СИСТЕМЫ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ (СИСТЕМЫ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ)

Международные стандарты систем промышленной безопасности:

ANSI/ISA 84.01-96;

DIN V 19520;

V VDE 0801;

IEC 61508;

IEC 61511.

Россия:

РД 03-418-01 Методические указания по проведению анализа риска опасных производственных объектов.

ГОСТ 27.310-95 Анализ видов, последствий и критичности отказов.

Категории взрывоопасности в России.

Requirement Class – RC, Anforderungs Klasse –AK по немецким стандартам DIN.

Safety Integrity Level – SIL по американским стандартам ISA и по стандартам Международной электротехнической комиссии IEC.

СООТВЕТСТВИЕ РОССИЙСКИХ И ЗАРУБЕЖНЫХ КАТЕГОРИЙ ВЗРЫВООПАСНОСТИ ПРОИЗВОДСТВ

Классы RC 4 – 5 – 6 соответствуют нашим III – II – I категориям взрывоопасности. Соответственно,
Уровень безопасности SIL 2 соответствует III категории взрывоопасности.
Уровень безопасности SIL 3 соответствует I – II категориям взрывоопасности.

Строгое соблюдение жестких требований безопасности должно быть непременным условием построения АСУТП непрерывных взрывоопасных технологических процессов нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств.

Признаки аварийной ситуации для котельной

- 1. Давление газа выше нормы.
- 2. Давление газа ниже нормы.
- 3. Давление воздуха ниже нормы.
- 4. Погасание факела газовой горелки.
- 5. Разрежение в топке недостаточно.
- 6. Отключение вентилятора (дымососа).

7. Уровень воды в котле ниже MIN.

- 8. Уровень воды в котле выше MAX.
- 9. Давление пара выше MAX.

10. Давление питательной воды ниже нормы.

11 Температура питательной воды ниже нормы.

Место ПАЗ в АСУ ТП

ПЛАС - Правила Локализации Аварийных Ситуаций

Перегрев
Пожар
Высокое давление
Загазованность
Алгоритм ПЛАС.
Поломка оборудования

Упрощенная функциональная схема ПАЗ печей установки атмосферной переработки нефти ОАО «НК РОСНЕФТЬ» – Туапсинский НПЗ»

Состав ПАЗ:

- датчики (сенсоры);
- логические и вычислительные устройства (контроллеры, ЭВМ);
- исполнительные устройства;
- устройства отображения информации, сигнализации;
- пульты оператора;
- оперативный персонал.

Назначение ПАЗ:

- автоматический перевод технологического процесса (ТП) в безопасное состояние при нарушении предопределенных условий;
- разрешение на продолжение нормальной работы ТП при отсутствии нарушения предопределенных условий;
- осуществление действий, направленных на предотвращение и устранение технологических нарушений;
- защита персонала от вредных и опасных факторов производства;
- архивирование и протоколирование предаварийных и аварийных ситуаций, а также действий оперативного персонала в этих ситуациях;
- выдача предупреждений и рекомендаций персоналу по аварийным ситуациям.

ФАКТОРЫ, КОТОРЫЕ НЕОБХОДИМО УЧИТЫВАТЬ ПРИ ПОСТРОЕНИИ ПАЗ

- 1. Категория взрывоопасности производства.
- 2. Последствия от «опасных» отказов ПАЗ (система не сработала в момент наступления опасного события)
- 3. Последствия от «безопасных» отказов ПАЗ (система ложно сработала и остановила производство при отсутствии опасного события)
- 4. Влияние «человеческого фактора» на производственный процесс.
- 5. Статистика по структуре отказов технических средств автоматизации :
    - Датчик 35 %
    - Контроллер 10 %
    - Исполнительный механизм 55 %

Причины не срабатываний или ложных срабатываний ПАЗ:

- Отказ центрального процессора контроллера;
- Отказ модулей ввода-вывода контроллера или станций распределенной периферии;
- Ошибка в программном обеспечении;
- Ошибки в техническом обслуживании и эксплуатации системы;
- Неправильная калибровка измерительных каналов;
- Неправильно выбранные предаварийные уставки;
- Отказы полевого оборудования (датчики, исполнительные устройства);
- Сбои в электропитании;
- Электромагнитные наводки.

