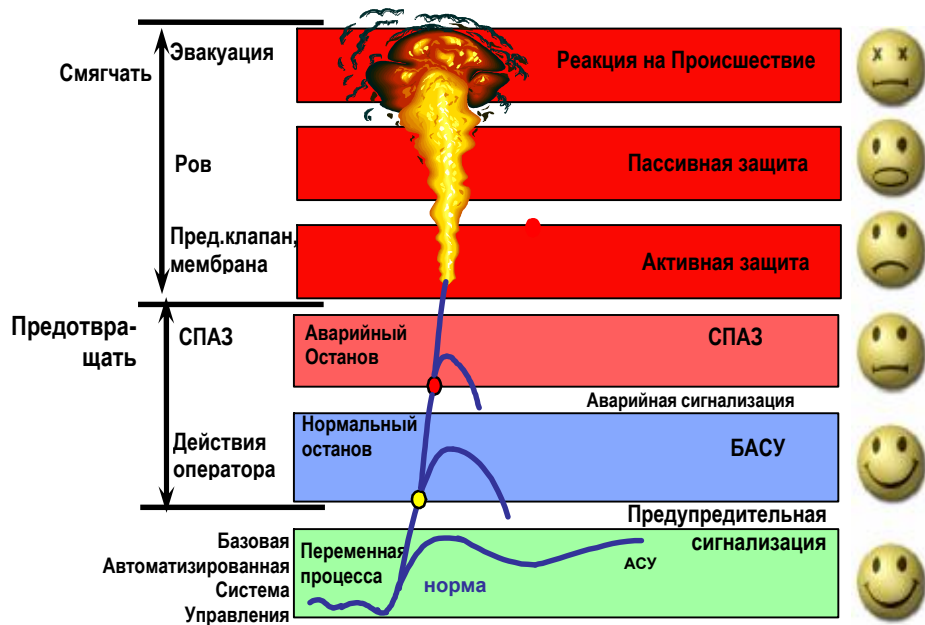
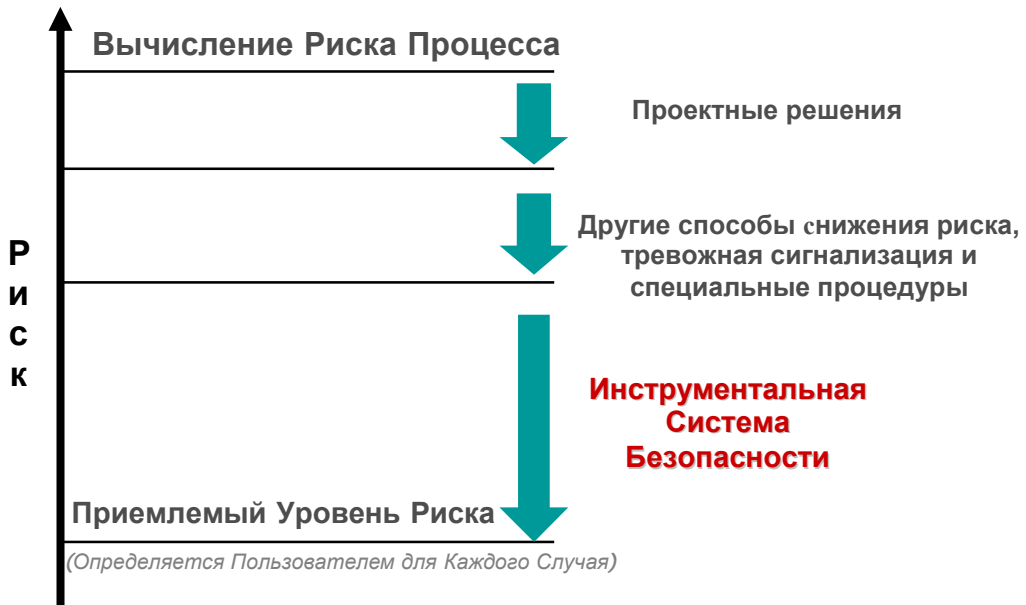


