НПП Промышленная Автоматизация

105077, г. Москва, ул. Средняя Первомайская, д.34, офис 3.
тел.: +7 (495) 603-8394, 603-8365
факс: +7 (495) 540-9708
E-mail: mail@indautomation.ru
web: www.indautomation.ru

Rockwell Automation
Authorized System Applicator and Solution
Allen-Bradley ROCKWELL SOFTWARE
Industrial Automation Products

ALLEN-Bradley Rockwell Automation

ControlLogix5555™ SIL 2

Системы СБ и ПАЗ

МОСКВА 2006

СОДЕРЖАНИЕ

ВВЕДЕНИЕ/ОБЩИЕ ПОЛОЖЕНИЯ

Сегодня промышленное производство столкнулось с ужесточением стандартов и правил безопасности в комплексе с жесткой конкуренцией по снижению себестоимости продукции и улучшению качества. Промышленное производство нуждается в безопасных, надежных системах СБ И ПАЗ для технологических установок с целью обеспечения безопасности персонала, собственности, окружающей среды и репутации. Использование в качестве систем СБ И ПАЗ оборудования ControlLogix™ производства Allen-Bradley, прошедшего сертификацию по Уровню Совокупной Безопасности (Safety Integrity Level (SIL)) 2 TUV, делает это проще, легче и быстрее, что позволяет соответствовать ужесточающимся стандартам и требованиям во всем мире.

1.1 Системы сертификации

1.1 SIL

Уровень **SIL** (Safety Integrity Level) - это цифровое обозначение, присваиваемое системе безопасности, которое отражает способность системы обеспечивать функции безопасности. Стандартом IEC 61508 определено четыре уровня безопасности. Чем выше уровень SIL, тем выше вероятность выполнения системой задачи обеспечения безопасности.

SIL	Требуемая надежность	Вероятность ошибки при выполнении заданной задачи (PFD)	Фактор снижения риска (RRF)
SIL 4	> 99.99 %	>= E-005 … < E-004	100 000 … 10 000
SIL 3	99.90 %	>= E-004 … < E-003	10 000 … 1 000
SIL 2	99.00 – 99.90 %	>= E-003 … < E-002	1 000 … 100
SIL 1	90.00 – 99.00 %	>= E-002 … < E-001	100 … 10

Качественно SIL может быть рассмотрен как вероятный ущерб, нанесенный персоналу, предприятию и обществу в случае ошибки системы безопасности:

«1» - Требуется незначительная защита Оборудования и Продукции.
«2» - Требуется значительная защита Оборудования и Продукции. Защита от возможных травм у обслуживающего персонала.
«3» - Требуется защита обслуживающего персонала и Общества (не катастрофическое воздействие).
«4» - Требуется защита от катастрофического воздействия на Общество.

Выбор требуемого уровня SIL для конкретного производства – это корпоративное решение, основывающееся на философии управления производством и уровне риска.

Сертификация оборудования ControlLogix ™ для уровня SIL 2 по TUV, подтверждает пригодность оборудования ControlLogix™ для использования в системах с уровнем безопасности по SIL 2:

- системы СБ и ПАЗ
- системы газовой и пожарной безопасности
- системы предотвращения выбросов
- системы контроля потоков

- системы управления и защиты компрессоров
- парки резервуаров
- буровые установки
- трубопроводы
- процессинг (непрерывное производство)
- бурение
- распределение электроэнергии
- очистка
- утилизация водных сбросов

В типовых отраслях промышленности:

- нефте-газо добыча
- нефтепереработка, нефтехимия
- химия
- энергетика

1.2 TUV

Сертификация TUV Anlagentechnik GmbH базируется на соответствии с требованиями стандарта IEC 61508 “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”(“Функциональная Безопасность Электронных/ Электрических/ Программируемых Электронных систем безопасности”). Она также включает в себя независимые от применения стандарты DIN V 19250 и VDE 0801, prEN 50156 для применения в системах ESD (СБ и ПАЗ), DIN EN 54 для систем газовой и пожарной безопасности, стандарты по электробезопасности и охране окружающей среды IEC 61131-2, EN 50178, EN 50081-2, EN 61000-2:2000.

