УДК 681.518.5

Безуб В.Н., Карасевич А.В.

СОВЕРШЕНСТВОВАНИЕ СИСТЕМ КОНТРОЛЯ И БЕЗОПАСНОСТИ АСУТП МЕТАЛЛУРГИЧЕСКОГО ПРОИЗВОДСТВА

Аннотация. В статье описана система, выявляющая причины пропадания важнейших логических сигналов и способствующая устранению нарушений штатного режима работы оборудования посредством логического контроля последовательности срабатывания сигналов с запоминанием события по времени при первой фиксации факта сбоя.

Ключевые слова: автоматизированные системы управления, информационная целостность, контроль целостности систем управления.

Анотація. У статті описана система, що виявляє причини пропажі найважливіших логічних сигналів і сприяюча усуненню порушень штатного режиму роботи устаткування за допомогою логічного контролю послідовності спрацьовування сигналів із запам'ятовуванням події за часом при першій фіксації факту збою.

Ключові слова: автоматизовані системи управління, інформаційна цілісність, контроль цілісності систем управління.

Summary. In article the system establishing the reasons of loss of the major logical signals and promoting elimination of violations of a regular operating mode of the equipment by means of logical control of sequence of operation of signals with storing of an event on time at the first fixing of the fact of failure is described.

Keywords: automated control systems, information integrity, control of integrity of control systems

Комплекс технических средств (измерительных, регулирующих, исполнительных, по сбору и обработке информации всех видов и т. д.) во взаимодействии с объектом управления и человеком (оператором, диспетчером, контролёром, руководителем участка) на основе рационально построенных форм и потоков информации образует автоматизированную систему управления (АСУ). В современную АСУ входят устройства для первичного формирования, автоматического извлечения и передачи, логической и математической обработки информации, устройства для представления полученных результатов, выработки управляющих воздействий и исполнительные устройства.

Автоматизация производства от степени задействования в процессе человека существенно различается - от частичной автоматизации до полной системы автоматического контроля. Рассмотрим комплексно автоматизированную систему, так как она является хорошим примером автоматизации с использованием полного набора подсистем и обратной связью для воздействия на объект управления (рис. 1).

