

SIL3
Pl e

Руководство по функциональной безопасности Реле безопасности серии АСТРА



ГОСТ Р МЭК 61508-2012

Содержание

Реле безопасности АСТРА		
1	Сфера действия	4
2	Проектирование	6
3	Показатели функциональной безопасности	6
4	Контрольные проверки и диагностика	8
5	Ввод в эксплуатацию	8
	Лист регистрации изменений	9

Данное руководство по функциональной безопасности разработано в соответствии с ГОСТ Р МЭК 61508-2012 для удовлетворения требований по функциональной безопасности.

В настоящем руководстве по функциональной безопасности приведены следующие сокращения:

- **Функциональная безопасность (Functional Safety)** - часть общей системы безопасности, обусловленная применением управляемого оборудования и системы управления и зависящая от правильности функционирования электрических/электронных/программируемых электронных систем, связанных с безопасностью, и других средств по снижению риска.
- **Отказобезопасность** - свойства изделия, ориентированные на сохранение безопасности в случае отказа.
- **ДБО (SFF - safety fail fraction)** - Доля Безопасных Отказов. Свойство элемента, связанного с безопасностью, определяемое отношением суммы средних частот безопасных отказов и опасных обнаруженных отказов к сумме средних частот безопасных и опасных отказов.

λ_{du} - интенсивность необнаруженных опасных отказов.

λ_{dd} - интенсивность обнаруженных опасных отказов.

ОАС (HFT - hardware fault tolerance) - Отказоустойчивость Аппаратных Средств.

ОАС = X означает, что X + 1 является минимальным числом отказов, которые могут привести к потере функции безопасности.

- **Средняя вероятность опасного отказа по запросу** (probability of dangerous failure on demand, PFDavg) - средняя неготовность Э/Э/ПЭС системы, связанной с безопасностью, обеспечить безопасность, т.е. выполнить указанную функцию безопасности, когда происходит запрос.
- **Средняя частота опасного отказа в час** (average frequency of a dangerous failure per hour, PFH) - средняя частота опасного отказа Э/Э/ПЭС системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.
- β - эффективность теста по выявлению опасных отказов.
- **Полнота безопасности (safety integrity)** - вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного периода времени.
- **УПБ (SIL - safety integrity level)** - Уровень полноты безопасности: дискретный уровень (принимаящий одно из четырёх значений), определяющий требования к полноте безопасности для функции безопасности, который ставится в соответствии с Э/Э/ПЭС системам, связанным с безопасностью.
- **PTI** — это интервал проверочных испытаний, обычно в месяцах, в течение которого будут обнаружены неисправности, НЕ обнаруженные с помощью онлайн-диагностики (при условии, что покрытие проверочных испытаний составляет 100%).

MTTFd - Среднее время до опасного отказа. Стандартом ISO 13849-1 MTTFd определяется как ожидаемое среднее время до опасного отказа.

1. Сфера действия

Типы реле безопасности

Настоящее руководство по функциональной безопасности распространяется на реле безопасности серии АСТРА производства Ступинского Электротехнического Завода. Список моделей перечислен в таблице 1.1

