# О создании конкурентоспособной АСУТП для АЭС нового поколения

**С.И. Антипов, В.П. Сивоконь (ОАО «Концерн Росэнергоатом»)**
**А.Б. Бутко, А.Н. Черняев (АО «ВНИИАЭС»)**

*Рассмотрены новые требования международных стандартов к обеспечению безопасности атомных электрических станций (АЭС), измененная концепция глубокоэшелонированной защиты и соответствующие подходы к проектированию современных конкурентоспособных АСУТП АЭС. Внимание обращено на архитектуру и выбор технических средств систем защиты реактора и проблему кибербезопасности, а также на решение этих вопросов в разрабатываемой АСУТП Курской АЭС-2.*

*Ключевые слова: АСУТП, атомные электрические станции, глубокоэшелонированная защита, кибербезопасность, конкурентоспособность.*

## Введение

В последние годы многие страны, развивающие атомную энергетику, и международные организации, связанные с этой отраслью, активно пересматривают нормативную базу в сторону повышения требований по ядерной безопасности АЭС.

Это вызвано в первую очередь двумя основными причинами:

• тяжелой аварией на АЭС Фукусима в марте 2011 г.;

• массовым повреждением центрифуг обогатительного производства в Иране в 2010 г. новым типом компьютерного вируса, способного фатально поражать промышленные контроллеры, в том числе АСУТП АЭС.

Как показал недавно проведенный анализ [1], уже разработанные и еще разрабатываемые в мире новые требования в части АСУТП АЭС касаются в основном следующих вопросов:

• соответствия архитектуры АСУТП новой концепции глубокоэшелонированной защиты (ГЭЗ), принятой Международным агентством по атомной энергии (МАГАТЭ), согласно стандартам МАГАТЭ по безопасности «Безопасность АЭС: Проектирование», (МАГАТЭ, Вена, 2012 — далее стандарты МАГАТЭ SSR-2/1), и рабочей группой западноевропейских ядерных регулирующих органов (RHWG WENRA), согласно документу Report: Safety of new NPP designs, RHWG WENRA, March 2013 – далее отчет WENRA;

• принципов классификации по безопасности оборудования и систем АЭС, включая АСУТП, приведенных в руководстве IAEA Safety Standards for protecting people and the environment. Specific Safety Guide No. SSG 30. Safety Classification of Structures, Systems and Components in Nuclear Power Plants (IAEA, Vienna, 2014);

• технических характеристик и качества АСУТП, в особенности надежности программируемых подсистем АСУТП, согласно отчету Licensing of safety critical software for nuclear reactors — Common position of seven European nuclear regulators and authorized technical support organisations. Report number: 2010:01, ISSN: 2000-0456 SRSA, January 2010 — далее отчет SENR 2010;01;

• обеспечения кибербезопасности на АЭС (дополнительный фактор, который не позволяет полагаться на высокую надежность аппаратуры АСУТП с ПО) согласно серии изданий IAEA Nuclear Security Series No. 17. Computer Security at Nuclear Facilities, IAEA, Vienna, 2011 — далее IAEA NSS No. 17 и стандарту IEC 62859 Ed. 1.0. Nuclear power plants — Instrumentation and control systems — Requirements for coordinating safety and cybersecurity, IEC, 2014 — далее IEC 62859 Ed. 1.0.;

• обеспечения наибольшей степени разнообразия систем защиты реактора.

Уместно отметить, что каждый раз после серьезной аварии на АЭС и других ядерных установках специалисты возвращались к анализу надежности и эффективности систем безопасности АЭС и вырабатывали соответствующие корректирующие меры. Кстати, в процессе таких усилий и концепция ГЭЗ была внедрена в АСУТП АЭС [2, 3]. Тем не менее, как показали события последних лет, безопасность АЭС пока не достигла уровня, на который многие рассчитывали (в том числе и по вероятностным оценкам безопасности). Поэтому задача дальнейшего усовершенствования систем безопасности (и АСУТП АЭС в целом) остается актуальной.

Рассмотрим предлагаемые новые подходы к обеспечению безопасности и соответствующему построению АСУТП АЭС более подробно.