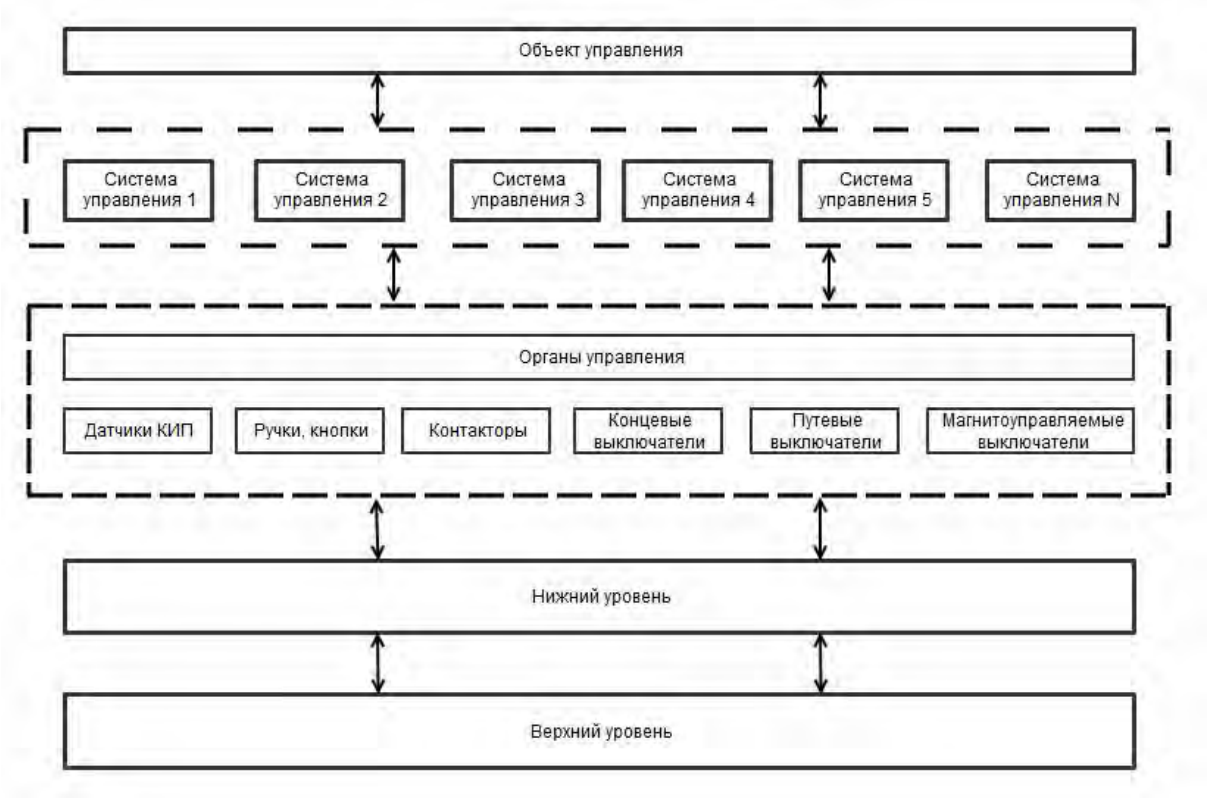

Рисунок 1. – Комплексно автоматизированная система

В последнее время кроме этих классических функциональных блоков добавляется система, контролирующая работу одного или нескольких функциональных блоков. На рис. 2 показано, как они группируются по функциональному, информационному и конструктивно-технологическому признакам, образуя на унифицированной элементной базе блочные наборы, из которых составляются необходимые агрегатные комплексы средств автоматизации.

Широкий интерес к защищенности промышленных систем возник не так давно, после серии инцидентов со специализированными компьютерными вирусами, такими как Flame и Stuxnet. Тогда выяснилось, что различные организации могут использовать в своих целях недостаточное внимание к информационной безопасности систем АСУ ТП. На волне этого много исследовательских лабораторий, центров, институтов начали заниматься анализом уязвимостей систем АСУТП. Большинство этих исследований касается кибер атак, промышленного шпионажа, вмешательств разведок иностранных государств, забывая о человеческом факторе, халатности, лени или мести обиженных сотрудников. Вектор направленности исследований проблематики можно увидеть в списке литературы.

Основная информация, циркулирующая в системах технологического управления – это информация о технологических процессах и управляющих воздействиях. Обладание этой информацией без физического доступа к объекту управления не дает возможности совершить кражу, что

 ISSN 1991-7848

резко ограничивает круг потенциальных нарушителей. Риски, связанные с мошенническими операциями в АСУТП, можно ограничить действиями внутреннего нарушителя – собственного персонала компании или компаний-партнеров. К примеру, для реализации схем с модификацией данных по расходу топлива на автозаправке надо иметь возможность слива и реализации этого топлива.

Наиболее распространенные угрозы безопасности связаны с монетизацией киберпреступности, т. е. с получением денежной выгоды от реализации тех или иных атак на инфраструктуру предприятия, промышленный шпионаж и в редких случаях – шантаж и заказные акции против конкурентов. Не смотря на это, АСУТП до последнего времени не являлись привлекательными для потенциального внешнего нарушителя. Остальные инциденты являются немонетизируемыми: месть уволенных работников, нарушение функционирования вредоносным кодом, случайные взломы хакерами.

Из вышеописанного следует, что количество публично известных нарушений функционирования подобных систем крайне невелико. Кроме того, в случае серьезных нарушений функционирования процессов, контролируемых системой управления, борьба с последствиями не будет отличаться от борьбы с техногенной аварией. Системы технологического управления рассчитываются на быстрое восстановление после сбоев как в случае автоматизации, так и без нее.

