БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ

2010 г. станет началом важных изменений в законодательстве по безопасности оборудования. Практически, некоторые из них уже действуют с 2005-2006 годов, с начала периода "наложения" норм действующих и новых стандартов в области систем управления обородуванием, относящихся к безопасности.

Отчасти, это касается ряда ключевых норм, покрываемых стандартом ISO 13849 и МЭК 61508, корреспондирующим с МЭК 62061 в сфере безопасности оборудования. Таким образом, важные статистические концепции, вытекающие из безопасности процессов и относящиеся в разных степенях к вероятности опасных повреждений, покрываются нормами по безопасности оборудования, выраженными в новых классификациях устройств безопасности и систем управления оборудованием, относящихся к безопасности. К этим классификациям относятся: "Уровни производительности" (PLs - Уровень производительностиs по ISO) и "Уровни целостности безопасности" (SILs - Safety Integrity Levels по МЭК). Классификации PL и SIL приходят на смену широко известным "Признакам Категорий" из "устаревшего" EN 954-1.

В 2008 МЭК завершил вторую редакцию стандарта МЭК TS 62046, включающего руководство по использованию датчиков безопасности в задачах защиты оборудования.

Эти новшества затронут законодательные институты по всему миру.

ЕВРОПЕЙСКИЕ ДИРЕКТИВЫ

Целью Директив ЕЭС является приведение законодательств стран-членов в соответствие с общими нормами, касающимися технических, экономических и прочих аспектов и упорядочить свободный оборот товаров, услуг и людей в пределах Европейского Союза.

Отчасти, там, где подразумевается безопасность персонала, приведение в соответствие законодательных норм выражается в формулировках и разрешениях Директив и Стандартов повышенной важности.

ДИРЕКТИВЫ Определение целей.

СТАНДАРТЫ Определение средств и методов достижения целей, определенных Директивами.
Продукция и услуги, отвечающие единым стандартам должны соответствовать Директивам.

Стадии внедрения Стандарта:
- Создание рабочей группы из экспертов - представителей стран-участников ЕЭС;
- Разработка проекта Стандарта и предоставление на экспертизу в государственные органы;l
- Разработка определяющих формулировок Стандарта, официальная публикация и принятие странами-участниками в свои законодательства.

Директивы, относящиеся к защите персонала::
- 89/391/EC "Здоровье и безопасность на рабочем месте - Рамочная директива"
- 89/655/EC "Использование рабочего оборудования" с исправлениями и добавлениями

Директивы, регулирующие компоненты безопасности::
- 98/37/EC (2006/42/EC, начиная с 29/12/2009) "Директивы об оборудовании"
- 2006/95/EC "Низковольтное оборудование"
- 2004/108/EC "Электромагнитная совместимость"

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

СОЦИАЛЬНЫЕ ДИРЕКТИВЫ

“Социальные директивы” 89/655/ЕС и 89/391/ЕС нацелены на усиление безопасности в рабочей среде.

Директивы:

- Определение превентивных мер, применимых к рабочей среде.
- Снабжение информацией по:
  - анализу рисков
  - программам предотвращения несчастных случаев и приведения оборудования к соответствию
  - процедурам, касающимся соответствия оборудования
  - ответственности работодателя
  - образованию и обучению персонала.
- Предписание о приведении имеющегося оборудования в соответствие с Директивой об Оборудовании.

ДИРЕКТИВЫ ПО ОБОРУДОВАНИЮ

“Директива об оборудовании 98/37/ЕС” и вступающая в силу 29.12.2009 Директива 2006/42/ЕС предназначены для производителей оборудования и компонентов безопасности и нацелены на:

- Определение требований по безопасности и защите здоровья для повышения уровня защиты рабочих, связанных с опасным оборудованием
- Проектирование, изготовление и распространение оборудования безопасности и частей на территории ЕЭС в соответствии с требованиями, истекающими из самих Директив
- Свободное обращение оборудования безопасности и частей в странах-участниках ЕЭС в соответствии с Директивами

Директива об Оборудовании:

- Применима к новым станкам и компонентам безопасности как проданным, так и взятым в аренду, к подержанным станкам, в случае продажи, аренды или займа
- Устанавливает основные требования безопасности, относящиеся к конструкции станков и компонентов безопасности и определяет соответствующие процедуры сертификации
- Является обязательной для станков и компонентов безопасности. Только отвечающая директиве продукция может распространяться на территории ЕЭС.

Процедуры сертификации

Директива:

- Покрывает обязательные процедуры для компонентов безопасности и станков высокой степени опасности, перечисленных в Приложении 4
- Покрывает упрощенные процедуры для станков малой и средней степени опасности, не перечисленных в Приложении 4
- Требует от производителя заведения технического досье на каждый вид продукции, устанавливающее принципы безопасности, применимые к конструкции, производству, транспортировке и техническому обслуживанию оборудования и компонентов безопасности.

Декларация соответствия

Для подтверждения соответствия продукции Директиве, производитель обязан:

- Нанести на продукцию маркировку CE
- Приложить декларацию CE о соответствии, свидетельствующую о соответствии Директиве.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Новая Директива об Оборудовании (2006/42/EC), опубликованная в 2006, на замену действующей версии, вступает в силу с 29/12/2009.

ГЛАВНЫЕ ЦЕЛИ ЗАМЕНЫ

Прозрачность

- Список оборудования, покрываемого Директивой является более точным
- Добавлены новые классы
- Границы, относящиеся к Директиве определены более четко
- Улучшены определения.

Законная достоверность

- Четвертый пункт гласит: "Для обеспечения законной достоверности для пользователей, границы настоящей Директивы и концепции, относящиеся к ее применению должны быть определены как можно точнее".

Улучшена применяемость

- Концепции, регулирующие номинацию уполномоченных органов являются более строгими
- Исследования рынка. Обязанности стран-членов определены более точно
- Добавлены правила по изъятию опасной продукции.

Пересмотрены процедуры оценки на соответствие

- Более не является возможным представление в уполномоченные органы технических файлов без прохождения сверки по последним требованиям
- Внутренняя инспекция процесса производства (Приложение VIII) требуется для всех процедур оценки на соответствие. Ответственность за инспекцию возлагается на производителя.

Пояснение к приложению с перечнем опасного оборудования и компонентов безопасности
В противоположность к MD 98/37/EC, MD 2006/42/EC, Приложение 4 с перечнем опасного оборудования и компонентов, относящихся к безопасности теперь включает логические устройства (т.к. ПЛК и др.).
Кроме этого, добавлено Приложение 5 для включения прочих компонентов безопасности.

ОСУЩЕСТВЛЕНИЕ ПЕРЕХОДА ОТ MD 98/37/EC К MD 2006/42/EC

Декларация о соответствии

- С учетом практических и технических аспектов, производители могут начать производство и продажу продукции в соответствии с новой Директивой об Оборудовании
- Директива 2006/42/EC вступает в законную силу с 29/12/2009
- Для продукции, произведенной до 29/12/2009, если дата первого распространения на рынке не определена, производитель может выпустить декларацию о соответствии со ссылкой на обе директивы. Ссылки на Директиву 98/37/EC должны быть постепенно удалены после 29/12/2009.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Сертификация

- Из-за изменений обязательных требований по охране здоровья и безопасности в новом Приложении I, ранние декларации утрачивают силу. В любом случае, декларации о соответствии должны быть переписаны со ссылками на новые директивы
- Сертификаты CE, выпущенные уполномоченными органами подлежат обновлению
- Новые сертификаты CE действуют в течении 5 лет (Приложение IX, пар. 9.3).

Действенность самостоятельной сертификации

- Процедуры, указанные в ст. 8, парагр. 2, разделе C Директивы 98/37/CE прекращают свое действие с 29/12/2009
- Тогда, производители, прошедшие сертификацию в соответствии с этими процедурами, должны пройти повторную сертификацию в порядке, установленном ст. 12, пар. 3 и 4 новой Директивы.

ДИРЕКТИВА О НИЗКОВОЛЬТНОМ ОБОРУДОВАНИИ

2006/95/EC нацелена на:

обеспечение контроля при конструировании и производстве электрических материалов, так, чтобы гарантировать защиту людей от рисков получения травмы при использовании этих материалов. Настоящая Директива применяется ко всем электрическим материалам, подразумевающим использование номинального напряжения в пределах:

- 50В и 1000В для переменного тока
- 75В и 1500В для постоянного тока.

Последняя версия Директивы вступила в силу с 16/01/2007.

ДИРЕКТИВА ОБ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ

Целью команды разработчиков “Директивы об электромагнитной совместимости” 2004/108/EC является обеспечение контроля при конструировании и производстве электрических приборов с тем, чтобы:

- В достаточной мере ограничить электромагнитное излучение во избежание его воздействия на работу электрических приборов
- Уровень собственной защиты к внешним помехам позволял электрическим приборам выполнять функции согласно их предназначению.

Настоящая Директива применима ко всем электрическим и электронными приборам, способным производить электромагнитные помехи, чья работоспособность может быть нарушена внешними факторами.