*Таблица 1. Иллюстрация разделения третьего уровня ГЭЗ на два подуровня 3a и 3b*

| Уровни и подуровни защиты в глубину | | Цель/задача | Основные средства решения задачи | Радиационные последствия | Категории режимов эксплуатации АЭС и соответствующие подсистемы АСУТП |
|---|---|---|---|---|---|
| 3 | 3a | Управление аварией для ограничения радиационных выбросов и защита от условий расплавления активной зоны | Система защиты реактора, системы безопасности, аварийные инструкции | Радиационное воздействие за территорией станции отсутствует или незначительно | Постулируемые единичные исходные события, СБ (аварийная защита – управляющая система безопасности технологическая) |
| | 3b | | Дополнительные функции безопасности, аварийные инструкции | | Выбранные постулируемые исходные события с множественными отказами, ДСЗ (СКУ ЗПУ) и дополнительные аварийные инструкции |

## Новые вызовы и подходы к обеспечению безопасности атомной энергетики. Изменение концепции глубокоэшелонированной защиты

На основании обзора публикаций последних лет можно выделить следующие основные вызовы и подходы к обеспечению безопасности АЭС.

• Постулированная МАГАТЭ и многими регулирующими органами необходимость учета множественных отказов, в том числе в системах безопасности, послужившая причиной разделения уровня три ГЭЗ на подуровни 3a и 3b. Характеристики этого разделения показаны в табл. 1 и описаны ниже. Эволюция концепции ГЭЗ подробно представлена в отчете WENRA, а на рис. 1 показана роль каждого из существующих сегодня пяти уровней ГЭЗ АЭС.

• Требование наличия на уровне 3b дополнительной системы защиты (ДСЗ), которая является основой системы контроля и управления для запроектных условий (СКУ ЗПУ). Она должна выполнять роль минимизации рисков при множественных отказах, включая отказы систем безопасности (СБ) на уровне 3a и быть «диверсной» по отношению к СБ (то есть отличаться от них разнообразием). Такие требования приводят многих разработчиков к предпочтению исполнения ДСЗ на «жесткой логике» (логике на базе электронных схем).

• Недоверие к очень высокой надежности любых программируемых систем безопасности согласно отчету SENR 2010:01.

• Возрастание риска и серьезности киберугроз и, как следствие, потребность в новых подходах и технических решениях в АСУТП для устранения или минимизации последствий этой проблемы согласно серии изданий IAEA NSS No. 17 и стандарту IEC 62859 Ed. 1.0.

• Необходимость полного отделения СКУ ЗПУ и тяжелых аварий от СБ и других подсистем АСУТП, включая их обеспечивающие системы.

В стандартах МАГАТЭ по безопасности АЭС, принятых МАГАТЭ в 2012 г. и детализированных в рабочей группе западноевропейских регулирующих органов в отчете WENRA в 2013 г., предложена усовершенствованная концепция ГЭЗ, ориентированная на дальнейшее повышение безопасности АЭС. В этой концепции сохранено пять известных ранее общепринятых уровней защиты. Серьезному изменению подвергся только уровень 3.

Введено четкое разделение между средствами и условиями действия подуровней защиты в 3a и 3b ГЭЗ. Главное — наличие на уровне 3b дополнительных средств защиты (автоматического и ручного действия) и дополнительных аварийных инструкций.

В качестве дополнительной системы защиты автоматического действия многими разработчиками предлагается упрощенная так называемая «диверсная» системы защиты, минимизирующая риски при отказе СБ на уровне 3a. В табл. 2 показана сравнительная экспертная оценка характеристик различных типов технических средств, которые обычно используются в системах безопасности АЭС и других ядерных установок.

Из табл. 2 вытекают следующие логически обоснованные варианты построения систем защиты на подуровнях 3a и 3b. Системы безопасности реали-

*Таблица 2. Сравнение характеристик, распространенных в АСУТП технических средств для выбора оптимальных решений по реализации СБ и ДСЗ (СКУ ЗПУ)*

| № | **Характеристика** | **Тип 1** Программируемые средства (ПЛК) | **Тип 2** Однократно программируемые микросхемы (FPGA, PLD и т.п.) | **Тип 3** Жесткая логика (логика на электронных схемах) |
|---|---|---|---|---|
| 1 | Вычислительная мощность (реализация сложных функций) | Очень высокая | Высокая | Низкая (для сложных алгоритмов) |
| 2 | Надежность (в области малых вероятностей отказа) | Неизвестная (считается недостаточно надежной для СБ) | Очень высокая | Высокая |
| 3 | Уязвимость к кибератакам | Высокая | Низкая (возможна только при изготовлении) | Отсутствует |
| 4 | Самодиагностика | Очень высокая | Высокая | Низкая (требует дополнительных устройств) |

зуются на технических средствах первого и второго типа, а ДСЗ — в основном на средствах третьего типа. В этом случае принципы разнообразия выполняются как в самих СБ (два комплекта: тип 1 и тип 2), так и в дополнительной системе защиты по отношению к СБ.

