

## ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ – SIL

Электроприводы с уровнем полноты безопасности до SIL 3





Компания AUMA — ведущий производитель электроприводов для автоматизации промышленной арматуры. Электроприводы AUMA отлично зарекомендовали себя как устройства, регулирующие потоки жидкостей, газов, порошков и гранулятов в системах подачи и отвода воды, трубопроводных сетях, на электростанциях, нефтеперерабатывающих заводах и в различных промышленных комплексах.

#### СПЕЦИАЛИСТ ПО ЭЛЕКТРОПРИВОДАМ

---

С момента основания компании в 1964 г. мы занимаемся разработкой, производством и сбытом электроприводов, а также предлагаем сервисное обслуживание. Наша продукция известна во всем мире благодаря своей долговечности, надежности и точности в работе.

Хотя компания AUMA представляет собой среднего размера предприятие, ей удалось стать одним из лидеров мирового рынка в своей отрасли. Сейчас в компании во всем мире работают в общей сложности более 2400 человек. Благодаря разветвленной сети торговых представительств и сервисных центров клиенты всегда могут рассчитывать на помощь наших специалистов более чем в 70 странах.



## AUMA АВТОМАТИЗИРУЕТ АРМАТУРУ

### ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

AUMA предлагает широкий ассортимент электроприводов с уровнем полноты безопасности до SIL 3. Наши устройства обеспечивают безопасную работу технических установок во всем мире. Показатели безопасности и уровни полноты безопасности наших устройств подтверждены испытательными институтами мирового значения.

В этой брошюре кроме подробной информации об уровне полноты безопасности устройств AUMA вы также найдете основные сведения о функциональной безопасности и классификации уровней SIL.

Дополнительные сведения, в частности показатели безопасности, а также различные документы (сертификаты, отчеты об испытаниях и наши исчерпывающие руководства «Функциональная безопасность — SIL») можно получить у нас по запросу или загрузить с сайта [www.auma.com](http://www.auma.com).

### СОДЕРЖАНИЕ

AUMA автоматизирует арматуру	3
Снижение рисков за счет функциональной безопасности	4
Стандарты МЭК 61508 и МЭК 61511	6
Пути обеспечения функциональной безопасности	7
Понятие о функции безопасности	8
Инструментальная система безопасности	9
Основные показатели безопасности	10
Определение класса SIL	12
Повышение класса SIL	13
Уровень полноты безопасности устройств AUMA	14
Встроенный блок управления AC .2 в исполнении SIL	16
Функции модуля SIL	18
Определение показателей безопасности для продукции AUMA	20
Показатели безопасности некоторых устройств AUMA	24
Дополнительная информация	25
Уровень полноты безопасности устройств AUMA. Обзор	26
Указатель	27

Безопасность современного промышленного оборудования приобретает все большее значение. Особенно это касается нефтегазовой, химической промышленности и электростанций.

Для контроля потенциально опасных процессов в наше время используются современные системы безопасности, срабатывающие в случае сбоя. В случае аварии такие системы, например, отключают оборудование, блокируют подачу опасных веществ, обеспечивают охлаждение и открывают редуцирующие клапаны. Для снижения рисков, исходящих от установки, системы безопасности должны быть надежными и всегда работоспособными.

Но как эксплуатационник и производитель устройства могут убедиться, что используемые системы надежны в эксплуатации и соответствуют предъявляемым требованиям? Как оценить риск выхода из строя?

Таким инструментом являются нормы функциональной безопасности МЭК 61508 и МЭК 61511. Сначала они описывают методы для оценки риска выхода из строя современных систем, зачастую с программным управлением, и определения мер для снижения рисков.

## ПОНЯТИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Согласно МЭК 61508, функциональная безопасность относится к системам, отвечающим за функции безопасности, выход из строя которых создает значительные риски для людей и окружающей среды.

Чтобы добиться функциональной безопасности, система в случае аварии должна привести оборудование в безопасное состояние или обеспечить сохранение такого состояния.

Иными словами, речь идет не об общих опасностях эксплуатации оборудования, таких, которые исходят, например, от вращающихся деталей, а об опасностях, которые могут возникнуть вследствие сбоя предохранительных функций.

Целью функциональной безопасности является снижение вероятности сбоев и возникновения рисков для людей и окружающей среды до приемлемых величин.

В целом, функциональная безопасность наряду с другими мерами (противопожарная безопасность, электробезопасность, взрывозащита и др.) значительно влияют на общую безопасность оборудования.

## СНИЖЕНИЕ РИСКОВ ЗА СЧЕТ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ



## ЧТО ТАКОЕ SIL?

Параметр SIL тесно связан с функциональной безопасностью. SIL (англ. Safety Integrity Level) в переводе с английского означает «уровень полноты безопасности» и представляет собой величину, отражающую способность системы обеспечить выполнение функций безопасности.

Чем больше опасность, исходящая от процесса или оборудования, тем выше требования к надежности предохранительных функций.

Стандарт МЭК 61508 определяет четыре уровня полноты безопасности: от SIL 1 до SIL 4.

SIL 4 соответствует самым высоким требованиям безопасности, а SIL 1 — самым низким. Для каждого уровня определены специфические степени вероятности сбоя, которые не должны превышать способность системы выполнять функции безопасности.

Необходимый уровень SIL рассчитывается на основе оценки рисков.

## РОЛЬ ПРОДУКЦИИ АУМА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ

Устройства АУМА применяются в системах, обеспечивающих выполнение функций безопасности. Поэтому мы в сотрудничестве с такими сертифицирующими организациями как TÜV и exida определили, каким уровням SIL соответствуют наши электроприводы, блоки управления и редукторы.

Для определения наиболее подходящих устройств, соответствующих конкретным требованиям к безопасности, проектировщики ориентируются на показатели безопасности.



## ПРОИСХОЖДЕНИЕ

После нескольких разрушительных техногенных катастроф, таких как массовая утечка диоксида в Севезо в 1976 г. и Бхопальская катастрофа в 1984 г., начался процесс стандартизации международных нормативов безопасности технических установок.

Так, например, в ЕС появилась директива Seveso I, а позже Seveso II 96/82/ЕС. Обе директивы были направлены на устранение опасностей при авариях с выбросом вредных веществ. Основная цель этих директив — защита людей, окружающей среды и материальных ценностей. В их рамках были введены конкретные предписания в отношении установок с высоким риском возникновения опасных ситуаций.

Для реализации этих директив сначала были разработаны национальные нормы функциональной безопасности. Первым международным стандартом стал МЭК 61508, вступивший в силу в 1998 г. В Германии с 2002 года применяется аналогичный стандарт DIN EN 61508.

## МЭК 61508

Стандарт МЭК 61508 представляет собой свод действующих во всем мире нормативов функциональной безопасности для электрических, электронных и программируемых электронных систем (E/E/PES), которые выполняют предохранительные функции. Требования стандарта при необходимости применяются и к другим компонентам, например механическим.

Целевой аудиторией стандарта являются проектировщики, эксплуатационники, а также производители устройств.

Он используется в качестве базовой нормы, независимой от области применения, и дополняется другими, специализированными стандартами, например, МЭК 61511 для промышленных процессов.

### Концепция снижения рисков

Системы безопасности решают задачу снижения рисков, которые исходят от процессов и агрегатов. Стандарт предполагает, что исключить все возможные риски невозможно. Однако он предлагает методы анализа и снижения рисков, а также методы количественной оценки остаточных рисков.

### Требования к системам безопасности

В стандарте описаны требования, которые предъявляются к системам безопасности и функциям безопасности, а также приведены определения уровней полноты безопасности (SIL). На основе этих описаний определяются требования к системным компонентам, соблюдение которых является предпосылкой для обеспечения их соответствия уровням SIL.

## Принятие во внимание жизненного цикла оборудования

Чтобы минимизировать вероятность сбоев, необходимо учитывать весь жизненный цикл компонентов от разработки до вывода из эксплуатации.

## МЭК 61511

Этот стандарт дополняет МЭК 61508 и направлен на промышленные процессы. Он определяет требования к системам безопасности, используемым в обрабатывающей промышленности для снижения рисков.

Данный стандарт, в первую очередь, важен для проектировщиков и эксплуатационников.

## СФЕРА ДЕЙСТВИЯ СТАНДАРТОВ

В настоящее время на территории ЕС стандарты МЭК 61508 и 61511 не являются обязательными, так как они не гармонизированы посредством директивы ЕС. Однако соблюдая их, как эксплуатационники, так и производители получают определенные преимущества:

- > Применение методики функциональной безопасности на потенциально опасных установках и системах сегодня является обязательным требованием.
- > Стандарты могут применяться для выполнения основополагающих требований директив ЕС, если в гармонизированном европейском стандарте приводятся ссылки на них или при отсутствии гармонизированного стандарта для сферы применения.
- > Различные ведомства и страховые компании все чаще требуют соблюдения стандартов МЭК 61508 и 61511 в качестве гаранта проведения анализа рисков и принятия мер по их снижению.
- > Операторы и производители могут быть уверены, что продукция с допуском SIL, проверенная по международным стандартам, имеет определенный уровень безопасности.