Для объектов III категории взрывоопасности функции защиты технологического процесса могут быть реализованы на **стандартных контроллерах РСУ** при выполнении следующих условий:

- Система защиты реализована на физически выделенных из РСУ (но не из АСУТП) технических средствах;
- Система защиты имеет резервирование по всем основным компонентам:
  - Модули ввода-вывода;
  - Платы контроллеров;
  - Сетевые интерфейсы;
  - Источники питания.

Надежность выполнения функций измерения и защиты для переменных, определяющих взрывоопасность процесса, на взрывоопасных объектах обеспечивается:

- Использованием полевого оборудования, имеющего специальный допуск на применение в системах, обеспечивающих безопасность процесса;
- Установкой дополнительных датчиков в соответствии с категорией взрывоопасности и типом технологического процесса;
- Установкой дополнительных исполнительных элементов;
- Наличием системы автоматизированного обслуживания полевого оборудования – *Plant Asset Management System;*
- Контролем значений технологически связанных параметров.

Применение различных архитектур систем безопасности в зависимости от категории взрывоопасности

Категория взрыво-опасности	RC	SIL	Архитектура системы	Пояснение
III	4	2	Нерезервиро-ванные (1oo1) или резервиро-ванные (1oo2) входы	Периодическое тестирование входов. Входы могут быть аналоговыми или дискретными
			ПЛК 1oo1D, или Стандартные контроллеры РСУ	ПЛК с двумя центральными процессорами или резервированными модулями управления, Или (по согласованию с технадзором) – выделенное резервированное оборудование РСУ
			Нерезервиро-ванные (1oo1) выходы	Периодическое тестирование выходов

Категория взрыво-опасности	RC	SIL	Архитектура системы	Пояснение
II	5	3	Резервированные (1oo2) входы	Оперативное тестирование входов Входы могут быть аналоговыми или дискретными
			Архитектуры ПЛК 1oo2D, 2oo3	Полностью резервированные (дублированные, троированные) системы
			Нерезервированные (1oo1) выходы	Оперативное тестирование выходов
I	6	3	Резервированные (1oo2 или 2oo3) входы	Оперативное тестирование входов Голосующие входы – аналоговые
			Архитектуры ПЛК 1oo2D, 2oo3	Полностью резервированные (дублированные, троированные) системы
			Резервированные (1oo2) выходы	Оперативное тестирование выходов

Для объектов III категории взрывоопасности (SIL2 и RC4) от системы требуется наличие самодиагностики, сторожевого таймера. Дополнительно не исключается возможность резервирования сенсоров, и с одним конечным управляющим устройством.

Приемлемый вариант по согласованию с территориальным органом Ростехнадзора – выделенное резервированное оборудование РСУ с резервированием модулей ввода-вывода, модулей управления, сетевых плат, источников питания.

Для объектов I и II категории взрывоопасности (SIL3 и RC 5-6) классический выбор – системы защиты с архитектурами 1oo2D и 2oo3 с дублированием сенсоров и управляющих устройств.

Для объектов всех категорий взрывоопасности настоятельно рекомендуется применение системы обслуживания полевого оборудования – *Plant Asset Management System*. Для объектов I и II категории взрывоопасности это должно быть обязательное требование.

Техническое задание на создание АСУТП в обязательном порядке согласовывается с территориальным органом Ростехнадзора. ***И самое главное:***
Вне зависимости от наличия и содержания западных сертификатов, разрешение Ростехнадзора имеет безоговорочный приоритет.

Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор) при выдаче Разрешений на применение технических устройств для создания автоматизированных систем управления и противоаварийной защиты не делает подразделения по категориям взрывоопасности объекта.

Таким образом, Разрешение Ростехнадзора подразумевает право на применение технических устройств на объектах всех категорий взрывоопасности.

Резервирование электропитания. Электропитание оборудования АСУТП, включая и полевое оборудование КИПиА, должно обеспечиваться от двух независимых источников. На случай отключения основных источников электроэнергии в качестве третьего независимого источника должен быть предусмотрен источник бесперебойного питания (UPS), способный обеспечить электропитанием полевое оборудование КИПиА и основное оборудование РСУ и ПАЗ, чтобы произвести перевод технологического объекта в безопасное состояние в течение наперед заданного интервала времени.