Однако низкая вероятность внешних атак на системы АСУТП не снижает актуальность угроз для систем управления. Согласно общепринятой практике, актуальность угрозы пропорциональна как вероятности реализации угрозы, так и возможному ущербу от ее реализации, а если говорить о возможном ущербе от реализации угрозы, тогда системы управления, особенно системы управления опасными производственными циклами или системы жизнеобеспечения целых городов и областей, будут вне конкуренции.

Возможный ущерб от реализации подобных атак включает, кроме финансовых потерь, репутационные риски и риски, связанные с потерей здоровья и жизни, а также риски возникновения экологических катастроф. Даже единичное нарушение функционирования систем технологического управления может привести к катастрофическим последствиям. Подобные инциденты в системах технологического управления, при их обнародовании, вызывают большой общественный резонанс.

По причине практически отсутствующей огласки про нечастые случаи кражи конфиденциальной информации или возникновении специализированных вирусов, способных создать аварийную ситуацию на производстве, компании, проектирующие комплексы АСУТП для промышленных предприятий, часто не заботятся о создании мер безопасности производства и контроле целостности информации. Некоторые компании-разработчики средств автоматизации создают отдельные

компоненты, повышающие уровень контроля и безопасности, но охватить все возможные варианты задач практически невозможно. Так же значительную роль играет неведение заказчика относительно всех возможностей средств автоматизации, что только усугубляет ситуацию.

Например, один из громких и резонансных инцидентов, показывающим уязвимость и возможность эксплуатации данной уязвимости сетей управления на практике, явился обнаруженный в июле 2010 г. вирусный код Stuxnet, который фактически является первым в истории вирусом, способным портить не только данные и программный код, но и вполне реальные машины и оборудование. Его появление не только выявило очередные уязвимости в операционных системах Microsoft, но и устремило взоры специалистов по информационной безопасности в абсолютно новую для них область – безопасность промышленных систем. Способ распространения, направленность и деятельность внедренного вируса в промышленность говорит о специализации вируса на крупные промышленные и стратегические объекты.

Следствием этого является необходимость создания системы безопасности в автоматизации, которая должна базироваться на безопасном выполнении поставленных задач перед технологическим персоналом, а также на максимально возможном воспрепятствовании возникновению аварийных ситуаций. Решение подобных задач позволит выявить потенциальные риски в комплексах АСУТП с помощью системы диагностики и контроля, которая сможет обеспечить исправное состояние ключевых узлов, и поможет уменьшить влияние человеческого фактора.

Из опыта эксплуатации средств АСУТП на различных предприятиях, можно сделать вывод об отсутствии действительно эффективных многоуровневых систем защиты в большинстве случаев. В некоторых случаях были замечены попытки решить проблемы безопасности самим обслуживающим персоналом с помощью стандартных средств, но подобные решения оставляют желать лучшего.

Когда проблемами безопасности занимаются неспециалисты в области безопасности или небольшой круг энтузиастов, они исходят из имеющегося у них опыта, при этом устраняя одни проблемы и создавая другие.

Ниже (таблица 1) приведены основные факторы, влияющие на уязвимость действующих систем по тем или иным причинам.

В настоящий момент, для унификации и типизации процессов и технологий существует целый ряд стандартов и рекомендаций. Заслуживают внимания и тщательного анализа и рекомендации производителей. Одним из примеров таких практических рекомендаций может быть руководство по проектированию и внедрению конвергированной Ethernet сети предприятия (Converged Plantwide Ethernet Designand Implementation Guide), разработанное компаниями Cisco и Rockwell Automation. Назначение этого документа – определение эталонных сетевых архитектур, ориентированных

 ISSN 1991-7848

на применение на производственных предприятиях и облегчающих объединение промышленных и корпоративных сетей с учетом требований по безопасности.