### Надежность программируемых СБ и проблема кибербезопасности

Надежность программируемых подсистем АСУТП АЭС, особенно систем безопасности, давно являлась предметом исследований и дискуссий на международном уровне (они, например, отражены в отчете SENR 2010:01 и материалах технического совещания МАГАТЭ [1], специально организованного по этому вопросу).

В последние годы эта проблема сильно усугубилась. С момента появления вирусов нового поколения определить реальную надежность программируемых систем управления, особенно с учетом угрозы преднамеренных кибернетических атак стало практически невозможно.

Совсем отказываться от микропроцессорной техники в АСУТП было бы опрометчиво, поскольку помимо выше указанной слабости она имеет и важные преимущества, отмеченные, например, в табл. 2.

Одним из способов достижения компромисса является комбинирование программируемых и непрограммируемых компонентов с максимально возможным использованием принципа разнообразия для исключения отказов по общей причине.

Однако возникает вопрос, как же все-таки следует относиться к расчетам надежности программируемых СБ, до сих пор предлагаемым надзорным органам некоторыми отечественными и зарубежными разработчиками АСУТП?

Для ответа на этот вопрос уместно привести содержание пункта 1.13.2.2 (Ограничения по заявляемой надежности) из отчета SENR 2010:01. В нем констатируется, что заявления об очень высокой надежности ПО не может быть доказано современными методами. Поэтому должно быть принято решение ограничить заявляемую надежность компьютерных систем. Обзор стандартов в атомной отрасли показывает, что к заявлениям о надежности компьютерных систем выше, чем 10 E-4 (по вероятности отказа на требование) надо относиться с большой осторожностью.

Тем не менее, следует отчетливо понимать, что даже при всех ограничениях и мер по борьбе с отказами по общей причине, принимаемых в АСУТП, обеспечение кибербезопасности не только не теряет своей актуальности, но и остается первоочередной задачей.

Для обеспечения кибербезопасности на АЭС, прежде всего, должна проводиться оценка рисков кибернетических угроз. Она должна включать, по меньшей мере, следующие меры и факторы:

- определение периметра сети АСУТП, по которому возможно несанкционированное воздействие и анализ окружающей этот периметр обстановки;
- определение угроз и их характеристик;
- оценка уязвимостей АСУТП;
- проработка различных сценариев атаки с оценкой уровня рисков;
- определение мер противодействия.

Например, одной из наиболее эффективных защитных мер считается разделение сети АСУТП объекта на сегменты (зоны) с возможным использованием в них разного ПО и контролем передачи данных на границах зон. В проектах АСУТП Курской АЭС-2 это уже предусмотрено.

### Разработка конкурентоспособной российской АСУТП в пилотном проекте для Курской АЭС-2

На основании выполненного обзора требований международных стандартов ОАО «Концерн Росэнергоатом» выпустил в декабре 2014 г. «Требования к базовой части АСУТП ВВЭР-ТОИ», которые легли в основу разрабатываемых в настоящее время АО «ВНИИАЭС» технических заданий на:

- АСУТП энергоблока Курской АЭС-2;
- Общестанционную АСУТП Курской АЭС-2.

