7.3 МЭК 62061) и ИСО 13849-1.

7.4.3 В соответствии с МЭК 62061 другие подсистемы, которые были разработаны в соответствии с МЭК, ИСО и другими стандартами, должны подчиняться требованиям 6.7.3 МЭК 62061.

8 Пример

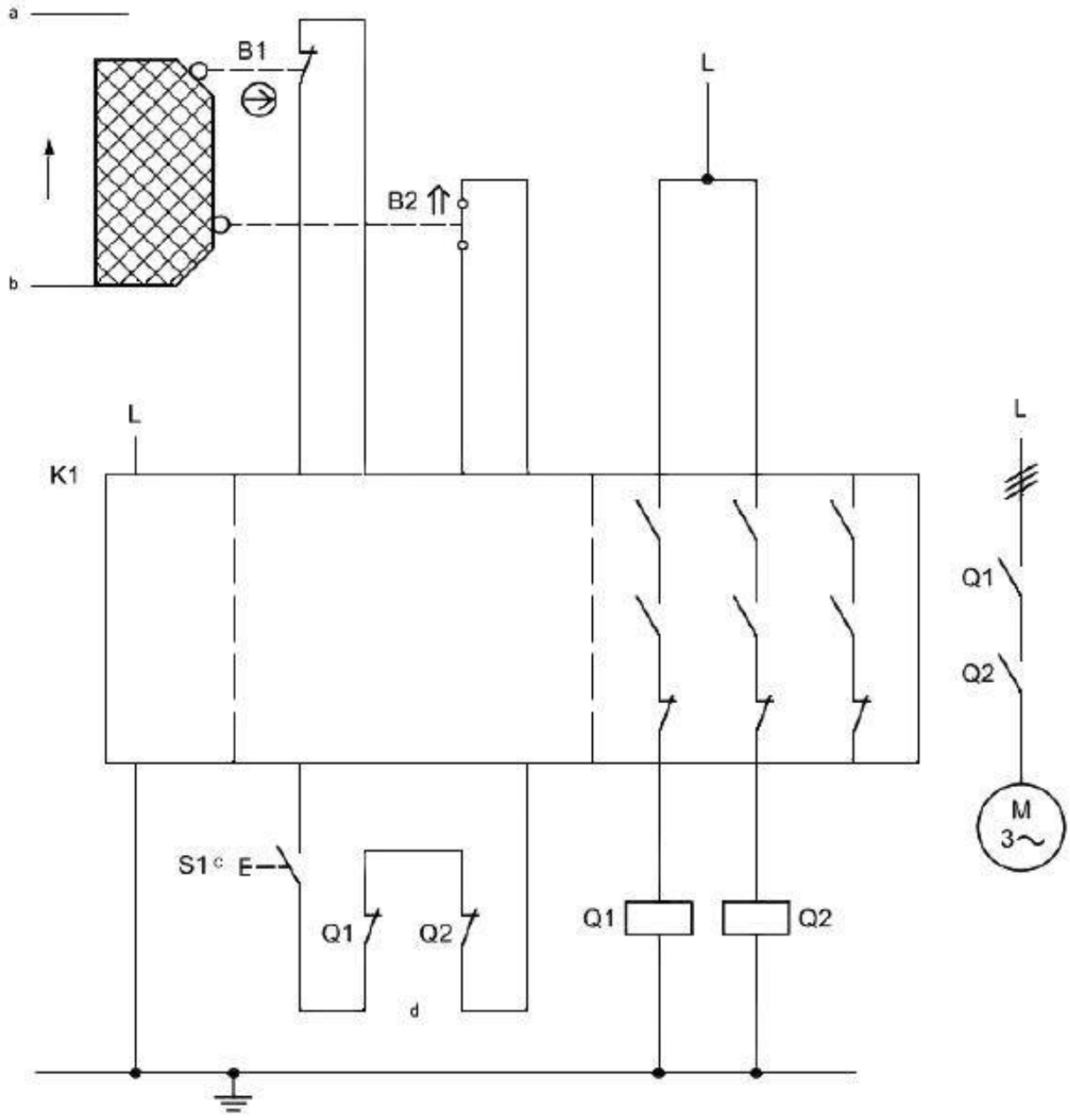
8.1 Общие положения

В следующем примере предполагается, что все требования стандартов были выполнены. Пример предназначен только для демонстрации конкретных аспектов применения стандартов.