TUV Anlagentechnik GmbH – единственное независимое агенство в мире, сертифицирующее инструментальные системы безопасности Safety Instrumented Systems (SIS). TUV уполномочен и авторизован законом как технический инспектор для разнообразных технических систем, включая инжиниринг безопасности для промышленных предприятий, процессов и продуктов во время производства и применения. Если продукт протестирован и соответствует строгим техническим требованиям, то он утверждается и сертифицируется по восьми классам (AK) 1-8. Эта сертификация требуется в большинстве европейских государств и все чаще запрашивается в других странах мира и США. Производитель оборудования предоставляет сертификат с детальным отчетом о инспекции и тестировании.

Соответствие между Уровнем Совокупной Безопасности SIL и классом TUV приведено в таблице:

SIL	**1**		**2**	**3**		**4**
TUV Class	**AK2**	**AK3**	**AK4**	**AK5**	**AK6**	**AK7**

TUV сертифицировал различные архитектуры логических устройств систем безопасности исходя из уровня резервирования контуров безопасности:

Таблица 1.

Поз.	Конфигурация	Утвержденный TUV режим работы	Утвержденный класс безопасности TUV	Частота нарушения технологического режима		TUV разрешенное время для восстановления логического устройства
				высокая	низкая	
1	1oo2	2-0	АК5 АК6	+		Отсутствует
2	2oo2	Не утвержден	Не утвержден		+	Отсутствует
3	1oo2D	2-1-0	АК5	+		72 часа
4	2oo2D	2-0	АК6	+		Отсутствует
5	1oo3	3-0	АК5 АК6	+		Отсутствует
6	2oo3	3-2-1-0	АК5 АК6		+	1500 часов

Поз. 1. Конфигурация 1oo2 (дублированный логический контур по схеме «ИЛИ», срабатывание СБ И ПАЗ при появлении сигнала опасного уровня в одном из контуров), для класса безопасности АК5, АК6 разрешается работа СБ И ПАЗ в случае исправности обоих контуров, режим (2-0).

Поз. 2. Конфигурация 2oo2 (дублированный логический контур по схеме «И», срабатывание СБ И ПАЗ при появлении сигнала опасного уровня в обоих контурах). Данная структура не утверждена по TUV для классов АК5, АК6.

Поз. 3. Конфигурация 1oo2D (дублированный логический контур по схеме «ИЛИ» с диагностикой, срабатывание СБ И ПАЗ при появлении сигнала опасного уровня в одном из логических контуров), при обнаружении неисправности в одном из контуров для класса безопасности АК5 разрешается работа СБ И ПАЗ в течение 72 часов, которые даются на устранение неисправности (замену модуля), режим (2-1-0).

Поз. 4. Конфигурация 2oo2 (дублированный логический контур по схеме «И», срабатывание СБ И ПАЗ при появлении сигнала опасного уровня в обоих контурах). При обнаружении неисправности в одном из контуров для класса безопасности АК6 не разрешается работа СБ И ПАЗ, требуется остановка технологии, режим (2-0).

Поз. 5. Конфигурация 1oo3 (троированный логический контур по схеме «ИЛИ», срабатывание СБ И ПАЗ при появлении сигнала опасного уровня в одном из контуров), при обнаружении неисправности одного из контуров для класса безопасности АК5, АК6 не разрешается работа СБ И ПАЗ, режим (3-0).

Поз. 6. Конфигурация 2oo3 (троированный логический контур по схеме «два из трех», срабатывание СБ И ПАЗ при появлении сигнала опасного уровня в двух из трех контуров), при обнаружении неисправности одного из контуров для класса безопасности АК5, АК6 разрешается работа СБ И ПАЗ в течение 1500 часов до устранения неисправности, при этом система деградирует до архитектуры 1oo2, режим (3-2-1-0).

2. Сертификация оборудования Allen-Bradley.

2.1 Надежность через дизайн.