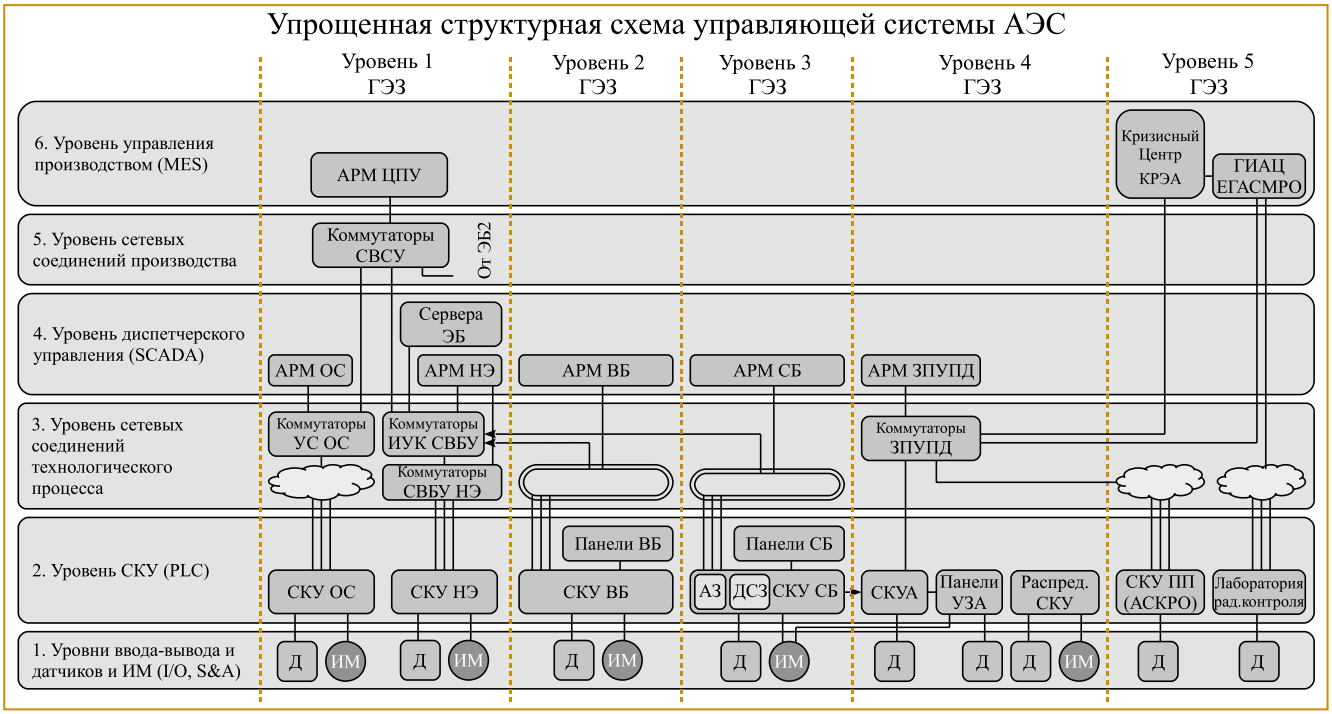
Первые версии этих технических заданий уже выпущены и разосланы на согласование в начале сентября 2015 г. На их основе предполагается разработать технические проекты блочной и общестанционной АСУТП Курской АЭС-2 (осень 2016 г.), которые будут отличаться принципиальной новизной. Эти технические проекты лягут в основу создания конкурентоспособных АСУТП новых АЭС с ВВЭР.

Разработка концептуальной структуры АСУТП находится в заключительной стадии (один из рассматриваемых, наиболее перспективных вариантов показан на рисунке).

Концептуальную структуру АСУТП АЭС можно представить по горизонтали уровнями ГЭЗ, а по вертикали — уровнями управления в соответствии с ГОСТ Р МЭК 62264 «Интеграция систем управления предприятием».

Выделяют следующие уровни управления. Уровень датчиков и исполнительных механизмов, уровень ввода/вывода, уровень ПЛК, уровень диспетчерского управления и уровень управления производственными процессами, далее — уровень систем класса MES. К каждому уровню управления в зависимости от уровня ГЭЗ предъявляются различные требования. При этом по вертикали уровни должны обладать максимальной степенью интеграции, в то время как по горизонтали должны быть максимально независимы.

Выполняемые алгоритмы управления распределены по уровням управления. Так, на уровне ввода/вывода информации (I/O уровень) располагаются технические средства, например, автоматы тепловой защиты, устройства плавного пуска, устройства ограничения тока, устройства защиты от сухого хода и т. д., реализующие в основном простейшие алгоритмы управления. Уровень ПЛК реализует алгоритмы регулирования и функционально-групповое управление, уровень диспетчерского управления и сбора данных