ДИРЕКТИВА ATEX

Директива Atex 94/9/EC применяется ко всем изделиям для использования во взрывоопасной атмосфере. Директива определяет минимальные требования к безопасности электрических приборов, используемых в средах, классифицируемых как опасные из-за рисков взрыва газов или пылевой взвеси.
Риски взрыва классифицируются по трем уровням:

- Категория 1 : максимальный уровень риска (зоны 0 и 20)
- Категория 2 : высокий уровень риска (зоны 1 и 21)
- Категория 3 : нормальный уровень риска (зоны 2 и 22).

Директива ATEX действует с 1/07/2003.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

УПОЛНОМОЧЕННЫЕ ОРГАНИЗАЦИИ

Роль уполномоченных организаций каждого государства-члена ЕЭС заключается в проведении оценки и проверки на применимость и соответствие Директивам, относящимся к оборудованию и компонентам безопасности.

Каждое государство отвечает за учреждение собственных организаций и осуществление над ними контроля.

Уполномоченные организации должны обладать достаточным опытом и ресурсами для осуществления своей деятельности по проведению проверок, анализа, технической поддержки, измерений и т.д..

КОМПЕТЕНТНЫЕ ОРГАНИЗАЦИИ

Компетентные организации уполномочены проводить проверки и сертификацию машин и компонентов безопасности на соответствие применяемым Директивам.

От каждого государства-члена ЕЭС требуется:

• Назначить компетентные организации и определить их задачи
• Предоставить список уполномоченных организаций в Европейскую Комиссию, а также, другим членам ЕЭС.

Европейская Комиссия публикует справочник всех уполномоченных организаций в Официальном журнале Европейской Комиссии с указанием переченя услуг, видов оборудования и систем безопасности, с которыми связана деятельность уполномоченных организаций.

ГАРМОНИЗИРОВАННЫЕ СТАНДАРТЫ

• Это технические стандарты, воплощенные для удовлетворения существенных требований Директив ЕЭС
• Эти стандарты написаны различными техническими комитетами, созданными на основании мандата Комиссии Европейского Союза
• Организации, одобряющие и утверждающие эти стандарты:
  - CEN (European Committee for Stiardization) - Европейский комитет по стандартизации
  - или CENELEC (European Committee for Electrotechnical Stiardization) - Европейский комитет по электротехнической стандартизации
• Эти стандарты публикуются в Официальном журнале Европейского комитета и в официальных изданиях каждого члена ЕЭС.

Статус стандартов

• prEN... предложенный стандарт (проект), еще окончательно не одобренный
• EN... утвержденный стандарт, вступивший в силу
• TS... техническая спецификация (или ТУ).

Европейские стандарты, относящиеся к безопасности делятся на 3 типа:

СТАНДАРТЫ ТИПА A
определяют основные принципы конструирования, применимые ко всем типам машин:
т.к... • EN ISO 12100 - 1,2 Безопасность оборудования - основные положения и принципы конструирования
• EN ISO 14121 - 1 Оценка риска.

СТАНДАРТЫ ТИПА B
разделены на два класса:
- Стандарты Типа B1: имеют отношение к определенным аспектам безопасности
т.к... • EN 999 Расположение защитного оборудования с учетом скорости приближения частей тела человека
• EN ISO 13857 Безопасные расстояния для защиты верхних конечностей
• EN 60204 Безопасность оборудования. Электрооборудование машин
• EN ISO 13849 - 1,2 Элементы систем управления, относящиеся к безопасности.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

- Стандарты Типа B2: имеют отношение к устройствам безопасности
т.к... • EN 61496-1 Электро-чувствительное защитное оборудование - Основные требования и испытания
• EN 61496-2 Электро-чувствительное защитное оборудование- Специфические требования к оборудованию, использующему активные оптоэлектронные защитные приборы (напр.: световые завесы)
• EN 61496-3 Электро-чувствительное защитное оборудование - Специфические требования к активным оптоэлектронным защитным приборам, реагирующим на диффузное отражение (напр.: лазерный сканер)
• EN ISO 13850 Устройства аварийного останова.

СТАНДАРТЫ ТИПА C
относятся к определенным видам оборудования:
т.к... • EN 692 Механические прессы
• EN 693 Гидравлические прессы
• EN 415 Упаковочное оборудование
• EN 415-4 Системы паллетизации
• EN ISO 10218 Промышленные роботы.

- Стандарты Типа C имеют превосходство над стандартами типов A и B.
- При отстутствии стандартов Типа C, соответствие Директивам может быть достигнуто на основе стандартов типов A и B.

Что за стандарт МЭК TS 62046 – Применение и внедрение электро-чувствительных защитных приборов?
МЭК TS 62046 Ч. 2 - 2008 дает рекомендации по установке и использованию электро-чувствительного защитного оборудования (ESPE). В основном, он применим к световым завесам, лазерным сканерам, бамперам и матам. МЭК TS 62046 определяет правила точного расположения электро-чувствительных приборов на оборудовании и их взаимодействия с СУ. Цель - обеспечение минимизации риска оператора за счет правильного выбора и применения защитных устройств.
МЭК TS 62046 содержит ключевые аспекты, связанные с ESPEs, такие как: правила выбора, использование, внедрение в СУ машин, а также, содержит сведения об особых функциях световых завес, включая Приглушение и Бланкирование.

СТАНДАРТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

На территории Российской Федерации в качестве национальных стандартов применяются международные стандарты и региональные стандарты других стран (ГОСТ Р 50.1.035-2001 «Рекомендации по стандартизации. Порядок применения международных и региональных стандартов в Российской Федерации»).
Применение международного или регионального стандарта может быть прямым или косвенным.
Прямое применение международного стандарта не связано с его принятием в нормативном документе, действующем в системе стандартизации РФ (ГСС РФ). В таком случае, международный стандарт применяется в том виде, как он издан соответствующей международной организацией на языке оригинала или в переводе (официальном) на русский язык.
Косвенное применение осуществляется методом утверждения стандарта РФ на основе международного или регионального стандарта. Возможны варианты полного и частичного применения.
Акроним, используемый в обозначении стандарта, указывает на страну или международную организацию, выпустившую стандарт.
Акронимы, используемые в обозначениях:
1. ИСО (ISO – International Organization for Stiardization) – Международная Организация по Стандартизации;
2. МЭК (IEC – International Electrotechnical Commission) – Международная Электротехническая Комиссия;
3. ЕН (EN – European Norms) – Европейские Нормы.
Если в российском документе используется аутентичный перевод без каких-либо изменений и дополнений, то обозначение стандарта выглядит, например, так: ГОСТ Р ИСО 13849-1-2003.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

МЭК и ИСО – международные организации, членом которых является Российская Федерация. В области безопасности оборудования и средств защиты на территории РФ, вместе со стандартами РФ, применяются стандарты этих организаций.
Законодательная деятельность ИСО и МЭК относится к сфере стандартов, деятельность ЕН – к сфере стандартов и директив. По назначению и правовому статусу, директива ЕН (ЕЭС) сравнима с Техническим регламентом, нормативно-правовым актом Российской Федерации, устанавливающим обязательные для применения и исполнения требования к объектам технического регулирования. Комплекс стандартов по безопасности оборудования подразделяется на три основных типа (А, В, С), установленных стандартом ГОСТ Р ЕН 414-2002 «Безопасность оборудования. Правила разработки и оформления стандартов по безопасности»: «…3.1 стандарты типа А (основополагающие стандарты по безопасности): Стандарты, содержащие основные концепции, принципы конструирования и общие аспекты, которые могут быть применены к оборудованию всех видов.
3.2 стандарты типа В (стандарты групповых вопросов безопасности): Стандарты, которые относятся к одному аспекту безопасности или к одному типу защитного устройства, которые могут быть применены к оборудованию широкого диапазона:
- стандарты типа В1 распространяются на определенные аспекты безопасности (например, безопасное расстояние, температура поверхности, шум);
- стандарты типа В2 распространяются на устройства, обеспечивающие безопасность (например, двуручное устройство управления, блокирующее устройство).
3.3 стандарты типа С (стандарты по безопасности машин): Стандарты, содержащие детальные требования по безопасности отдельных видов машин или группы однородных машин..»

К основным стандартам, составляющим Тип А, относится серия стандартов ГОСТ ИСО 12100 «Безопасность оборудования. Основные понятия, общие принципы конструирования».

Стандарты Типа В1

ГОСТ ИСО 13849-1-2003 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1: Общие принципы конструирования», разработанный на основе ISO 13849-1:1999. ГОСТ ИСО 13855-2006 «Безопасность оборудования. Расположение защитных устройств с учетом скоростей приближения частей тела человека» (EN 999).
ГОСТ Р 51334-99 «Безопасные расстояния для предохранения верхних конечностей от попадания в опасную зону» (EN 294).
ГОСТ Р 51838-2001 «Безопасность машин. Электрооборудование производственных машин. Методы испытаний».

Стандарты Типа В2

МЭК 61496-(1, 2) «Безопасность оборудования. Электрочувствительные предохранительные устройства».
МЭК 62061:2005 «Безопасность машин и механизмов. Функциональная безопасность электрических, электронных и программируемых электронных систем управления, связанных с безопасностью» (системы E/E/PE).
ГОСТ Р МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (системы E/E/PE).

