# Критерии выбора компонентов с уровнем SIL 3 для РСУ и систем ПАЗ в соответствии со стандартами МЭК

## Часть 1

*Глизенте Ландрини*

**В настоящей статье описаны критерии выбора компонентов для использования в распределённых системах управления (РСУ) и различных системах обеспечения безопасности с уровнями SIL 2 и SIL 3, рекомендованные в стандартах МЭК 61508 и 61511, а также даны практические примеры применения этих критериев.**

Прежде чем читатель начнёт знакомиться с данной статьёй, необходимо заметить, что она является второй в цикле статей, которые посвящены функциональной безопасности систем, связанных с обеспечением безопасности производственных технологических процессов, и тематически продолжает статью, опубликованную двумя номерами ранее [1]. Предыдущая статья содержит определения основных показателей безопасности, методики их расчёта и применения на этапе технического обслуживания, необходимые комментарии и примеры, поэтому новая публикация к этим вопросам уже не возвращается.

### Архитектуры систем

Архитектуры систем, связанных с обеспечением безопасности, и используемые в них компоненты весьма разнообразны. Во многих случаях для повышения надёжности и отказоустойчивости используют системные архитектуры с резервированием (рис. 1). Кратко рассмотрим основные наиболее широко применяемые варианты таких архитектур.

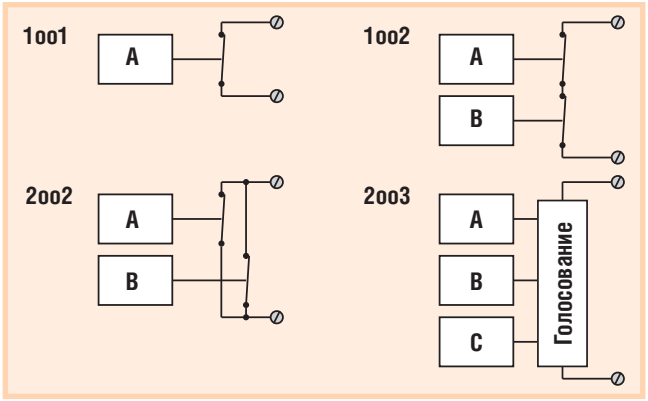


**Рис. 1. Примеры архитектур систем**

Эффект резервирования

*Таблица 1*

| Архитектура | Интенсивность безопасных отказов за год $\lambda_S$/год | MTBF$_S$ (лет) | Интенсивность опасных отказов за год $\lambda_D$/год | MTBF$_D$ (лет) |
|---|---|---|---|---|
| 1oo1 | 0,0400 | 25 | 0,0200 | 50 |
| 1oo2 | 0,0800 | 12,5 | 0,0004 | 2500 |
| 2oo2 | 0,0016 | 625 | 0,0400 | 25 |
| 2oo3 | 0,0048 | 208 | 0,0012 | 833 |

Предположим, что устройство с архитектурой 1oo1 имеет интенсивность (вероятность) безопасных отказов 0,04/год и интенсивность опасных отказов 0,02/год [1]. Для этих условий в табл. 1 сравниваются значения средней вероятности отказа на запрос выполнения функции безопасности PFDavg (Average Probability of Failure on Demand) и среднего времени наработки на отказ MTBF, соответствующие системам с различной архитектурой. Результаты сравнения показывают сильно отличающийся эффект от применения разных видов резервирования.

### Архитектура 1oo1 (один из одного)

Для исходной симплексной системы (без резервирования) с архитектурой 1oo1 (один из одного) безопасным отказом является размыкание релейного контакта и отключение системы, что вызывает ложный останов. Принятая интенсивность отказов в данном случае равна 0,04/год; это означает, что в заданный период времени (1 год) существует вероятность ложного отключения системы, равная 4%. Иными словами, это может трактоваться так, что в течение года 4 системы из 100 либо 1 система из 25 вызовут ложный останов контролируемого технологического процесса или что среднее время между ложными остановами (MTBF$_S$) для данной системы равно 25 годам.