В отличие от других производителей для получения сертификации семейства ControlLogix™ по SIL 2, компания Rockwell Automation не нуждалась в создании специальной линии оборудования, разработанной в соответствии с требованиями SIL 2. Глубокая диагностика и высокий уровень надежности является стандартом для процессоров ControlLogix™, модулей ввода/вывода и коммуникации. Таким образом, стандартный дизайн легко обеспечивает надежность, необходимую для достижения сертификации по SIL 2.

2.2 Стандартный дизайн приносит дополнительную экономию.

Сертификация по SIL 2 получена для стандартного оборудования семейства ControlLogix™, что не требует дополнительного обучения персонала, отсутствуют проблемы с запасными частями. Вот почему большинство ведущих нефтехимических компаний используют сегодня ControlLogix™, экономя более 80% по сравнению со стоимостью других решений.

Независимые исследования подтвердили, что Доля Безопасных и Опасных Обнаруживаемых Отказов в Общем Количестве Отказов (Safe Failure Fractions (SFF)) процессора превышают 95%. Диагностика модулей ввода/вывода, включая выходы, с функцией пульс-теста для проверки работоспособности, обеспечивает упреждающие сообщения о потенциальных нарушениях до того, как они произойдут.

Анализ промышленных испытаний подтверждает высокую надежность, включая высокое Среднее Время Наработки на Отказ (Mean Time Between Failures (MTBF)). Например, компоненты ControlLogix™ для единичного контура безопасности 24 VDC имеют значение MTBF более одного миллиона часов или 100 лет до первого возможного отказа! Также полевые испытания по измерению Вероятности Ошибки в Выполнении Заданной Функции Безопасности (Probability of Failure on Demand (PFD)) достигают значения 10^{-6}. Такая эффективность устанавливает новые стандарты по надежности и производительности – увеличение безопасности, продуктивности и прибыли за счет уменьшения времени простоев, неплановых остановов.

Тестирование оборудования и программного обеспечения ControlLogix™ 5555 выполнены компанией TUV Anlagentechnik GmbH. В результате испытаний 2002-09-30 получен сертификат № 968/EZ 135.00/02, позволяющий использовать ***нерезервированный*** вариант ControlLogix™ для построения систем управления и СБ И ПАЗ.

Rockwell Automation также производит широкий спектр как продуктов безопасности от сенсоров безопасности до Процессоров безопасности по SIL 3, так и систем безопасности в комплексе.

2.3 Сертифицированное оборудование семейства ControlLogix™.

Следующее оборудование ControlLogix™ сертифицировано для использования в приложениях по SIL 2:

Таблица 2.

Category	Catalog Number	Description	Series	Firmware Revision
Controllers	1756-L55M13	Logix processor w/ 1.5Mb memory	A	10.27 11.32
	1756-L55M16	ControlLogix 5555 Controller w/ 7.5Mb memory	A	10.27 11.32
Communication Modules	1756-CNB / -CNBR	ControlNet Communication Modules	D	5.27 5.38
	1756-DHRIO	DH+/RIO Bridge / Scanner Module	C	5.3
	1756-ENBT	Ethernet Communication Module	A	1.33
Digital I/O Modules	1756-IA16I	120vac Isolated Input Module	A	2.2
	1756-IA8D	120vac Diagnostic Input Modules	A	2.6
	1756-IB16D	24vdc Diagnostic Input Module	A	2.6
	1756-IB16I	24vdc Isolated Input Modules	A	2.2
	1756-IB32	DC Input - 32pt	B	3.5
	1756-OA16I	120vac Isolated Output Module	A	2.1
	1756-OA8D	120vac Diagnostic Output Module	A	2.4
	1756-OB16D	24vdc Diagnostic Output Module	A	2.3
	1756-OB16I	24vdc Isolated Output Module	A	2.1
	1756-OB32	DC Output - 32pt	A	2.4
	1756-OB8EI	24vdc Isolated Output Module	A	2.3
	1756-OW16I	N.O. Isolated Relay Output - 16Pt	A	2.1
	1756-OX8I	Isolated Relay Output Module	A	2.1
Analog I/O Modules	1756-IF16	Single-ended Analog Input Module - 16pt	A	1.5
	1756-IF6I	Isolated Analog Input Module - 6pt	A	1.9
	1756-IF8	Analog Input Module	A	1.5
	1756-IR6I	RTD Input Module	A	1.9
	1756-IT6I	Thermocouple Input Module	A	1.9
	1756-IT6I2	Enhanced Thermocouple Input Module	A	1.11
	1756-OF6CI	Isolated Analog Output Module- Current - 6pt	A	1.9
	1756-OF6VI	Isolated Analog Output Module- Voltage - 6pt	A	1.9
	1756-OF8	Analog Output Module	A	1.5
System Components	1756-A4, A7, A10, A13 and A17	ControlLogix Chassis	B	N/A
	1756-PA75	120vac Standard Power Supply	A	N/A
	1756-PA75R	120vac Redundant Power Supply	A	N/A
	1756-PB75	24vdc Standard Power Supply	A	N/A
	1756-PB75R	24vdc Redundant Power Supply	A	N/A
	1756-PSCA	Power Supply Chassis Adapter	A	N/A
	1756-PSCA2	Redundant Power Supply Chassis Adapter	A	N/A