Таблица 1

Большое количество «собственных» разработок программно-аппаратных решений при создании АСУ ТП	
Длительный срок эксплуатации систем	
Закрытость систем	– Разработка в расчете, но выполнение в доверенной среде закрытых индустриальных сетей – Использование специализированных протоколов и средств связи, а также часто низкая скорость их роботы – Отсутствие ревизий систем и кода на безопасность – Разработка без учета лучших практик разработки безопасного кода
Фиксированные конфигурации	– Отсутствие возможности своевременного обновления ПО и установки последних исправлений безопасности – Отсутствие возможности установки наложенных средств безопасности (например, антивирусного ПО) и их своевременного обновления – Использование паролей и настроек безопасности по умолчанию, включая настоятельные рекомендации производителя не менять данные значения
Производительность	– Системы технологического управления оперируют информацией в реальном времени, дополнительные проверки систем безопасности мешают
Открытые стандарты	– Новое поколение систем технологического управления работает на открытых стандартах (прежде всего протоколы TCP/IP). При этом, даже, в случае разделения сетей (технологической, офисной, сети Интернет) связи сохраняются для технологических нужд (пересылка информации, удаленное управление)
Консервативный подход к проблемам безопасности (заключающийся, как правило, в периметровой защите и разделении сетой). Возможности управления доступом в рамках прикладных систем ограничены	
Информация (технологическая) не является основным объектом защиты систем, часто не является конфиденциальной	
Основной объект защиты – управляющее воздействие	

В настоящее время, инфраструктура ПАО «ЕВРАЗ–ДМЗ им. Петровского» так же нуждалась в доработке своей системы безопасности, в первую очередь - обезопасить существующие системы автоматизации от человеческого фактора, т.е. от случайного или намеренного воздействия обслуживающего персонала, действия которого могут привести к трагическим последствиям или техногенной катастрофе. Подобными и другими вопросами промышленной безопасности существующих автоматизированных систем в доменном цехе активно последние четыре года занимаются специалисты отдела эксплуатации АСУТП при содействии научных работников Днепропетровской металлургической академии.

На рис. 2 приведено достигнутый результат – многоуровневая системы защиты и контроля.

Рисунок 2. – Многоуровневая системы защиты и контроля

Немаловажную роль стоит отводить поддержке используемого программного обеспечения, а именно своевременному обновлению операционных систем, технологического и промышленного ПО, запрет на использование нелегальных приложений и использование антивируса. В настоящий момент уже прекращена поддержка таких распространенных операционных систем, как Windows XP и Windows 7, поэтому, в целях безопасности, необходимо рассмотреть переход на ОС нового поколения, поддерживаемые и обновляемые разработчиком. Этот вопрос касается и программного обеспечения верхнего уровня – средства программирования промышленных контроллеров и SCADA-системы, в последних версиях которых уделено много внимания вопросам безопасности и защиты информации, разграничение прав действий и функций пользователей и их тщательной настройке.

Следующим этапом необходимо обеспечить внутреннюю безопасность системы, а именно контроль и анализ действий технологического и обслуживающего персонала. На ПАО «ЕВРАЗ – ДМЗ им. Петровского» уже реализовано и функционирует в течение нескольких лет подсистема аудита верхнего и нижнего уровней, фиксирующая все действия персонала. С её

 ISSN 1991-7848

помощью возможно выяснить, кто, когда и каким образом выполнял изменения в системе нижнего и верхнего уровней, начиная от подключений к серверу визуализации заканчивая изменениями, вносимыми в логические контроллеры. Подсистема аудита, функционирующая немногим более трех лет, уже успела доказать свою эффективность, позволив выявить несоответствия между регистрацией действий самим дежурным персоналом с фактически выполняемыми изменениями. К тому же, использование аудита изменений позволяет выявить сотрудников, выполнивших неквалифицированные действия, которые, в иных случаях, могли привести к необратимым последствиям.