Примером опасного отказа может быть случай, когда контакты реле привариваются и не могут разомкнуться в нужный момент. Принятая интенсивность такого отказа равна 0,02/год; это означает, что вероятность отказа системы на выполнение запроса в заданный период времени (1 год) равна 2% или

- в течение года 2 системы из 100 не выполнят запрос,
- в течение года 1 система из 50 не выполнит запрос,
- $MTBF_D$ (для опасных отказов) равно 50 (1/0,02) годам.

## Архитектура 1oo2 (один из двух)

Система с дублированной архитектурой 1oo2 имеет выходные контакты, соединённые последовательно и замкнутые при включённом питании. Системе достаточно одного канала, чтобы обеспечить аварийное отключение. Если любой из каналов может остановить систему, а каналов в системе в два раза больше, чем в симплексной системе (1oo1), то и ложных отключений может быть в два раза больше. Поэтому и интенсивность таких событий увеличивается с 0,04 до 0,08/год. Это означает, что 8 систем из 100 дадут ложное выключение в течение года или что $MTBF_S$ составляет 12,5 лет.

Опасный отказ для такой системы наступает, когда в обоих каналах одновременно произошли опасные отказы, так как, если только один выходной контакт «залип», второй ещё может отключить систему. Интенсивность одновременных отказов составляет 0,02 × 0,02 = 0,0004/год. Это означает, что за год 4 системы из 10 000 или 1 система из 2500 не выполнят запрос, или что вероятность отказа системы за 2500 лет равна 1, или что $MTBF_D$ равно 2500 годам.

Другими словами, системы с архитектурой 1oo2 отличаются высокой безопасностью (вероятность опасного отказа системы крайне мала), однако они имеют в два раза большую вероятность ложных срабатываний, что нежелательно с точки зрения потерь продукции, связанных с простоем.

## Архитектура 2oo2 (два из двух)

Система с дублированной архитектурой 2oo2 имеет выходные контакты, соединённые параллельно. В данном случае оба канала должны быть обесточены, чтобы остановить процесс. Отказ в работе такой системы наступает, если происходит опасный отказ в одном из каналов. Поскольку система имеет в два раза больше компонентов (каналов), чем симплексная система (1oo1), количество опасных отказов в ней может быть в два раза большим. Поэтому принятая для симплексной системы интенсивность опасных отказов 0,02/год здесь увеличивается в два раза до 0,04/год, то есть за год 4 системы из 100 или одна из 25 не выполнят запрос, а $MTBF_D$ = 25 годам.

Ложное срабатывание в данной системе происходит, когда в обоих каналах одновременно случается безопасный отказ. Интенсивность таких одновременных отказов составляет 0,04 × 0,04 = 0,0016/год. Это означает, что за год 16 систем из 10 000 дадут ложное срабатывание, или 1 система допустит ложное срабатывание в 625 лет, или $MTBF_S$ = 1/0,0016 = 625 лет.

Таким образом, система с архитектурой 2oo2 защищает от ложных срабатываний (вероятность безопасного отказа очень мала), однако по части опасных отказов она менее безопасна, чем даже нерезервированная система с архитектурой 1oo1, что нежелательно с точки зрения обеспечения общей безопасности. Это не означает, что система 2oo2 «плохая» или что она не должна использоваться. Если соответствующее значение PFDavg удовлетворяет нас с позиций обеспечения требуемого уровня безопасности, то такая архитектура приемлема.

## Архитектура с тройным модульным резервированием 1oo3 (один из трёх)

Системы с тройным модульным резервированием (Triple Modular Redundancy – TMR) были широко распространены в середине 80-х годов прошлого века, поскольку тогда компьютерные системы имели ограниченный уровень диагностики. Например, если в системе были только два сигнала и они не совпадали, то не всегда можно было определить, какой из них правильный. Добавление третьего канала решало эту проблему.