Стандарты Типа С

Данные стандарты содержат детальные требования по безопасности отдельных видов машин или групп однородных машин. Примеры стандартов:
ГОСТ 12.2.113-2006 «Прессы кривошипные. Требования безопасности»;
ГОСТ Р ЕН 12717-2006 «Безопасность металлообрабатывающих станков. Станки сверлильные»;
ГОСТ ЕН 13128-2006 «Безопасность металлообрабатывающих станков. Станки фрезерные (включая расточные)»;
ГОСТ Р 53010-2008 «Прессы гидравлические. Требования безопасности»;
ГОСТ ЕН 12478-2006 «Безопасность металлообрабатывающих станков. Станки крупные токарные с числовым программным управлением и центры обрабатывающие крупные токарные»;
и т.д..

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

ОЦЕНКА РИСКА

Европейский стандарт EN ISO 14121-1 предлагает систематизированный порядок исследования рисков, связанных с оборудованием с целью выбора и принятия наиболее подходящих мер по снижению или устранению рисков.

В США такой же порядок исследования приведен в Техническом отчете - ANSI Technical Report B11.TR3.

Таким образом, оценка риска может быть выполнена в 4 этапа:

1. Выявление ограничений машины
- заключается в исследовании намеренного использования и всех предвиденных случаев неиспользования в отношении к уровню подготовки, опыта и ответственности персонала.

2. Распознавание опасных явлений
с перечислением этих явлений:
• Риски и опасности от источников (механические, электрические, химические и др.)
• Опасные ситуации (ручная загрузка-выгрузка, доступ в систему и т.п.)
• Случаи, которые могут вызвать повреждения (отказ оборудования или аномальные явления).

В течении всего жизненного цикла оборудования, включая вывод из эксплуатации и демонтаж.

3. Анализ риска.
Любая распознанная опасная ситуация вытекает из соотношения следующих составляющих:
• Тяжесть травмирования и опасность жизни и здоровью (обратимая, не обратимая, смертельная)
• Вероятность получения травмы, как следствие от частоты и продолжительности подвержения опасности
• Вероятность избежания опасности с учетом:
  - быстроты событий,
  - возможности оператора увидеть опасность и быстро среагировать,
  - возможности уклониться.

4. Оценка риска.
В процессе анализа и оценки риска требуется определить: требуется ли снижение риска или каким образом можно добиться безопасности. Если требуется снижение риска, принятые меры защиты должны быть оценены на предмет их способности обеспечить требуемое снижение риска.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

СИСТЕМЫ УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ, ОТНОСЯЩИЕСЯ К БЕЗОПАСНОСТИ

Системы управления, от котрых зависит безопасность оборудования должны быть сконструированы так, чтобы обеспечить минимальную вероятность возникновения функциональных ошибок. Иными словами, любая ошибка не должна привести к утрате функций безопасности.
В Европе, для удовлетворения этих требований настоятельно рекомендуется использовать гармонизированные стандарты, разработанные по распоряжению Европейской Комиссии (обязательное декларирование на соответствие). При возникновении несчастного случая, использование гармонизированных стандартов позволяет экономить время и траты, свзанные с потдверждением соответсвия систем управления, относящихся к безопасности требованиям Директивы об оборудовании.
Здесь приведены основные концепции новых стандартов ISO 13849-1 и МЭК 62061, заменяющие положения стандарта EN954-1 и являющиеся регламентрующим инструментом для систем управления оборудованием.

Старый EN 954-1 Элементы систем управления, связанные с обеспечением безопасности. Часть 1: Основные принципы конструирования.

Элементы систем управления, связанные с обеспечением безопасности, соответствующие стандарту EN 954-1применялись до 29 декабря 2009. С 29 декабря 2009 вводится обязательное соответствие стандартам ISO 13849-1 и МЭК 62061.

В стандарте EN 954-1, действующем с1996, системы управления, относящиеся к безопасности классифицируются по пяти категориям.

Категории безопасности

Для различных частей оборудования могут быть определены различные уровни риска. Поэтому, степень (категория) меры безопасности принимается в зависомости от существующего риска для каждой части оборудования.

Для выбора оптимальной категории в отношении существующего риска используется хорошо известная таблица.

Выбор Категории

S Тяжесть травмирования:
S1 Легкая травма (обычно обратимая).
S2 Тяжелая травма (обычно не обратимая) или смерть.

F Частота и продолжительность подвержения опасности:
F1 Редко и не продолжительно.
F2 Часто или непрерывно, постоянно.

P Возможность избежания опасности:
P1 Возможно в некоторых случаях.
P2 Почти не возможно.

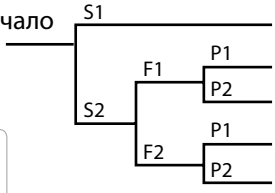


ТАБЛИЦА КАТЕГОРИЙ

Категории				
B	1	2	3	4
■	■	□	□	□
▪	■	■	□	□
	▪	■	■	□
		▪	■	□
			▪	■

■ Подходящая категория

□ Завышенная категория

▪ Возможная категория при условии применения дополнительной защиты

В Категориях B и 1 способность сопротивления отказам основана на прочности компонентов.
В Категориях 2, 3, 4 способность сопротивления отказам основана на управлении рисками.
В Кат. 2 отказ контролируется через мониторинг циклов, в Кат. 3 - через дублирование, в Кат. 4 - через мониторинг и дублирование.

Примечание: Категории не являются обязательно иерархическими.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

КАТЕГОРИЯ	ТРЕБОВАНИЯ	ПОВЕДЕНИЕ СУ	ПРИНЦИПЫ БЕЗОПАСНОСТИ
B	Приборы должны быть разработаны, произведены и соединены согласно соотв. стандартам с тем, чтобы они выдерживали ожидаемое воздействие.	Неисправность может привести к потере функции безопасности.	Использование выбранных компонентов.
1	Должны применяться требования категории B. Необходимо использовать успешно испытанные компоненты.	Неисправность может привести к потере функции безопасности, но вероятность неисправности ниже, чем в категории B.	
2	Должны применяться требования категории 1. Функция безопасности должна проверяться через соотв. интервалы СУ машины.	Неисправность может привести к потере функции безопасности между проверками. Потеря функции безопасности обнаруживается в ходе проверки.	Использование структуры и цепи безопасности, способной обнаружить неисправность и остановить машину.
3	Должны применяться требования категории 1. Одиночная неисправность не должна приводить к потере функции безопасности; там, где практически возможно, одиночная неисправность должна обнаруживаться.	Не все неисправности могут быть обнаружены. Накопление выявленных неисправностей может приводить к потере функции безопасности.	
4	Должны применяться требования категории 1. Одиночная неисправность не должна приводить к потере функции безопасности; одиночная неисправность обнаруживается во время или до следущего запроса функцией безопасности.	Неисправность должна быть обнаружена вовремя и не должна привести к потере функции безопасности.	

Ограничения стандарта EN 954-1

Поведение системы при неисправности не может быть единственным путем оценки производительности системы управления, связанной с обеспечением безопасности.
Другие факторы, такие, как надежность компонентов, могут играть важную, иногда, решающую роль.
Эта концепция признается стандартом EN 954-1 в Приложении B: “надежность компонентов и используемые в рассматриваемой задаче технологии могут вызвать отклонение от предусмотренной категории.”
В этом случае процесс выбора категории заключается в следующем:

- Определение номинальной или рекомендуемой категории, основанной на анализе риска (по таблице рисков)
- Уточнение категории, основанной на надежности компонентов, используемой технологии и др..

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Вторая фаза в процессе выбора категории является, в основном, эмпирической; стандарт не содержит на этот счет инструкций. Почти всегда категория выбирается "без вариантов", ссылаясь на таблицу рисков и не учитывая других факторов или появившихся изменений, через субъективный подход, на основании которого трудно доказать безопасность системы.

К тому же, экстенсивное использование программируемой электроники в системах управления оборудованием подчеркивает недостатки детерминистской модели, не пригодной для комплексных систем управления, использующих ПЛК, линии связи, исполнительные устройства с переменной скоростью и программируемые датчики.
В оценке производительности комплексных систем, относящихся к безопасности, лучше использовать оценку вероятности способности систем обеспечивать безопасность, когда это необходимо. Или, иными словами, оценивать вероятность возникновения опасного сбоя в заданный период времени, учитывая надежность компонентов.

Новые стандарты

Для восполнения недостатков EN 954-1 были приняты два новых стандарта: ISO 13849-1:2006 и МЭК 62061:2005. Новые стандарты совмещают вероятность и известные концепции детерминизма, охватывая технический прогресс в области промышленного оборудования.

Оба этих стандарта согласованы с Директивой 98/37/EC, касательно следующего обязательного требования к безопасности:

Приложение I : 1.2 Управление

Тоже самое касается новой Директивы об оборудовании 2006/42/EC (Приложение I: 1.2 Системы управления).

Два стандарта показывают различия и наложения, касающиеся, особенно, критериев применения.

Стандарт ISO 13849-1 распространяется на все виды применяемых технологий обеспечения безопасности, не зависимо от вида используемой энергии: механической, гидравлической, пневматической, электрической.
Стандарт определяет пять назначенных архитектур безопасности.