# ПУТИ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

## ОЦЕНКА ТЕХНИКИ БЕЗОПАСНОСТИ

Чтобы обеспечить функциональную безопасность, необходимо сначала проанализировать опасности, которые характерны для оборудования или процесса. Признанные методы определения рисков собраны в нормативах МЭК 61508 и 61511.

Дифференцированная оценка техники безопасности выявляет процессы, которые подразумевают различные риски. Это позволяет выработать целевые мероприятия по уменьшению уровня опасности.

### Идентификация опасных процессов

Сначала необходимо проверить, какие процессы могут создавать опасности для людей и окружающей среды при выходе из-под контроля.

### Определение требований SIL

Для каждого потенциально опасного процесса затем проводится оценка степени опасности и уровня ущерба, возникшего по причине сбоя.

Для оценки можно использовать приведенный ниже график рисков. В зависимости от степени опасности и вероятности ее возникновения делается вывод, нуждается ли процесс в защите с помощью функции безопасности, и какой уровень SIL такая функция должна обеспечивать.

### Подбор необходимых элементов

Для внедрения функции безопасности с требуемым уровнем SIL проводится подбор необходимых элементов.

Чтобы упростить этот этап, производители проверяют свою продукцию на предмет ее соответствия различным уровням SIL.

### Проверка требований SIL

Анализ показателей безопасности применяемых устройств позволяет проверить, обеспечивает ли функция безопасности необходимый уровень SIL. Если нет, необходимы дополнительные меры.

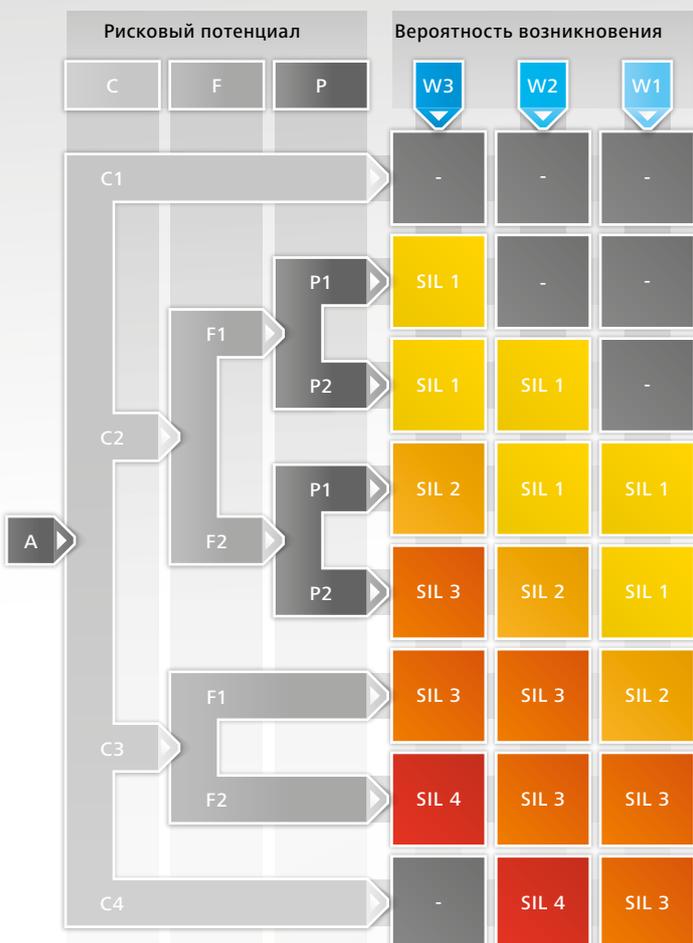


График рисков для оценки безопасности в соответствии с МЭК 61508/61511

- A Исходная точка для оценки снижения рисков
- C Размер ущерба**
  - C1 Травма малой степени тяжести одного человека или малый ущерб окружающей среде
  - C2 Тяжелые необратимые травмы или смерть одного человека
  - C3 Смерть нескольких человек
  - C4 Смерть большого количества людей
- F Предотвращение опасности**
  - F1 Возможно при определенных условиях
  - F2 Практически невозможно
- P Время пребывания человека в опасной зоне**
  - P1 Редко — часто
  - P2 Часто — длительное пребывание
- W Вероятность возникновения**
  - W3 Относительно высокая
  - W2 Малая
  - W1 Очень малая
- SIL Требуемый уровень полноты безопасности**
  - SIL 1 Самые низкие требования к безопасности
  - SIL 4 Самые высокие требования к безопасности



## ПОНЯТИЕ О ФУНКЦИИ БЕЗОПАСНОСТИ

Функции безопасности — это защитные меры, которые принимаются только в случае аварии с целью предотвращения нанесения ущерба людям, окружающей среде и материальным ценностям. Функциональная безопасность обеспечивается тогда, когда функции безопасности в аварийных ситуациях работают надежно.

К типичным функциям безопасности относятся, например, автоматическое аварийное отключение процесса, контроль и ограничение давления в котле.

При управлении арматурой особое внимание уделяется следующим функциям безопасности:

- > Аварийное открытие и закрытие (аварийное отключение, англ. ESD — Emergency Shutdown)
- > Аварийное состояние покоя/останова
- > Контрольный сигнал конечного положения

### АВАРИЙНОЕ ОТКРЫТИЕ НА ПРИМЕРЕ РЕДУКЦИОННОГО КЛАПАНА

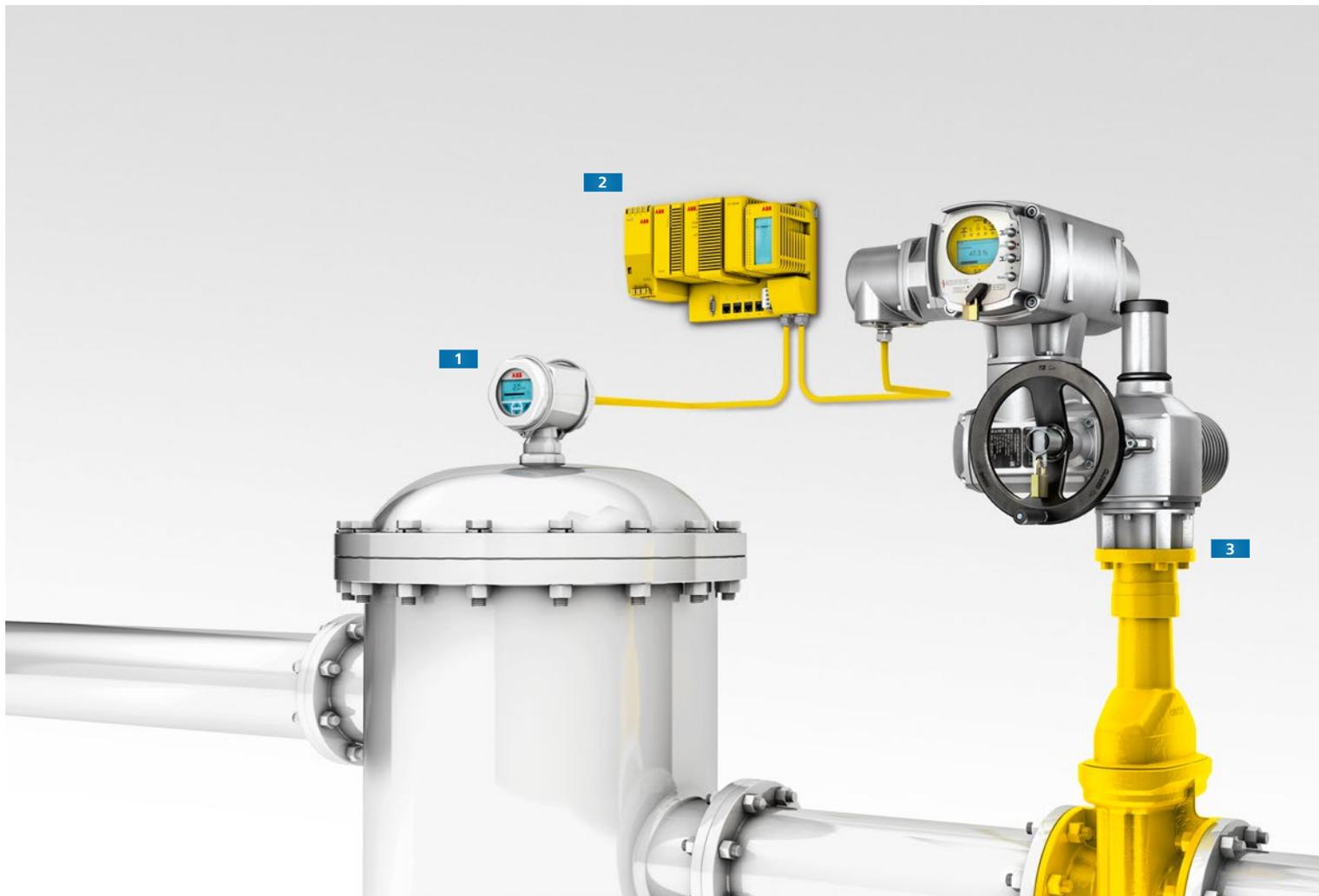
Чтобы предотвратить превышение давления в котле, в качестве функции безопасности предусмотрено открытие редукционного клапана.