Запрещение на ведение технологических процессов и работу оборудования с неисправными или отключенными системами контроля, управления и защиты. Согласно ПБ 09-540-03 п. 6.9.2, запрещается ведение технологических процессов всех категорий взрывоопасности, а также работа оборудования с неисправными или отключенными системами контроля, управления и защиты.

Кратковременное отключение защиты. Допускается в исключительных случаях для непрерывных процессов по **письменному распоряжению** ***главного инженера данного производства / установки*** (вместо руководителя предприятия по п. 6.9.3 ПБ) кратковременное отключение защиты по отдельному параметру, и только в дневную смену.

Дополнительные оперативные панели ПАЗ. Кроме средств визуализации РСУ, для систем ПАЗ необходимо предусматривать панели, которые оснащаются средствами для оперативной выдачи команд управления блокирующими устройствами, операциями пуска-останова, и сигнализацией состояния блокировок, исполнительных органов и источников энергопитания.

Световая и звуковая сигнализация о загазованности воздушной среды. Во взрывоопасных помещениях и снаружи перед входными дверями предусматривается световая и звуковая сигнализация о загазованности воздушной среды.

Для контроля загазованности в производственных помещениях, рабочей зоне открытых наружных установок должны устанавливаться средства автоматического газового анализа с сигнализацией предельно допустимых концентраций.

Все случаи загазованности должны фиксироваться в АСУТП *(а не просто регистрироваться приборами, как сказано в пункте 6.4.1 ПБ 09-540-03).*

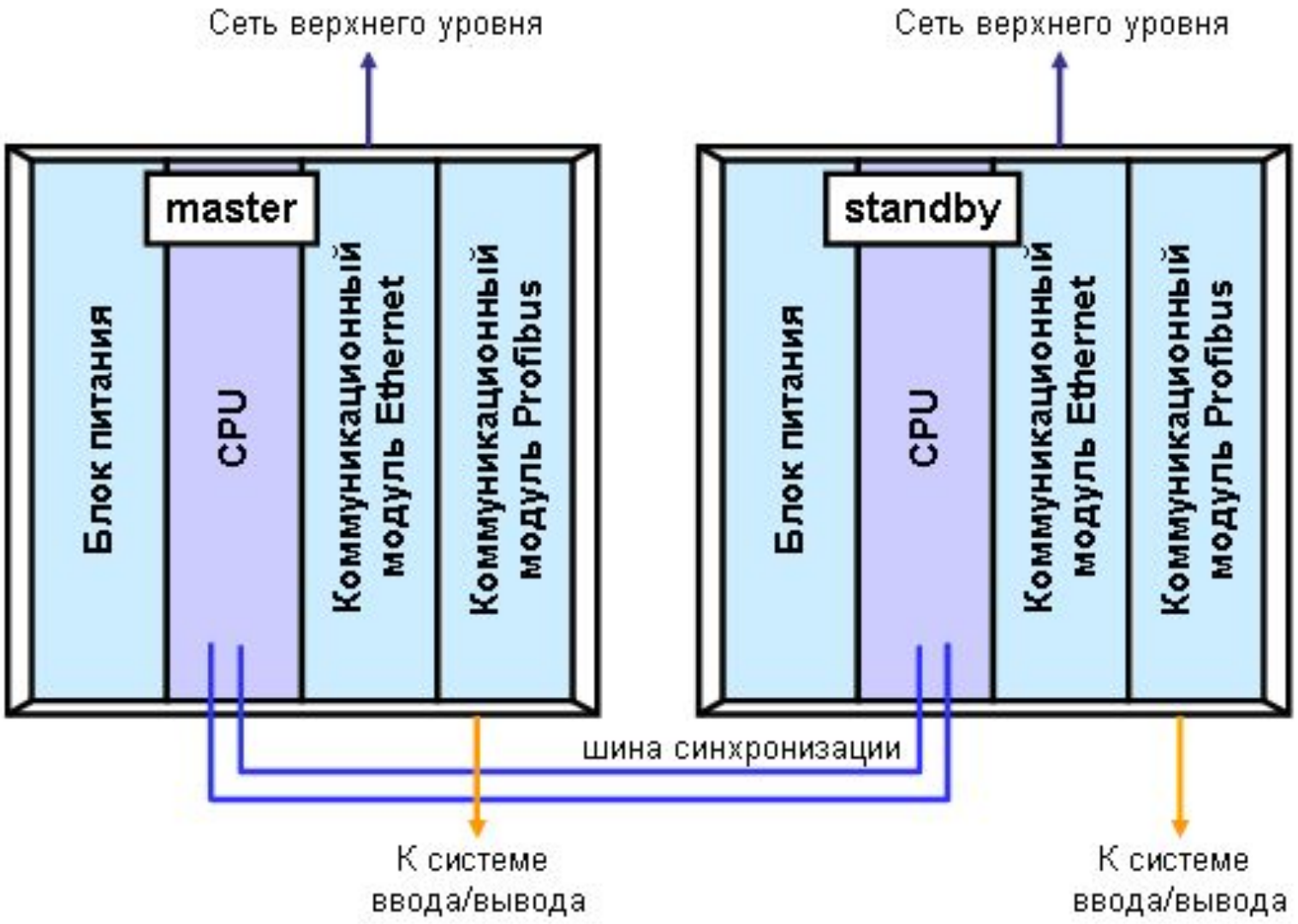
Хорошо спроектированные системы для решения критических задач безопасности находят **баланс между безопасностью и надежностью** посредством выбора адекватного резервирования, и высоким уровнем диагностики полевого оборудования и программируемых логических устройств. Целостность системы после запуска обеспечивается правильным выбором частоты и глубины тестирования.