Большую роль в технологическом процессе играет и подсистема сигнализаций. С ее помощью, технологический персонал может увидеть сообщаемые системой АСУТП отклонения в своей работе и немедленно принять соответствующие меры по восстановлению штатного функционирования. Сообщения имеют вид всплывающих окон или мерцающих надписей, и представляющих в графическом виде узел системы, в котором произошло отклонение заданных параметров, позволяя персоналу быстро определить значимость проблемы и необходимости вызова соответствующей службы для ее устранения. Одновременно с этим присутствует сводка всех поступающих аварийных сообщений, которые будут отображаться до момента подтверждения их просмотра.

В виду того, что доменное производство сопряжено с определенными рисками возникновения критических ситуаций, множество узлов и механизмов системы оснащено блокировками, выполняющими функции аварийного останова работы части системы. К таким объектам можно отнести баллоны, работающие под давлением, трассы доменного и природного газов и другие объекты, способные создать угрозу катастрофического или техногенного характера. Для отслеживания и анализа сработавших блокировок, технологическому персоналу предоставляется отчет в виде таблицы с количеством срабатываний и значениями параметров.

Одна из подсистем, внедренных в АСУТП в последнее время, является подсистема контроля логических цепей ПЛК, и направлена на анализ работы механизмов в нижнем уровне, т.е. на уровне логических контроллеров, ипризвана повысить контроль над последовательностью возникновения неисправностей логических цепей. В комплексах АСУТП описывают различные узлы системыв основном с помощью языка программирования LadderDiagram, представляющим собой набор логических сигналов, объединенных в общую цепь, и имеющим на выходе цепи результаты конъюнкции и дизъюнкции этих сигналов. Простейшими элементами языка являются контакторы, которые можно образно уподобить контактам реле или кнопки. Контакты отождествляются с переменными, а состояние контактаявляется значением переменной. Результат на выходе определяет управляющие сигналы для работы

механизмов, разрешение и запрет на их работу, и согласованную работу всех механизмов системы в целом.

Диагностика состояния логических цепей затруднена, поскольку цепь отображает только текущее состояние, и определить ее предыдущее состояние, например причину отключения, не представляется возможным. Данная подсистема позволяет отследить последовательность отключения сигналов цепи, и оперативно выявить истинную причину некорректной работы ключевых логических цепей, наглядно представляя изменение состояния цепи в разные промежутки времени. Все измененные состояния наблюдаемых цепей записываются в систему длительного хранения данных, позволяя накапливать статистическую информацию и выявлять тенденцию нарушенной работы устройств.

В целом, ниже (таблица 2) приведен перечень мероприятий, который должен стать базовым стандартом.

Таблица 2

Предотвращение ошибок персонала	Предотвращение преднамеренных («хулиганских») действий сотрудников
– формирование требований по защите информации в процессе разработки и внедрения систем АСУТП; – организация мониторинга действий персонала и состояния критичных компонентов АСУ ТП; – проведение обязательного повышения квалификации персонала, занятого обслуживанием АСУ ТП; – тщательный подбор и подготовка персонала для решения поставленных задач, включая личную ответственность за совершаемые действия.	– ограничение полномочий пользователей в использовании программной среды АСУ ТП рамками их должностных обязанностей; – контроль роботы с переносными устройствами и устройствами ввода/вывода; – применение строгой аутентификации при доступе к программной среде АСУ ТП; – формирование строгой антивирусной политики и повсеместное применение средств антивирусной защиты; – проведение регулярных инструктажей об ответственности, возложенной на сотрудников, занятых в эксплуатации ключевых компонент АСУ ТП; – резервное копирование ключевых компонент АСУ ТП и средств, задействованных в обеспечении их безопасности; – автоматизированный мониторинг состояния защищенности ЛВС АСУ ТП.

Автоматизированные и автоматические системы технологического управления прочно интегрированы в современное промышленное производство. Вероятность атаки на подобные системы ниже, чем на многие другие, но ответственность, связанная с их защитой, в некоторых случаях несоизмеримо выше.