Датчик непрерывно контролирует давление в котле. Когда давление в системе поднимается до недопустимого уровня, безопасная система на базе ПЛК исходит из того, что система неисправна, и подает приводу сигнал открытия для безопасного сброса давления в котле.

### АВАРИЙНЫЙ ОСТАНОВ НА ПРИМЕРЕ ШЛЮЗА

Во время нахождения судна между воротами шлюза функция безопасности надежно удерживает их от закрытия.

Функция аварийного останова может применяться, в том числе в целях блокировки. В этом случае шлюз можно закрыть только при отсутствии сигнала аварийного останова.



## ИНСТРУМЕНТАЛЬНАЯ СИСТЕМА БЕЗОПАСНОСТИ

Функция безопасности реализуется с помощью элементов так называемой инструментальной системы безопасности (англ. Safety Instrumented System, SIS). Такая система стандартно состоит из датчика, контроллера верхнего уровня и исполнительного узла. При управлении арматурой исполнительный узел включает в себя электропривод и арматуру.

Оценивая соответствие функции безопасности требуемому уровню SIL, необходимо учитывать показатели всех элементов инструментальной системы безопасности (см. также стр. 12).

### Компоненты стандартной инструментальной системы безопасности (SIS)

- 1 Датчик
- 2 Контроллер верхнего уровня
- 3 Исполнительный узел, состоящий из электропривода и арматуры

# ОСНОВНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

При оценке потенциальной опасности процесса для каждой функции безопасности определяется уровень SIL, который она должна обеспечивать. После этого подбираются технические средства для реализации функции безопасности. Для присвоения устройству класса SIL применяются методы расчета вероятности по стандартам МЭК 61508 и 61511.

Ниже будут рассмотрены основные показатели безопасности.

## СРЕДНЯЯ ВЕРОЯТНОСТЬ ОТКАЗА (ПАРАМЕТР PFD)

Значение параметра  $PFD_{avg}$  (Средняя вероятность опасных отказов по запросу) показывает среднюю вероятность несрабатывания функции безопасности после подачи сигнала на ее включение.

Стандарт МЭК 61508 определяет допустимый диапазон вероятности отказа для каждого уровня SIL.

SIL 1 — самый низкий уровень безопасности. SIL 4 — самый высокий уровень. Чем выше уровень безопасности, тем ниже допустимая вероятность несрабатывания предохранительной функции при запросе.

Безопасность системы зависит не только от величины рисков в случае аварии. Важным фактором также является ожидаемая частотность наступления аварии и, таким образом, интенсивность запросов на выполнение соответствующей функции безопасности.

Стандарт МЭК 61508 различает два режима интенсивности запросов: низкая и высокая (непрерывная).

### Режим низкой интенсивности запросов

В этом режиме интенсивность запросов на выполнение функций безопасности не превышает одного раза в год. Как правило, это относится к функциям безопасности обрабатываемой промышленности там, где применяются электроприводы.

Это касается только функции безопасности. Привод, который одновременно применяется и для функции безопасности, и для обычного открытия и закрытия арматуры, в обычном режиме может переключать арматуру намного чаще. Однако рассчитываемая вероятность сбоя, при которой требуется аварийное закрытие арматуры, не должна превышать одного раза в год.

### Режим высокой интенсивности запросов (или режим непрерывных запросов)

В этом режиме запросы на выполнение функции безопасности поступают непрерывно или чаще одного раза в год.

В этом режиме в качестве единицы измерения безопасности применяется вероятное количество отказов в час или значение PFH (англ. Probability of Failure per Hour).

## Допустимые значения PFD для режима низкой интенсивности запросов

Уровень полноты безопасности	Допустимое значение $PFD_{avg}$ (низкая интенсивность запросов)	Теоретически допустимое количество сбоев при запросе на выполнение функции безопасности
SIL 1	$\geq 10^{-2} \dots < 10^{-1}$	Допускается один опасный сбой в 10 лет
SIL 2	$\geq 10^{-3} \dots < 10^{-2}$	Допускается один опасный сбой в 100 лет
SIL 3	$\geq 10^{-4} \dots < 10^{-3}$	Допускается один опасный сбой в 1000 лет
SIL 4	$\geq 10^{-5} \dots < 10^{-4}$	Допускается один опасный сбой в 10 000 лет

Значения PFD сначала рассчитываются отдельно для каждого элемента системы технической безопасности.

Однако уровень SIL определяет совокупную безопасность всех элементов системы. Для этого необходимо на основе значений PFD отдельных элементов рассчитать общее значение PFD функции безопасности.

## ИНТЕНСИВНОСТЬ ОТКАЗОВ

При оценке безопасности системы важную роль играет анализ вероятных источников отказов.

При анализе интенсивности отказов различают опасные и неопасные отказы. Неопасные отказы не оказывают влияния на работу функции безопасности. Затем требуется определить, подвергается ли отказ диагностике.

## ДОЛЯ БЕЗОПАСНЫХ ОТКАЗОВ (SFF)

Параметр SFF (англ. Safe Failure Fraction) показывает процент неопасных и обнаруженных опасных отказов из общего количества отказов. Отказ считается безопасным, если он не может перевести систему в опасное состояние.

Чем выше значение этого параметра, тем ниже вероятность опасного отказа системы. Значение 62%, например, означает, что 62 отказа из 100 не оказывают влияния на работоспособность системы.

## ОТКАЗОУСТОЙЧИВОСТЬ ОБОРУДОВАНИЯ (HFT)

Параметр HFT (англ. Hardware Fault Tolerance) показывает способность аппаратного блока обеспечивать выполнение функции безопасности в случае сбоя или ошибки.

Значение отказоустойчивости N означает, что сбои, порядковый номер которых равен N + 1 или выше, могут привести к отказу функции безопасности. Если отказоустойчивость равна нулю, то уже первая ошибка может стать причиной отказа функции безопасности.

Значение отказоустойчивости, как правило, можно повысить за счет резервирования (см. также стр. 13).

## ТИП УСТРОЙСТВА

Стандарт МЭК 61508 разделяет устройства на простые и сложные.

### Простые устройства — тип А

Для устройств типа А («простых» устройств) характерно то, что реакция их узлов на сбой полностью известна. «Простые» устройства состоят, например, из реле, резисторов, транзисторов. Сложные электронные узлы, такие как микроконтроллеры, в устройствах типа А отсутствуют.

### Сложные устройства (тип В)

В конструкцию устройств типа В входят электронные узлы, например микроконтроллеры, микропроцессоры и интегральные микросхемы. При наличии таких узлов сложно определить все ошибки, особенно для программно-управляемых функций.

### Чем сложнее устройство, тем выше требования.

Ниже представлены две таблицы, из которых видно, что требования к устройствам типа В значительно выше, чем к устройствам типа А.

### SFF и HFT для устройств типа А

SFF (доля безопасных отказов)	HFT (отказоустойчивость оборудования)		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 ... < 90%	SIL 2	SIL 3	SIL 4
90 ... < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

### SFF и HFT для устройств типа В

SFF (доля безопасных отказов)	HFT (отказоустойчивость оборудования)		
	0	1	2
< 60%	недопустимо	SIL 1	SIL 2
60 ... < 90%	SIL 1	SIL 2	SIL 3
90 ... < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

## СРЕДНИЙ ПЕРИОД РАБОТЫ МЕЖДУ ОТКАЗАМИ (MTBF)

Средний период работы между отказами (англ. Mean Time Between Failures) в количестве лет показывает теоретическое время работы системы между двумя последовательными сбоями. Данный параметр отражает надежность системы, и его не следует путать со сроком службы или сроком эксплуатации системы.

Решающим фактором, определяющим надежность функции безопасности, всегда является уровень полноты безопасности всей системы, а не отдельного компонента. По этой причине недостаточно учитывать только показатели PFD отдельных элементов системы.

## КЛАСС SIL ФУНКЦИИ БЕЗОПАСНОСТИ

Для того чтобы рассчитать класс SIL функции безопасности, в самом простом случае необходимо сложить значения PFD отдельных элементов системы. Полученный результат затем сравнивается с допустимой общей вероятностью отказов требуемого уровня SIL.

На рисунке ниже показан пример того, что применение элементов только класса SIL 2 не гарантирует соответствие всей функции безопасности классу SIL 2. Класс SIL 2 присваивается только в том случае, если параметр PFD для всех элементов в целом находится в пределах требований SIL 2.