Снижение Риска с Современными Инструментальными Системами Безопасности

Введение	3
Снижение риска – главный приоритет	4
Стандарты безопасности дают указания.....	5
МЭК 61508	5
Уровни полноты безопасности	6
МЭК 61511: стандарт по безопасности для перерабатывающих отраслей промышленности	7
Основные тенденции в области инструментальных систем безопасности ...	8
Фокус на всеобщей безопасности	9
Автоматический мониторинг и тестирование полевых приборов	10
Интегрированная системой управления, но независимая от неё	11
Повышенная гибкость и масштабируемость	12
Учет всех состояний процесса	13
Использование промышленной стандартной ОС.....	14
Рекомендации Пользователям	15



Безопасность Через Уровни Защиты



Снижение Риска Является Главным Приоритетом

Введение

С момента публикации стандарта МЭК 61508 по функциональной безопасности и, немного позднее, стандарта МЭК 61511 по безопасности для перерабатывающих отраслей, среди предприятий значительно возрос интерес к проведению всестороннего анализа рисков и опасностей, и использованию сертифицированных Инструментальных Систем Безопасности (ИСБ, **Safety Instrumented Systems, SIS**). Поскольку специалисты приобретают всё больше знаний по вопросам безопасности, они фокусируются на достижении всеобщей безопасности с автоматическим мониторингом и тестированием полевых приборов. Пользователи желают,

Повышенное внимание к всеобщей безопасности

Автоматический мониторинг и тестирование полевых приборов

Тесная интеграция с системами управления

Повышенная гибкость и масштабируемость

Расширенная функциональность в зависимости от состояния процесса

Использование стандартных операционных систем

Основные тенденции в промышленной безопасности

чтобы Инструментальная Система Безопасности соответствовала их потребностям в более эффективном по стоимости решении через интеграцию с системами управления, увеличению интервалов тестирования и масштабируемости архитектуры. Они также ищут улучшенные возможности по изменению условий возникновения алармов в зависимости от условий процесса и организации последовательных процедур останова в случае опасности. С выходом в

свет стандарта безопасности МЭК 61511 для перерабатывающих отраслей, теперь нет оправданий для пользователей, не использующих экономически эффективные подходы к безопасности.

Сегодня большинство причин отказа ПАЗ заключается не в выходе из строя логического вычислителя, а в неисправности полевых приборов. Система противоаварийной защиты должна следить за здоровьем всего контура, обладая встроенной возможностью проверки исправности полевых приборов. Следовательно, обеспечение интегрированного решения по безопасности от сенсора до привода должно быть важнейшим критерием при выборе SIS.

Сегодня доступны регулирующие клапаны, которые имеют очень малую вероятность заклинивания штока и протечки сальника. Также на рынке доступны контроллеры клапанов и приводы, сертифицированные по TÜV. Инструментальная система безопасности должна включать тестирование на частичный ход клапана как свою неотъемлемую часть.

Сегодня поставщики предлагают одинаковые системы для оперативного управления и для организации ПАЗ, в которых используются одинаковые

способы конфигурирования, языки программирования и процедуры по обслуживанию. Две системы обмениваются данными друг с другом, но с соответствующим уровнем защиты от выхода из строя одной из-за отказа другой. Выбирайте систему, которая обеспечивает гибкость в конфигурировании логических вычислителей с расширенными возможностями использования функциональных блоков.

Очень важно выбрать систему, которая интегрирует информацию о состоянии полевых приборов в логику своей работы. Пользователи должны использовать систему, которая обеспечивает прозрачное конфигурирование и удобные условия для работы и обслуживания с необходимым разделением функций безопасности и управления. Пользователи должны убедиться, что они выбирают систему, которая обеспечивает соответствие Международным Стандартам Безопасности с наименьшими затратами.