Таблица 1.1

№	Наименование	Артикул	Назначение	Режим сброса	Выходная группа
1	АСТРА-АВ-3НО1НЗ-АР-24U	63031101	Для подключения кнопок аварийного останова, тросовых аварийных выключателей, концевых выключателей калиток защитных ограждений	Автоматический	3xНО, 1xНЗ
2	АСТРА-АВ-2НО2НЗ-АР-24U	63022101		Автоматический	2xНО, 2xНЗ
3	АСТРА-АВ-3НО1НЗ-РМ-24U	63031102		Ручной	3xНО, 1xНЗ
4	АСТРА-АВ-2НО2НО-РМ-24U	63022102		Ручной	2xНО, 2xНЗ
5	АСТРА-АВ-3НО1НЗ-АР-230А	63031103		Автоматический	3xНО, 1xНЗ
6	АСТРА-АВ-2НО2НЗ-АР-230А	63022103		Автоматический	2xНО, 2xНЗ
7	АСТРА-АВ-2НО2НОТ-АР-24D	63040104		Автоматический	2xНО, 2xНО с задержкой
8	АСТРА-АВ-2НО2НОТ-РМ-24D	63040105		Ручной	2xНО, 2xНО с задержкой
9	АСТРА-ДБ-3НО1НЗ-П-24D	63031201	Для подключения датчиков безопасности: световые шторки, бесконтактные датчики ограждений, лазерные сканеры		3xНО, 1xНЗ
10	АСТРА-ДБ-2НО2НЗ-П-24D	63022201			2xНО, 2xНЗ
11	АСТРА-ДБ-3НО1НЗ-Н-24D	63031202			3xНО, 1xНЗ
12	АСТРА-ДБ-2НО2НЗ-Н-24D	63022202			2xНО, 2xНЗ
13	АСТРА-ДБ-3НО1НЗ-ПН-24D	63031203			3xНО, 1xНЗ
14	АСТРА-ДБ-2НО2НЗ-ПН-24D	63022203			2xНО, 2xНЗ
15	АСТРА-КДР-3НО1НЗ-24U	63031301	Пульты оператора с обязательным контролем двух рук		3xНО, 1xНЗ
16	АСТРА-КДР-2НО2НЗ-24U	63022301			2xНО, 2xНЗ
17	АСТРА-МБ-3НО1НЗ-АР-24U	63031401	Для подключения матов безопасности в 2-проводном и 4-проводном исполнении	Автоматический	3xНО, 1xНЗ
18	АСТРА-МБ-2НО2НЗ-АР-24U	63022401		Автоматический	2xНО, 2xНЗ
19	АСТРА-МБ-3НО1НЗ-РМ-24U	63031402		Ручной	3xНО, 1xНЗ
20	АСТРА-МБ-2НО2НЗ-РМ-24U	63022402		Ручной	2xНО, 2xНЗ
21	АСТРА-МБ-3НО1НЗ-О-24U	63031403			3xНО, 1xНЗ
22	АСТРА-МБ-2НО2НЗ-О-24U	63022403			2xНО, 2xНЗ
23	АСТРА-МБ-3НО1НЗ-О-230А	63031404			3xНО, 1xНЗ
24	АСТРА-МБ-2НО2НЗ-О-230А	63022404			2xНО, 2xНЗ
25	АСТРА-МР-4НО2НЗ-24D	63042501	Модули расширения контактной группы	-	4xНО, 2xНЗ
26	АСТРА-МР-8НО4НЗ-24D	63084502			2xНО, 2xНЗ
27	АСТРА-ПА3-1НО-24D	63010001	Модули сопряжения сигналов датчиков систем ПА3	-	1xНО
28	АСТРА-ПА3-2НО-24D	63020002			2xНО
29	АСТРА-ПА3-1НО-М-24D	63010003			1xНО
30	АСТРА-ПА3-1НО1НЗ-24D	63011004			1xНО, 1xНЗ
31	АСТРА-ПА3-1НО1НЗ-СПР-24D	63011005			1xНО, 1xНЗ
32	АСТРА-РС-2ПК-РПМ-2-24D	63022801	Безопасные реле сопряжения		2xНО/НЗ
33	АСТРА-РС-2НО2НЗ-РПМ-5-24D	63022802			2xНО, 2xНЗ
34	АСТРА-РС-3НО1НЗ-РПМ-5-24D	63031802			3xНО, 1xНЗ
35	АСТРА-РС-1НО1НЗ-М-24D	63011802			1xНО, 1xНЗ

Область применения

Реле безопасности серии АСТРА:

- АСТРА-АВ...;- реле безопасности
- АСТРА-ДБ...;- реле безопасности
- АСТРА-КДР...;- реле безопасности
- АСТРА-МБ...;- реле безопасности
- АСТРА-МР...;- реле безопасности
- АСТРА-ПАЗ...; реле безопасности для сопряжения сигналов датчиков безопасности систем ПАЗ
- АСТРА-РС... - безопасные реле сопряжения

Описание изделий

Реле безопасности в основном применяются в системах безопасности персонала для автоматизации производств, с такими устройствами безопасности как кнопка аварийной остановки, концевые датчики дверей защитных ограждений, световые завесы безопасности и т. п. Реле безопасности также применяются в системах ПАЗ для развязки дискретных сигналов датчиков систем безопасности.

Реле безопасности позволяют гарантированно остановить оборудование или отключить электропитание в случае возникновения неисправности или опасности нанесения вреда здоровью персонала.

Реле безопасности серии АСТРА предназначены для использования в системах аварийного останова, связанных с безопасностью, где безопасным состоянием является обесточенное состояние.

Реле безопасности серии АСТРА-ПАЗ используют отказоустойчивую технологию и архитектуру с тройным резервированием.