Стандарт МЭК 62061 распространяется только на электрические системы управления.
Стандарт содержит формулы расчета надежности подсистем только для четырех типов архитектур, определенных в документе, но может быть применен и для других архитектур. Это позволяет привести конструкции подсистем в соответствие с требованиями стандарта ISO 13849-1: 1999 (EN 954-1).

ISO 13849-1 Элементы систем управления, связанные с обеспечением безопасности. Часть 1: Основные принципы конструирования.

ISO 13849-1 это пересмотренная версия стандарта EN 954-1.

Комплексные математические формулы из теории надежности систем заменены предварительно расчитанными таблицами.

Некоторые понятия стандарта EN 954 остались без изменения, т.к. категории, дублирование, мониторинг.
Многое подверглось изменениям, например: таблица рисков, таблица выбора категорий и др..
Категории более не играют решающей роли, как в стандарте EN 954-1.

Метод категорий в оценке сопротивляемости систем опасным сбоям заменен Уровнями Производительности (PL), выражающими способность систем управления, относящимся к безопасности (SRP/CS) обеспечивать защиту при определенных рабочих условиях.

Основным параметром в оценке уровня PL является Средняя Вероятность Опасного Сбоя в течении часа (PFHd).
Сбой считается опасным, если он, не будучи обнаруженным, приводит к блокировке защитной функции.

Всего уровней производительности 5: PLa, PLb, PLc, PLd, PLe.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Средняя вероятность опасного сбоя в течении часа

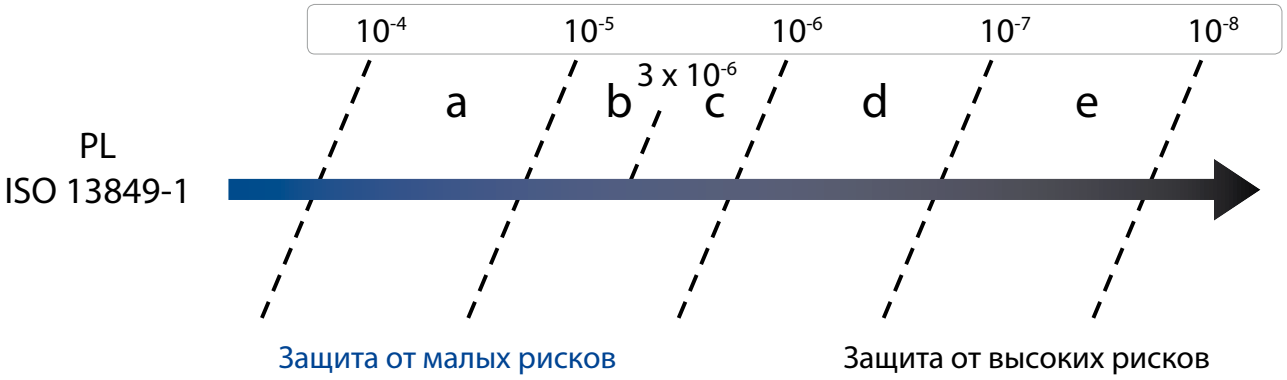


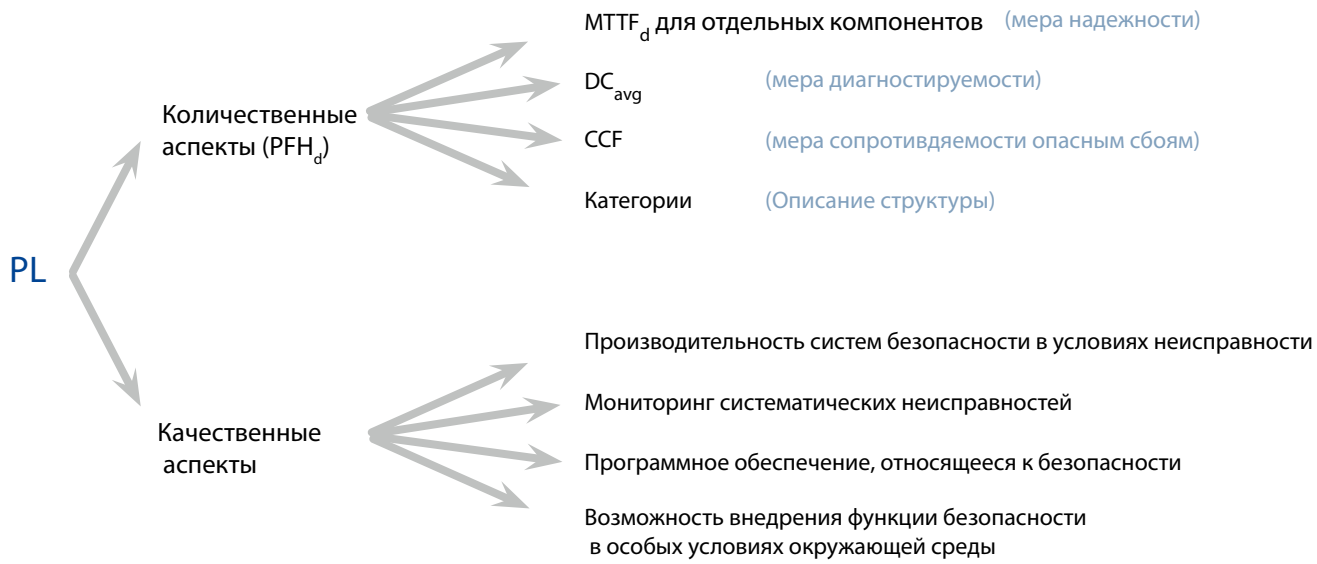
Таблица 3 из ISO 13849-1

Чем больше вклад в снижение риска, тем меньше вероятность опасного сбоя в течении часа.

Уровень производительности PL, определяемый архитектурой систем управления, надежностью компонентов, способностью быстрого выявления внутренней неисправности, оказывает потенциальное влияние на функциональную безопасность и качество конструкции.

Таблица ниже отражает обобщенные обязательные количественные и качественные требования к конструкции систем управления по ISO 13849-1.

См. словарь - Стр. 26



БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Претендуя на данный уровень производительности PL, дополнительно к оценке средней вероятности опасного сбоя в течении часа, необходимо также удостоверить соответствие требованиям к качеству, установленным в стандарте.

Заявленный уровень PL должен быть обоснован с помощью стандарта ISO 13849-2 "Элементы систем управления, связанные с обеспечением безопасности - Процедуры, определяющие обоснованность, анализ и тестирование для оценки:
- Обеспечиваемых функций безопасности
- Полученной категории
- Достижимого уровеня производительности.

ВНИМАНИЕ!

Средняя вероятность опасного сбоя в течении часа - лишь один из параметров, требуемых для назначения уровня PL.
Заявленный уровень PL в обязательном порядке должен быть подтвержден соответствием всем требованиям, включая:
- Мониторинг систематических неисправностей
- Использование прочных и надежных компонентов
- Работа в соответствии с хорошим техническим опытом
- Учет условий окружающей среды, в которых будут работать системы безопасности
- При использовании нового программного обеспечения: исполнение всех организационных мероприятий по модели типа V, показанной на Рис. 6 в стандарте ISO 13849-1 и удовлетворение требований к разработке и применению встраиваемых систем.

Конструирование систем управления по ISO 13849-1, в общем, может быть выполнено за восемь шагов:

1 – Установление функции безопасности на основе анализа рисков
2 – Назначение требуемого уровня производительности (PLr) используя диаграмму рисков
3 – Выбор архитектуры системы и метода самодиагностики
4 – Техническая разработка системы управления
5 – Расчет $MTTF_d$, DCavg и проверка CCF
6 – Расчет PL с использованием Таблицы 5
7 – Проверка уровня PL и сравнение с требуемым уровнем PLr (если PL < PLr - возврат к шагу 3)
8 – Утверждение.