Снижение риска – главный приоритет

Риск обычно определяется как комбинация вероятности и возможных последствий незапланированного события. То есть, насколько часто оно может происходить и насколько плохо будет, если оно произойдет. При-

Оборудование работает на пределе возможностей
Переходные режимы работы (пуск, останов, смена режима, смена персонала)
Использование опасного сырья
Производство опасных изделий
Присутствие необученного персонала
Отсутствие культуры безопасности

Факторы, увеличивающие риск

мерами событий и соответствующих им рисков в промышленности могут служить смерть людей или потеря конечностей, загрязнение окружающей среды, повреждение оборудования и потеря продукции. Для многих производителей потеря имиджа компании также может быть существенным фактором риска. Прибавьте к этому реальности растущих экологических проблем, трудности соответствия федеральным нормам, и угрозу судебной тяжбы, и легко понять, почему снижение риска становится всё более важным для большинства производственных предприятий.

Наилучшим способом снижения риска на промышленном предприятии является использование технологических процессов, которые изначально безопасны. Однако, такие процессы редко применимы в современных условиях. Риски существуют везде, где хранятся, производятся или обрабатываются взрывоопасные или токсичные материалы.

Поскольку невозможно полностью устранить все риски, производитель должен согласиться с таким уровнем риска, который в данном случае

приемлем. После определения основных источников опасности, следует провести анализ опасностей и рисков путем выявления вероятности их происхождения и тяжести их последствий. Специфические для каждого предприятия условия, такие как плотность ближайших поселений, внутренние маршруты проезда транспортных средств, и метеорологические условия должны также быть приняты во внимание при исследовании рисков.

Соблюдение экологических нормативов
Соблюдение требований контролирующих органов
Требования стандартов безопасности
Поддержание имиджа компании

Факторы, снижающие риск

После того, как анализ опасностей и рисков определил собственно риски, можно определить находятся ли они ниже допустимых уровней. Базовые автоматизированные системы управления, со встроенной поддержкой алармов и средств ручного управления, обеспечивают первый уровень защиты и снижают риск на промышленном предприятии. В случае если базовая автоматическая система управления не снижает риск до допустимого уровня, требуются дополнительные меры защиты. Они включают инструментальные системы безопасности, механизмы аппаратных блокировок, предохранительные клапаны и защитные рвы. Для полной эффективности, каждая подсистема защиты должна работать независимо от всех других.

Стандарты безопасности дают указания

С момента публикации стандарта МЭК 61508 по промышленной безопасности и, немного позднее, стандарта МЭК 61511 по безопасности для перерабатывающих отраслей среди предприятий значительно возрос интерес к проведению всестороннего анализа рисков и опасностей и применению сертифицированных Инструментальных Систем Безопасности (ИСБ, **Safety Instrumented Systems, SIS**). Эти стандарты дают указания по наилучшим методам работы и предлагают рекомендации, но не освобождают пользователей этих стандартов от ответственности в части безопасности. Стандарты описывают не только технические детали, а также планирование, документирование и другие процедуры для управления безопасностью в течение всего времени жизни системы.

МЭК 61508

Стандарт Безопасности МЭК 61508, опубликованный Международной Энергетической Комиссией, применим к широкому диапазону отраслей

промышленности и технологических процессов, и, в основном, предназначен для производителей и поставщиков. Стандарт МЭК 61508 состоит из семи частей, в которых рассматриваются все вопросы от постулирования общих требований к безопасности до рассмотрения требований к специальным системам и соответствующим случаям их использования. Стандарт является общим и может напрямую использоваться как основной или использоваться международными организациями в качестве базы для разработки стандартов для конкретных отраслей промышленности, например, машиностроительной, перерабатывающей или атомной. При внедрении системы безопасности пользователю рекомендуется выбирать только ту, которая сертифицирована независимой организацией, например TÜV или FM.

Следует учесть, что сертификат, полученного от независимой организации, следует рассматривать параллельно с Руководством по Безопасности системы. Этот документ определяет ограничения по использованию подсистемы противоаварийной защиты. Руководство для хорошей системы ПАЗ представляет собой тонкую брошюру с минимальным количеством ограничений. Опасайтесь систем, для которых это руководство представляет собой толстую книгу – это показатель того, что существуют сложности и ограничения при использовании ИСБ.