Тройное модульное резервирование используется там, где необходимо обеспечить функциональную безопасность в течение длительного периода без остановок оборудования для обслуживания (5-10 лет). TMR также применяется, когда надо обеспечить уровень безопасности SIL 3, а доступны только устройства с уровнем SIL 1.

## Архитектуры 2oo3 (два из трёх) и 1oo2D (один из двух с диагностикой)

Система с архитектурой 2oo3 использует голосование. Решение в ней принимается на основе результатов голосования два из трёх. Что сначала удивляет людей, так это то, что система 2oo3 имеет более высокую интенсивность ложных срабатываний, чем система 2oo2, и большую вероятность отказов, чем система 1oo2. Однако архитектуры 1oo2 и 2oo2 неудовлетворительны с точки зрения опасных отказов и ложных срабатываний, в то время как системы с архитектурой 2oo3 имеют хорошие показатели по отказам обоих видов (безопасным и опасным).

Благодаря совершенствованию аппаратной части и программного обеспечения теперь отказы в компьютерной системе с двойным резервированием могут диагностироваться достаточно хорошо, что позволяет определить, какой из двух каналов исправен в случае, если между ними возникает разногласие. В промышленности эту новую двойную архитектуру систем называют 1oo2D. Такие системы сертифицированы независимыми агентствами (например, TÜV и FM) на том же уровне безопасности, что и TMR-системы.

К сожалению, сертификация безопасности не касается показателей ложного срабатывания. Это создаёт условия для того, чтобы производители TMR-систем критиковали системы 1oo2D по данным показателям. Однако нельзя назвать такую критику заслуженной, так как благодаря непрерывному совершенствованию технологии ПЛК, используемых в системах безопасности, некоторые системы 1oo2D на базе таких контроллеров имеют хорошие показатели по уровню ложных срабатываний.

Преимущества архитектур 2oo3 или 1oo3 остаются существенными, когда приходится иметь дело с неинтеллектуальными устройствами, такими как термопары, термометры сопротивления, реле, датчики давления и другие подобные компоненты.

**Пример**

Очень хорошая термопара имеет среднее время между отказами MTBF = 500 лет и PFDavg = 0,0005/год.

Интенсивность отказов λ = 1/MTBF = 0,002. Интенсивность опасных недетек-

тируемых отказов $\lambda_{DU}$ может быть принята равной $\lambda/2 = 0{,}001$.

Используя для измерения одного параметра три термопары вместо одной, получим:
$\lambda = 0{,}006$;
MTBF = 166 лет;
PFDavg = 0,000001/год;
$PFDavg_{\beta=10\%} = 0{,}00005$/год.

Окончательный выбор архитектуры системы должен осуществляться с учётом экономических факторов (стоимости) наряду с другими показателями.

## Отказы по общей причине (связанные отказы)

В части 4 стандарта МЭК 61508 дано следующее определение отказа по общей причине: «отказ, который является результатом одного или нескольких событий, вызывающих одновременный отказ двух или более отдельных каналов в многоканальной системе, приводящий к отказу системы в целом» [2]. Эти отказы оказывают существенное влияние на надёжность и безопасность системы, поэтому должны учитываться в соответствующих моделях.

Четыре категории отказов: опасные и безопасные, детектируемые и недетектируемые – можно дополнительно разделить следующим образом:

**SDN** – безопасный, детектируемый, обычная причина (Safe, Detected, Normal cause);
**SDC** – безопасный, детектируемый, общая причина (Safe, Detected, Common cause);
**SUN** – безопасный, недетектируемый, обычная причина (Safe, Undetected, Normal cause);
**SUC** – безопасный, недетектируемый, общая причина (Safe, Undetected, Common cause);
**DDN** – опасный, детектируемый, обычная причина (Dangerous, Detected, Normal cause);
**DDC** – опасный, детектируемый, общая причина (Dangerous, Detected, Common cause);
**DUN** – опасный, недетектируемый, обычная причина (Dangerous, Undetected, Normal cause);
**DUC** – опасный, недетектируемый, общая причина (Dangerous, Undetected, Common cause).