В процессе внедрений АСУ ТП во многих случаях меры по безопасности начинаются и заканчиваются на границе между технологическим и корпоративным сегментами ЛВС. Но чтобы противодействовать современным угрозам в сфере АСУ ТП, недостаточно

 ISSN 1991-7848

поставить межсетевой экран на границе и установить на серверах и АРМ антивирус. Нужно применять технологии безопасности ниже, внутри АСУ ТП, на уровне серверов, ПЛК и интеллектуальных датчиков и исполнительных механизмов.

Экономический эффект от внедрения систем безопасности будет достигаться за счет снижения простоев агрегатов, возможности ретроспективного анализа причин сбоев в работе оборудования, а также снижения расхода человеческих ресурсов на восстановление хронологии аварийных ситуаций. Кроме того, дальнейшее развитие систем безопасности позволит значительно эффективнее выявлять проблемные узлы в комплексах промышленного оборудования и таким образом повышать общий показатель экономической эффективности предприятия.

Комплексная система, контролирующая работу остальных функциональных блоков на данный момент отсутствует, зато есть готовые решения от различных корпораций, с разной функциональной нагрузкой. То есть, нет комплексного решения, которое смогло бы отслеживать все изменения и вмешательства на всех уровнях нашей системы автоматизированного управления. Различные службы, обслуживающие подсистемы приносят свой процент неточности на окончательные данные, так неправильно настроенный датчик искажает полноту картины. При увеличении и разветвлении АСУ, ввод специалистов КИП, электроотдела, весового оборудования или, к примеру АСУ увеличивают возможность влияния человеческого фактора, наводок, сбоев, несанкционированного доступа и т.д. которые нужно выявлять, архивировать, прогнозировать и предупреждать их появление. Данную проблему рассмотрим детальнее, так как есть готовые внедренные решения от концерна производителя программно-технических комплексов автоматизации Allen – Bradley.

Стандартный режим работы системы – автоматический, однако вмешательства в ее работу неизбежны по двум основным причинам: физические неисправности отдельных узлов при штатной работе и необходимость проведения наладочных работ во время ремонтов. Поскольку нештатные ситуации грозят простоями производства, их устранение требует принятия оперативных решений. Все вмешательства должны производиться обдуманно, с соблюдением мер безопасности и согласоваться с другими службами, однако на практике оказалось, что временно «обойти» неисправность при помощи изменений логики контроллеров значительно быстрее, чем устранить саму неисправность. Так как подобные манипуляции зачастую являются прямым нарушением техники безопасности, то записи о них не производились. Как следствие, неисправности не ликвидировались вовсе, а о внесенных изменениях персонал мог забыть, что грозило новыми нарушениями в работе системы и создавало риски, как для жизни персонала, так и для оборудования.

Как пример можно привести такую ситуацию по САУ “Загрузка” доменной печи: при обычной работе коксовый или рудный бункер

открывается только при выборе в программе соответствующего материала, но для ремонта затвора бункера, чтобы была возможность открывать и закрывать его без зависимости работы остальной системы исключается проверка вида материала. Данные об этом действии не были занесены в дежурный журнал. Поэтому по завершению ремонта блокировка не была восстановлена, что привело к одновременному высыпанию двух порций материала в один скип (рис. 1).