Изделия могут применяться в связанных с безопасностью системах, в соответствии с ГОСТ Р МЭК 61508, в режимах работы lowdemandmode (с низкой частотой запросов) или highdemandmode (с высокой частотой запросов): УПБ (SIL) в одноканальной архитектуре.

Уровень полноты безопасности SIL

В многоканальной архитектуре уровень полноты безопасности может достичь уровня УПБЗ (**SIL 3**).

Соответствие SIL по ГОСТ Р МЭК 61508 оценивается независимой организацией с выдачей сертификата соответствия в добровольной системе сертификации ГОСТ Р. Сертификат действителен для всех устройств, выпущенных в обращение до истечения срока действия этого сертификата, в течение всего срока службы устройства.

2. Проектирование

Функция безопасности

Функция безопасности заключается в немедленном отключении защитного выхода в соответствии с требованиями безопасности.

Безопасное состояние Безопасное состояние определяется тем, что выходной защитный контакт находится в разомкнутом состоянии.

Время отклика

Время замыкания контактов: (TRC) ≤ 300 мс

Время размыкания контактов: (TRR) ≤ 30 мс

Время реакции на ошибку

Время реакции на ошибку ≤ 30 мс

3. Показатели функциональной безопасности

Показатели в соответствии с ГОСТ Р МЭК 61508:

Модели: АСТРА-АВ...; АСТРА-ДБ...; АСТРА-КДР...; АСТРА-МБ...; АСТРА-МР...;

Режим работы	С низкой частотой запросов	
Уровень полноты безопасности оборудования	SIL3	
Стойкость к систематическим отказам	CCO3	
HFT	1	
Тип	A	
SFF	≥ 90%	
PFD _{avg}	≤ 10 ⁻⁴ (при PTI = 20 лет)	
PFH	≤ 10 ⁻⁸ (при PTI = 20 лет)	
PTI	≥ 20 лет	
MRT	0 ч	
MTTR	0 ч	
Категория	Cat.4	
PL	PLe	
MTTFd	≥ 30 лет (Высокий)	
DCavg	≥ 99% (Высокий)	
CCF (отказ по общей причине)	> 65 scores	

Модели: АСТРА-РС...; АСТРА-ПАЗ... в 1-канальной архитектуре (используется один канал в применении 1oo1 с HFT=0)

Режим работы	С низкой частотой запросов	
Полнота безопасности аппаратных средств	SIL2	
Стойкость к систематическим отказам	CCO1	
Тип устройства/Подсистема (МЭК 61508)	A	
ДБО (SFF)	1oo1 (HFT=0)	97% (> 60%, соотв. УПБ 2 (SIL 2))
	1oo3 (HFT=2)	35% (< 60%, соотв. УПБ 2 (SIL 2))
Средняя вероятность опасного отказа по запросу (PFD _{AVG})	1.04E-03 (при PTI = 10 лет, 10% от УПБ 2 (SIL 2))	
β = βD (для 1oo3)	2.5%	
MRT = MTTR	0 Часов	

Модели: АСТРА-РС...; АСТРА-ПА3... в архитектуре с резервированием (дублированный канал в применении 1oo2 с HFT=1)

Режим работы	С низкой частотой запросов
Полнота безопасности аппаратных средств	SIL3
Стойкость к систематическим отказам	CCO1
Тип устройства/Подсистема (МЭК 61508)	A
Средняя вероятность опасного отказа по запросу (PFD_{AVG})	1.04E-03 (при РТИ = 10 лет, 15% от УПБ 3 (SIL 3))
$\beta = \beta_D$ (для резервированных частей)	2.5%
MRT = MTTR	0 часов

Параметры, указанные в таблице выше, рассчитаны без учета вероятности отказа источника питания

Модели реле безопасности	λ_s	λ_d	λ_{dd}	λ_{du}
Модели с цепью ручного режима сброса	775 FIT	600 FIT	594 FIT	6 FIT
Все остальные модели	769 FIT	600 FIT	594 FIT	6 FIT

Доля Безопасных Отказов ДБО (SFF):

ДБО(SFF)>99%

Средняя вероятность опасного отказа по запросу (PFD_{AVG})

Интервал T_{proof}	1 год	2 года	3 года	10 лет	20 лет
Средняя вероятность опасного отказа по запросу (PFD_{AVG})	1.33E-06	2.66E-06	3.99E-06	1.33E-05	2.69E-05

Средняя частота опасного отказа в час (PHF)