## Отказы по общей причине, β–фактор и их влияние на расчёт PFDavg

Для учёта отказов по общей причине в математическую модель расчёта PFDavg

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

## Искробезопасные подсистемы ввода/вывода от Invensys и Pepperl+Fuchs

Invensys Process Systems (IPS), известная международная компания, предоставляющая решения в области автоматизации промышленных технологий, программного обеспечения и консалтинговых услуг, выполнила совместную работу с компанией Pepperl+Fuchs, ведущим поставщиком решений с видом взрывозащиты «искробезопасная электрическая цепь» для обрабатывающих отраслей промышленности, чтобы предложить простое объединение искробезопасных систем ввода/вывода и системы распределённого управления I/A Series® компании IPS.

Интегрированные модули, включающие в себя встроенные барьеры искробезопасности и средства сопряжения с полевыми устройствами, являются простейшим решением для установки устройств ввода/вывода во взрывоопасных зонах, которое отличается низкой стоимостью и минимальной площадью основания. Такое объединение предоставляет пользователям прозрачный интерфейс, с помощью которого они могут настроить, сконфигурировать и обслуживать искробезопасные системы с использованием инструментальных программных средств I/A Series®. Решение сертифицировано для применений во взрывоопасных зонах классов 1 и 2.

Простая интеграция технологий IPS и Pepperl+Fuchs предоставляет много преимуществ для пользователей. Так как искробезопасные модули можно менять, устанавливать без отключения питания и без получения разрешения на производство работ во взрывоопасной зоне, обслуживание их проще и безопаснее, к тому же коэффициент готовности является высоким со встроенным резервированием в коммуникационных модулях, источниках питания и шинных интерфейсах. IPS предлагает встроенное решение в совместимых с HART модулях, поэтому пользователи систем I/A Series® могут управлять искробезопасными HART совместимыми полевыми устройствами от любого поставщика. А так как интеграция с технологией I/A Series® также обеспечивает совместимость с Field Device Manager на базе технологии FDT, то заказчики могут настраивать и обслуживать интеллектуальные устройства на основе общей операционной техники управления. ●

## ICONICS и Kepware осваивают рынок встраиваемых систем

Компания ICONICS в сотрудничестве с компанией Kepware Technologies создала программный комплекс на платформе Windows CE для организации систем управления, визуализации и других решений для реализации человеко-машинного интерфейса.

ICONICS и Kepware, занимающие лидирующие позиции в области программного обеспечения для АСУ ТП, объединили свои усилия для выпуска на рынок новых решений на базе платформы Windows® CE. Это инновационное программное обеспечение позволит использовать передовые технологии SCADA и лучшие разработки в области передачи и обработки данных. Подобный альянс даёт возможность использовать наиболее экономичные решения для OEM-проектов.

Примером может служить проект автоматизации сборочных линий автогиганта AUDI, где автоматизированные рабочие места (АРМ) отдельных участков были выполнены на базе панельных компьютеров. Неоспоримыми преимуществами подобных проектов являются решения Kepware и ICONICS в части коммуникаций, организации доступа к данным, в поддержке режимов управления рабочим столом АРМ/серверов на основе операционных систем Windows Embedded и Windows CE.