Определение элемента, относящегося к безопасности и назначение требуемого уровня производительности - PLr

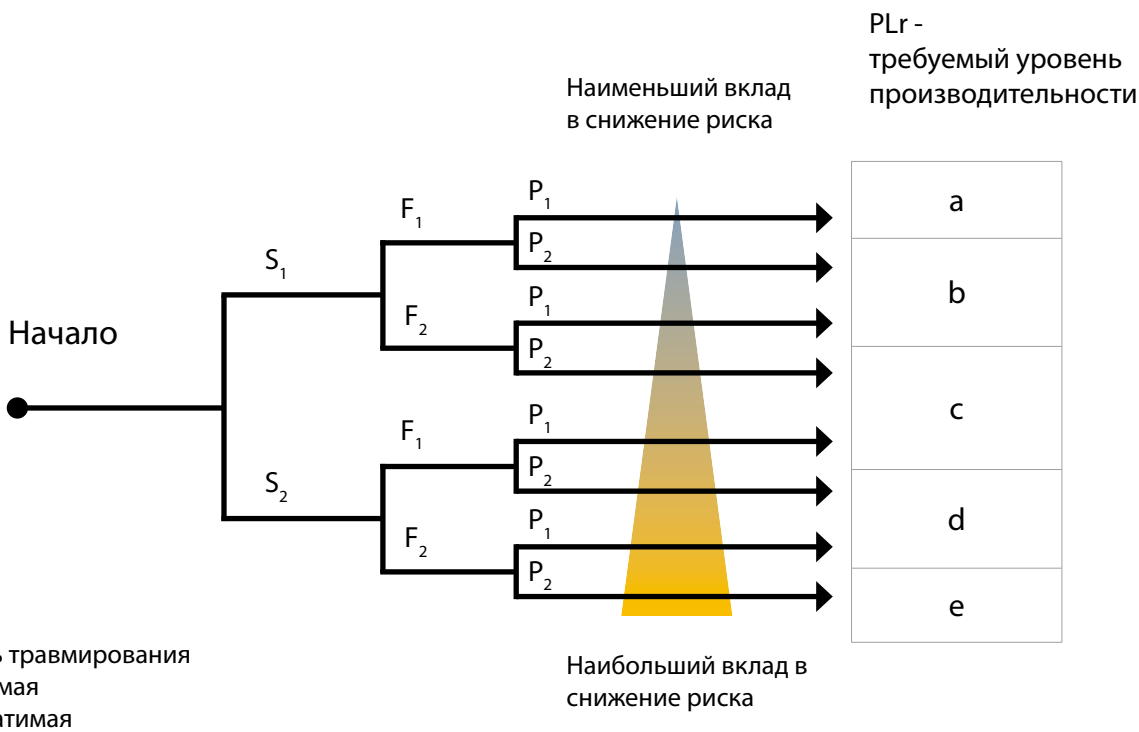
Установление функции безопасности и назначение требуемого уровня производительности - PLr.
Для каждой функции безопасности (см. ISO 14121 – Оценка рисков) разработчик определяет требуемый уровень производительности PLr на основании оценки вклада, требуемого для снижения риска.
Данный вклад не покрывает все риски, исходящие от машины, только часть, относящуюся к конкретной задаче.

Параметр PLr представляет требуемый уровень производительности функции безопасности в поставленной задаче.
Параметр PL представляет уровень безопасности внедряемого оборудования.
PL должен быть равным или больше уровня PLr.

С помощью древовидной схемы можно выявить вклад функции безопасности, необходимый для снижения риска и ясно определить требуемый уровень безопасности PLr.

Если требуется установить несколько функций безопасности, требуемый уровень производительности PLr должен быть определен для каждой из них.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ



S тяжесть травмирования
S1 обратимая
S2 не обратимая

F частота или время подвержения риску
F1 изредка / короткое
F2 постоянно / продолжительное

P возможность избежания риска или ограничения опасности
P1 возможно в данных условиях
P2 почти не возможно

Примечание: в противоположность Категориям стандарта EN954-1, уровни PLrs полностью "иерархичны". PLr(e) вносит наибольший вклад в снижение риска, тогда как PLr(a) вносит наименьший.

Конструирование систем управления (СУ), относящихся к безопасности и оценка уровня PL

Конструктор принимает решение о том, какой уровень производительности PLr требуется в задаче и разрабатывает схему СУ, удовлетворяющую PLr. Затем, производится расчет фактического уровня производительности PL. Он должен быть не ниже требуемого уровня PLr.

Рис. 3 показывает как получить фактический уровень PL: должен быть произведен расчет средней вероятности опасного отказа СУ в течении часа (PFHd).

Методы расчета средней вероятности опасного отказа СУ в течении часа (PFHd) предполагают, что все нижеперечисленные элементы известны:

- Нормативное значение отказа (λ) (норма отказа)
- Процентное распределение нормы отказа между всеми состовляющими режимов отказа (Пример. Для ключей положительного действия режимы отказа следующие: контакт не открывается, когда требуется в 20% случаев и не закрывается в 80% случаев. Следовательно: не открытие = λ x 0,2, не закрытие = λ x 0,8)
- Влияние каждого отказа на производительность СУ (опасный отказ = λd, не опасный отказ = λs)
- Распознанный процент отказа (встроенной системой автоматической самодиагностики) вне общего опасного отказа: λdd = λd x DC.
- Не распознанный процент отказа (встроенной системой автоматической самодиагностики) вне общего опасного отказа: λdu = λd x (1-DC).

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Для упрощения вычислений стандарт ISO 13849-1 предлагает таблицы с предварительными расчетами для различных комбинаций категорий, $MTTF_d$ и DCavg, произведенными по модели Маркова (сети Маркова-Петри).

Значение $MTTF_d$	Диапазон $MTTF_d$
Низкое	3 года ≤ $MTTF_d$ < 10 лет
Среднее	10 лет ≤ $MTTF_d$ < 30 лет
Высокое	30 лет ≤ $MTTF_d$ < 100 лет

Значение DCavg	Диапазон DC / DCavg
Нет	DC < 60%
Низкое	60% ≤ DC < 90%
Среднее	90% ≤ DC < 99%
Высокое	99% ≤ DC

Тогда, задача сводится к: выбору архитектуры, расчету DCavg по отношению к применяемому методу самодиагностики, упрощенному расчету $MTTF_d$ для цепи, разработанной и проверенной согласно требованиям к функционированию независимых каналов (CCF) в архитектурах с дублированием (Кат. 2, 3 и 4).

В каждой из 7 колонок представлена адоптированная комбинация категории и DCavg (Рис. 5 из ISO 13849-1). Расчетный $MTTF_d$ определяет - какая часть колонки должна быть рассмотрена. Соотв. уровень PL показан в левой части таблицы.

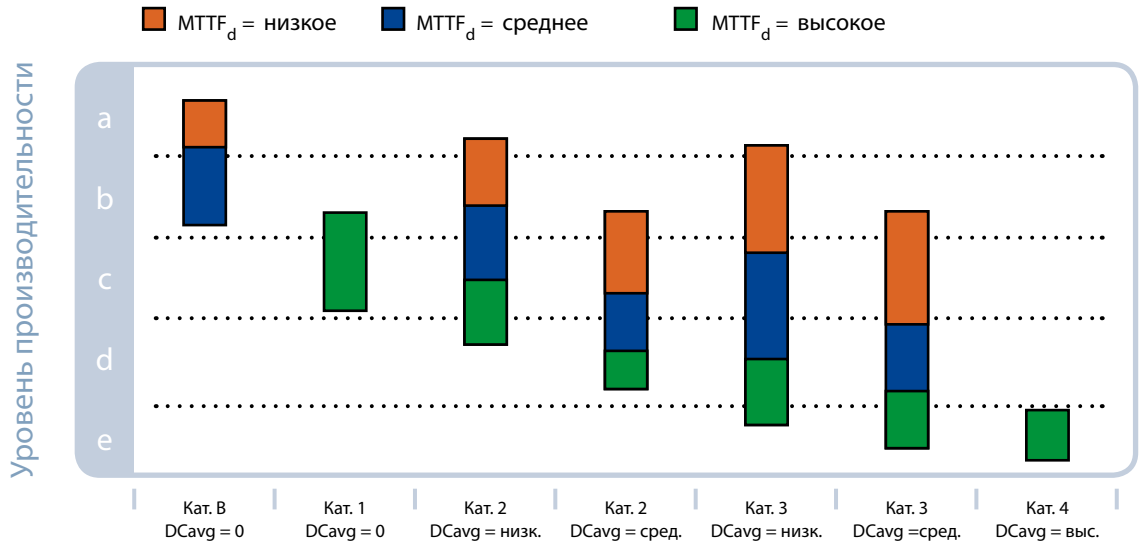


Рис. 5 из ISO 13849-1

Столбец в колонке может перекрывать до трех возможных значений PL. Например, для Кат. 3, DCavg = сред. и $MTTF_d$ = низкое, возможны три варианта: PLb, PLc, PLd. В подобных случаях уровень PL может быть уточнен с помощью Таблицы K.1 в Приложении K к стандарту (здесь не приводится). Таблица включает детализированные значения средней вероятности опасного сбоя в течении часа и PL по отношению к существующему значению $MTTF_d$ и применяемой комбинации категории и DCavg.

Стандарт применим также в случае использования в системе управления одной и более архитектур из пяти, установленных в стандарте. Каждая из архитектур соответствует своей категории из EN 954-1.

В системах, разработанных по EN 954-1, выбор категории непосредственно связан с анализом риска по предложенной схеме. Стандарт ISO 13849-1 является более гибким, предлагая несколько доступных вариантов для каждого уровня производительности. В Таблице 5 приведен пример, в котором уровню PLc соответствует 5 альтернативных вариантов:

1. Категория 3 с $MTTF_d$ = низкий и DCavg средний.
2. Категория 3 с $MTTF_d$ = средний и DCavg низкий.
3. Категория 2 с $MTTF_d$ = средний и DCavg средний.
4. Категория 2 с $MTTF_d$ = высокий и DCavg низкий.
5. Категория 1 с $MTTF_d$ = низкий.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Комбинация нескольких элементов управления (SRP/CS) и общий уровень производительности PL

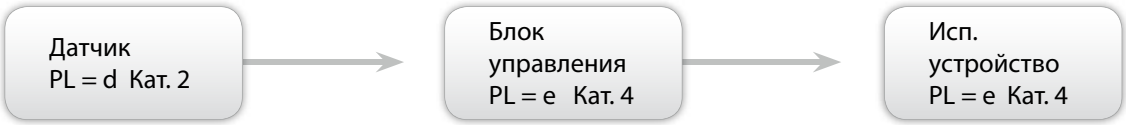
SRP/CS - safety related parts of control system - элементы систем управления, связанные с обеспечением безопасности

Функция безопасности может включать один и более элементов SRP/CSs, также, функция безопасности может использовать SRP/CS как с одинаковыми, так и с разными архитектурами.
Когда функция безопасности получается из нескольких, последовательно подключенных элементов, т.к. световая завесаs, блок управления, исполнительное устройство, для каждого из которых уровень PL известен, стандарт предлагает простой метод расчета общего уровня PL.