8.2 Пример проектирования и подтверждения соответствия связанной с безопасностью системы управления, реализующей заданную функцию управления, связанную с безопасностью

8.2.1 Этот упрощенный пример предназначен для демонстрации использования в СБЭСУ или СБЭ/СУ подсистем или СБЭ/СУ, которые соответствуют МЭК 62061 и (или) ИСО 13849-1. Данный пример основан на реализации функции безопасности, описанной как связанная с безопасностью функция останова, выполняющая контроль положения перемещаемого ограждения, с заданным уровнем полноты безопасности УПБ 3 или требуемым уровнем безопасности $УБ_Т$ *e*, как показано на рисунке 1.

Рисунок 1 - Пример реализации функции безопасности



⇑ Показано во включенном положении

a - открыто; b - закрыто; c - ПУСК; d - контур обратной связи.

Рисунок 1 - Пример реализации функции безопасности

8.2.2 Приведенная ниже информация необходима для спецификации требований к безопасности для данного примера.

Функция безопасности

Связанная с безопасностью функция останова инициируется защитным устройством: открытие перемещаемого ограждения инициирует функцию безопасности БО (безопасный останов).

Описание функции:

- обеспечение безопасности гарантируется перемещаемым ограждением (защитной решеткой). Открытие блокируемого защитного ограждения обнаруживается с помощью двух позиционных переключателей $B1/B2$, информация с которых о состоянии контакта (замкнут или разомкнут) или о соответствующей комбинации контактов обрабатывается центральным модулем безопасности $K1$. $K1$ приводит в действие два контактора $Q1$ и $Q2$, срабатывание которых прерывает или предотвращает связанные с опасностью движения или состояния;

- с целью обнаружения неисправностей $K1$ проверяет позиционные переключатели. $K1$ выявляет неисправности в $Q1$ и $Q2$ с помощью теста запуска. Считается, что команда запуска выполнена успешно, если предварительно сработали $Q1$ и $Q2$. Тестирование запуска открытием и закрытием блокируемого защитного ограждения не требуется;

- функция безопасности не нарушается в случае отказа компонента. Если неисправности обнаруживаются в процессе работы системы или в процессе открытия и закрытия блокируемого защитного ограждения, то срабатывают $Q1$ и $Q2$ и работа системы прекращается;

- если в период между двумя последовательными выполнениями открытия / закрытия и закрытия / открытия блокируемого защитного ограждения произошло более двух неисправностей, то это может привести к нарушению функции безопасности.

8.2.3 Также необходимо выполнить следующие требования:

- должны соблюдаться базовые и хорошо проверенные принципы безопасности (например, снижение на 50% тока нагрузки для контакторов $Q1$ и $Q2$) и выполняться требования категории B. Должны быть реализованы схемы защиты (например, защита контактов);

- для срабатывания позиционных переключателей гарантируется стабильное расположение защитных устройств;

- переключатель $B1$ должен являться позиционным переключателем с позитивным размыканием в соответствии с [9], приложение K;

- провода питания к позиционным переключателям $B1$ и $B2$ должны быть проложены отдельно или с защитой.

8.2.4 От производителей должна быть получена следующая информация для каждого элемента проекта СБЭ/СУ:

- модуль безопасности $K1$ по заявлению завода-изготовителя[1)] удовлетворяет требованиям категории 4, значение УБ равно *e* и предельное требование к УПБ равно 3;

[1)] Этот модуль рассматривается как подсистема, и $MTTF$ его отдельных каналов не требуется (см. пп.7.2.1.1).