OEM-решения Kepware усиливают обе платформы, поскольку прикладные файлы весьма компактны, позволяют осуществлять отладку вне производства, а затем загружать готовые проекты на съёмные носители встраиваемых систем. ICONICS на протяжении многих лет использует протоколы Kepware для «настольных платформ». Партнёрство с Kepware открывает возможность совместной поддержки платформы для встраиваемых систем на базе Windows CE. Как отмечают эксперты компании ARC Advisory Group, такое взаимовыгодное сотрудничество лидеров рынка АСУ ТП принесёт серьёзные положительные результаты для OEM-разработчиков встраиваемых систем. ●

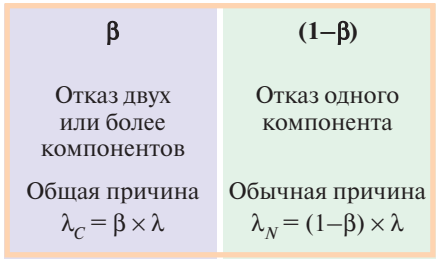


**Рис. 2. Подразделение интенсивностей обычных отказов и отказов по общей причине (β-фактор)**

вводится параметр β – это статистический параметр, который позволяет учесть отказы такого рода. Использование модели с параметром β делает возможным получение более близкого к реальности значения параметра надёжности системы. β-модель разделяет интенсивности отказов компонентов (рис. 2) на две группы:

- интенсивность обычных отказов (normal mode failure rate) – $\lambda_N$ (отказ только одного компонента);
- интенсивность отказов по общей причине (common mode failure rate) – $\lambda_C$ (отказ двух или более компонентов).

Общая площадь прямоугольника на рис. 2 представляет суммарную интенсивность отказов (λ). В его левой части стрессовое воздействие достаточно велико, что приводит к отказу двух или нескольких компонентов вследствие одной и той же причины.

Взаимосвязь этих двух групп определяется следующими формулами:

$\lambda_C = \beta \times \lambda$;
$\lambda_N = (1-\beta) \times \lambda$.

Четыре категории интенсивностей отказов SU, SD, DU и DD в β-модели подразделяются следующим образом:

$\lambda_{SUN} = (1-\beta) \times \lambda_{SU}$;
$\lambda_{SUC} = \beta \times \lambda_{SU}$;
$\lambda_{SDN} = (1-\beta) \times \lambda_{SD}$;
$\lambda_{SDC} = \beta \times \lambda_{SD}$;
$\lambda_{DUN} = (1-\beta) \times \lambda_{DU}$;
$\lambda_{DUC} = \beta \times \lambda_{DU}$;
$\lambda_{DDN} = (1-\beta) \times \lambda_{DD}$;
$\lambda_{DDC} = \beta \times \lambda_{DD}$.

*Таблица 2*

**Формулы для расчёта PFDavg с учётом β-фактора**

| Архитектура | Упрощённая формула | Упрощённая формула с учётом β-фактора |
|---|---|---|
| 1oo2 | $\frac{1}{3}(\lambda_{DU} \times TI)^2$ | $\frac{1}{3}[(1-\beta) \times \lambda_{DU} \times TI]^2 + \frac{1}{2}(\beta \times \lambda_{DU} \times TI)$ |
| 1oo2D | $\frac{1}{3}(\lambda_{DU} \times TI)^2$ | $\frac{1}{3}[(1-\beta) \times \lambda_{DU} \times TI]^2 + \frac{1}{2}(\beta \times \lambda_{DU} \times TI)$ |
| 2oo2 | $\lambda_{DU} \times TI$ | $(1-\beta) \times \lambda_{DU} \times TI + \frac{1}{2}(\beta \times \lambda_{DU} \times TI)$ |
| 2oo3 | $(\lambda_{DU} \times TI)^2$ | $[(1-\beta) \times \lambda_{DU} \times TI]^2 + \frac{1}{2}(\beta \times \lambda_{DU} \times TI)$ |
| 1oo3 | $\frac{1}{4}(\lambda_{DU} \times TI)^3$ | $\frac{1}{4}[(1-\beta) \times \lambda_{DU} \times TI]^3 + \frac{1}{2}(\beta \times \lambda_{DU} \times TI)$ |

