

АСУ ТП НЕФТЕГАЗОВОЙ ОТРАСЛИ: В НОГУ СО ВРЕМЕНЕМ

Виртуальный «круглый стол» нашего журнала в этот раз посвящен актуальным вопросам, связанным с автоматизацией нефтегазовой отрасли. Его участниками стали представители четырех крупнейших компаний-производителей: ABB, Mitsubishi Electric, Schneider Electric и Siemens.



▲ **СЕРГЕЙ ТИТОВ**, менеджер по развитию бизнеса (нефтегазовый сектор) ООО «Мицубиси Электрик (РУС)»



▲ **ВИКТОР НАТЫКАЧ**, руководитель группы инжиниринга подразделения «Нефть, газ и нефтехимия» департамента автоматизации процессов ABB в России



▲ **ДМИТРИЙ ПЛУТАХИН**, руководитель направления «Решения для нефтехимии» компании «Сименс» в России



▲ **АНДРЕЙ ЧЕРТКОВ**, руководитель группы технической поддержки компании Schneider Electric в России и СНГ



▲ **МАКСИМ КИРЕЕВ**, технический консультант по бренду Trisoplex, сертифицированный инженер по функциональной безопасности компании Schneider Electric в России и СНГ

Падение цен на «черное золото» не стало препятствием для развития новых технологий в нефтегазовой отрасли — наоборот, сейчас как никогда важно сделать производственные процессы более эффективными, т. е. выгодными и автоматизированными. По-прежнему большую роль играет и обеспечение безопасности — причем не только экологической. Из-за использования «Интернета вещей», открытых протоколов и удаленного доступа возрастает потребность и в защите от возможных кибератак.

Каковы основные направления развития современных систем автоматизации и информатизации нефтегазовой отрасли? «Основной тенденцией развития управляющих систем является возрастающая взаимная интеграция отдельных систем автоматизации в единое информационное пространство. При этом на управляющую систему уже возлагаются не только традиционные

функции по автоматизации технологического процесса, но и задачи его оптимизации в целях достижения того или иного показателя эффективности, например удержания требуемого уровня суточной добычи нефти на месторождении», — считает **Сергей Титов** («Мицубиси Электрик (РУС)»). Также важную роль, как отметил **Дмитрий Плутяхин** («Сименс»), играют унификация решений, сокращение времени реализации проектов, стандартизация инжиниринга, строгое соблюдение норм безопасности производства, а также уменьшение размеров оборудования.

Из-за постепенного истощения разработанных залежей нефти возникает потребность в освоении более труднодоступных месторождений. В связи с этим, например, «в арсенале АСУ ТП имеются средства автоматизированной диагностики оборудования», — говорит **Виктор Натыкач** (ABB). — Это позволяет не только

сэкономить на проведении регламентных мероприятий, но и снизить требования к уровню квалификации эксплуатационного персонала. Также с помощью современных систем автоматизации можно легко организовать удаленный доступ к объекту для профессионального анализа информации, получаемой от технологического оборудования». Кроме того, в России важно учитывать климатические условия, подчеркивает **Дмитрий Плутяхин** («Сименс»). Еще один вариант решения, помогающего освоить труднодоступные месторождения нефти, — безлюдные технологии. Для их эффективного использования, как считает **Сергей Титов** («Мицубиси Электрик (РУС)»), необходимо соблюдать два условия: «во-первых, встроенный «интеллект» удаленных локальных подсистем, необходимый для выполнения алгоритмов управления технологическими объектами, а во-вторых, гарантированный информационный

доступ к любому технологическому объекту даже в условиях нестабильной связи — для этого в АСУ применяются технологии резервирования каналов передачи данных, а также специализированные протоколы телемеханики».

ЧЕЛОВЕКО-МАШИННЫЙ ИНТЕРФЕЙС

В системе автоматизации большое значение имеет человеко-машинный интерфейс (Human-Machine Interface, HMI), поскольку именно от его удобства и надежности зависит правильность действий технологов-операторов. Вместе с тем для оптимизации рабочего процесса и безопасности персонала необходимо минимизировать человеческий фактор, что также можно сделать с помощью HMI — например, используя контроль доступа, резервирование и дублирование команд, говорит **Дмитрий Плутахин** («Сименс»).

Виктор Натякач (ABB) условно делит HMI современной системы автоматизации на мнемосхему и лист событий: «Правильно разработанные мнемосхемы должны быть не перегружены лишними деталями, выдержаны в спокойной цветовой гамме, все активные элементы сигнализации активируются только в случае необходимости привлечения внимания оператора. А список аварийных событий сейчас стараются сделать наиболее оптимальным. Сервис по оптимизации аварийных сообщений состоит из нескольких этапов — анализа системы аварийных сообщений с применением специализированных программных инструментов, проработки концепции аварийных оповещений с представителями оперативной и технологической службы заказчика, разработки, а также имплементации рекомендаций, созданных в соответствии с проработанной концепцией и собранной статистикой работы системы».