- контакторы $Q1$ и $Q2$ имеют механически связанные контактные элементы, соответствующие [9], приложение L.

8.2.5 Следующее замечание может быть сделано к проекту СБЭ/СУ и (или) СБЭСУ.

Категория 4 может быть достигнута только тогда, когда несколько механических позиционных переключателей для различных устройств защиты не соединены последовательно (т.е. не соединены каскадно). В противном случае сбои в переключателях не могут быть обнаружены.

8.2.6 Расчет вероятности отказа в соответствии с ИСО 13849-1

На рисунке 2 показана логическая подсистема (модуль безопасности $K1$), к которой подсоединены элементы двухканальных входа и выхода. Так как рассматриваемая блок-схема является абстракцией на уровне аппаратных средств подсистемы, связанной с безопасностью, последовательность подсистем непринципиальна. Поэтому рекомендуется, чтобы подсистемы, имеющие одинаковую структуру, быть сгруппированы вместе, как показано на рисунке 3. Это упрощает расчет УБ, так как получаемая оценка $MTTF_d$ канала сокращается в несколько раз до граничного значения для $MTTF_d$ канала равного 100 годам.

Рисунок 2 - Блок-диаграмма подсистемы, связанной с безопасностью

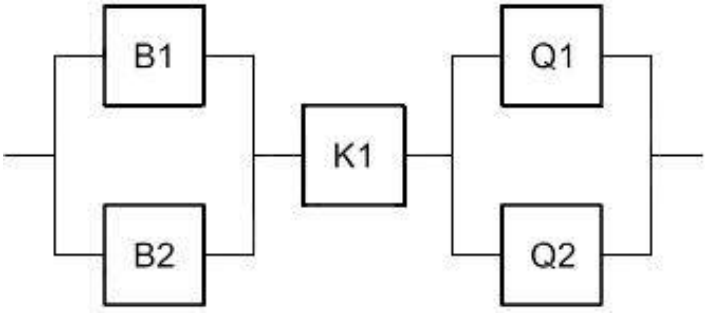
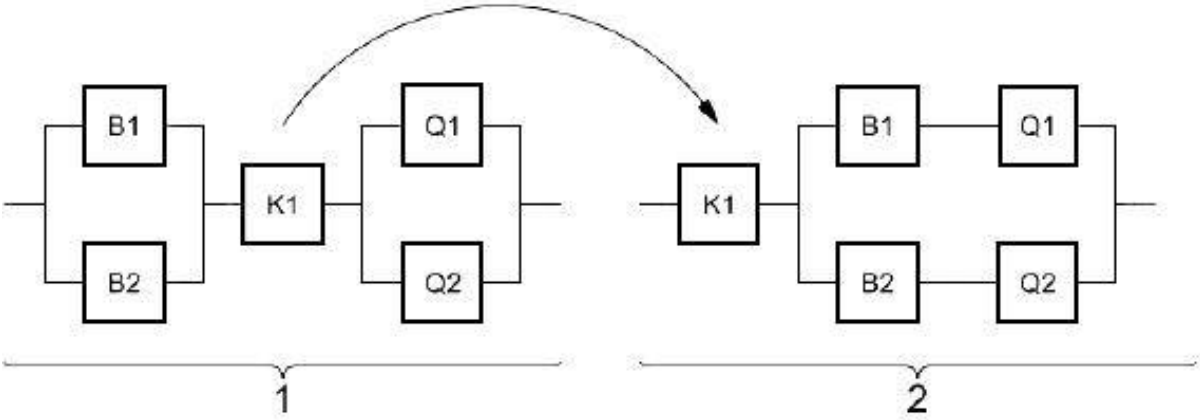


Рисунок 2 - Блок-диаграмма подсистемы, связанной с безопасностью

Рисунок 3 - Блок-диаграмма подсистемы, связанной с безопасностью, для вычисления по ИСО 13489-1