3. Выбор структуры и оборудования системы СБ и ПАЗ.

В вопросе выбора изначально справедливо ориентироваться на оборудование, сертифицированное по TUV, т.к. требования Госгортехнадзора к системам СБ И ПАЗ не имеют специальных требований по надежности к оборудованию систем безопасности.

При выборе структуры систем СБ И ПАЗ чрезвычайно важно точно определиться с требуемым уровнем SIL для вашего производства, точно определить последствия и вероятность отказа системы СБ И ПАЗ.

С одной стороны, заниженный уровень SIL и экономия на средствах системы безопасности, использование средств автоматизации, не предназначенных (не сертифицированных TUV) для работы в качестве систем безопасности, приводит к тому, что производство будет функционировать за порогом своего риска, подвергая повышенной опасности персонал, окружающую среду и/или свои капиталовложения.

С другой стороны, выбор логического устройства с высоким SIL может существенно уменьшить объем средств, предназначенных на закупку полевого КИП, отсечной арматуры, оборудования средств искрозащиты, предназначенных для работы с логическим контроллером, в комплексе образуя «систему» СБ и ПАЗ.

На практике нередки случаи, когда высоконадежные троированные логические устройства, расположенные в кондиционируемых помещениях, работают в комплексе с ненадежными нерезервированными датчиками и исполнительными механизмами, располо-

женными на открытых установках под воздействием низких и высоких температур, агрессивных сред, высокой влажности, вибрации и т.д.

В настоящее время любые неоправданные затраты недопустимы и вопрос увеличения надежности системы СБ и ПАЗ должен рассматриваться в **КОМПЛЕКСЕ** с датчиками, исполнительными механизмами, системой электроснабжения, соответствующей подготовкой персонала, своевременным тестированием компонентов системы безопасности и прочими техническими и организационными мероприятиями.

4. Система СБ и ПАЗ на оборудовании ControlLogix™.

Сертификация TUV позволяет использовать в приложениях по SIL 2 нерезервированные контроллеры ControlLogix™, построенные из состава оборудования, приведенного в Таблице 2.
С другой стороны, предписания Госгортехнадзора требуют независимость СБ И ПАЗ от системы РСУ и дублирование системы безопасности.

В соответствии с этим на выбор проектировщика системы СБ И ПАЗ предлагается два варианта структуры системы:
- структура с резервированными процессорами и нерезервированными модулями ввода/вывода (Рис. 1)
- полностью дублированная система безопасности (Рис. 2) для критических объектов с архитектурой по схеме 1oo2D (голосование один из двух).

Рис. 1. Структурная схема системы СБ И ПАЗ с резервированным центральным процессором и нерезервированными модулями ввода/вывода.