*Упрощенная концептуальная структура АСУТП АЭС, где Д – датчики, ИМ – исполнительные механизмы, СКУ ОС – системы контроля и управления общестанционные, СКУ НЭ – СКУ нормальной эксплуатации, СВБУ – система верхнего блочного уровня, ИУК – информационно-управляющий контур, УС ОС – управляющие системы общестанционные, АРМ ОС – автоматизированные рабочие места общестанционные, ЭБ – энергоблок, СВСУ – система верхнего станционного уровня, АРМ ЦПУ – АРМ центрального пункта управления, ГЭЗ – глубокоэшелонированная защита, АРМ ВБ – АРМ важные для безопасности, АРМ СБ – АРМ систем безопасности, АЗ – аварийная защита, ДСЗ – дополнительная система защиты, ЗПУПД – защищенный пункт управления противоаварийными действиями, СКУА – СКУ при авариях, УЗА – управление запроектными авариями, КРЭА – Концерн Росэнергоатом, СКУ ПП – СКУ противоаварийного планирования, ГИАЦ ЕГАСМРО – главный информационно-аналитический центр единой государственной автоматизированной системы мониторинга радиационной обстановки.*

(SCADA уровень) выполняет сложные (общеблочные) алгоритмы, например, переход с одного уровня мощности на другой, пуск, останов и т.д. На уровне MES реализованы алгоритмы управления АЭС в целом, большинство алгоритмов не входит в состав оперативного управления.

На каждом уровне управления реализован человеко-машинный интерфейс. Для уровня I/O — местные пульты управления и органы управления, расположенные непосредственно в шкафах управления, для уровня ПЛК — панели диспетчерского управления, расположенные в резервной зоне управления на блочный и резервный пункты управления, для SCADA и MES уровня — автоматизированные рабочие места.

Помимо функциональных уровней управления (I/O, ПЛК, SCADA и т.д.) в концептуальной структуре АСУТП АЭС показаны уровни сетевого взаимодействия в связи с предъявляемыми к ним требованиями. На уровнях 1, 4, 5 ГЭЗ применяются недетерминированные протоколы передачи данных множественного доступа с прослушиванием несущей и обнаружением столкновений CSMA/CD, такие как Ethernet. На уровнях 2 и 3, то есть в СБ и в системах нормальной эксплуатации, важных для безопасности, применяются детерминированные протоколы передачи данных CSMA/CA, такие как Token Ring и FDDI.

В соответствии с НП 001 97 «Общие положения обеспечения безопасности атомных станций» технические средства АСУТП первого уровня ГЭЗ концептуальной структуры АСУТП АЭС можно отнести к 4 или 3 классу безопасности в зависимости от выполняемых ими функций, второго уровня ГЭЗ — к 3 классу безопасности, третьего уровня ГЭЗ — к 2 и 3 классу безопасности.

Как видно из рисунка, в структуру АСУТП АЭС внедрены принципиально новые решения на нескольких уровнях ГЭЗ. В проекте предусмотрена ДСЗ, ЗПУПД, который обеспечивает работу персонала и связь с кризисным центром КРЭА и системой мониторинга радиационной обстановки в случае аварийных ситуаций.

Для связи АРМ ЗПУПД с системами энергоблока используются различные способы передачи информации, обеспечивающие работоспособность системы при различных авариях:

- цифровые проводные линии связи;
- цифровые беспроводные линии связи;
- аналоговые линии связи, объединяющие сигналы с помощью мультиплексора.

Постававарийная мониторинговая система (PAMS) и система регистрации важных параметров эксплуатации являются частью защищенного пункта управления противоаварийными действиями (ЗПУПД).

### Первоочередные задачи по созданию конкурентоспособной АСУТП АЭС

Среди множества задач, стоящих перед отечественными разработчиками АСУТП АЭС, первоочередными являются:

- выпуск технического проекта на АСУТП блока 1 Курской АЭС-2 (2016 г.);
- выпуск технического проекта на общестанционную АСУТП Курской АЭС-2 (2016 г.);
- получение положительного заключения МАГАТЭ по результатам международной экспертизы новых технических проектов АСУТП (2017–2018 гг.);
- создание (доработка, лицензирование) современных технических средств АСУТП, удовлетворяющих запросам самых требовательных инозаказчиков (2018 г.);
- увеличение доли российских технических средств АСУТП в поставках оборудования АЭС за рубежом (с 2018 г.).