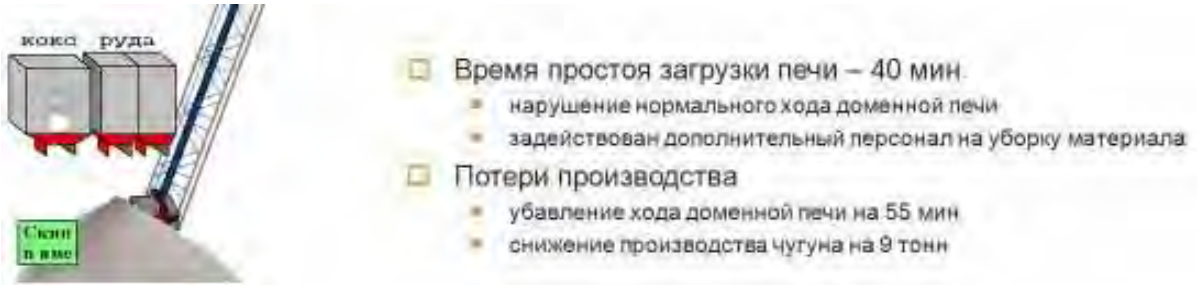

Рисунок 3. – Последствия исключения проверки заданного материала

Разбор происшествий существенно усугубляет отсутствием фиксации действий в системе управления. Поскольку дежурный персонал АСУТП, дежурный электрик и сменный технологический персонал работает в одних и тех же бригадах, для снижения коллективной ответственности зачастую предоставляется недостоверная информация о производимых ими действиях, либо вообще замалчивается.

В итоге практически невозможно достоверно и точно оценить принимаемые персоналом решения, произведенные вмешательства в систему на разных уровнях, а также, в случае возникновения аварийных ситуаций или простоев, восстановить картину происшествия, и проанализировать действия персонала или поведение механизмов.

На ПАО «ЕВРАЗ - ДМЗ им. Петровского» в доменном производстве используются промышленные программируемые контроллеры компании Allen–Bradley,поэтому рассмотрим детальнее программное предложение AssetCentre Rockwell Software. Данный продукт предназначен дляконтроля действий персонала, который обслуживает нижний и верхний уровень рассматриваемой системы. Программа имеет удобный вид, с множеством настроек, которые позволяют получить данные о любых изменениях производимых в логике нижнего или верхнего уровня.

Аудит нижнего уровня представлен в виде таблицы, в которой указан время, источник, ресурс, имя и сообщение изменение в котором описывается само изменение. В настройках можно задать параметры поиска из баз данных, так при знании, что нужно искать, можно легко найти требуемое сообщение. Данный отчет можно сохранить в различных форматах, из распространённых – PDF, DOC, XLS. Пример отчета приведен на рис. 4, он иллюстрирует реальную проблему, произошедшую 2 октября 2012 года на ДП-3, о которой писалось выше.

 ISSN 1991-7848

Occurred Time	Source	Location	Resource	Username	Message
02.10.2012 12:17:19	RSLogix 5000	RS-01	PKZ3	RS-01\admin	Modified Rung [50] in Routine [\OTHER\MNEMO] New Neutral Text: [[XIC(PP_5P),] [XIC(PP_3RR),XIC(PP_3RK),XIC(PP_3KR),XIC(PP_3SM)] [OTE(_S1_9VDW),OTE(_SB_89VDW)];] Old Neutral Text: [XIC(PP_5P)[,][XIC(PP_3RR) ,XIC(PP_3RK) ,XIC(PP_3KR) ,XIC(PP_3SM)] [OTE(_S1_9VDW) ,OTE(_SB_89VDW)];]
02.10.2012 12:17:24	RSLogix 5000	RS-01	PKZ3	RS-01\admin	Modified Rung [50] in Routine [\OTHER\MNEMO] New Neutral Text: [[XIC(PP_5P),][XIC(PP_3RR) [,],XIC(PP_3RK),XIC(PP_3KR),XIC(PP_3SM)] [OTE(_S1_9VDW),OTE(_SB_89VDW)];] Old Neutral Text: [[XIC(PP_5P) ,][XIC(PP_3RR) ,XIC(PP_3RK) ,XIC(PP_3KR) ,XIC(PP_3SM)] [OTE(_S1_9VDW) ,OTE(_SB_89VDW)];]

Рисунок 4. – Пример отчета изменений в нижней логике

С помощью аудита верхнего уровня можно установить кто и когда, каким образом делал изменения в системе верхнего уровня, начиная от подключений к серверу визуализации заканчивая изменениями вносимые в SCADA. Отчет представляет собой таблицу с последними 500 изменениями.