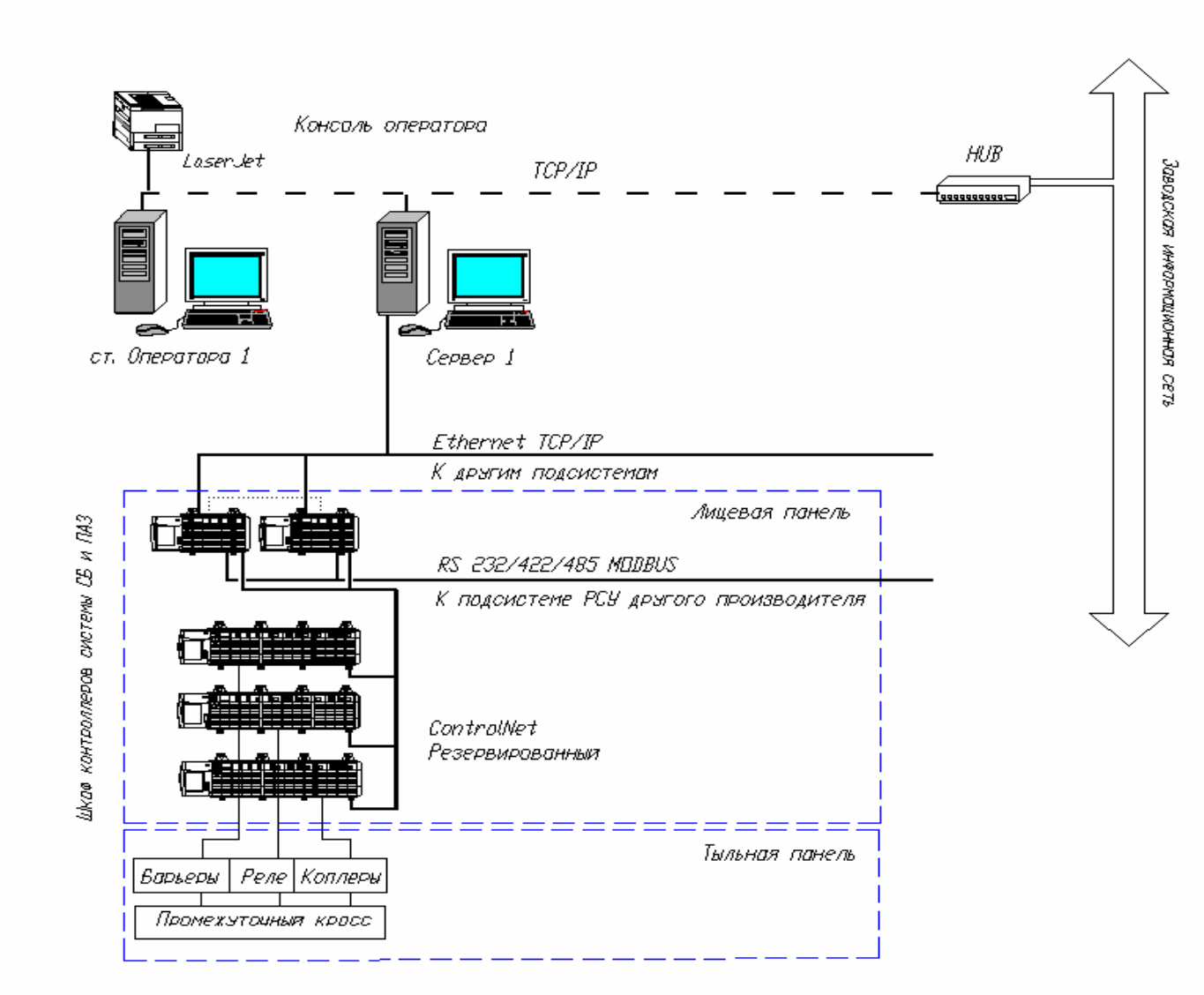