### Список литературы


1. *Sivokon V.* Implementation of new international and European Regulators' requirements to NPP digital I&C in Rosenergoatom's documentation. IAEA Technical Meeting on Evaluation and Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants. Daejeon, Republic of Korea, 23-26 September 2014.
2. *Aleite W.* Defence in depth by "Leittechnique" systems with graded intelligence. Int. Symposium on Nuclear Power Plant Control and Instrumentation, Munich, Oct. 1982, IAEA publication. Vienna. 1983. p. 301-319.
3. *Сивоконь В.П.* Совершенствование аварийной защиты ядерных реакторов // Атомная техника за рубежом.1988. № 9. стр. 3-10.



***Антипов Станислав Иванович*** *– зам. ген. директора, директор по АСУТП,*
***Сивоконь Владимир Петрович*** *– канд. техн. наук, руководитель проектного офиса по развитию АСУТП,*
*ОАО "Концерн Росэнергоатом",*
***Бутко Андрей Борисович*** *– и.о. первого зам. ген. директора, главного конструктора,*
***Черняев Алексей Николаевич*** *– канд. техн. наук, зам. руководителя управления – начальник отдела АО "ВНИИАЭС".*
*Контактный телефон (495) 783-01-43.*
*E-mail: sivokon-vp@rosenergoatom.ru*


### «Солнечные острова»: применение контроллеров Saia®PCD3 в поддержку инновационной технологии использования солнечной энергии на большой территории

Концепция «солнечного острова» была разработана в CSEM, научно-прикладном центре, который находится в г. Невшатель (Швейцария). Важное преимущество этого подхода заключается в неподвижном креплении всех солнечно-тепловых компонентов «острова», то есть они не должны перемещаться вслед за солнцем. Вместо этого поворачивается весь «остров», обеспечивая точную ориентацию на солнце. Для реализации этого платформа плавает по круговому каналу, заполненному водой. Пар, который образуется в результате отраженного солнечного излучения, можно использовать для выработки электроэнергии, получения пресной воды или водорода.

Контроллеры Saia®PCD, благодаря высочайшей вычислительной мощности, словно изначально были предназначены для поддержки такой новаторской технологии. Экспериментальная модель «солнечных островов» располагается в Рас-эль-Хайме, в Объединенных Арабских Эмиратах. Это сооружение диаметром 80 м и массой 250 т ежегодно вырабатывает электроэнергию в объеме 1,2 ГВт•ч. Экспериментальная установка была построена в пустыне, но в будущем можно также создавать значительно более крупные установки на море.

Авторы "островов" решили отказаться от солнечных батарей. Здесь использован принцип "солнечные концентраторы — трубы с водой — пар — турбина — генератор". КПД такой схемы, возможно, не самый впечатляющий (порядка 15%), зато зеркала-концентраторы дешевле, чем фотоэлектрические преобразователи, да и остальная техника также не особенно сложна и дорога.

Для такой системы желательно иметь концентраторы параболической формы. И также необходимо предусмотреть систему их поворота вслед за солнцем. В противном случае эффективность "усвоения" солнечной энергии резко падает (http://www.374.ru/).

Таким образом, платформа должна исключительно точно следовать за солнцем. Это достигается при помощи особо точного алгоритма, который передает комбинацию положения, определяемого GPS-устройствами, и времени дня непосредственно в контроллер Saia®PCD3, обеспечивая управление позиционированием платформы при помощи двигателей.

*Солнечно-термический «остров» в г. Рас-эль-Хайме (Объединенные Арабские Эмираты)*

Эта позиция критически важна. Ошибка не должна превышать 0,0267°, что соответствует 2 см от внешней стены. Первые испытания вращения платформы были убедительными. Платформа, масса которой составляет 250 т, а площадь поверхности приблизительно 5500 м², выполняет поворот на 280 гр. со скоростью 8 см/с. Перед оценкой возможностей выработки пара требуются дальнейшие испытания.

Помимо позиционирования платформы, контроллеры Saia®PCD3 должны регулировать давление воздуха под мембраной, которая служит опорой для всех зеркал и поддерживает уровень воды во внешнем канале. Для этого контроллер использует сеть PCD3. T665 RIO Ethernet. Она упрощает монтаж всех датчиков и исполнительных механизмов, расположенных на периферии «острова» или рядом с ней.

Подразделение CSEM в Рас-эль-Хайме выбрало оборудование компании Saia-Burgess из-за высокой гибкости использования и вычислительной мощности контроллеров Saia®PCD, а также благодаря поддержке местного интегратора и производителя системы.

*Http://www.saia-pcd.ru*