## ОПРЕДЕЛЕНИЕ КЛАССА SIL

Расчет общего значения PFD функции безопасности



Если расчеты показывают, что выбранные узлы оборудования не позволяют достичь требуемого уровня SIL, для повышения класса SIL можно принять дополнительные меры, например провести диагностику и обеспечить резервирование.

### ТЕСТ ЧАСТИЧНОГО ХОДА КЛАПАНА (PVST)

Во время теста через равные промежутки проверяется работа устройства. Арматура (управляемая приводом) совершает определенный ход, а затем возвращается в исходное положение. При этом контролируется действительное движение привода.

Тест PVST является признанной методикой повышения готовности отдельных элементов, обеспечивающих выполнение функции безопасности. Профилактическая диагностика позволяет исключить опасные сбои, поэтому вероятность отказов снижается.

### КОНТРОЛЬНОЕ ИСПЫТАНИЕ

Во время контрольного испытания система проходит полную проверку. Если интервал между двумя повторными проверками сокращается, например с двух до одного года, возможно повышение класса SIL в связи с более быстрым обнаружением неизвестных ошибок.

### РЕЗЕРВИРОВАНИЕ

Резервирование также повышает вероятность выполнения функции безопасности в случае аварии. При этом в резерве могут находиться как минимум два устройства системы безопасности.

В зависимости от требований безопасности применяются различные конфигурации MoN («M из N»). Например, в конфигурации 1oo2 («один из двух») достаточно одного устройства, чтобы обеспечить выполнение функции безопасности. В конфигурации 2oo3 («два из трех») должны работать два устройства из трех. Конкретное исполнение зависит от требуемой функции безопасности.

Применение резервирования может повысить отказоустойчивость оборудования и класс SIL.

Для систем уровня SIL 3 согласно МЭК 61511, как правило, используется схема резервирования, например 1oo2.

## ПОВЫШЕНИЕ КЛАССА SIL

Система с резервированием для надежного открытия



Система с резервированием для надежного закрытия



Основная задача проектировщика и эксплуатационника состоит в том, чтобы использовать только такие компоненты, которые соответствуют требованиям к безопасности. Чтобы помочь с выбором своим клиентам, компания AUMA определила показатели безопасности и класс SIL электроприводов, блоков управления и редукторов своего производства.

Обзор всех устройств AUMA, подвергнутых оценке, приведен на странице 26. Более подробный обзор показателей безопасности избранных приводов приведен на странице 24.

## ФУНКЦИИ БЕЗОПАСНОСТИ

Показатели безопасности и класс SIL зависят от предохранительной функции, которую выполняет устройство в случае аварии с целью приведения системы в безопасное состояние.

В связи с тем, что основной функцией электроприводов является закрытие и открытие арматуры, безопасности данных процессов уделяется основное внимание.

## УРОВЕНЬ ПОЛНОТЫ БЕЗОПАСНОСТИ УСТРОЙСТВ AUMA



### ЭЛЕКТРОПРИВОДЫ SA И SQ БЕЗ ВСТРОЕННОГО БЛОКА УПРАВЛЕНИЯ

Электроприводы SA и SQ сами по себе, без встроенного блока управления, соответствуют уровню полноты безопасности SIL 2. Это в равной мере касается версий SAR и SQR для режима регулирования, а также SAEx и SQEx для взрывоопасных зон.

Работу функций технического управления для таких электроприводов обеспечивает заказчик.



### ЭЛЕКТРОПРИВОДЫ SA И SQ СО ВСТРОЕННЫМ БЛОКОМ УПРАВЛЕНИЯ AC .2 В ИСПОЛНЕНИИ SIL

Во встроенных блоках управления AC .2 и ACExC .2 в исполнении SIL функции безопасности выполняются через отдельную плату.

Электроприводы с этим блоком управления соответствуют уровню SIL 2. Соответствие уровню SIL 3 обеспечивается за счет резервирования.

Широкие функциональные возможности AC .2 остаются доступными в стандартном режиме работы.

Подробнее о блоке управления AC .2 в исполнении SIL смотрите на следующих страницах.

### Аварийное открытие и закрытие

По команде функции безопасности привод движется в конечное положение ОТКРЫТО или ЗАКРЫТО.

Такие функции безопасности в качестве дополнительной меры диагностики можно также использовать вместе с тестом частичного хода клапана (PVST).

### Аварийное состояние покоя/останова

По команде функции безопасности двигатель привода отключается. Принимаются меры против нежелательного запуска двигателя.

### Контрольный сигнал конечного положения

При достижении конечных положений ОТКРЫТО/ЗАКРЫТО или при достижении момента срабатывания электромеханический блок выключателей подает соответствующий сигнал. Данная функция не является нормативной функцией безопасности. Однако, как показывает опыт, она повышает показатели безопасности.



#### ЭЛЕКТРОПРИВОДЫ SA И SQ СО ВСТРОЕННЫМ БЛОКОМ УПРАВЛЕНИЯ AC .2 В СТАНДАРТНОМ ИСПОЛНЕНИИ

Приводы со встроенным блоком управления AC .2 или ACExC .2 в стандартном исполнении во всех рассматриваемых вариантах соответствуют уровню SIL 1.

AC .2 позволяет сконфигурировать функции безопасности «Аварийное открытие и закрытие» (ESD) и «Безопасное состояние покоя/останова».



#### ЭЛЕКТРОПРИВОДЫ SA И SQ СО ВСТРОЕННЫМ БЛОКОМ УПРАВЛЕНИЯ AM

Электроприводы со встроенным блоком управления AM или AMEx во всех рассматриваемых исполнениях соответствуют уровню SIL 2.

Функции аварийного открытия и закрытия могут выполняться на выбор через стандартные входы для открытия и закрытия либо через отдельный аварийный вход.



#### РЕДУКТОРЫ GK, GST, GS И GF

Мы также определили показатели безопасности редукторов AUMA GK, GST, GS и GF. Все рассматриваемые редукторы соответствуют уровню SIL 2.

Встраиваемый блок управления AC .2 от компании AUMA в исполнении SIL является современным решением для систем безопасности до уровня SIL 3. Функции безопасности выполняются только через безопасный модуль SIL. В нормальном режиме доступен весь объем функций AC .2.

## ДОПУСК TÜV ДЛЯ СИСТЕМ SIL2/SIL3

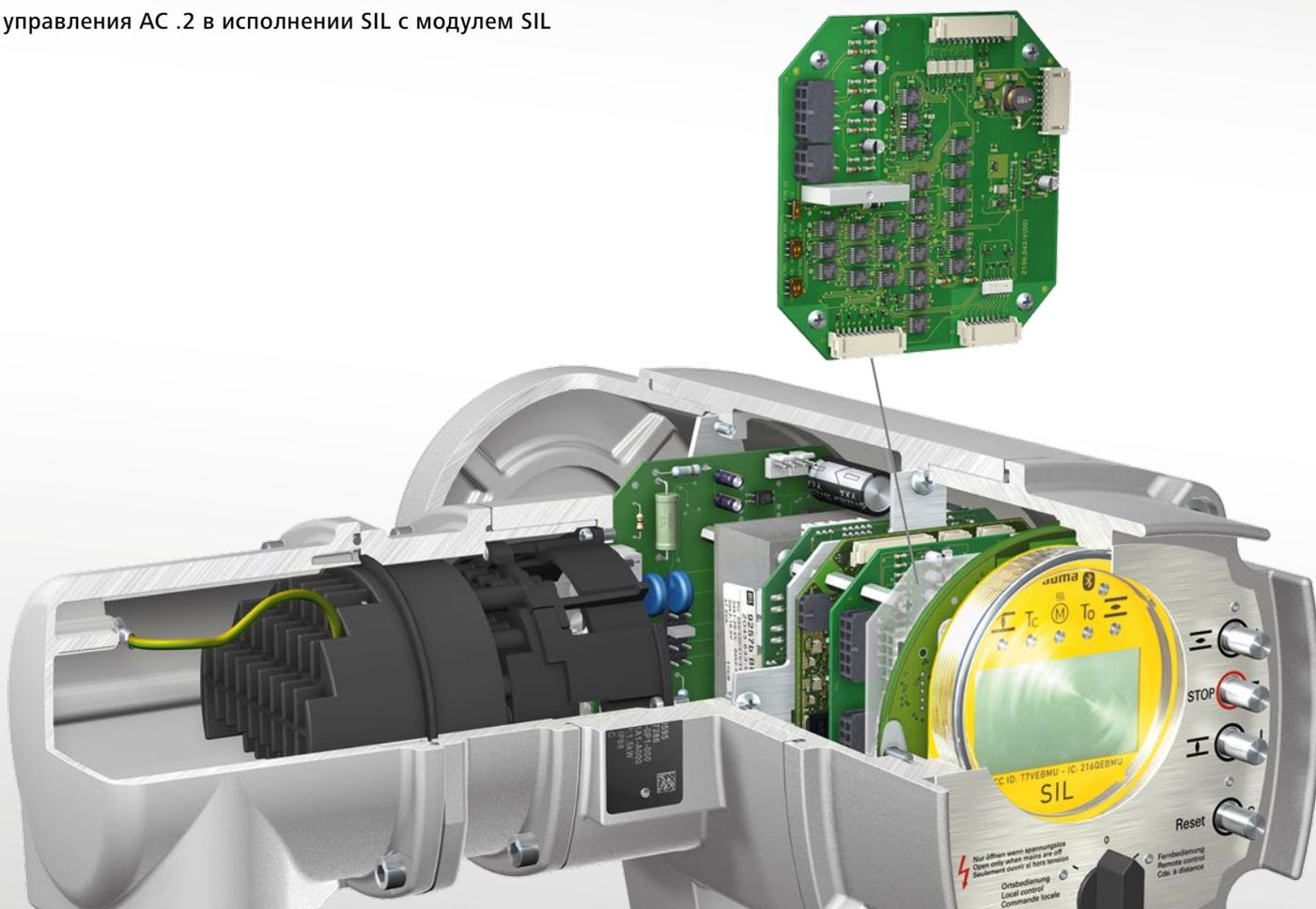
Блок управления AC .2 отличается многообразием функций и большим выбором настроек. Благодаря свободно конфигурируемому параллельному интерфейсу и полевой шине он без проблем интегрируется в современные системы управления. Блок управления AC .2 идеально подходит для сложных режимов управления и регулирования. Дополнительные функции диагностики — сбор рабочих данных и контроль факторов, влияющих на срок службы, — дополнительно увеличивают уровень безопасности и эксплуатационную готовность привода.