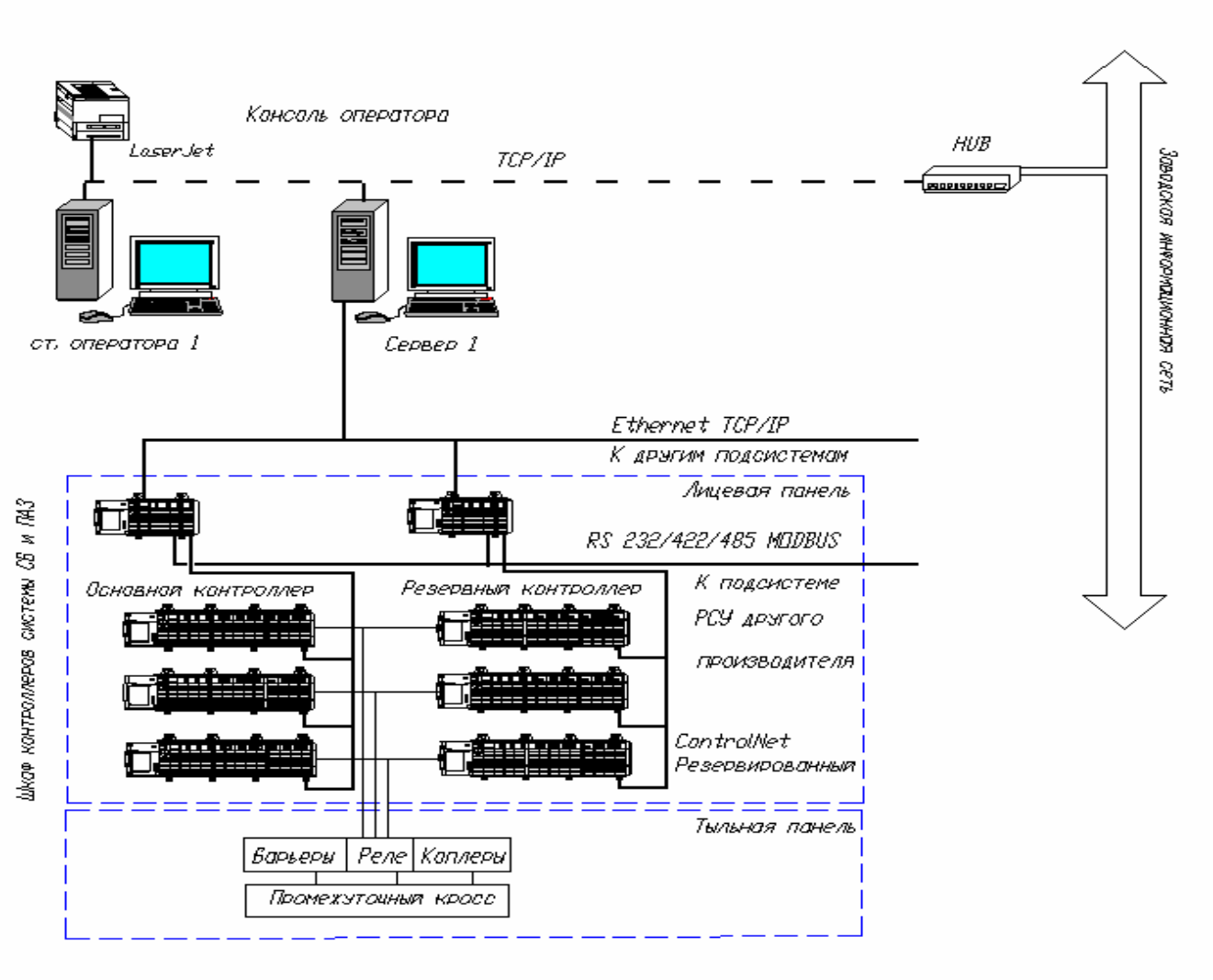