Уровни полноты безопасности

Полнота безопасности определяется как вероятность удовлетворительного выполнения системой требуемых функций, связанных с безопасностью, при соответствующих условиях, в течение определенного промежутка времени. Уровень Полноты Безопасности (УПБ, **Safety Integrity Level, SIL**) определяется как дискретный показатель для указания требований по полноте безопасности для функций безопасности. Уровень Полноты Безопасности определяется путем оценки риска, но он не является мерой риска. УПБ является мерой ожидаемой надежности системы или функции.

Уровень Полноты Безопасности (УПБ)	Вероятность Отказа по Запросу (низкая интенсивность запросов)	Вероятность Отказа по Запросу (высокая интенсивность запросов)
1	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$
2	$\geq 10^{-3} \dots < 10^{-2}$	$\geq 10^{-7} \dots < 10^{-6}$
3	$\geq 10^{-4} \dots < 10^{-3}$	$\geq 10^{-8} \dots < 10^{-7}$
4	$\geq 10^{-5} \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$

Уровни Полноты Безопасности

Примечания:

Низкая интенсивность запросов:

Когда действия выполняются в качестве реакции на параметры процесса или другие условия (не более чем один раз в год)

Высокая интенсивность запросов:

Когда действия выполняются непрерывно для обеспечения функциональной безопасности

МЭК 61511: стандарт по безопасности для перерабатывающих отраслей промышленности

Стандарт МЭК 61511 разработан специально для перерабатывающих отраслей промышленности. Стандарт описывает наилучшие методы безопасной работы для всех пользователей, внедряющих современные ИСБ. В то время как МЭК 61508 состоит из семи частей, МЭК 61511 имеет только три:

- Часть 1: Основы, определения, требования к системе, аппаратному и программному обеспечению
- Часть 2: Руководство по применению
- Часть 3: Руководство по определению требуемого уровня полноты безопасности

Часть 1 стандарта МЭК 61511 является нормативной, в то время как части 2 и 3 предназначены только для информации. Часть 1 МЭК 61511 структурирована так, чтобы придерживаться модели жизненного цикла системы безопасности. Анализ опасностей и рисков использует концепцию уровней защиты и определяет модель уровней полноты безопасности, разработанную в стандарте МЭК 61508. Здесь также описаны ключевые моменты, на которые стоит обратить внимание при разработке требований к системе безопасности. Такие вопросы, как разделение систем, общая причина отказа, реакция на выявление отказа, аппаратная надежность и доказательства в использовании также описываются в этой части.

МЭК 61508	МЭК 61511
Общий стандарт по безопасности для широкого применения	Специальный стандарт по безопасности для перерабатывающих отраслей промышленности
Применим ко всем системам, связанным с безопасностью, и внешним устройствам по снижению риска	Применим только к Инструментальным Системам Безопасности
В основном для производителей и поставщиков систем и приборов промышленной безопасности	В основном для проектных организаций, системных интеграторов и пользователей систем и приборов промышленной безопасности

Основные Отличия между Стандартами МЭК 61508 и МЭК 61511

Требования по безопасности к программному обеспечению включают, рассматривая эти элементы как часть архитектуры, связь с аппаратным обеспечением, инструментальные функции безопасности, уровни полноты безопасности, планирование проверок программного обеспечения, вспомогательные инструменты, тестирование, интеграцию и модификацию. Два дополнительных раздела описывают требования по приемке системы на заводе-изготовителе и требования по установке и пусконаладке.

Вторая часть стандарта предоставляет собой практическое руководство по составлению спецификации, проектированию, установке, эксплуатации и обслуживанию инструментальных функций безопасности и связанных с ними инструментальных систем безопасности, как это определено в первой части стандарта. Большое количество материала для второй части взято из технического отчета **ISA dTR84.0.02**, который описывает подходы к вычислению показателей работы инструментальных систем безопасности.