Сергей Титов («Мицубиси Электрик (РУС)») согласен с тем, что HMI не должен быть перегружен лишними параметрами, и обращает внимание на такой класс программных продуктов, как виртуальные тренажеры, которые представляют собой точную копию HMI системы управления с математической моделью технологического процесса. Пред-

варительное обучение операторов на таких тренажерах, по его мнению, способно существенно снизить риск от неправильных действий персонала при эксплуатации реальных систем.

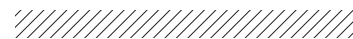
В современных условиях увеличения размера систем и объема данных краугольным камнем улучшения общих принципов дизайна HMI становится обеспечение ситуационной осведомленности, считает **Андрей Чертков** (Schneider Electric). «Операторы могут принимать эффективные решения, только если они полностью осведомлены о текущей ситуации. В концепции ситуационной осведомленности выделяются три основных уровня: восприятие, осознание и прогнозирование. Большинство приложений HMI помогает операторам достичь только первого уровня, т. е. восприятия (отображая числовое значение, обозначающее текущий сигнал от датчика, в определенном месте экрана). Но HMI также может наглядно отображать и ожидаемое значение сигнала датчика, т. е. обеспечивать второй уровень ситуационной осведомленности. Непосредственное предоставление оператору информации об ожидаемых значениях позволит неопытным операторам работать так же эффективно, как и их опытные коллеги. Но в большинстве случаев даже опытные операторы не всегда могут достичь до наивысшего уровня ситуационной осведомленности — прогнозирования. Для обеспечения прогнозирования система должна предоставить оператору информацию, на основе которой он сможет определить, следует ли ему предпринять какие-либо действия, а также понять возможные последствия его действия или бездействия. Эффективность работы операторов можно повысить с помощью удобной структуры окон и оптимальных элементов дизайна, а также консультирования персонала по принятию решений на основе сообщений аварийной сигнализации».

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

В последние тридцать лет значительно обострились и приобрели глобальный масштаб экологические проблемы. Это особенно актуально для нефтегазовой отрасли, в которой авария может легко превратиться в техногенную катастрофу (как это

произошло, например, с нефтяной платформой Deepwater Horizon в США в 2010 г.). «Несомненно, приоритет экологической безопасности максимален, так как в нефтегазовой промышленности она неразрывно связана с безопасностью труда и здоровья», — говорит **Дмитрий Плутахин** («Сименс»).

Ряд техногенных катастроф в середине 1980-х гг. привел к необходимости переосмысления подходов к оценке риска, а также инициировал появление таких стандартов в области безопасности технологических процессов, как DIN 19250 и ANSI S84, которые были приняты как единый стандарт — IEC 61508, «Функциональная безопасность систем электрических/электронных/программируемых электронных». **Максим Киреев** (Schneider Electric) подчеркнул, что «в указанных стандартах введено понятие «жизненного цикла безопасности» инструментальных систем безопасности SIS (Safety Instrumented Systems). Он охватывает все этапы — от производства технических средств и их обслуживания до списания. Помимо этого, документ детально регламентирует требования к различным архитектурам микропроцессорных систем, которые применяются в качестве систем противоаварийной защиты (ПАЗ). Вышеуказанные стандарты Международной электротехнической комиссии (МЭК) IEC61508/61511 в настоящее время получили мировое признание. Главным критерием допуска технических средств инструментальных систем безопасности SIS является общий уровень опасности производственного объекта, оцениваемый по числу возможных человеческих жертв, загрязнению окружающей среды и экономических потерь в случае возникновения аварии. Для определения необходимого снижения риска в документе описаны такие методологии, как, например, HAZOP — анализ опасностей и работоспособности, LOPA — анализ уровня защит, и др. Они позволяют перейти к назначению уровня полноты безопасности SIL для каждого инструментально контура безопасности SIF (Safety Instrumented Function) — от датчика до исполнительного элемента. УПБ SIL (Safety Integrity Level) представляет собой дискретный



уровень от минимального SIL 1 до максимального SIL 4, который определяет требуемое снижение риска и необходимые показатели надежности систем ПАЗ. В настоящее время ведущие российские компании нефтегазовой индустрии приступили к разработке отраслевых стандартов, взяв за основу стандарты МЭК.

Помимо введения строгих стандартов безопасности, одним из инструментов повышения уровня экологической безопасности при построении систем автоматизации в нефтегазовой отрасли является применение энергоэффективных технологий — в качестве примера таких технологий **Сергей Титов** («Мицубиси Электрик (РУС)») приводит частотно-регулируемый привод, который широко внедряется нефтяными компаниями.