Но самое главное – квалифицированным персоналом.

Ведущие фирмы-производители систем **ПАЗ**

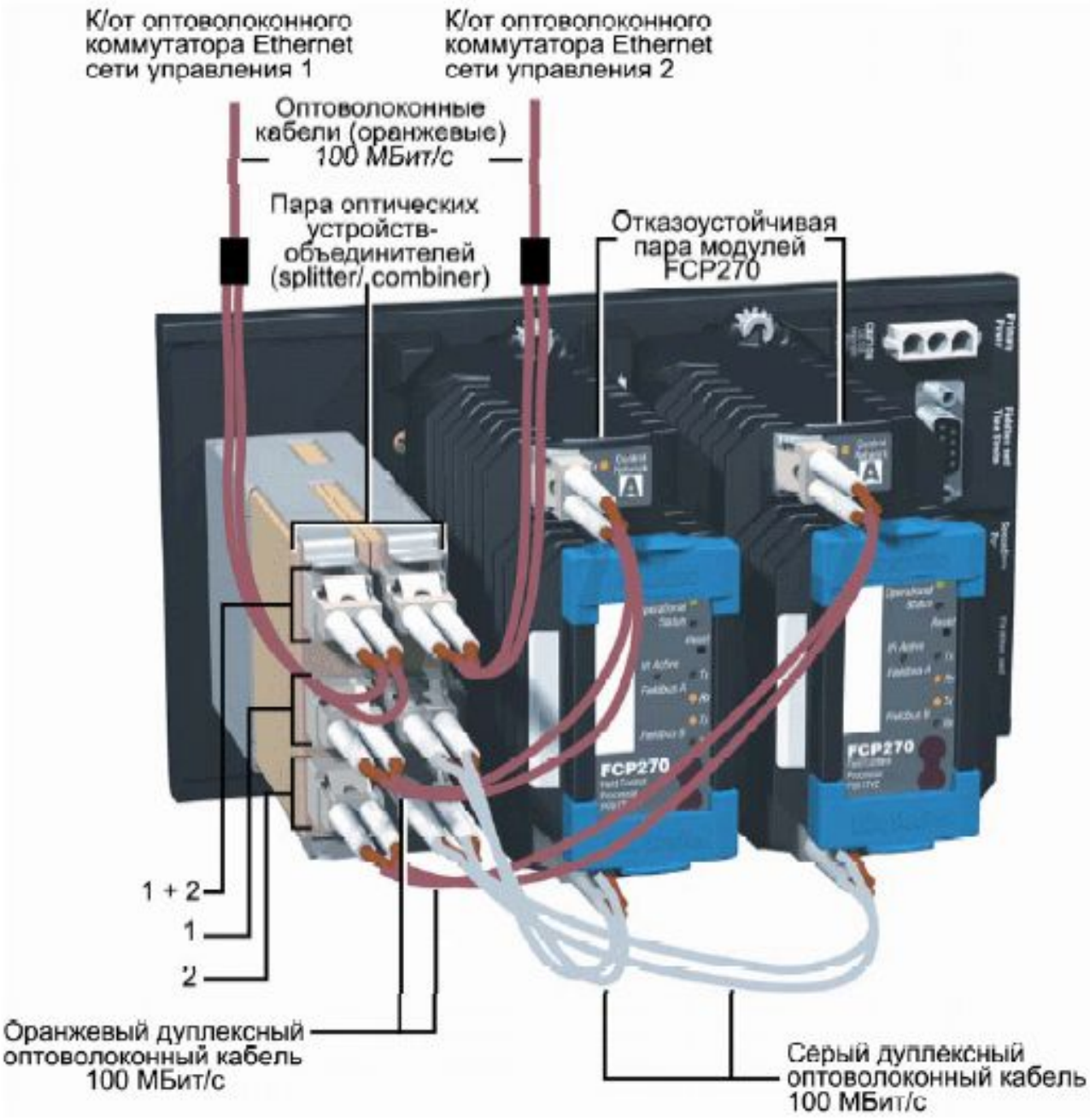
- ABB
- HIMA
- Honeywell
- Siemens Energy & Automation
- Yokogawa.
- GE-Fanuc
- ICS
- Triconex.