1 - Представление аппаратных средств: три подсистемы на уровне СБК/СУ; 2 - Упрощенное логическое представление: две подсистемы на уровне СБК/СУ

Рисунок 3 - Блок-диаграмма подсистемы, связанной с безопасностью, для вычисления по ИСО 13489-1

Вероятность отказа модуля безопасности $K1$ заявляется изготовителем и учитывается в конце расчета (2,31x10^{-9}/ч (величина производителя), соответствует УБ, равному *e*). Для остальных подсистем вероятность отказа рассчитывается следующим образом:

- $MTTF_d$. Для механической части $B1$ значение B_{10d} установлено равным 1000000 циклов (значение производителя). Для позиционного переключателя $B2$ значение B_{10d} составляет 500000 циклов (значение производителя). За 365 рабочих дней в году, 24 рабочих часов в день и времени цикла 900 с (15 мин) число циклов $n_{ОП}$ в год для этих компонентов рассчитывается с помощью уравнений (С.2) и (С.7) из ИСО 13849-1 и будет равно 35040 циклам:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \frac{с}{ч}}{t_{цикла}} = \frac{365 \frac{д}{г} \times 24 \frac{ч}{д} \times 3600 \frac{с}{ч}}{900 \frac{с}{цикл}} = 35040 \text{ циклов/г}$$

$$MTTF_{d,B1} = \frac{B_{10d}}{0,1 \times n_{op}} = \frac{1000000 \text{ циклов}}{0,1 \times 35040 \frac{циклов}{г}} = 285 \text{ лет}$$

$$T_{10d,B1} = \frac{B_{10d}}{n_{op}} = \frac{1000000 \text{ циклов}}{35040 \frac{циклов}{г}} = 28,5 \text{ лет}$$

$$MTTF_{d,B2} = \frac{B_{10d}}{0,1 \times n_{op}} = \frac{500000 \text{ циклов}}{0,1 \times 35040 \frac{циклов}{г}} = 143 \text{ года}$$

$$T_{10d,B2} = \frac{B_{10d}}{n_{op}} = \frac{500000 \text{ циклов}}{35040 \frac{циклов}{г}} = 14,3 \text{ лет}$$

Значение T_{10d} для $B2$ равно 14,3 лет. По истечении этого времени $B2$ должен быть заменен, если предполагается, что вся СБЭ/СУ должна функционировать в течение 20 лет;

- для контакторов $Q1$ и $Q2$ значение B_{10} при работе под индуктивной нагрузкой установлен срок службы в 1000000 циклов (значение производителя). Если 50% отказов считаются опасными, то значение B_{10d} удваивается по сравнению с B_{10}:

$$MTTF_{d,Q1/Q2} = \frac{B_{10d}}{0{,}1 \times n_{op}} = \frac{2000000\,циклов}{0{,}1 \times 35040 \frac{циклов}{г}} = 571\,год$$

$$T_{10d,Q1/Q2} = \frac{B_{10d}}{n_{op}} = \frac{2000000\,циклов}{35040 \frac{циклов}{г}} = 57{,}1\,лет$$

;

- для обоих каналов $MTTF_d$ вычисляется с помощью выражения D.1 из ИСО 13849-1.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{\mathrm{MTTFdi}}$$

$$\frac{1}{MTTF_{d,Ch1}} = \frac{1}{285\,л} + \frac{1}{571\,г} = \frac{1}{190\,л}$$

$$\frac{1}{MTTF_{d,Ch2}} = \frac{1}{143\,г} + \frac{1}{571\,г} = \frac{1}{114\,л}.$$

Это дает для $MTTF_{d,Ch1}$ 190 лет, а для $MTTF_{d,Ch2}$ - 114 лет. В соответствии с ИСО 13849-1 $MTTF_d$ обоих каналов ограничено до 100 лет, и в этом случае, так как $MTTF_d$ обоих каналов равны, после вычисления ограничения для них не нужно выполнять симметризацию;