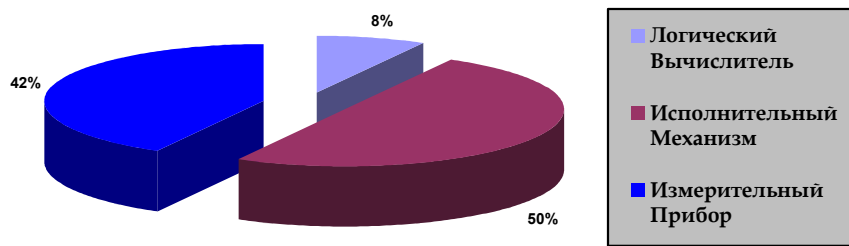
Третья часть стандарта представляет собой руководство по проведению анализа опасностей и рисков. Она обеспечивает информацией по основным концепциям определения риска, связи риска с полнотой безопасности и определению допустимых уровней рисков. Стандарт по безопасности **ANSI/ISA-84**, предшествующий международным стандартам по безопасности, скоро будет обновлен для более точного соответствия стандарту МЭК **61511**.

Основные тенденции в области инструментальных систем безопасности

По мере того, как предприятия приобретают всё больше знаний по вопросам безопасности, они проводят более тщательный анализ опасностей и рисков для более точного определения своих потребностей. Они ищут пути снижения риска фокусируясь на всеобщей безопасности. Они хотят, чтобы ИСБ удовлетворяли их потребностям в более экономически эффективном способе интеграции с системами управления. Они также ищут более гибкую архитектуру с улучшенной масштабируемостью, повышенной функциональностью по изменению пределов алармов в соответствии с условиями процесса, и процедурами для случаев возникновения опасности.

Фокус на всеобщей безопасности

Основной причиной отказа инструментальной системы безопасности является не отказ логических вычислителей, а неполадки с полевыми приборами. Разработка схем голосования и расширенной диагностики для логических вычислителей была мощным шагом вперед. Однако, причиной более **90** процентов отказов являются не логические вычислители, а датчики и приводы клапанов.



Основные Причины Отказов ИСБ

Современная система защиты должна иметь возможность проверки состояния каналов ввода/вывода и полевых приборов. Фактически, мониторинг состояния оборудования ввода/вывода должен быть изначально заложен в её архитектуре. Такими примерами могут быть:

- Проверка сенсора
- Мониторинг параметров окружающей среды, таких как температура и влажность, которые вызывают ухудшение характеристик сенсора
- Дрейф показаний датчика

Отказы электронных компонент по общей причине часто происходят из-за влияния условий окружающей среды. Большинство электронных приборов отказывают при превышении рабочих значений температуры и влажности, которые должны тщательно отслеживаться. Калибровка сенсора также становится интегральной частью ИСБ. Использование

1.	Интеграция данных о состоянии полевых приборов в логическом вычислителе
2.	Установка недоверенного статуса сигнала при сомнительных показаниях датчика
3.	Сравнение значений аналоговых и цифровых сигналов для проверки достоверности

Интегрированный Подход к Безопасности Процесса

открытых протоколов, таких как **HART** и, в принципе, **FOUNDATION Fieldbus**, позволяет проводить удаленный мониторинг, диагностику и подтверждение характеристик полевых приборов.

Сегодня также используются технологии по повышению работоспособности клапанов. Использование в системах безопасности контроллеров клапанов, которые не диагностируют состояние механиз-

мов клапана автоматически, вызывает беспокойство по поводу возможности срабатывания клапана по запросу. Регулирующие клапаны спроектированы так, чтобы иметь малую вероятность заклинивания штока и протечки сальника, а для тестирования и диагностики их состояния сегодня коммерчески доступны приводы и контроллеры, сертифицированные TUV. ИСБ должна включать тест на частичный ход штока как неотъемлемую часть архитектуры.

Автоматический мониторинг и тестирование полевых приборов

Сегодня доступны сертифицированные интеллектуальные датчики и исполнительные механизмы, способные передавать данные о своём состоянии логическому вычислителю. Это повышает готовность системы, поскольку отказавший датчик может быть сразу же заменен или же его показания могут быть проигнорированы стратегией голосования. Также, проблемы с исполнительными механизмами могут быть диагностированы более быстро, не допустив развития опасной ситуации.

С применением цифрового контроллера клапана становится доступным тест на частичный ход клапана. Эта процедура дает гораздо больше диагностики, чем при ручном тестировании, а также не подвергает риску обслуживающий персонал, обычно тестирующий приборы в полевых условиях. Наконец, клапан не требуется демонтировать из контура безопасности на период проведения теста.