КИБЕРБЕЗОПАСНОСТЬ

Такие современные технологии, как удаленный доступ и управление с мобильных устройств, имеют много разных достоинств, но являются уязвимыми для кибератак, которые могут угрожать в итоге всей АСУ ТП. «Уровень доверия предприятий к этим технологиям крайне низок, особенно у опасных производств в нефтегазовой отрасли, — отмечает **Виктор Натыкач** (ABB), — и такой консервативный подход вполне оправдан. Тем не менее производители АСУ, следуя тренду, задаваемому заказчиком, предлагают некоторые подходы к улучшению информационной безопасности систем. Из таких новинок можно выделить решения на основе проактивных антивирусов и систем аудита информационной безопасности. Проактивный антивирус отличается от традиционного решения тем, что не требует регулярного обновления базы данных сигнатур вредоносного кода. Если традиционный антивирус сканирует файлы, так или иначе используемые операционной системой, на наличие потенциально вредоносного кода, то проактивный антивирус действует по принципу «белого списка»: запускаемый код сверяется со списком разрешенных к исполнению и в случае несоответствия его запуск приостанавливается, а сообщение о потенциальном вторжении отправляется системному администратору. Для закрытых

от внешнего мира систем, таких как большинство АСУ ТП, этот подход является оптимальным. Последнее время производители систем автоматизации также стали предлагать решения, обеспечивающие регулярный аудит АСУ ТП на предмет соответствия требованиям информационной безопасности. Такие системы могут предлагаться в виде продукта или сервиса. Сами по себе системы аудита информационной безопасности, конечно, не являются новинкой. Новшеством тут стало то, что создает такое программное обеспечение разработчик системы автоматизации, что позволяет учесть все нюансы архитектуры и реализации АСУ ТП».

Помимо антивирусов и аудита, участники круглого стола упомянули такие решения, как фаерволы и контроль доступа к управляющей программе. **Сергей Титов** («Мицубиси Электрик (РУС)») добавил, что в современных АСУ ТП обязательно должны быть предусмотрены механизмы фильтрации трафика в сетях Ethernet, защита (в том числе аппаратная) от изменения прикладного программного обеспечения контроллеров и многоуровневая аутентификация пользователей.

В свою очередь, **Андрей Чертков** (Schneider Electric) рассказал о возможностях централизованного обеспечения информационной безопасности промышленного предприятия, которое включает в себя и антивирусное сканирование, и обнаружение несанкционированного вторжения, и систему предотвращения потери данных, и процедуру повышения «прочности» операционной системы, и систему резервного хранения и восстановления.

ПРОМЫШЛЕННАЯ РЕВОЛЮЦИЯ 4.0

Безусловно, нефтегазовый сектор является одним из приоритетных направлений развития Industry 4.0, однако в силу сложности непрерывных технологических процессов создание виртуальных моделей для этой отрасли, как отметил **Дмитрий Плутахин** («Сименс»), требует привлечения значительных ресурсов. Тем не менее объектно ориентированный подход, суть которого как раз заключается

в представлении реальных производственных единиц, достаточно широко применяется для построения современных АСУ ТП. «В то же время, — указывает **Виктор Натыкач** (ABB), — развитие полевых устройств автоматизации (контрольно-измерительных приборов и исполнительных механизмов) идет по пути увеличения их функциональности. Все чаще для коммуникации полевых устройств и АСУ применяются цифровые интерфейсы. Современные полевые шины позволяют не только управлять устройствами и получать от них диагностическую информацию, но и организовывать распределенные интеллектуальные системы, которые могут работать без участия центрального контроллера». **Сергей Титов** («Мицубиси Электрик (РУС)») соглашается с важностью использования промышленного «Интернета вещей», поскольку «для достижения максимальных показателей эффективности производства, надежности и безопасности операторам-технологам важно получать доступ к информации о состоянии работы даже самых элементарных устройств. И производители оборудования обеспечивают такую возможность, интегрируя сетевые технологии в элементы АСУ ТП. Если попробовать предсказать будущее в развитии сетевых технологий IoT в промышленной автоматизации нефтегазовой отрасли, то здесь, на мой взгляд, все активнее будут развиваться методы и средства беспроводной передачи данных. Уже сейчас лидеры среди производителей оборудования промышленной автоматизации предлагают своим заказчикам контрольно-измерительное оборудование со встроенными модулями беспроводной передачи данных. Но все же до сих пор применение данного типа устройств не носит массового характера. Возможно, в ближайшем будущем, после решения ряда технических задач, таких как повышение помехоустойчивости, кибербезопасности, срока службы элементов питания, дальности связи — наступит период широкого применения беспроводных сетевых технологий, в том числе и в системах АСУ ТП для нефтегазового комплекса» ●