Опередилите элемент с уровнем PL = PL низкий.

PL (низкий)	n (низкий)		PL
a	> 3 ≤ 3		- a
b	> 2 ≤ 2		a b
c	> 2 ≤ 2		b c
d	> 3 ≤ 3		c d
e	> 3 ≤ 3		d e

Полученный с помощью этой таблицы PL относится к значениям надежности в серединах каждого интервала в Таблице 3 из ISO 13849-1.



имеем: PL низкий = d N низкий = 1 (< 3)

тогда: PL общий = d

и средняя вероятность опасного сбоя в течении часа будет равняться величине между 1 x 10^{-6} и 1 x 10^{-7} (См. Таблицу 3 из ISO 13849-1).

МЭК 62061 Безопасность оборудования – Функциональная безопасность электрических, электронных и программируемых электронных систем управления.

Стандарт МЭК 62061 вытекает из МЭК 61508 – Функциональная безопасность электрических, электронных и программируемых электронных систем управления, относящихся к безопасности.

Стандарт МЭК 61508 состоит из семи разделов. Первые три раздела определяют требования безопасности к оборудованию и программному обеспечению; остальные содержат информацию для поддержки пользователя по правильному применению.

Стандарт МЭК 62061 сохраняет черты МЭК 61508, упрощая при этом требования к безопасности (как для оборудования, так и для программного обеспечения), адаптируя эти требования к специфическим нуждам промышленного оборудования.
Требования к безопасности рассматриваются только в "режиме повышенного спроса", т.е. при запросе функции безопасности чаще, чем один раз в год. Стандарт базируется на двух основных концепциях:

- Управление функциональной безопасностью
- Уровень полноты безопасности.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Управление функциональной безопасностью

МЭК 62061. Определяются все аспекты конструирования, необходимые для достижения требуемого уровня функциональной безопасности, начиная от требований к документации, процесса конструирования и заканчивая утверждением.

Каждая конструкция должна иметь собственный План Функциональной Безопасности, должным образом задокументированный и дополненный при необходимости.

План Функциональной Безопасности определяет лиц, их функциональные обязанности и ресурсы, требуемые для разработки и внедрения системы безопасности.

Уровень полноты безопасности (SIL)

Требования и методология включают:

- определение функциональных требований к каждой внедряемой функции безопасности
- присвоение уровня полноты безопасности (SIL) для каждой предусмотренной функции безопасности
- разработка элементов SRECS, соответствующих внедряемой функции безопасности
- апробация и утверждение элементов SRECS.

Присвоение SIL

Присвоение SIL производится с помощью метода, приведенного в Приложении А (при этом, также принимается методология МЭК 61508-5).

Для каждого определенного риска необходимо оценить:

- Степень тяжести (Se) возможного повреждения
- Частоту и время (Fr) подвержения опасности
- Вероятность опасного события (Pr), связанного с режимом работы машины
- Возможность избежать опасность (Av).

Последствия	Тяжесть Se	Класс Cl					Частота и продолжительность Fr		Вероятность опасного события Pr		Избегание Av	
		4	5-7	8-10	11-13	14-15						
Смерть, потеря глаза, руки	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≥ 1 часа	5	Оч. выс.	5		
Постоянн.: потеря пальцев	3		OM	SIL 1	SIL 2	SIL 3	< 1 часа - ≥ 1 дня	5	Приемл.	4		
Обратимые: лечение	2			OM	SIL 1	SIL 2	< 1 дня - ≥ 1 2 недель	4	Возмож.	3	Не возм.	5
Обратимые: первая помощь	1				OM	SIL 1	< 1 2 недель - ≥ 1 1 года	3	Редко	2	Возможно	3
							< 1 1 года	2	Ничтожн.	1	Вероятно	1

OM (Other Measures - Прочие меры) = Рекомендуется использовать другие параметры.

Из суммы признаков частоты, вероятности и избегания выводится класс вероятности опасности:

$$Cl = Fr + Pr + Av$$

Для получения SIL надо совместить существующий Cl с идентифицированным уровнем тяжести (Se).

Это повторяющийся процесс. Фактически, в зависимости от предпринятых защитных мер, некоторые параметры могут меняться , т.к. Fr или Pr. В данном случае, процесс прсвоения SIL должен быть повторен с использованием новых измененных параметров.

Предусмотрено три уровня полноты безопасности: SIL 1, SIL 2, SIL 3.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Средняя вероятность опасного сбоя в течении часа (PFH_d)

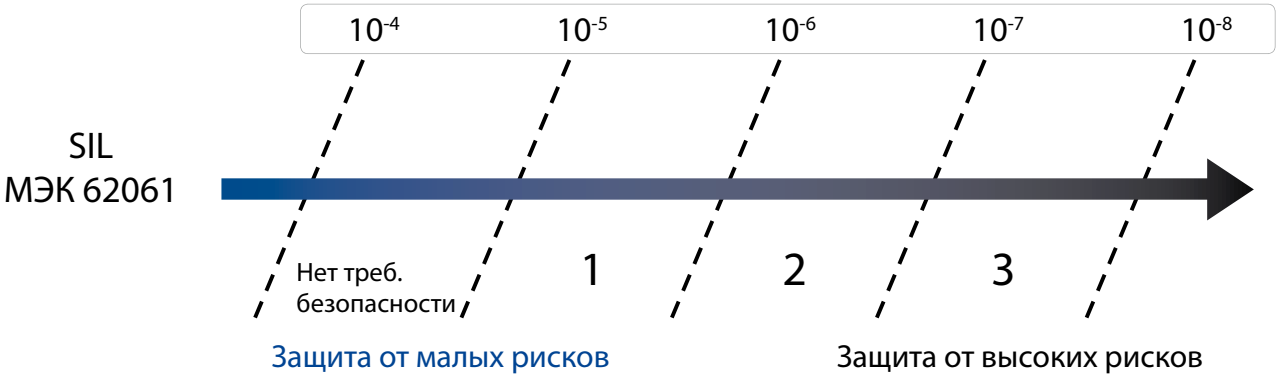


Таблица 3 из МЭК 62061

Таким образом, SIL представляет уровень безопасности, присваемый элементу СУ (SRECS) с целью получения его полноты в рабочих условиях.
Главным параметром, который используется в определении SIL (Safety Integrity Level), является вероятность опасного сбоя в течении часа (PFH_d).
Чем выше SIL, тем меньше вероятность того, что элемент SRECS не обеспечивает ожидаемой безопасности.

Параметр SIL должен быть определен для каждой отдельной функции безопасности.

Процесс разработки и конструирования

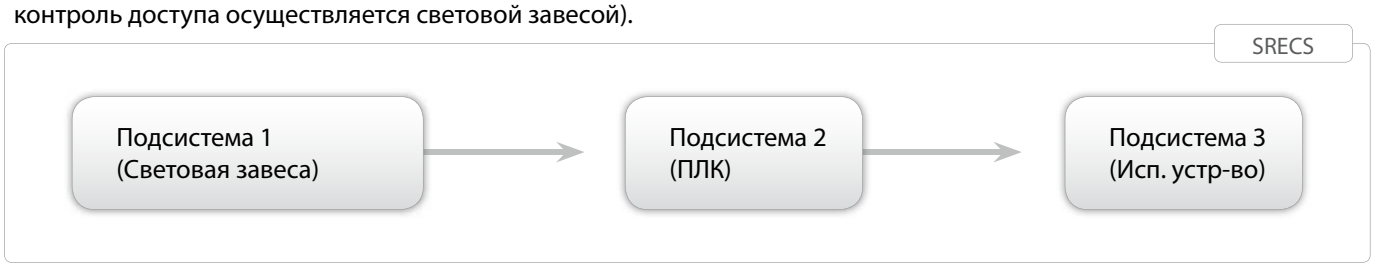
Каждая функция безопасности, определенная через анализ рисков, должна быть описана в виде:

- Операционных требований (режим работы, время цикла, условия окружающей среды, время отклика, время взаимодействия с другими компонентами, уровень электромагнитной совместимости и т.п.)
- Требований безопасности (SIL).

Каждая функция безопасности должна быть разбита на функциональные блоки, т.к.: блок входных данных, блок обработки данных, блок выходных данных.