Благодаря модулю SIL, разработанному компанией AUMA, эти функции также доступны для систем уровня SIL 2 и SIL 3. Электроприводы SA и SQ с блоком управления AC .2 в исполнении SIL сертифицированы TÜV Nord и допущены к применению в системах с уровнем до SIL 3.



## ВСТРОЕННЫЙ БЛОК УПРАВЛЕНИЯ AC .2 В ИСПОЛНЕНИИ SIL

Блок управления AC .2 в исполнении SIL с модулем SIL



Модуль SIL представляет собой дополнительную плату, которая отвечает за выполнение функций безопасности. Плата устанавливается во встроенные блоки управления АС .2 и АСEx .2.

Если в случае аварии подается запрос на выполнение функции безопасности, стандартная логика блока АС .2 отключается, а функция безопасности выполняется через модуль SIL.

В модуле SIL применяются только сравнительно простые компоненты (транзисторы, резисторы, конденсаторы), отказы которых полностью изучены. По этой причине блок управления АС .2 в исполнении SIL относится к устройствам типа А. Определенные показатели безопасности допускают использование в системах SIL 2, а со схемой резервирования (1oo2) — SIL 3.

Электропривод с блоком управления АС .2 в исполнении SIL сочетает в себе две функции. Во-первых, стандартные функции АС .2 можно использовать в обычном режиме работы. Во-вторых, через встроенный модуль SIL блок отвечает за выполнение функций безопасности.

Функции безопасности всегда более приоритетны по отношению к задачам обычного режима. Таким образом, при подаче команды функции безопасности стандартная логика блока управления шунтируется.

Если привод с блоком АС .2 в исполнении SIL применяется только в качестве системы безопасности, то от управления через стандартную систему на базе ПЛК можно отказаться.



#### Обработка сигнала в стандартной системе с блоком АС .2 в исполнении SIL

Блок АС .2 приводится в действие двумя вышестоящими системами управления (на базе ПЛК): стандартной системой на базе ПЛК и безопасной системой на базе ПЛК, то есть с допуском SIL. Управление работой в обычном режиме осуществляется посредством команд, отправляемых со стандартной системы на базе ПЛК, которые обрабатываются посредством стандартной логики блока АС .2.

В случае аварии нормальный режим работы прерывается, и управление приводом осуществляется через встроенный модуль SIL посредством сигналов безопасной системы на базе ПЛК.

## ВАРИАНТЫ КОНФИГУРАЦИИ

Блок управления AC .2 в исполнении SIL характеризуется разнообразием возможностей конфигурации. На заводе согласно спецификациям клиента настраивается функция безопасности и точка отключения хода. Настройка осуществляется с помощью DIP-переключателей модуля SIL.

### Функции безопасности

С помощью блока управления AC .2 в исполнении SIL могут выполняться следующие функции безопасности:

- > Аварийное открытие и закрытие (Safe ESD, Emergency Shut Down)  
Электропривод перемещается в заданном направлении в положение ОТКРЫТО или ЗАКРЫТО. Для повышения безопасности используется дублированный вход для сигналов.
- > Безопасный останов (Safe STOP)  
В данном случае команда стандартной системы на базе ПЛК на открытие или закрытие выполняется только при наличии разрешающего сигнала модуля SIL.  
При отсутствии разрешающего сигнала открытие или закрытие прекращается или вообще не начинается.
- > Аварийное открытие/закрытие в комбинации с аварийным остановом  
В этом случае функция аварийного открытия/закрытия имеет более высокий приоритет.

Дополнительно возможна безопасная отправка сигнала обратной связи о достижении конечного положения через электропривод.

### Критерии отключения

Как и для обычного режима, условия отключения привода можно настроить и для функций безопасности. Тогда как в обычном режиме критерии отключения обеспечивают защиту арматуры и привода, при поступлении запроса на выполнение функции безопасности обязательное открытие или закрытие арматуры может иметь более высокий приоритет. В этом случае повреждение привода или арматуры практически исключается.

Для функций безопасности предусмотрены следующие критерии отключения:

- > Отключение по положению с защитой от перегрузки  
Блок управления отключает привод сразу после достижения заданного конечного положения в направлении открытия или закрытия. В случае превышения крутящего момента вследствие, например, попадания постороннего предмета на шток арматуры, привод во избежание повреждения арматуры отключится до достижения конечного положения.
- > Отключение по конечному положению  
Электропривод останавливается при достижении конечного положения ОТКРЫТО или ЗАКРЫТО, вне зависимости от крутящего момента.
- > Отключение по крутящему моменту  
Электропривод останавливается только при достижении конечного положения и заданного крутящего момента.
- > Отключение неактивно  
Моментные и концевые выключатели шунтируются, чтобы арматура открывалась и закрывалась в любом случае. Во избежание перегрева двигателя в этом режиме рекомендуется применять блок управления AC .2 в исполнении SIL с функцией термозащиты.

## КОНТРОЛЬ ХОДА ПРИВОДА

С помощью электромеханической системы контроля хода привода и модуля SIL можно осуществлять мониторинг надежности системы. Если привод не выполняет отправленную команду по истечении заданного времени, модуль SIL подает общий сигнал ошибки.

Система контроля хода активна и в обычном режиме.

## БЕЗОПАСНЫЕ ВХОДЫ И ВЫХОДЫ

Модуль SIL снабжен тремя безопасными входами и двумя безопасными выходами:

- > 1 дублированный вход для аварийного открытия/закрытия (можно настроить либо на открытие, либо на закрытие);
- > 1 вход для аварийного останова или отпирания в направлении открытия;
- > 1 вход для аварийного останова или отпирания в направлении закрытия;
- > 1 выход для подачи общего сигнала ошибки SIL;
- > 1 выход для сигнала «Система готова к работе».

## ДИСПЛЕЙ

Данные о состоянии модуля SIL (выполнение функции безопасности, наличие общей ошибки и др.) отображаются соответствующими значками и текстом на дисплее блока управления AC .2.



Для обоснованного определения класса SIL устройств AUMA применяется расчет показателей безопасности. Для этого стандарты МЭК 61508 и 61511 предусматривают две разные методики: оценку аппаратного обеспечения и полную оценку.

#### Оценка аппаратного обеспечения

Компания AUMA провела оценку аппаратного обеспечения выпускаемых устройств. Сюда относятся электроприводы SA и SQ, встроенные блоки управления AM и AC .2 в стандартном исполнении, а также редукторы GS и GF.

#### Полная оценка

Для интегрированного блока управления AC .2 в исполнении SIL, напротив, была проведена полная оценка с привлечением TÜV Nord. При этом учитывались не только случайные, но и систематические сбои во всех важных фазах жизненного цикла продукта от составления спецификации до вывода из эксплуатации.