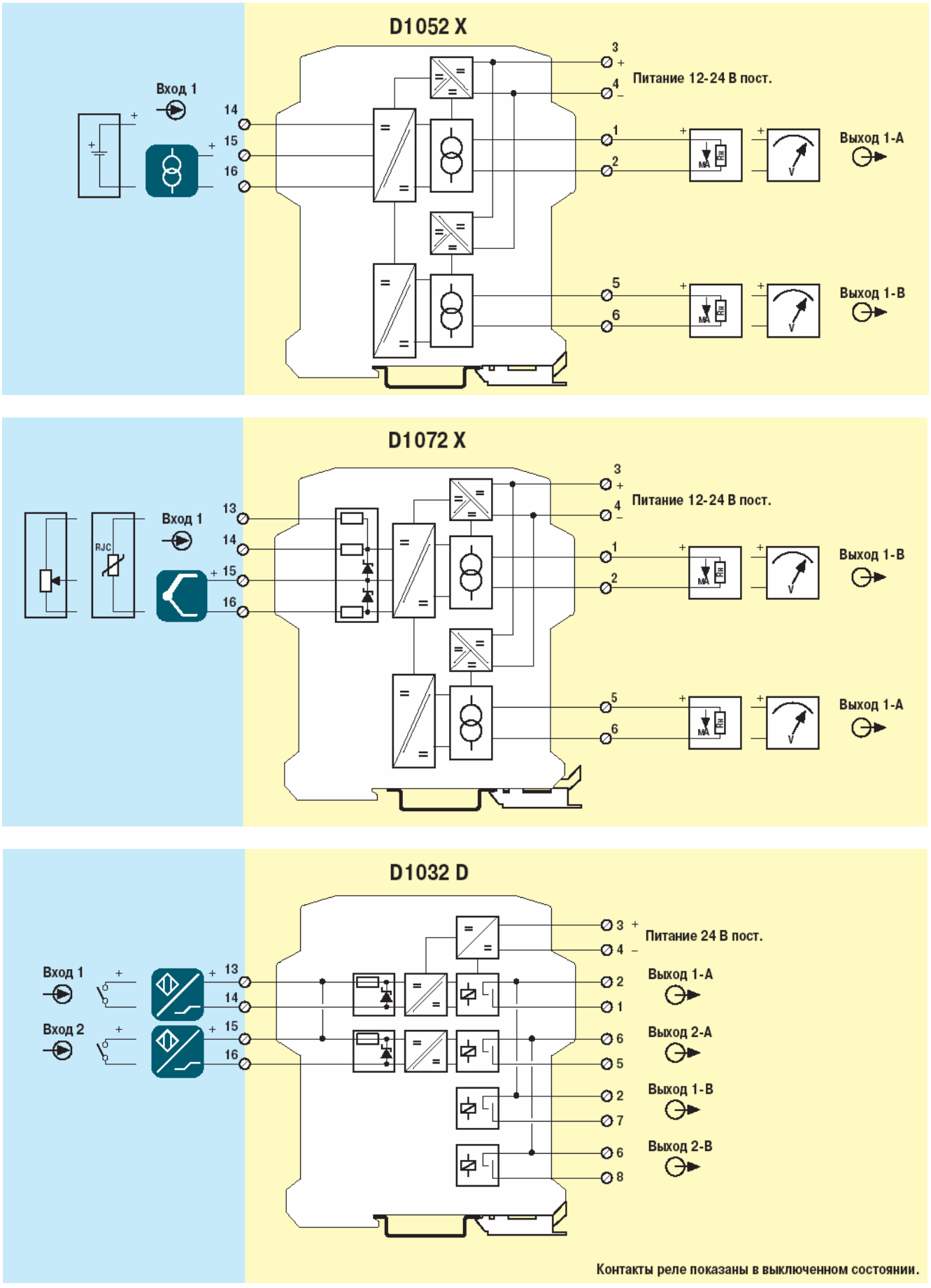
Рис. 2. Структурная схема дублированной системы СБ И ПАЗ.