- DC_{avg}: Значение DC (охват диагностикой), равное 99% для $B1$ и $B2$, основано на контроле достоверности размыкания / формирования комбинации контактов в $K1$. Значение DC, равное 99% для контакторов $Q1$ и $Q2$, обеспечивается их регулярным контролем, который выполняет $K1$ во время своего запуска. Установленные значения DC соответствуют DC_{avg} для каждой подсистемы. DC_{avg} будет рассчитываться по формуле E.1 из ИСО 13849-1. Так как для каждого отдельного компонента значение DC составляет 99%, значение DC_{avg} также будет равно 99%;

- адекватные меры против отказов по общей причине в подсистемах $B1/B2$ и $Q1/Q2$ (70 баллов): разделение (15), испытанные компоненты (5), защита от перенапряжения и т.д. (15) и условия окружающей среды (25+10);

- срок службы: для упрощенного подхода в ИСО 13849-1 предполагается срок службы 20 лет;

- подсистемы $B1/B2/Q1/Q2$ соответствуют категории 4 с большим значением $MTTF_d$ (100 лет) и большим значением DC_{avg} (99%). В результате средняя вероятность опасных отказов равна 2,47x10^{-8}/ч (см. ИСО 13849-1, таблица K.1). После добавления подсистемы $K1$ средняя вероятность

опасного отказа станет равной 2,70x10^{-8}/ч. Это соответствует значению УБ, равному *e*.

8.2.7 Вычисление вероятности отказа в соответствии с МЭК 62061

8.2.7.1 В соответствии с 6.6.2 МЭК 62061 систему можно разделить на три подсистемы: $B1/B2$, K и $Q1/Q2$, как показано на блок-схеме связанной с безопасностью системы.

8.2.7.2 Для подсистемы К вероятность отказа равна 2,31x10^{-9}/ч и предельное требование для УПБ, равное 3, для модуля безопасности $K1$ заявляется заводом-изготовителем.

8.2.7.3 Для остальных подсистем вероятность отказа может быть оценена следующим образом:

- подсистемы $B1/B2$. Для механической части $B1$ значение B_{10d} установлено равным 1000000 циклов (значение производителя). Для позиционного переключателя $B2$ значение B_{10d} составляет 500000 циклов (значение производителя). За 365 рабочих дней в году, 24 рабочих часов в день и времени цикла 15 мин значение числа рабочих циклов C равно 4 в час для этих компонентов. Интенсивность отказов рассчитывается как 0,1x C/B_{10d} = 4,00x10^{-7}/час. Для $B2$ интенсивность отказов будет равна 8,00x10 $^{-7}$/ч.

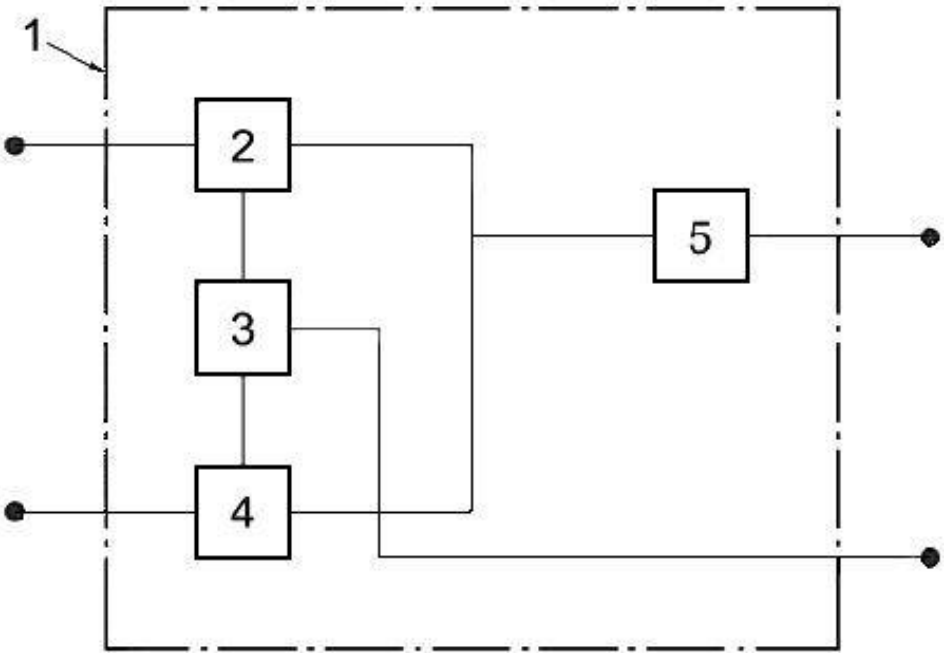
Примечание - Число рабочих циклов применения, C, согласно МЭК 62061 соответствует среднему числу операций в год n_{op} согласно ИСО 13849-1. Так как C определен как число циклов в час, а n_{op} как число циклов в год, справедливо следующее соотношение:

$$C = \frac{n_{op}}{365 \times 24}.$$

Таким образом, среднее число часов работы системы в день и количество дней в году влияет на величину C так же, как и на n_{op};

- логическое представление архитектуры рассматриваемой подсистемы соответствует логическому представлению архитектуры подсистемы типа D (см. 6.7.8.2.5 МЭК 62061) и показано на рисунке 4.

Рисунок 4 - Логическое представление подсистемы типа D



1 - подсистема типа D; 2 - элемент подсистемы с $\lambda_{D\text{№}1}$; 3 - диагностическая функция(и); 4 - элемент подсистемы с $\lambda_{D\text{№}2}$; 5 - отказ по общей причине

Рисунок 4 - Логическое представление подсистемы типа D

- элементы подсистемы (переключатели $B1$ и $B2$) имеют разную конструкцию, поэтому для определения PFH_D подсистемы используется следующее уравнение (D.1) из 6.7.8.2.5 МЭК 62061:

$$\lambda_{DssD} = (1-\beta)^2\{[\lambda_{De1}\times\lambda_{De2}\times(DC_1+DC_2)]\times T_2/2+$$
$$+[\lambda_{De1}\times\lambda_{De2}\times(2-DC_1-DC_2)]\times T_1/2\}+\beta\times(\lambda_{De1}+\lambda_{De2})/2,$$
$$PFH_{DssD} = \lambda_{DssD}\times 1\text{ч},$$

где T_2 - интервал диагностических проверок. Для подсистемы $B1/B2$ эта величина равна 15 мин;

T_1 - интервал между контрольными проверками или срок службы в зависимости от того, что меньше. Для подсистемы $B1/B2$ длительность срока службы равна 125000 ч (14,3 лет) при заданной интенсивности использования на основе наименьшего значения T_{10d} для элемента подсистемы (см. С.4.2 ИСО 13849-1). Переключатель $B2$ имеет наименьшее значение T_{10d}. Интервал между контрольными проверками (см. предисловие МЭК 62061) определяется равным 20 годам (175200 ч), что больше, чем срок службы. Поэтому T_1 равно 125000 часов;

β - восприимчивость к отказам по общей причине. Эта величина равна 5% (0,05), так как ее оценка, равная 42 баллам, была получена по упрощенной методике, представленной в МЭК 62061, приложение F. Разделение (5+5+5), оценка / анализ (9) и условия окружающей среды (9+9);

λ_{De1} - интенсивность опасных отказов 1-го элемента подсистемы. Для переключателя $B1$ она равна 4,00x10^{-7}/ч (см. выше);

DC_1 - охват диагностикой 1-го элемента подсистемы. Для переключателя $B1$ он оценивается в 99% на основе контроля достоверности замыкания / размыкания контактов $B1$ и $B2$ совместно с $K1$;

λ_{De2} - интенсивность опасных отказов 2-го элемента подсистемы. Для переключателя $B2$ она равна 8,00x10^{-7}/ч (см. выше);

DC_2 - охват диагностикой 2-го элемента подсистемы. Для переключателя $B2$ он оценивается в 99% на основе контроля достоверности замыкания / размыкания контактов $B1$ и $B2$ совместно с $K1$.