Резервированный контроллер



Резервированный контроллер Simatic S7-400H

Резервированный контроллер FCP270 фирмы FOXBORO



МЕРЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПОЛЕВОГО ОБОРУДОВАНИЯ

- 1. Постоянное сравнение показаний резервированных аналоговых датчиков. Сигнализация или останов процесса при слишком больших расхождениях.
- 2. Сравнение показаний датчиков безопасности со значениями связанных технологических параметров. Сигнализация при неправдоподобных изменениях.
- 3. При каждом предаварийном останове программный контроль согласованности показаний датчиков и условий останова.
- 4. Сигнализация оператору о любых нарушениях регламентной процедуры останова.
- 5. Извещение оператора, если исполнительное устройство не сработало в отведенное время.
- 6. Извещение оператора если исполнительное устройство сработало без соответствующей команды системы ПАЗ.
- 7. Периодическое тестирование элементов, находящихся длительное время в неизменном состоянии.
- 8. Классификация, сигнализация и архивирования всех событий, изменений в системе ПАЗ.

ЯЗЫК ПРОГРАММИРОВАНИЯ КОНТРОЛЛЕРОВ ПАЗ

Для разработки систем противоаварийной защиты, как правило, используется язык

Ladder Logic Diagrams –

Графические средства описания логических схем (лестничные диаграммы).

Проблемно-ориентированные языки высокого уровня, позволяющие:

- Создавать программы произвольной структуры,
- Оперативно их корректировать,
- Сохранять результаты решения задач в базе данных,
- Организовывать запуск задач по запросу и по времени с соответствующими приоритетами, –

для разработки прикладных программ защиты, как правило, не используются. И это правильно. Так как при создании систем противоаварийной защиты необходимо в максимально возможной степени ограничивать число степеней свободы.

Для подтверждения того, что прикладное программное обеспечение удовлетворяет Спецификации требований безопасности, предусматривается следующее:

- Анализ проекта, демонстрирующий, что все требования, установленные в Спецификации требований безопасности, нашли свое воплощение в проекте;
- Анализ алгоритмов, реализующих функции защиты;
- Разработка специальных тестов для проверки реакции программного обеспечения на обработку данных, выходящих за нормальные границы; на команды, на вводы данных с клавиатуры, и другие действия;
- Программное обеспечение должно быть протестировано для определения его реакции на присутствие аппаратных дефектов.

Диагностика ПАЗ

Диагностические тесты. Диагностика может быть выполнена с помощью разнообразной комбинации методов, включая:

- Автоматические встроенные тесты, предусмотренные в пределах приобретенного оборудования ПАЗ (например, внутренние тесты модулей ввода-вывода);
- Автоматический тест, встроенный как часть специфического проекта (например, контрольное чтение выходных сигналов через входные точки);
- Сторожевые таймеры, сравнение сигналов, обнаружение обрывов и т.п.;
- Сравнение резервированных сигналов.