Для построения систем СБ И ПАЗ используются барьеры искробезопасности производства GM International, сертифицированные по SIL 2, клеммное оборудование, реле, коплеры, дублированные источники питания производства PHOENIX CONTACT, приборные шкафы производства RITTAL.

В дублированной системе применяются барьеры искробезопасности / дубликаторы производства GM International (два независимых выхода для одного входа): D1052X – один аналоговый вход / два аналоговых выхода, D1072X – температурный преобразователь один универсальный вход / два независимых выхода, D1032D – два дискретных входа / четыре независимых выхода.

Рис. 3. Типовые схемы подключения барьеров искробезопасности GM International.



Система электропитания состоит из двух бесперебойных источников питания (PowerWare) соответствующей мощности (трехфазный вход, оборудованный АВР / однофазный выход 220VAC).

Каждый контроллер дублированной системы СБ и ПАЗ питается от своего независимого бесперебойного источника питания.

Применяются независимые дублированные источники питания 24VDC:
- источники питания внешних цепей (дискретные сигналы состояния электрооборудования типа «сухой контакт», не требующие искрозащиты);
- источники питания внутренних цепей (питание активных барьеров, цепей дискретных выходных модулей);
- источники питания приборов КИП в исполнении Exd (сигнализаторы уровня, анализаторы, датчики погасания пламени и т.д.).

Процессоры (основной и резервный) устанавливаются в независимые шасси 1756-A7 с независимыми источниками питания 1756-PA75.

В каждое процессорное шасси 1756-A7 установлено:
- резервированный модуль связи 1756-CNBR для организации внутренней сети ControlNet (5 Мбод) предназначенной для связи процессора с шасси модулей ввода/вывода;
- модуль связи 1756-ENBT для организации информационно-управляющей сети Ethernet/IP (Ethernet Industrial Protocol), связывающей контроллеры ControlLogix5555, станции оператора, СБ и ПАЗ с РСУ (как вариант);
- модуль (и) MVI56-MCM (два универсальных порта RS232/ RS422/RS485) для организации интерфейса с оборудованием других производителей по протоколу MODBUS.

Модули ввода-вывода устанавливаются в одно (или несколько) шасси 1756-A17(A4,A7,A10,A13), укомплектованное (ые) своим источником питания 1756-PA75 и модулем связи 1756-CNBR (Для критических процессов могут быть применены резервированные источники питания 1756-PA75R).

Шасси с модулями ввода/вывода устанавливаются на лицевой стороне приборных шкафов RITTAL 2000x800x600, на тыльной стороне располагаются клеммники, барьеры искробезопасности.

ОБЩИЕ ВЫВОДЫ

- Для построения систем СБ и ПАЗ используйте оборудование, предназначенное и сертифицированное для этих целей;
- Правильный выбор требуемого уровня SIL позволит осуществлять безопасную работу за разумные деньги;
- Система СБ и ПАЗ – это комплексный подход в выборе оборудования от датчика-контроллера до исполнительного устройства.

Приложение A. Копия сертификата TUV

TÜV Rheinland/
Berlin-Brandenburg

TÜV

TÜV Anlagentechnik GmbH
Automation, Software und Informationstechnologie

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 135.00/02

Product tested	Safety Related Programmable Electronic System Control Logix	**Manufacturer**	Rockwell Automation Inc. Automation Control & Information Group 1 Allen-Bradley Drive USA-Mayfield Heights, OH 44124-6118 United States of America
Type designation	Control Logix modules as listed in the Safety Reference Manual, Publication Number 1756-RM001A, Table 1.1	**Intended application**	Safety Related Programmable Electronic System for process control, emergency shut down and where the safe state is typical the de-energized state
Codes and standards forming the basis of testing	IEC 61508, Part 1 - 7:2000 VDE 0801:1990 and Amendment A1:1994 DIN V 19250:1994 prEN 50156-1:CDV 2000 (SIL 2) EN 54-2:1997 EN 61131-2:1994 and Amendment A11:1996, A12:2000 DIN EN 50178 :1998 EN 50081-2:1993 EN 61000-6-2:2000		
Test results	The system is suitable for safety related applications up to SIL 2 (IEC 61508), RC 4 (DIN V 19250) considering the results of the test report no. 968/EZ 135.00/02 dated 2002-09-30.		
Specific requirements	For the use of the systems the test report mentioned above, the Safety Reference Manual, the User Manuals and the actual revision of the official list of product documentation, hardware modules and software components released by Rockwell Automation and approved by TÜV Rheinland have to be considered.		

TÜV Rheinland

Der Prüfbericht Nr. 968/EZ 135.00/02 vom 2002-09-30 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report No. 968/EZ 135.00/02 dated 2002-09-30 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorised to affix the test mark shown opposite to products which are identical with the product tested.

TÜV Anlagentechnik GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

2002-09-30
Date

Company seal

Signature