Интервал T_{proof}	1 год	2 года	3 года	10 лет	20 лет
Средняя частота опасного отказа в час (PHF)	3.03E-10	3.03E-10	3.04E-10	3.06E-10	3.09E-10

Среднее время до опасного отказа (MTTFd)

MTTFd≈188 лет

Параметры безопасности указанные в таблице выше рассчитаны на основе следующих допущений:

- Частота отказов каждого компонента основана на базе данных Siemens SN29500
- Частота отказов компонентов постоянна в течение всего срока службы устройства
- Вышеуказанные рассчитанные параметры основаны на макс. температуре окружающей среды 60°C плюс повышение температуры из-за аппаратных компонентов.
- Равное распределение используется для соотношения видов отказов каждого

компонента.

- Вышеуказанные рассчитанные параметры не учитывают интенсивность отказов внешних устройства, например датчики, кабели и т. д.
- Виды отказов можно определить как

Виды отказов	Категория
Отказ не оказывает воздействие на функцию безопасности и нормальный режим работы	Невливающий отказ
Отказ приводит к тому, что выход находится в обесточенном состоянии	Безопасный отказ, λ_s
Отказ приводит к тому, что выход находится под напряжением	Опасный отказ, λ_d

4. Контрольные проверки и диагностика

Процедура контрольной проверки

Согласно ГОСТ Р МЭК 61508-2 должны проводиться периодические контрольные проверки для выявления потенциально опасных отказов, которые иначе не обнаруживаются при диагностических проверках.

Функциональность подсистемы необходимо периодически проверять в зависимости от применяемого PFD_{AVG} в соответствии с данными, представленными в данном руководстве.

Ответственность за определение типа контрольного испытания и интервала времени лежит на операторе. Рекомендуется выполнять это не реже одного раза в 3 года для приложений SIL3.

Контрольные проверки и испытания должны проводится только квалифицированным персоналом.

Необходимое вспомогательное оборудование:

Цифровой мультиметр с точностью выше 0,1 %.

Процедура:

Контрольная проверка реле безопасности служит для выявления неисправности контактной группы реле: цепи выходной группы контактов должны менять свое состояние (замкнуто/разомкнуто) при снятии и подаче напряжения питания при замкнутых цепях активации и сброса.

5. Ввод в эксплуатацию



При вводе изделий в эксплуатацию необходимо выполнять условия, содержащиеся в техническом паспорте на конкретное изделие. Подключение реле безопасности осуществляется по схеме, указанной техническом паспорте.

Лист регистрации изменений

[illegible]



О Компании

ООО «Ступинский электротехнический завод» - крупное предприятие с полным циклом производства электротехнической продукции, расположенное в г. Ступино. ООО «Ступинский электротехнический завод» начал свою работу в 2017 году. Сегодня это российский завод, выпускающий электротехническую продукцию под брендом STEZ®.

Производственные линии СТЭЗ построены на основе самых современных технологий с полным соответствием всем отраслевым стандартам в области производства электротехники, в том числе европейским стандартам безопасности.

Производство располагает самыми современными автоматизированным оборудованием, что означает высокую производительность и гарантию стабильного качества выпускаемой продукции.

Все изделия, производимые на заводе, проходят российскую сертификацию и соответствуют требованиям ТР ТС. АвалонЭлектроТех – российское научно-производственное объединение с 20-летней экспертизой в области электротехники и промышленной автоматизации, лидер на рынках РФ и ЕАЭС.

Системы
видеонаблюдения



Барьеры
искрозащиты



Реле
безопасности



Системы
электропитания



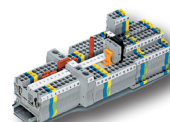
Сетевые
технологии



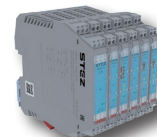
Промышленные
разъемы и кабели



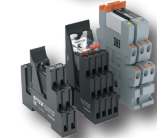
Электротехнические
клеммы



Интерфейсные
модули



Интерфейсные
реле



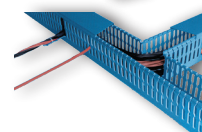
УЗИП



Автоматические
выключатели



Электромонтажные
принадлежности



ООО «НПО «АвалонЭлектроТех»
121205, Москва, территория Инновационного центра
«Сколково», ул. Алессандро Вольта, д1, стр. 1
Тел.: +7 (495) 933-85-48

СТУПИНСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ЗАВОД
ООО «СТЭЗ»
142821, Московская область, Г.О. Ступино,
Д. Шматово, ул. Индустриальная, ВЛД.6