- Процедура тестирования должна быть максимально простой и быстрой;
- Замена дефектных компонентов должна производиться в реальном времени;
- Процедура замены должна быть простой и понятной, чтобы провести ее быстро и безошибочно;
- Кроме того, должна быть продумана процедура деблокировки полевых устройств с целью поверки, калибровки и обслуживания.

Ограничение доступа к элементам ПАЗ

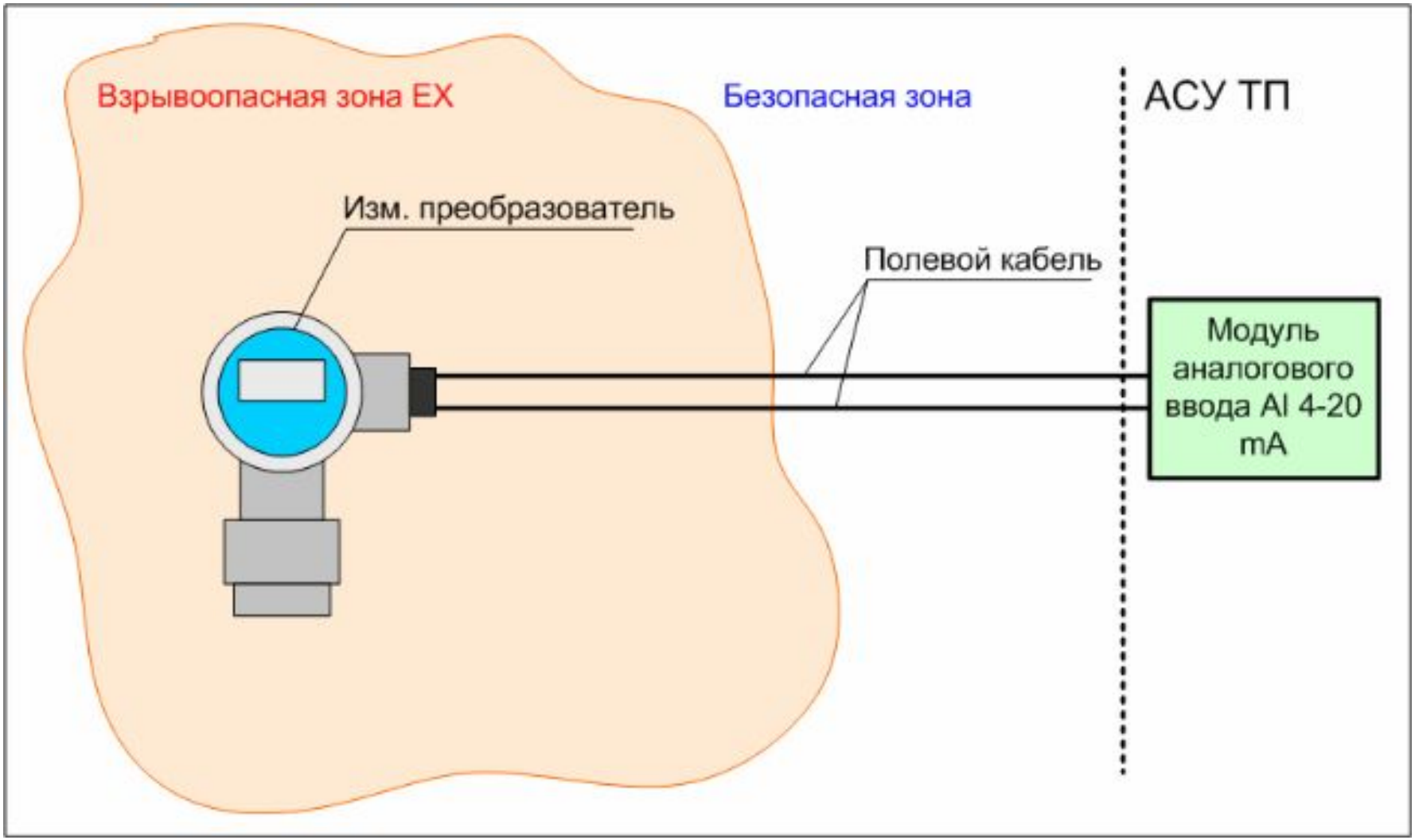
Должны быть предусмотрены специальные средства контроля над доступом к системе безопасности, включая все главные компоненты системы:

- Логические решающие устройства;
- Интерфейсы технического обслуживания;
- Функции тестирования системы ПАЗ;
- Функции деблокировки;
- Отключение тревожной сигнализации ПАЗ;
- Сенсоры;
- Конечные исполнительные элементы.