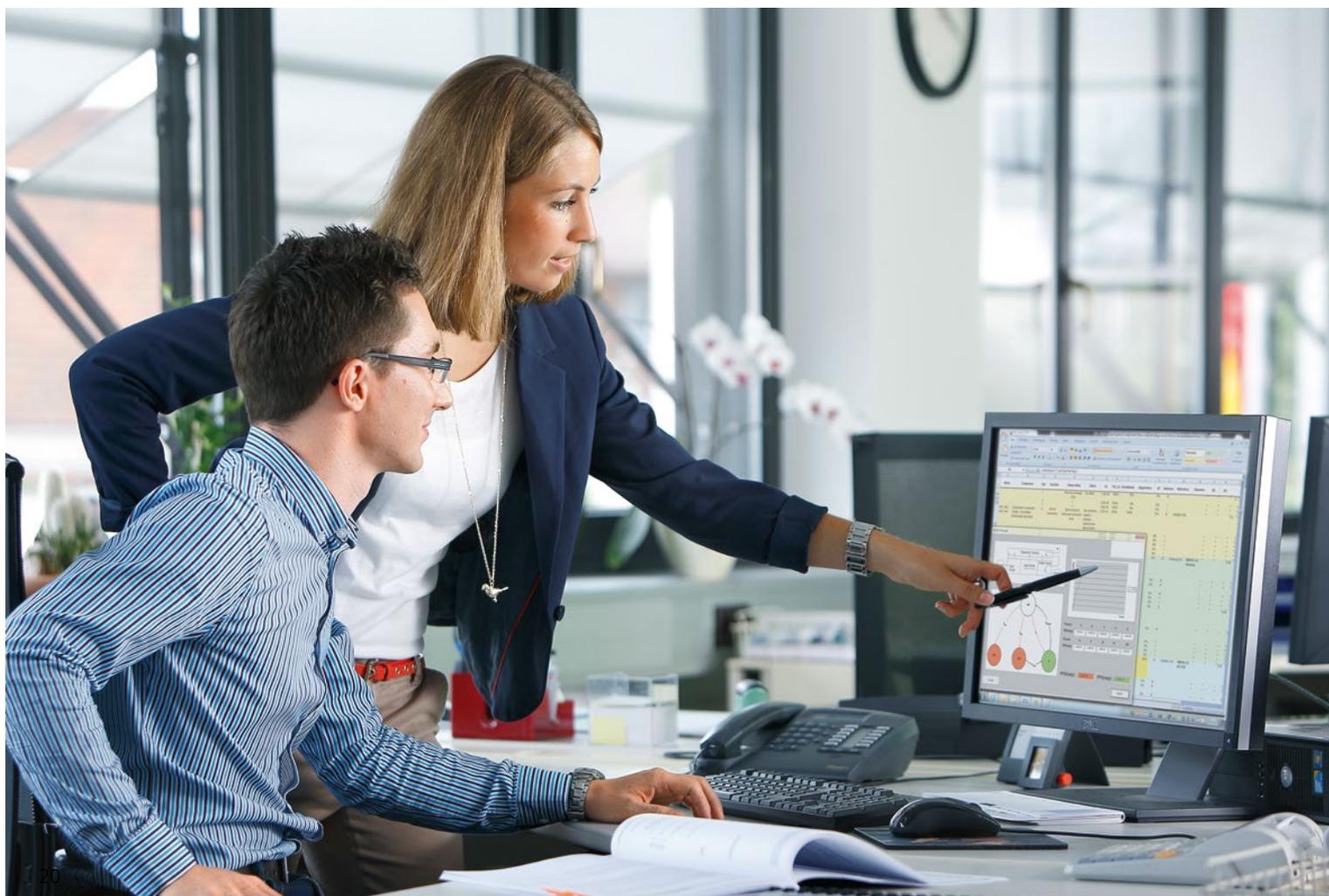
#### ОЦЕНКА АППАРАТНОГО ОБЕСПЕЧЕНИЯ ВЫПУСКАЕМЫХ УСТРОЙСТВ

Для аттестации уже выпускаемых узлов стандарты МЭК 61508 и 61511 предусматривают проверку на основе оценки аппаратного обеспечения устройств.

Показатели безопасности рассчитываются для каждого из отдельных элементов, а затем на их основе присваивается класс SIL.

В качестве основы для оценки аппаратного обеспечения блоков управления применяются данные родового типа, а для приводов — накопленные данные.

## ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ ДЛЯ ПРОДУКЦИИ АУМА



### Данные родового типа

К данным родового типа относится статистически полученная интенсивность отказов отдельных узлов, которая заносится в так называемые «Книги данных для анализа надежности». Примеры: норматив Siemens SN 29500, справочник exida.

Показатели безопасности электронных узлов, применяемых в устройствах AUMA, в частности блоках управления, рассчитываются по данным справочника exida.

### Накопленные данные

У механических узлов количество данных родового типа невелико. Поэтому надежность узлов оценивается по накопленным данным, например по сигналам ошибок во время гарантийного срока и результатам испытаний.

При определении показателей безопасности приводов AUMA были проанализированы данные за последние десять лет.

### FMEDA

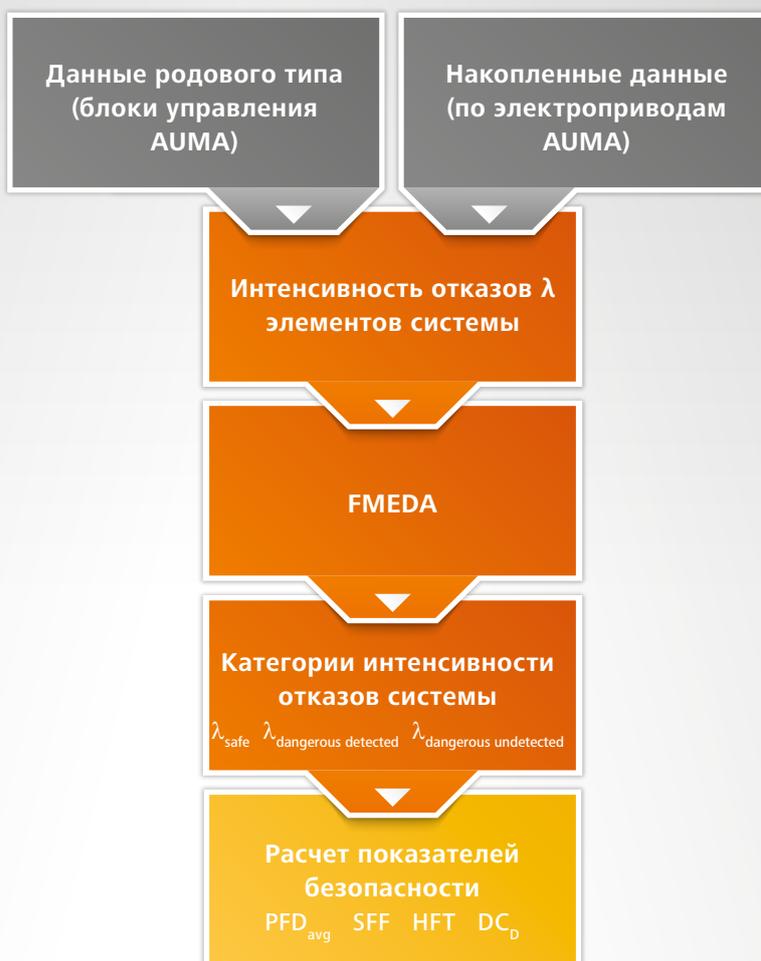
FMEDA (Failure Mode Effects and Diagnostic Analysis, анализ, включающий определение типа сбоя, его воздействия и вероятности определения в ходе диагностики) — это методика расчета показателей безопасности, рекомендуемая в стандарте МЭК 61508.

Анализ осуществляется поэтапно с регистрацией всех данных.

С помощью методики FMEDA проверяются возможные сценарии сбоев, а также оценивается вероятность их наступления. Кроме того, определяется степень опасности возможного сбоя, а также возможность его диагностики и обнаружения.

На основе полученной интенсивности отказов рассчитывается вероятность отказа ( $PFD_{avg}$ ), доля неопасных отказов (SFF) и коэффициент диагностического покрытия неисправностей ( $DC_D$ ).

### Расчет показателей безопасности



Встроенный блок управления AC .2 в исполнении SIL представляет собой новую разработку, поэтому для него была проведена полная оценка согласно стандарту МЭК 61508. Испытывалась общая система, состоящая из электропривода SA .2 и блока управления AC .2 в исполнении SIL. Сертификацию проводила организация TÜV Nord.

**Предмет проверки**

В отличие от проверки аппаратного обеспечения уже выпускаемых продуктов, полная оценка испытание новых разработок дополнительно включает в себя проверку и сертификацию процессов разработки и производства. Такие меры необходимы для минимизации возможных систематических отказов.

Ниже приведена схема, на которой показаны основные задачи полной оценки согласно стандарту МЭК 61508. При этом рассматриваются как систематические сбои устройства, так и случайные отказы.