*Таблица 3*

**Сравнение PFDavg для различных β-факторов**

| PFDavg | RRF |
|---|---|
| 1oo1: 0,005/год | 1oo1: 200 |
| 1oo2: 0,00003/год (без учёта β-фактора) | 1oo2: 33333 = 200 × 166,6 |
| 1oo2: 0,00082/год (β-фактор 1%) | 1oo2: 12195 = 200 × 61 |
| 1oo2: 0,00028/год (β-фактор 5%) | 1oo2: 3571 = 200 × 17,8 |
| 1oo2: 0,00053/год (β-фактор 10%) | 1oo2: 1897 = 200 × 9,48 |

Значения β-фактора могут быть разными для каждой группы, и их расчёт не простой, поэтому обычно используется только одно значение для компонента или для электрической части SIF. Например, одинаковое значение используется для датчика-преобразователя, барьера искробезопасности и ПЛК, в то же время для оконечного исполнительного элемента используется другое значение β. Рекомендации по выполнению расчётов приведены в части 6 (приложение D) стандарта МЭК 61508.

β-фактор должен учитываться в тех случаях, когда резервирование компонентов или субсистем используется для снижения PFDavg. С учётом β-фактора формулы для расчёта PFDavg трансформируются к виду, представленному в табл. 2.

Типичные значения β лежат в диапазоне от 1 до 10%. Второе слагаемое в формулах соответствует вкладу в PFDavg, обусловленному β-фактором и полученному по сравнению с архитектурой 1oo1 (симплексной).

Как можно видеть из приводимого далее примера, второе слагаемое в формуле (зависящее от β) имеет существенно большее значение, чем первое. Поэтому в резервированных системах β-фактор ограничивает величину снижения PFDavg относительно значения PFDavg для архитектуры 1oo1 примерно до 100 раз при β= 0,01 (1%) и лишь до 20 раз при β= 0,05 (5%).

**Пример**

$\lambda_{DU} = 0{,}01$/год;
$TI = 1$ год;
β= 0,05.

Для архитектуры 1oo2 формула имеет вид:

$$PFDavg = \frac{1}{3}[(1-\beta) \times \lambda_{DU} \times TI]^2 +$$
$$+ \frac{1}{2}(\beta \times \lambda_{DU} \times TI) =$$
$$= \frac{1}{3}[(0{,}95 \times 0{,}01]^2 + \frac{1}{2}(0{,}05 \times 0{,}01) =$$
$$= 0{,}00003 + 0{,}00025 = 0{,}00028/\text{год}$$

Значения PFDavg для различных β-факторов приведены в табл. 3.

Выводы:

- без учёта β-фактора PFDavg архитектуры 1oo2 в 166,6 раз ниже PFDavg архитектуры 1oo1;
- при β-факторе 1% PFDavg архитектуры 1oo2 в 61 раз ниже PFDavg архитектуры 1oo1;
- при β-факторе 5% PFDavg архитектуры 1oo2 в 17,8 раз ниже PFDavg архитектуры 1oo1;
- при β-факторе 10% PFDavg для архитектуры 1oo2 в 9,48 раз ниже PFDavg архитектуры 1oo1.

Обычно используется β-фактор 5%. Если к безопасности системы предъявляются более высокие требования, используется β-фактор 10%. В частности, такой β-фактор используется применительно к клапанам и датчикам-преобразователям, для которых нет достаточных статистических данных по их надёжности. β-фактор, равный 1%, допускается использовать, только если резервируемые компоненты изготовлены не одним и тем же производителем или они используют различные конструктивные принципы и различные технологии. ●

## Литература

1. Глизенте Ландрини. Интегральные уровни безопасности в соответствии со стандартами МЭК 61508 и 61511 и анализ их связи с техническим обслуживанием // Современные технологии автоматизации. – 2009. – № 1. – С. 72-79.

2. Стандарт МЭК 61508. Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью.

**Автор – генеральный директор компании GM International S.r.l. (Италия)**