8.2.7.4 Если значения этих параметров подставить в формулу, то получим $PFH_D = 3{,}04\text{x}10^{-8}$.

8.2.7.5 Аналогично для подсистемы $Q1/Q2$. Для контакторов $Q1$ и $Q2$ значение B_{10} при работе под индуктивной нагрузкой установлен срок службы в 10^6 циклов (значение производителя). Если 50% отказов считаются опасными, то значение B_{10d} удваивается по сравнению с B_{10}. С учетом предполагаемого выше значения для C интенсивность отказов каждого контактора будет равна 2,00x10^{-7}/ч.

8.2.7.6 Логическое представление архитектуры подсистемы $Q1/Q2$ соответствует логическому представлению архитектуры подсистемы типа D (см. 6.7.8.2.5 МЭК 62061) и показано на рисунке 4. Элементы подсистемы (контакторы $Q1$ и $Q2$) имеют одинаковую конструкцию, поэтому для определения PFH_D подсистемы используется уравнение (D.2) из 6.7.8.2.5 МЭК 62061:

$$\lambda_{DssD} = (1-\beta)^2([\lambda^2_{De} \times 2 \times DC] \times T_2/2 + [\lambda^2_{De} \times (1-DC)] \times T_1) + \beta \times \lambda_{De},$$

$$PFH_{DssD} = \lambda_{DssD} \times 1\,\text{ч},$$

где T_2 - интервал диагностических проверок. Для подсистемы $Q1/Q2$ эта величина равна 15 мин;

T_1 - интервал между контрольными проверками или срок службы в зависимости от того, что меньше. Для подсистемы $Q1/Q2$ длительность срока службы равна 500000 ч (57,1 лет) при заданной интенсивности использования на основе значения T_{10d} для элемента подсистемы (см. ИСО 13849-1, п.С.4.2). Интервал между контрольными проверками (см. МЭК 62061, предисловие) определяется равным 20 годам (175200 ч), что меньше, чем срок службы. Поэтому T_1 равно 175200 часов;

λ_{De} - интенсивность опасных отказов каждого элемента подсистемы (контакторы $Q1$ и $Q2$) равна 2,00x10^{-7}/ч;

DC - охват диагностикой каждого элемента подсистемы (контакторы $Q1$ и $Q2$) равен 99% на основе регулярного контроля механически связанных зеркальных контактов с помощью $K1$ в процессе запуска;

β - восприимчивость к отказам по общей причине. Эта величина равна 5% (0,05), так как ее оценка, равная 42 баллам, была получена по упрощенной методике, представленной в МЭК 62061, приложение F: разделение (5+5+5), оценка / анализ (9) и условия окружающей среды (9+9).

Если значения этих параметров подставить в формулу, то получим $PFH_D = 1{,}01\text{x}10^{-8}$.

8.2.7.7 На подсистемы $B1/B2$ и $Q1/Q2$ затем накладываются архитектурные ограничения, приведенные в таблице 5 МЭК 62061. См. таблицу 2.

Таблица 2 - Архитектурные ограничения подсистем. Максимальное значение УПБ, которое может быть достигнуто для функции управления этой подсистемой, связанной с безопасностью

Доля безопасных отказов	Устойчивость к отказам аппаратных средств (см. примечание 1)		
	$N = 0$	$N = 1$	$N = 2$
$<$60%	Не оговаривается (см. примечание 3)	УПБ 1	УПБ 2
60% - 90%	УПБ 1	УПБ 2	УПБ 3
90% - 99%	УПБ 2	УПБ 3	УПБ 3 (см. примечание 2)
$\geq$99%	УПБ 3	УПБ 3 (см. примечание 2)	УПБ 3 (см. примечание 2)

Примечания

1 Отказоустойчивость аппаратных средств N означает, что $N+1$ отказ приведет к потере функции управления, связанной с безопасностью.