**Систематические отказы**

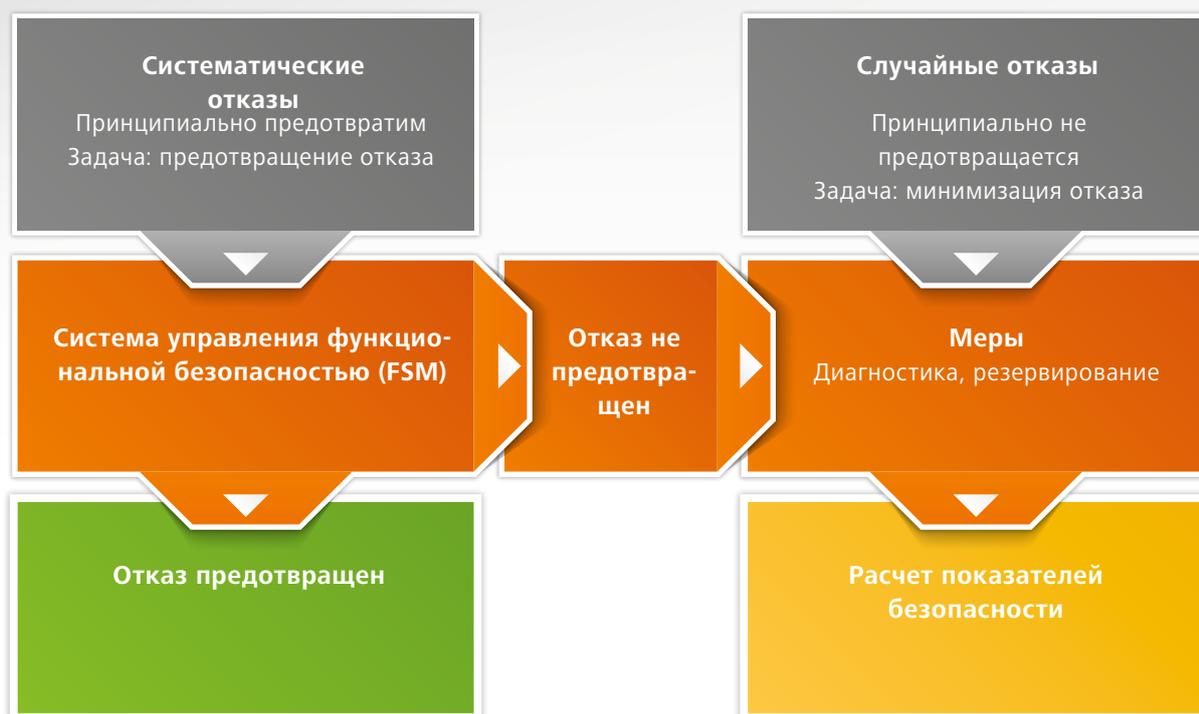
Систематические отказы, как правило, связаны с конструкторскими ошибками и производственным браком, поэтому их достаточно легко предотвратить. С помощью системы управления функциональной безопасностью обнаруживаются источники систематических отказов и принимаются соответствующие меры по их предотвращению.

**Система управления функциональной безопасностью (FSM)**

Система FSM может рассматриваться в качестве расширения системы контроля качества. Благодаря предписанным правилам и нормам большая часть источников систематических ошибок легко устраняется.

## ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ ДЛЯ ПРОДУКЦИИ АУМА

Основной алгоритм полной оценки



**Случайные отказы**

Случайные отказы — это отказы, которые, например, возникают вследствие внешних факторов. Случайные отказы относятся к принципиально неустранимым отказам. По этой причине требуется принимать меры по их минимизации.

Таковыми мерами, например, являются контроль и диагностика системы, а также резервирование.

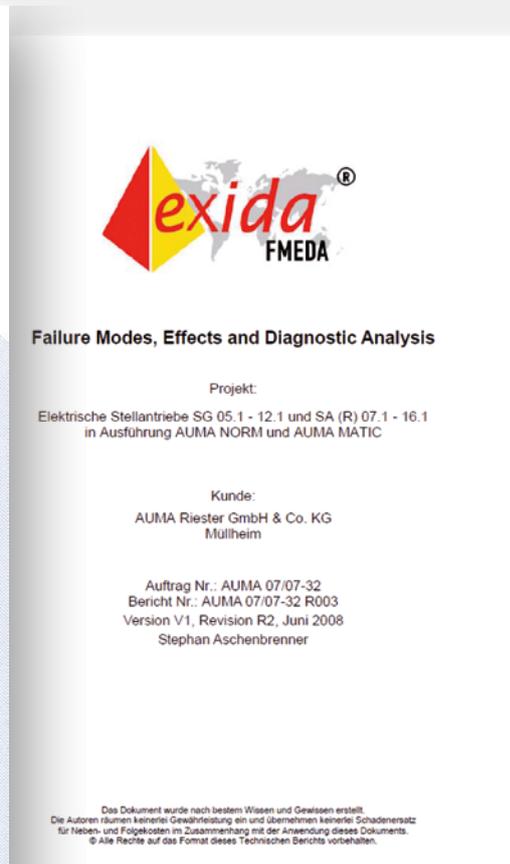
**Расчет показателей безопасности**

Чтобы определить остаточный риск, необходимо количественно рассчитать отказы, которые могут возникнуть после принятия всех мер по обеспечению безопасности. Для этого производится вычисление показателей безопасности и параметров вероятности отказа, которые затем передаются конечному потребителю.

Порядок такой проверки аналогичен оценке аппаратного обеспечения существующей продукции (см. страницу 21).

Сертификаты, отчеты об испытаниях и расчеты показателей безопасности устройств AUMA являются результатом тесного сотрудничества с TÜV Nord и exida. Обе организации являются ведущими мировыми сертифицирующими агентствами в области функциональной безопасности.

В таблице на странице 26 представлены все устройства AUMA, которые сертифицированы и прошли проверку на безопасность.



# ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ НЕКОТОРЫХ УСТРОЙСТВ АУМА

Ниже приводятся показатели безопасности некоторых приводов и блоков управления.

Показатели безопасности зависят от функции безопасности и соответственно от подходов обеспечения работоспособности. Показатели безопасности приводов со встроенным блоком управления зависят от исполнения электрической схемы в связи с применением различных компонентов, интенсивность отказов которых, разумеется, также разная. В общей сложности были рассчитаны показатели безопасности примерно 150 разных версий.

Мы охотно предоставим вам дополнительные данные по запросу.

## МНОГООБОРОТНЫЕ ПРИВОДЫ SA/SAR 07.2 — SA/SAR 16.2 И SAEX/SAREX 07.2 — SAEX/SAREX 16.2 БЕЗ ВСТРОЕННОГО БЛОКА УПРАВЛЕНИЯ



Отчет exida	AUMA 10/03-053 R006 [F1]	AUMA 10/03-053 R006 [F2]
Функция безопасности	Аварийное открытие и закрытие	Аварийное открытие и закрытие с PVST <sup>1</sup>
$\lambda_{safe}$	367 FIT	367 FIT
$\lambda_{DD}$	0 FIT	162 FIT
$\lambda_{DU}$	203 FIT	41 FIT
$DC_D$	0%	80%
SFF	64%	92%
$T_{[proof]} = 1 \text{ год}$	$PFD_{avg} = 1,05 \times 10^{-3}$	$PFD_{avg} = 4,96 \times 10^{-4}$
$T_{[proof]} = 2 \text{ года}$	$PFD_{avg} = 1,92 \times 10^{-3}$	$PFD_{avg} = 6,55 \times 10^{-4}$
$T_{[proof]} = 5 \text{ лет}$	$PFD_{avg} = 4,53 \times 10^{-3}$	$PFD_{avg} = 1,13 \times 10^{-3}$
Класс SIL <sup>2</sup>	SIL 2 (1oo1)/SIL 3 (1oo2) <sup>3</sup>	SIL 2 (1oo1)/SIL 3 (1oo2) <sup>3</sup>

## МНОГООБОРОТНЫЕ ПРИВОДЫ SA/SAR 07.2 — SA/SAR 16.2 С БЛОКОМ УПРАВЛЕНИЯ AC 01.2 В ИСПОЛНЕНИИ SIL

В качестве примера показаны данные многооборотного привода с контакторами в качестве силовой части.



Сертификат TÜV	SEBS-A. 150445/14 V1.0	SEBS-A. 150445/14 V1.0
Функция безопасности	Safe ESD (аварийное открытие и закрытие)	Safe STOP (аварийный останов)
$\lambda_{safe}$	185 FIT	591 FIT
$\lambda_{DD}$	766 FIT	89 FIT
$\lambda_{DU}$	167 FIT	200 FIT
$DC_D$	82%	30%
SFF	85%	77%
$T_{[proof]} = 1 \text{ год}$	$PFD_{avg} = 2,01 \times 10^{-3}$	$PFD_{avg} = 1,69 \times 10^{-3}$
Класс SIL <sup>2</sup>	SIL 2 (1oo1)/SIL 3 (1oo2) <sup>3</sup>	SIL 2 (1oo1)/SIL 3 (1oo2) <sup>3</sup>

1. Тест частичного хода клапана необходимо проводить как минимум 1 раз в месяц.
2. Класс SIL показывает, что расчетные данные находятся в диапазоне соответствующего уровня SIL. Однако это не означает выполнение всех условий МЭК 61508.
3. Обеспечение соответствия уровню SIL 3 возможно за счет резервирования (1oo2).

## УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Параметр	Описание	Параметр	Описание
$\lambda_{safe}$	<b>Лямбда безопасная (англ. Lambda Safe) — количество безопасных отказов на единицу времени.</b> Значение $\lambda$ показывает интенсивность отказов, то есть количество отказов элемента на единицу времени. Интенсивность отказов применяется для расчета вероятности отказа. Параметр FIT (англ. Failure in Time) показывает количество отказов за $10^9$ часов. 1 FIT равен одному отказу на $10^9$ часов или одному отказу на 114 000 лет. Отказ считается безопасным, если в случае его возникновения система не переходит в опасное состояние.	SFF	<b>SFF Safe Failure Fraction — доля неопасных отказов</b> Процентное количество неопасных отказов, т. е. отказов, которые не могут привести к опасному выходу системы из строя или обнаруживаются в ходе диагностики. Чем выше значение этого параметра, тем ниже вероятность опасного отказа системы. Значение 62%, например, означает, что 62 отказа из 100 не оказывают влияния на работоспособность системы.
$\lambda_{DD}$	<b>Лямбда обнаруженных опасных отказов (англ. Lambda Dangerous Detected) — количество обнаруженных опасных отказов на единицу времени</b> Параметр показывает количество обнаруженных в ходе диагностики опасных отказов на $10^9$ часов. Отказ элемента считается опасным, если при его возникновении невозможно выполнить функцию безопасности.	$T_{proof}$	<b>Интервал между контрольными испытаниями</b> Показатели безопасности действительны для установленного периода работы. По окончании этого периода требуется проводить контрольное испытание, чтобы убедиться в работоспособности устройства. Параметр PFD можно улучшить за счет более частых контрольных проверок. Однако их не имеет смысла проводить чаще одного раза в год.
$\lambda_{DU}$	<b>Лямбда необнаруженных опасных отказов (англ. Lambda Dangerous Detected) — количество необнаруженных опасных отказов на единицу времени</b> Параметр показывает количество не обнаруженных в ходе диагностики опасных отказов на $10^9$ часов.	$PFD_{avg}$	<b>Вероятность отказа (функции безопасности) по запросу (англ. Probability of Failure on Demand)</b> Средняя вероятность отказа функции безопасности при запросе на ее выполнение.
$DC_D$	<b>Диагностическое покрытие опасных отказов (англ. Diagnostic Coverage of Dangerous Failures) — коэффициент диагностического покрытия опасных отказов</b> Процент обнаруженных диагностикой опасных отказов $\lambda_{DD}$ из всего количества опасных отказов.	Класс SIL	Определение соответствия уровню полноты безопасности на основе значения $PFD_{avg}$ компонента, при необходимости с учетом ограничений, обусловленных структурой системы. Основанием служит интервал $T_{proof}$ за один год. Необходимо учесть, что уровень SIL всей системы рассчитывается из суммы значений PFD всех элементов (см. также стр. 12).

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

В настоящей брошюре приводятся только начальные сведения по теме функциональной безопасности. Более подробные сведения по данной теме в частности можно найти в следующих источниках:

- > стандарт МЭК 61508, части 1—7;
- > стандарт МЭК 61511, части 1—3;
- > справочник Funktionale Sicherheit, Josef Börcsök;
- > atp edition, выпуск 1-2/2011.

# УРОВЕНЬ ПОЛНОТЫ БЕЗОПАСНОСТИ УСТРОЙСТВ АУМА. ОБЗОР

На все устройства АУМА, которым присвоен класс SIL, можно запросить декларации соответствия и отчеты об испытаниях непосредственно в компании АУМА.

Примеры приведены на странице 24.

Привод/редуктор	Блок управления	Класс SIL	Функция безопасности
SA/SAR 07.2 — 16.2 SAEx/SAREx 07.2 — 16.2	без блока управления	SIL 2 <sup>1</sup>	Аварийное открытие и закрытие (ESD) Аварийное состояние покоя/останова Контрольный сигнал конечного положения
	AM 01.1/02.1 AMEXC 01.1 AMEXB 01.1	SIL 2 <sup>1,3</sup>	Аварийное открытие и закрытие (ESD) Аварийное состояние покоя/останова Контрольный сигнал конечного положения
	AC 01.2 в исполнении SIL ACEXC 01.2 в исполнении SIL	SIL 2 <sup>1</sup> SIL 3 <sup>2</sup>	Аварийное открытие и закрытие (ESD) Аварийный ОСТАНОВ Контрольный сигнал конечного положения
	AC 01.2 (стандартное исполнение) ACEXC 01.2 (стандартное исполнение)	SIL 1 <sup>1)3)</sup> SIL 2 <sup>2)3)</sup>	Аварийное открытие и закрытие (ESD) Аварийное состояние покоя/останова Контрольный сигнал конечного положения
SQ/SQR 05.2 — 14.2 SQEx/SQREx 05.2 — 14.2	без блока управления	SIL 2 <sup>1</sup>	Аварийное открытие и закрытие (ESD)
	AM 01.1/02.1 AMEXC 01.1	SIL 2 <sup>1,3</sup>	Аварийное открытие и закрытие (ESD) Аварийное состояние покоя/останова
	AC 01.2 в исполнении SIL ACEXC 01.2 в исполнении SIL	SIL 2 <sup>1</sup> SIL 3 <sup>2</sup>	Аварийное открытие и закрытие (ESD) Аварийный ОСТАНОВ
	AC 01.2 (стандартное исполнение) ACEXC 01.2 (стандартное исполнение)	SIL 1 <sup>1)3)</sup> SIL 2 <sup>2)3)</sup>	Аварийное открытие и закрытие (ESD) Аварийное состояние покоя/останова
GK 10.2 — 25.2	—	SIL 2 <sup>1</sup>	—
GST 10.1 — 40.1	—	SIL 2 <sup>1</sup>	—
GS 50.3 — 250.3, GS 315 — 500	—	SIL 2 <sup>1</sup>	—
GF 50.3 — 250.3	—	SIL 2 <sup>1</sup>	—

1 Одноканальная система, 1oo1 («один из одного»)

2 Система с резервированием, 1oo2 («один из двух»)

3 В зависимости от электрической схемы и функции безопасности

## **D**

DIN EN 61508 6  
DIN EN 61511 6

## **E**

exida 21, 23

## **F**

FMEDA 21

## **H**

HFT 11

## **M**

MTBF 11

## **P**

PVST 13

## **S**

SFF 11, 25  
SIL 5, 10

## **A**

Анализ рисков 7

## **B**

Вероятность отказа 10, 25  
Вероятность сбоя в час 10  
Вероятность сбоя при запросе 10, 25  
Встроенный блок управления 15, 26

## **G**

График рисков 7

## **D**

Данные родового типа 21  
Диагностическое покрытие 25  
Доля безопасных сбоев 11  
Доля неопасных отказов 11, 25

## **Z**

Значение PFD 10, 25  
Значение PFH 10  
Значения лямбда 25

## **I**

Интенсивность отказов 11, 25  
Интервал между контрольными испытаниями 25

## **K**

Класс SIL  
Продукция AUMA 14, 15, 25, 26  
Улучшение 13  
Контрольное испытание 13, 25  
Коэффициент диагностического покрытия неисправностей 25

## **M**

Многооборотные приводы 15, 26  
Модуль SIL 17, 18  
МЭК 61508 4, 6  
МЭК 61511 4, 6

## **H**

Накопленные данные 21  
Неполнооборотные приводы 15, 26

## **O**

Общее значение PFD 12  
Отказоустойчивость оборудования 11  
Оценка техники безопасности 7  
Ошибка  
Систематический 22  
Случайный 23

## **P**

Повторное испытание 13, 25  
Показатели безопасности  
Определения 10  
Оценка 21, 22, 23  
Продукция AUMA 24, 26

## **P**

Редукторы 15, 26  
Режим высокой интенсивности запросов 10  
Режим непрерывных запросов 10  
Режим низкой интенсивности отказов 10  
Режимы работы 10  
Резервирование 13

## **C**

Система безопасности 6  
Систематические отказы 22  
Случайные отказы 23  
Средний период работы между отказами 11  
Средняя вероятность опасного сбоя при запросе 10, 25  
Средняя вероятность отказа 10, 25

## **T**

Тест частичного хода клапана 13  
Тип устройства 11

## **Y**

Уровень полноты безопасности 5  
Устройство типа А 11  
Устройство типа В 11

## **Ф**

Функциональная безопасность  
Нормативы 6  
Определение 4  
Функция безопасности 4, 8, 18

**AUMA Riester GmbH & Co. KG**

Aumastr. 1  
79379 Muellheim  
Germany  
Tel +49 7631 809-0  
Fax +49 7631 809-1250  
info@auma.com

**ООО «ПРИВОДЫ АУМА»**

Россия  
141402 Московская область,  
г. Химки, квартал Клязьма, 1Г  
тел.: +7 495 755 60 01  
факс: +7 495 755 60 03  
aumarussia@auma.ru

Дочерние предприятия и представительства AUMA  
есть в 70 странах. Подробную контактную  
информацию  
вы найдете на сайте нашей компании.  
**www.auma.com**