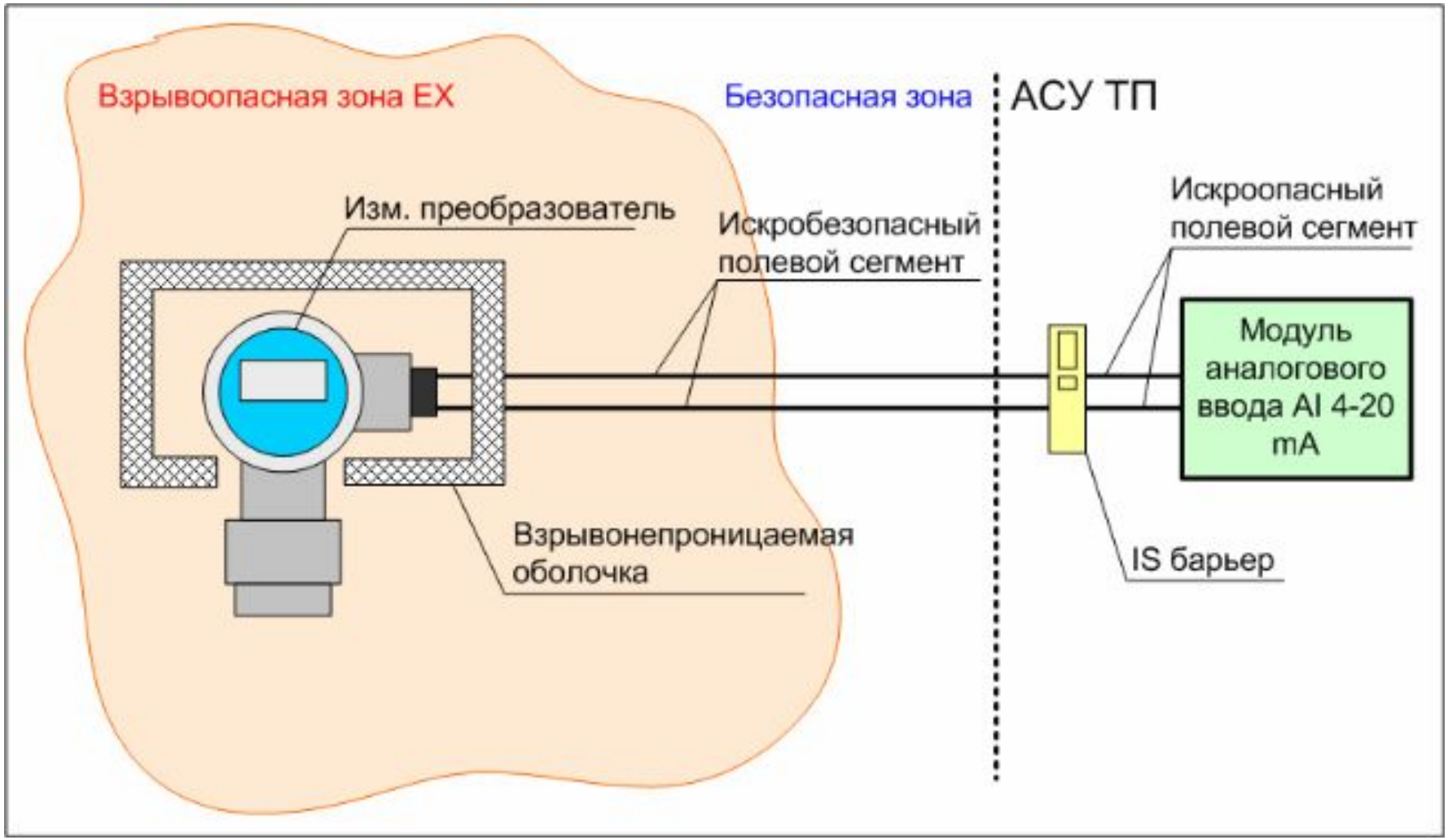
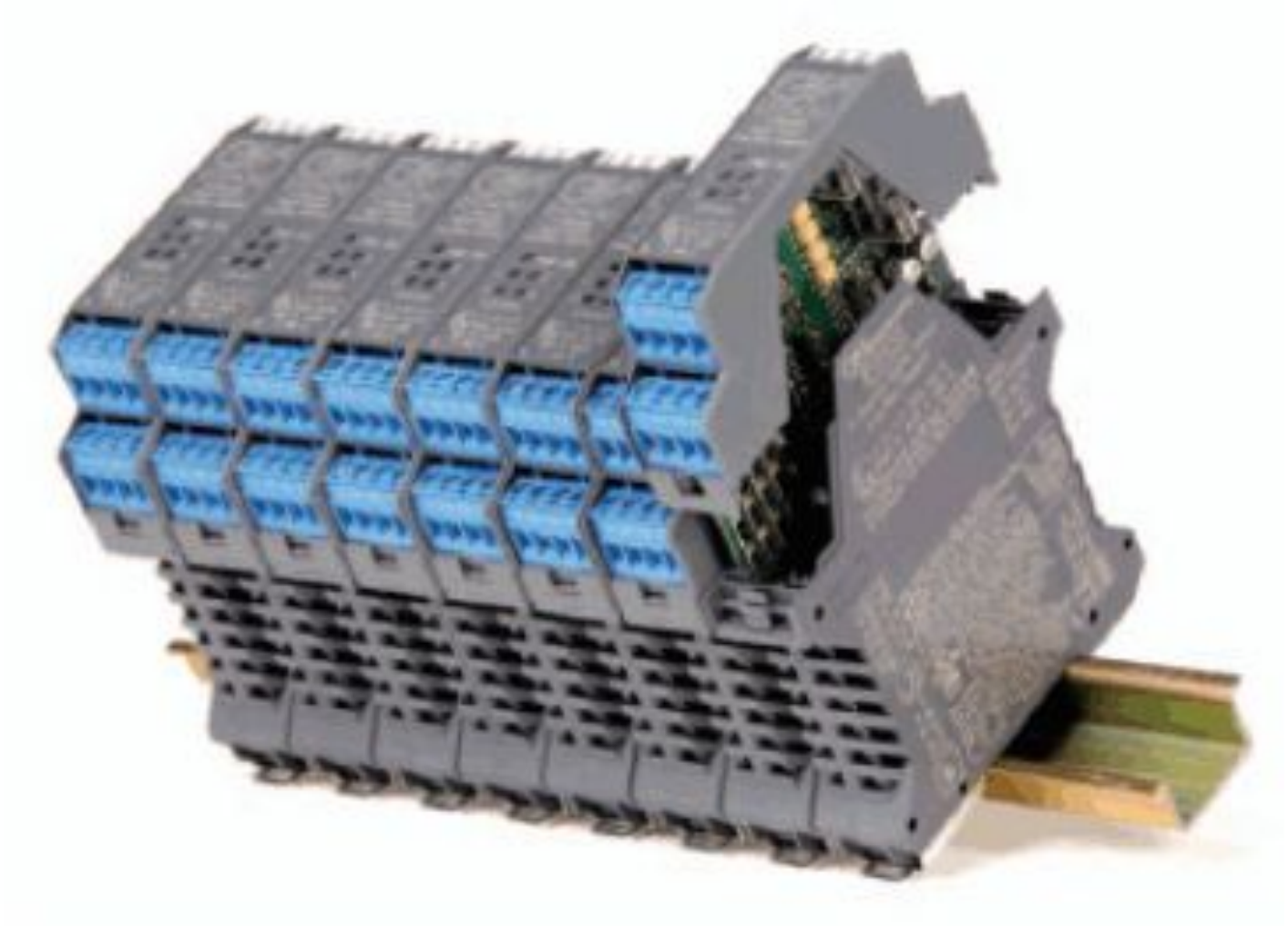
Защита доступа может предусматривать:

- Стойки системы – под замок и на физический ключ;
- Доступ "только чтение";
- Коды доступа, Пароли;
- Административные ограничения и т.п.

РАБОТА АППАРАТУРЫ АСУТП ВО ВЗРЫВООПАСНОЙ ЗОНЕ



ВЗРЫВОЗАЩИТНОЕ ОБОРУДОВАНИЕ АСУТП



Барьеры искробезопасности компании GM International