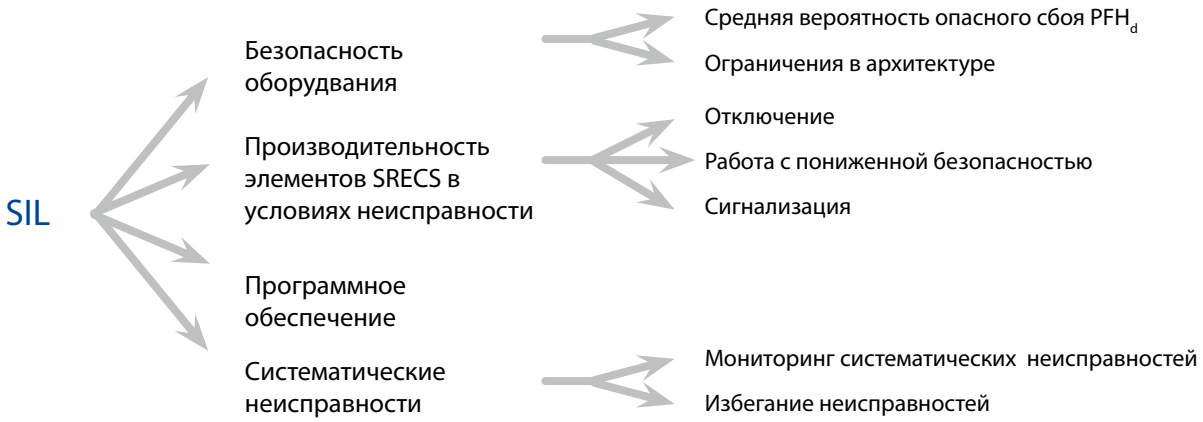
Подсистема ассоциируется с каждым функциональным блоком.
Иными словами, подсистемы будут состоять из электрических компонентов, соединенных друг с другом.

В результате внедрения элементов SRECS появляются типовые архитектуры, как показано ниже (в данном случае контроль доступа осуществляется световой завесой).



БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Элементы SRECS, удовлетворяющие требованиям безопасности учитывают следующие аспекты:



Каждая подсистема должна состять из электрических цепей, годных для достижения требуемого SIL.

Максимальный уровень SIL, достижимый подсистемой обозначается - SILCL (SIL claim).

Уровни SILCLs подсистем зависят от PFH_d, ограничений архитектуры, производительности в условиях неисправности и способности избегать систематические неисправности.

Программное обеспечение, относящееся к безопасности

SW - software - программное обеспечение - ПО

При создании программного обеспечения, код программы должен быть разработан согласно соответствующим стандартам, в следующем порядке:

Примечание 1: ПЛК безопасности, шины безопасности, исп. устройства, световые завесы и, в целом, весь комплекс устройств, относящихся к безопасности со встроенной программируемой логикой и ПО должны отвечать всем требованиям применимых промышленных стандартов и стандарта МЭК 61508 в отношении функциональной безопасности.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

ВНИМАНИЕ!

Вероятностный аспект это лишь одна из сторон, рассматриваемых при назначении уровня SIL.
Претендуя на конкретный SIL, заявитель должен доказать и документально подтвердить:

- Использование системы менеджмента и технологии, необходимых для достижения требуемого уровня безопасности
- Разработанный, обновляемый План Функциональной Безопасности
- Избегание систематических неисправностей, насколько возможно
- Оценку производительности систем безопасности в существующих условиях окружающей среды
- Разработку ПО с учетом всех организационных требований.

Расчет подсистем PFH_d

Для расчета подсистемы PFH_d прежде всего необходимо выбрать архитектуру. Стандарт предлагает четыре назначенные архитектуры с упрощенными формулами для каждой из них.
В расчете используются следующие параметры:

λ_d = Степень опасной неисправности для каждого элемента подсистемы. Выводится из известной степени неисправности λ путем процентного распределения, на основе анализа производительности подсистемы после возникновения неисправности (Опасная неисправность = λd или Не опасная неисправность = λs).

T1 = Контрольный тест. Интервал контрольного теста (внешней проверки и восстановления системы до состояния “как новый”) обычно совпадает со временем жизни системы (20 лет).

T2 = Интервал теста диагностики. В зависимости от конструкции устройства, функция диагностики может быть выполнена внутренней цепью элемента SRECS или другими элементами SRECSs..

DC = Diagnostic Coverage - Диагностическое покрытие:
Данный параметр представляет процент опасных неисправностей, которые могут быть обнаружены из всех возможных опасных неисправностей.
DC зависит от применямой технологии самодиагностики.
Учитывая, что возникновение неисправности всегда возможно (иначе не будет основания для определения λ), эти технологии не всегда равно эффективны и чувствительны (в зависимости от того, что некоторые виды неисправностей могут быть продолжительными), от чего обнаружение всех неисправностей является не возможным. Тогда, подходящая архитектура цепи может позволить обнаружение наиболее опасных неисправностей, а параметр DC может быть определен для оценки эффективности встроенной технологии самодиагностики. Стандарт МЭК 62061 не содержит данных для расчета DC в отношении применяемых технологий диагностики. Тем не менее, могут быть использованы данные из Приложения A, МЭК 61508-2.

β = Фактор неисправности в общих случаях. Выражает степень функциональной независимости каналов в дублированных системах.

Получив расчет подсистемы PFH_d посредством фрмул из МЭК 62061, важно убедиться в том, что соответствующий SILCL, полученный из Таблицы 3 МЭК 62061 (см. стр. 21), соответствует ограничениям назначенной архитектуры. Макисмальный уровень SILCL, который может быть достигнут данной подсистемой ограничивается допуском дефектов и частью безопасной неисправности SFF (см. таблицу ниже).

Часть безопасной неисправности (SFF)	Допуск дефектов оборудования		
	0	1	2
SFF < 60%	Не допускается	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 3
SFF ≥ 99%	SIL 3	SIL 3	SIL 3

Таблица 5 из МЭК 62061

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Часть безопасной неисправности подсистемы (SFF) это, по определению, те неисправности из общего числа, которые не ведут к опасным последствиям.

$$SFF = (\Sigma\lambda s + \Sigma\lambda dd) / (\Sigma\lambda s + \Sigma\lambda dd + \Sigma\lambda du).$$

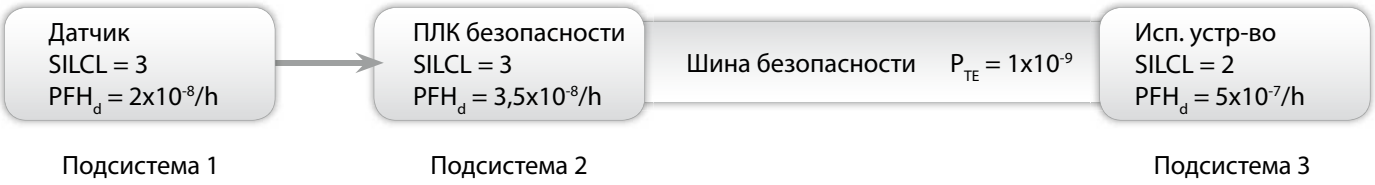
λdd (степень опасных неисправностей, которые могут быть обнаружены) и λdu (степень опасных неисправностей, которые не могут быть обнаружены) выводятся из известной эффективности применяемой технологии самодиагностики.

Когда параметры PFH_d и SILCL для каждой подсистемы известны, можно рассчитать полный уровень SIL элемента SRECS.

Полная вероятность опасного сбоя в течении часа элемента SRECS будет равняться сумме вероятностей опасного сбоя в течении часа всех задействованных подсистем, включая, при необходимости вероятность опасного сбоя линий связи (PTE), относящихся к безопасности:

$$PFH_D = PFH_{D1} + \ldots + PFH_{DN} + P_{TE}$$

Зная PFH_d, итоговый уровень SIL элемента SRECS можно получить из Таблицы 3.
Затем, для каждой подсистемы уровень SIL нужно сравнить с SILCL. Уровень SIL, присваемый элементу SRECS должен быть меньшим или равным наименьшему уровню SILCL для любой подсистемы.



$$\mathbf{PFH_d(система) = PFH_d\ (пс1) + PFH_d\ (пс2) + PFH_d\ (пс3) + P_{TE} = 5{,}56x10^{-7}/h}$$

SIL = 2

ВЫВОДЫ

Процедуры, приведенные в стандарте ISO 13849-1, по сравнению с МЭК 61508, позволяют в более простой форме произвести оценку Средней Вероятности Опасного Сбоя в течении часа, предлагая более прагматичный подход, более востребованный в машиностроении.

Сохраняя Категории и другие положения, т.к. функции безопасности и график рисков, стандарт ISO 13849-1 становится "плавным" продолжением стандарта EN 954: 1996.

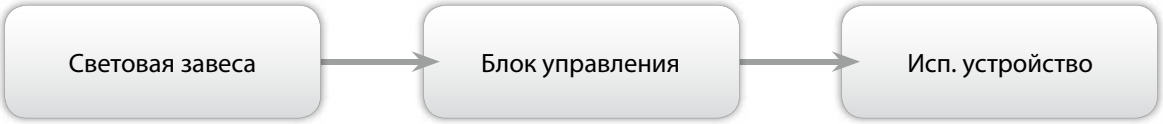
Имея тесную связь с EN 954-1:1996, новый ISO 13849-1 устраняет недостатки этого стандарта. Новый стандарт предусматривает применение комплексных технологий: программируемой электроники, шин передачи данных, различных архитектур и является более подходящим для конструирования при совместном использовании стандарта МЭК 62061.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Точное равенство между уровнями PL и SIL не может быть определено.
Тем не менее, с позиции вероятности можно провести сравнение PL и SIL, поскольку эти параметры используют одну и туже концепцию, а именно, Среднюю Вероятность Опасного Сбоя в течении часа, которая определяет степень сопротивляемости систем неисправностям.