Одним из требований стандарта МЭК **61511** является изъятие каждого компонента ИСБ из контура безопасности и полное его тестирование – интервал между тестами зависит от типа компонент и требуемого Уровня Полноты Безопасности. Автоматизация процедур по тестированию, в комбинации с сертифицированными приборами, показатели надежности которых подтверждены независимыми организациями, позволяет существенно увеличить интервал между тестами, соответственно увеличивая время непрерывной работы производства.

Интегрированная системой управления, но независимая от неё

Многие предприятия используют разделение контроллеров обслуживающих контуры безопасности от контроллеров для оперативного управления и оптимизации. Контроллеры для ИСБ приходят от узкого круга поставщиков, которые добавляют в них избыточную диагностику и получают сертификат TUV. В прошлом, практически не существовало альтернативы использованию абсолютно разных систем для управления и безопасности. Некоторые пользователи даже требовали использовать системы управления и безопасности от разных производителей.

Существует много других существенных причин для выполнения функций по безопасности и управлению в разных контроллерах:

- Независимые отказы – снижение риска одновременного отказа систем управления и безопасности
- Безопасность – изменения в системе управления не должны вызывать изменений или повреждения соответствующей ИСБ
- Разные требования для контроллеров безопасности – система безопасности спроектирована так, чтобы её отказ был безопасным, в то время как система управления должна обеспечить максимальную степень готовности. Инструментальная система безопасности также имеет дополнительные инструменты такие, как расширенная диагностика, проверка ошибок в программном обеспечении, защищенные хранилища данных и отказоустойчивость

Общее пространство данных
Улучшенная безопасность пользователей
Одинаковые инженерные инструменты
Видимые различия между средами работы систем управления и безопасности на уровне рабочих станций
Соответствующая защита доступа
Существенное снижение затрат на интеграцию

Выгоды от Улучшенной Интеграции Систем Безопасности и Управления

Стандарт МЭК 61508 является в этом вопросе немного двусмысленным; ибо он строго рекомендует разделение систем, но не обязует к этому. Сегодня большое количество пользователей всё чаще находят логические причины использования одинаковых систем для функций управления и безопасности, поскольку это уменьшает осложнения, связанные с различием процедур и языков программирования, требованиями по установке и обслуживанию. Также, всегда

существует риск использования различных процедур для подобных задач из-за ошибок человека и возможных проблем с безопасностью.

Вполне очевидными видятся финансовые преимущества использования одинаковых систем – снижение затрат на оборудование систем, конфигурирование, обучение и запасные части происходит из-за уменьшения требуемого ассортимента и количества оборудования. Дополнительные

расходы на сервисное обслуживание и техническую поддержку, возникающие из-за различия систем, теперь просто отсутствуют.

Некоторые производители систем управления и безопасности сегодня предлагают похожие системы для реализации соответствующих функций, которые включают одинаковые системы визуализации (ЧМИ), методы конфигурирования, языки программирования и процедуры обслуживания. Ключевым моментом к пониманию является то, что, несмотря на разделение систем друг от друга, различие аппаратного и программного обеспечения, они имеют общий интерфейс для конфигурирования, оперативного управления и обслуживания. Это позволяет пользователям достигнуть определенных выгод в процессе эксплуатации, соответствуя при этом требованиям безопасности по разделению систем. Системы управления и безопасности открыто обмениваются информацией друг с другом, но имеют соответствующую защиту от взаимного повреждения.

Повышенная гибкость и масштабируемость

Большинство Инструментальных систем безопасности, используемых сегодня для задач управления критическими контурами или противоаварийной защиты, имеют архитектуру Тройного Модульного Резервирования (**Triple Modular Redundancy, TMR**, схема голосования

Изменяемая конфигурация контроллера для изменчивых потребностей безопасности и работоспособности

Каждый модель работает с небольшим числом контуров

Несколько контроллеров для больших применений

Элементы Гибкости и Масштабируемости Системы Безопасности

2oo3) и Двойного Резервирования с Диагностикой (схема голосования **1oo2D**). Однако, поставщики ИСБ активно предлагают другие архитектуры. Они включают **Quad (2oo4D)**, Пара с Запасным, а также Кластерную конфигурацию. Всё чаще поставщики предлагают гибкость конфигурации, когда пользователь имеет возможность соединения между собой двух или более ПЛК для