2 УПБ 4 в качестве предельного требования в настоящем стандарте не рассматривается. Об УПБ 4 см. МЭК 61508-1.

3 См. 6.7.6.4 МЭК 62061 или для подсистем, где было применено исключение сбоев к тем сбоям, которые могут привести к опасным отказам, см. п.6.7.7.

8.2.7.8 Каждая подсистема имеет долю безопасных отказов, равную 99% (на основе их охвата диагностикой), и отказоустойчивость аппаратных средств, равную 1. Поэтому предельное требование к УПБ (ПТУПБ) для каждой подсистемы равно 3.

8.2.7.9 Для подсистемы $K1$ значения $PFH_D = 2{,}31 \times 10^{-9}$/ч и ПТУПБ равно 3 были заявлены производителем (см. выше).

8.2.7.10 Поэтому максимальный УПБ, который может быть получен на основе наименьшего ПТУПБ, равен 3.

8.2.7.11 Значения PFH_D каждой подсистемы далее суммируются:

3,04x10^{-8} (подсистема $B1/B2$)+2,31x10^{-9} (подсистема $K1$)+1,01x10^{-8} (подсистема $Q1/Q2$)=4,28x10^{-8}.

Полученное значение соответствует диапазону от $\geq 10^{-8}$ до $<10^{-7}$, представленному в МЭК 62061, таблица 3. Поэтому, если все другие требования МЭК 62061 выполнены, эта функция безопасности обеспечивает УПБ 3.

8.3 Заключение

8.3.1 Результаты выполненных расчетов для этого простого примера с использованием метода из ИСО 13849-1 дает среднюю вероятность опасных отказов, равную 2,70x10^{-8}/ч (т.е. соответствующую УБ, равному *e*), а при использовании метода, описанного в МЭК 62061, дает вероятность опасных отказов, равную 4,28x10^{-8}/ч (т.е. соответствующую УПБ 3). Разница между этими результатами находится в пределах ожидаемой оценки погрешности и, следовательно, показывает приемлемый уровень соответствия между обоими стандартами.

8.3.2 Существуют некоторые различия между двумя стандартами в том, как учитывается β (восприимчивость к отказам по общей причине) для избыточных систем. Это может привести к небольшому, но приемлемому отклонению (как показано в данном примере) между PFH_D, полученными по двум стандартам. Методология ИСО 13849-1 предполагает, что $\beta = 2\%$, если выполнены обоснованные меры, представленные в ИСО 13849-1, таблица F.1. В МЭК 62061 структурированная таблица F.1 используется другим способом. Применение этой таблицы позволяет получить значение β фактора в диапазоне от 1% до 10%. Каждый метод определения β применяется только в контексте методологии проектирования подсистемы соответствующего стандарта.

Библиография

[1] IEC 62061, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

[2] ISO 13849-1, Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

[3] IEC 61511-1, Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

[4] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

[5] ISO 14121-1, Safety of machinery - Risk assessment - Part 1: Principles

[6] IEC 61508-5, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5. Examples of methods for the determination of safety integrity levels

[7] ISO 13849-2, Safety of machinery - Safety-related parts of control systems - Part 2: Validation

[8] IEC 61800-5-2, Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional

[9] IEC 60947-5-1:2003, Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices

---

УДК 621.5:814.8:006.354 ОКС 35.200

Ключевые слова: безопасность функциональная, безопасность оборудования, системы управления электрические, электронные и программируемые электронные, функциональная безопасность электронных систем управления оборудованием, требования

Электронный текст документа
подготовлен ЗАО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2014