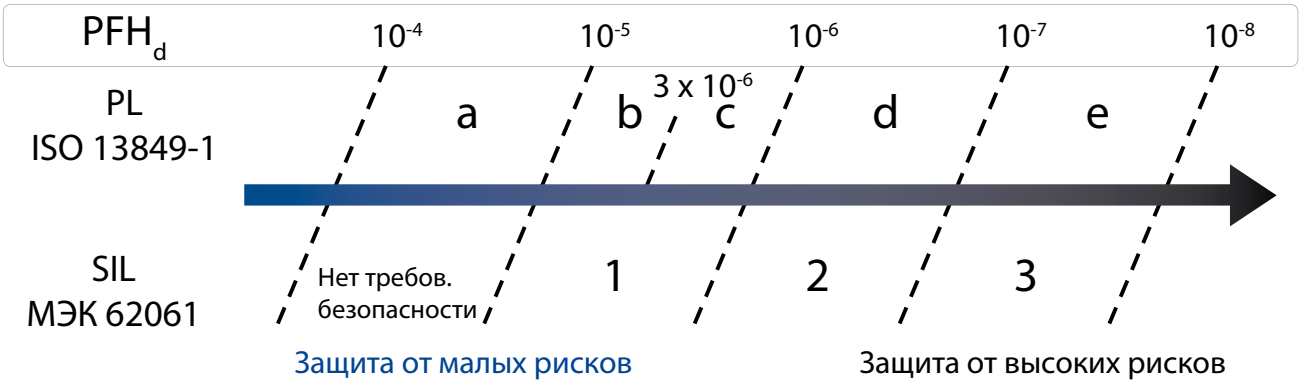
Также, хотя оба стандарта используют одну концепцию вероятности, результаты могут отличаться из-за различий в порядке расчетов. Фактически, для оценки PFH_d, МЭК 62061 определяет процедуру, основанную на формулах, вытекающих из теории надежности систем. В таких случаях, как: уменьшенное количество компонентов, высокая эффективность встроенной технологии самодиагностики, результаты могут оказаться более хорошими. Тогда, оценка вероятности опасного сбоя в течении часа может быть произведена быстрее, с помощью упрощенной методики, предлагаемой стандартом ISO 13849-1, использующей приблизительные таблицы, которые учитывают в т.ч. наиболее худшие сценарии. Однако результаты расчетов PFH_d по ISO 13849-1, менее значимы, чем по МЭК 62061.

Поэтому, требуется дополнительное внимание при расчете полного уровня PL для последовательных систем, т.к.:



Если результирующая вероятность опасного сбоя в течении часа всей системы является суммой значений PFH_d элементов, расчитанных в соответствии с МЭК 62061 без использования расчетов по ISO 13849-1, необходимо принять во внимание ограничения к элементам, исходящие из категорий, которые ограничивают макс. уровень PL, достигающий существующего уровня, определенного стандартом ISO 13849-1 (см. Таблицу 5 стандарта).
Иначе, расчетный уровень PL может оказаться выше действительного.

В качестве основного руководства может быть использована нижеследующая таблица, учитывая то, что диапазон вероятности опасного сбоя в течении часа не является действительным значением SIL и PL.



БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

Словарь

Обознач.	Описание	Стандарт	Описание
β (Beta)	Фактор неисправности в общих случаях	МЭК 62061	Степень функциональной независимости каналов во многоканальных системах; в пределах от 0.1 до 0.01 зависит от полученного CCF.
λ (Lambda)	Степень неисправности	МЭК 62061	Произвольная частота неисправностей. Известная, как Степень неисправности, выражает количество неисправностей за 1 час. Ее инверсия известна, как Среднее Время Между Неисправностями (MTBF), выраженное в часах. Произвольные неисправности возникают в результате внезапного воздействия накопленного напряжения, превышающего конструкционную прочность компонентов. Могут появиться неожиданно. Метод расчета PFH_d, данный в обоих стандартах относится только к оценке произвольных неисправностей. Единица измерения степени неисправности - FIT (Failure In Time - неисправность за время), равная одной неисправности за триллион рабочих часов (FIT=1 означает одну неисправность за 10^9 часов).
λs	Степень безопасной неисправности	МЭК 62061	Степень безопасной неисправности. Неисправности, не несущей вредных последствий для СУ. СУ продолжает обеспечивать защиту.
λd	Степень опасной неисправности	МЭК 62061	Степень опасной неисправности. Неисправности, ведущей к снижению или утрате защиты. СУ не обеспечивает защиту.
λdd	Степень опасной, обнаруживаемой неисправности	МЭК 62061	Степень опасной, обнаруживаемой неисправности. Которая может быть автоматически обнаружена встроенной системой самодиагностики.
λdu	Степень опасной, не обнаруживаемой неисправности	МЭК 62061	Степень опасной, не обнаруживаемой неисправности. Которая НЕ может быть автоматически обнаружена встроенной системой самодиагностики. Определяет значение PFH_d и, далее - SIL или PL.
Кат.	Категория	ISO 13849-1	Кятегория - основной параметр, который рассматривается при получении уровня PL. Выражает производительность элементов SRP/CS по их спсособности противостоять неисправностям. Предусмотрено пять категорий, зависимых от структурного расположения компонентов.
CCF	Общая причина неисправности	ISO 13849-1 МЭК 62061	Неисправности, вызванные общими причинами. Обеспечивает степень независимости в системах с дублированными каналами. Наибольшее возможное значение - 100.
DC	Диагностическое покрытие	ISO 13849-1 МЭК 62061	Снижение вероятности опасного сбоя, благодаря работе автоматической системы самодиагностики. Мера эффективности системы в обнаружении собственной возможной неисправности. Выражается в % (60-99).
$MTTF_d$	Среднее время до опасного сбоя	ISO 13849-1	Среднее время работы до потенциально-опасного сбоя (не характерного), выраженное в годах. Может относится к отдельному компоненту, отдельному каналу или к целой системе.

БЕЗОПАСНОСТЬ В РАБОЧЕЙ ЗОНЕ

PFH_d	Вероятность опасного сбоя в течении часа	МЭК 62061	Вероятность опасного сбоя в течении часа. Количественное представление фактора снижения риска, обеспечиваемого системой управления.
PL	Уровень производитель-ности	ISO 13849-1	Уровень производительности. В стандарте ISO 13849-1 мера управления неисправностями оценивается с использованием Уровеней производительности (PL). Выражает способность систем SRP/CS осуществлять функцию безопасности в предвиденных рабочих условиях. Всего уровней PL пять: PLa, PLb, PLc, PLd, PLe. PLe выражает самый высокий уровень снижения риска, PLa - самый низкий.
Обознач.	Описание	Стандарт	Описание
PLr	Требуемый уровень производитель-ности	ISO 13849-1	Требуемый уровень производительности. Выражает вклад каждого элемента SRP/CS в снижение риска. PLr определяют с помощью кривой риска.
SIL	Уровень полноты безопасности	МЭК 62061	Уровень полноты функции, связанной с безопасностью. Один из трех дискретных уровней выражает способность СУ, связанной с безопасностью противостоять неисправностям в соответствии со стандартом МЭК 62061. Уровень 3 соответствует самой высокой степени защиты, уровень 1 - самой низкой.
SILCL	SIL заявленный	МЭК 62061	Макс. уровень SIL, обеспечиваемый подсистемой по отношению к архитектуре и способности обнаруживать неисправности.
SRP/CS	Элементы СУ, связанные с безопасностью	ISO 13849-1	Часть системы управления машиной, способная поддерживать безопасное состояние машины.
SRECS	Элементы СУ, связанные с безопасностью: электрические, электронные, программируемые	МЭК 62061	Электрические, электронные и программируемые электронные элементы систем управления, сбой которых немедленно приводит к увеличению фактора риска, связанного с работой машины.
T1	Интервал контрольного теста	МЭК 62061	Интервал контрольного теста. Контрольный тест это внешняя ручная операция, нацеленная на обнаружение неиспраных компонентов и упадок производительности, не могущих быть обнаруженными системой самодиагностики. Единицей измерения является время (месяцы и более, обычно, годы).
T2	Интервал диагностического теста	МЭК 62061	Интервал функции самодиагностики. Это - время между тестами по обнаружению возможной внутренней неисправности. Тесты производятся автоматически, с помощью встроенных схем SRECS. Единицей измерения является время (от миллисекунд до часов).
SFF	Часть безопасной неисправности	МЭК 62061	Часть всего размера неисправности, которая является не опасной. Показывает долю в прцентах не опасных неисправностей по отношению к общему числу неисправностей СУ, связанной с безопасностью.