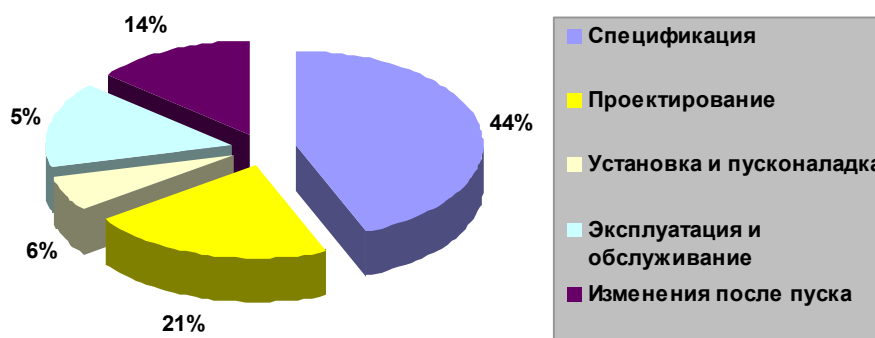
снижения интенсивности отказов и повышения готовности.

Контроллеры безопасности становятся всё более масштабируемыми. Их размеры уменьшаются, один контроллер способен обрабатывать определенное количество параметров, а для работы с большим количеством параметров понадобится некоторое количество таких контроллеров. Это хорошая новость для пользователей, поскольку теперь им не потребуется приобретать большие и дорогостоящие системы, избыточные для большинства приложений.

Учет всех состояний процесса

Современная ИСБ обеспечивает возможность простого последовательно-го выполнения команд (без заикливания) для проведения надлежащим образом останова технологического процесса при обнаружении опасных ситуаций. Поскольку базовая автоматизированная система управления может остановить технологический блок при появлении критического аларма, поручение ИСБ функций по останову всего производства ведет к существенному снижению риска. Функциональные блоки ИСБ также могут проводить изменение пределов возникновения алармов в зависимости от условий процесса, что типично для систем управления периодически процессами.

Стандарт МЭК 61511 требует, чтобы все включения байпасов и обходных схем управления отображались в журнале событий и алармов системы и тщательно отслеживались. Современная ИСБ помогает реализовать это, предлагая эту функциональность как стандартную. Это поможет удостовериться, что требуемые уровни доступа автоматически сконфигурированы в соответствии с требованиями УПБ рассматриваемого контура и что не требуется дополнительного конфигурирования для отображения активных байпасов и обходных схем.



Большинство Отказов ИСБ Связано с Инженерным Обеспечением

Существует другой хороший повод для поиска ИСБ с расширенной сертифицированной встроенной функциональностью. Исследование, проведенное Агентством по Безопасности Здоровья и Окружающей среды, Великобритания, показало, что **85** процентов отказов ИСБ связаны с инженерным обеспечением, притом, что около **60** процентов отказов заложены в ИСБ на стадии проектирования. Поэтому вполне понятно, что ИСБ должна быть поставлена с такой функциональностью, чтобы как можно проще следовать наилучшей практике работы, как это заложено в

МЭК 61511, и соответствующим образом конфигурировать систему. Достичь намеченных целей гораздо проще с использованием функциональных блоков с богатой функциональностью.

Использование промышленной стандартной ОС

Для работы логического вычислителя ИСБ крайне важно использование операционной системы (ОС) с высокой надежностью работы. Фактически, операционная система логического вычислителя должна быть сертифицирована на уровень критичности не менее, чем значение УПБ для контуров, на которых работает ИСБ. В то же время, требование по уменьшению расходов на обслуживание в сочетании с доступностью современных микропроцессорных технологий, создали потребность в стандартных и коммерчески доступных операционных системах для логических вычислителей в инструментальных системах безопасности. Серийно выпускаемая ОС, была сертифицирована независимым Агенством и поэтому предоставляет существенные преимущества для поставщиков и пользователей Инструментальных систем безопасности.

Проверена в Использовании

Тщательно протестирована

Корректная система извещений об отказе и поправок в работе

Преимущества Использования Стандартных Промышленных Операционных Систем в ИСБ

Рекомендации Пользователям

- Используйте МЭК 61511 как стандарт по безопасности Вашего предприятия.
- Проводите тщательный и основанный на стандартах анализ опасностей и рисков для определения соответствующих уровней защиты для Вашего производства.
- Основываясь на проведенном анализе опасностей рисков, выберите сертифицированную инструментальную систему безопасности, соответствующую Вашим требованиям по управлению рисками.
- Выбирайте такую инструментальную систему безопасности, которая тесно интегрируется с базовой автоматизированной системой управления, обеспечивая при этом необходимый уровень разделения.
- Используйте систему, обеспечивающую интегрированное решение по безопасности от сенсора до привода.
- Производите постоянный мониторинг состояния полевых приборов и автоматически тестируйте приборы когда это возможно.
- Используйте систему с гибкой конфигурацией, обеспечивающую легкость географического разнесения и масштабируемость.
- Используйте систему с сертифицированными функциональными блоками с богатыми возможностями, которые учитывают в логике своей работы состояние полевых приборов и обеспечивают легкость проектирования и конфигурирования.
- Уделяйте должное внимание решениям с готовыми операционными системами, сертифицированными на применение в области промышленной безопасности.
- Используйте систему, повышающую безопасность при одновременном повышении готовности путем использования автоматического тестирования и расширенной диагностики, охватывающей весь контур.
- Опасайтесь толстых руководств по безопасности. Выбирайте систему с минимальным количеством ограничений и запретов.

Автор: Асиш Гош (Asish Ghosh)
Редактор: Чентал Полсонетти (Chantal Polsonetti)

Используемые Акронимы: Для получения полного перечня используемых в промышленности акронимов, обратитесь на страницу нашего сайта в Интернет: www.arcweb.com/Community/terms/terms.htm

ANSI	American National Standards Institute	OPSYS	Operating System
BPCS	Basic Process Control System	OSHA	Occupational Safety & Health Administration
DCS	Distributed Control System	PLC	Programmable Logic Controller
ESD	Emergency Shutdown (system)	PSM	Process Safety Management
FM	Factory Mutual	SIL	Safety Integrity Level
HART	Highway Addressable Remote Transducer	SIS	Safety Instrumented System
HAZOP	Hazard & Operability	TMR	Triple Modular Redundancy
HMI	Human Machine Interface	TÜV	Technischer Überwachungs Verein (Technical Inspection Association)
HSE	Health, Safety and Environmental Agency		
МЭК	International Electrotechnical Commission		

Основанная в 1986 году, компания организация ARC Advisory Group является лидером в области инновационных решений для многих отраслей промышленности. Наши аналитики обладают экспертным знанием индустрии и достаточным опытом для нахождения наилучшего ответа даже для самых сложных вопросов Вашего бизнеса. Мы фокусируемся на простых, но важных решениях: повышая отдачу от Ваших активов и их эксплуатационные характеристики, снижая общую стоимость владения, ускоряя время начала получения прибыли от проекта, и повышая прибыль его участников.

Вся информация в этом документе является собственностью ARC и защищена авторскими правами. Запрещается воспроизведение документа или его части без предварительного разрешения ARC. Информация, приведенная ARC в этом документе, основана на независимом исследовании.

Вы можете оценить услуги и ценность информации из постоянно проводимых ARC исследований, а также обратиться к опыту наших сотрудников, воспользовавшись нашими Консультативными Услугами. Консультативные услуги компании ARC специально предназначены для людей, ответственных за разработку стратегий и направлений развития для своих организаций. Для получения информации о подписке, пожалуйста, свяжитесь с нами:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Тел: 781-471-1000, Факс: 781-471-1100, Email: info@ARCweb.com
Посетите наш сайт ARCweb.com



3 ALLIED DRIVE DEDHAM MA 02026 USA

BOSTON, MA | PITTSBURGH, PA | PHOENIX, AZ | SAN FRANCISCO, CA