Данная программа появилась в ноябре 2011 года и легко встроилась в существующую систему. Уже с первых дней работы программы выявились несоответствия между журналом регистрации изменений и фактически выполненными изменениями. В период с ноября по декабрь 2011 года, с помощью AssetCentre удалось выявить свыше 50 несоответствий в записях журнала регистрации изменений, по сравнению с 2010 годом. В прошествии двух месяцев количество изменений в системе сократилось в 2 раза, из чего можно сделать вывод – многие, ранее выполненные изменения не требовались, или были не настолько критичными чтобы производить изменения в системе, и могли привести к непредсказуемым последствиям. Ими могли оказаться блокировки на критически важные сигналы, такие как давление доменного газа на БВН, уровень засыпи, давление в печи и т.п. Программный комплекс AssetCentre выполняет функцию защиты системы нижнего и верхнего уровней, тем самым, исключая человеческий фактор. Для наглядности приведем официальную статистику задокументированных изменений в месяц, произведенных дежурным персоналом на протяжении последних трех лет, взятую в отделе АСУ ТП ПАО «ЕВРАЗ - ДМЗ им. Петровского» приведенную на рис. 5.

Как видно, количество зафиксированных вмешательств в систему возросло более чем в 3 раза, по сравнению с аналогичными периодами за предыдущие годы. Каждая конкретная ситуация фиксируется в автоматическом режиме, и подробно разбирается на встречно-сменном собрании. Внедрение системы FT AssetCentre позволило значительно повысить качество выполняемой работы, уровень безопасности, а также свести к минимуму вмешательство в работу системы без необходимости, о чём свидетельствует спад уровня зафиксированных вмешательств к концу текущего года.

Рисунок 5. – Усредненное количество изменений в системах АСУ в месяц, зафиксированных в дежурном журнале

Используя программное решение AssetCentre, мы частично уменьшим человеческий фактор, контролируя вмешательство специалистов, которые непосредственно работают с нижним или верхним уровнем и имеют возможность вносить изменения в логику системы управления, зафиксировав выполненные ими изменения. Если обратить внимание на рис. 1, мы увидим что кроме верхнего (вывод информации, сбор в базы данных) и нижнего (контролеры, их программирование) есть еще другие системы, в которых возможно внести изменения. Для специалиста никакого труда не представляет подпереть датчик, реле или замкнуть контакт физически. При этом в данной программе при составлении отчета никакой информации предоставлено не будет.

При использовании AssetCentre мы увидим только изменения сделанные специалистом который будет вносить изменения в логику, или давать какие ни будь команды из верхнего уровня, то есть таким образом мы частично уменьшаем человеческий фактор в лице специалистов которые работают непосредственно с нижнимили верхним уровнем. При этом никаким образом нельзя получить данные о том что будет происходить непосредственно на механизме которым управляем.

Выводы

Оптимально выбранная система контроля должна обеспечивать нас достаточной информацией по интересующим вопросам, начиная от объекта управления заканчивая нижним уровнем. Система должна быть достаточно сложной и гибкой, чтобы работать с различными типами данных. АСУ часто дополняется новыми функциональными блоками, новыми

 ISSN 1991-7848

подсистемами. Совершенный вариант системы контроля должен также уметь обучатся нововведениям. Поэтому, на наш взгляд, система контроля должна быть построена с использованием нейронных сетей. Это обеспечит достаточную гибкость, возможность работы с различными типами данных (дискретные и аналоговые) и обучаемость.

ЛИТЕРАТУРА

1. Сбор данных в системах контроля и управления. Практическое руководство. (Парк Дж., Маккей С., серия "Безопасность и системы промышленной автоматизации. Опыт практического применения").

2. Нестеров А.Л. - Проектирование АСУТП. Методическое пособие. Книга 1 – 2006г.

3. Нестеров А.Л. - Проектирование АСУТП. Методическое пособие. Книга 2 – 2009г.

4. Федоров Ю.Н. – Справочник инженера по АСУТП: проектирование и разработка. Инфра-Инженерия., Москва 2008.

5. Обзор информационной безопасности АСУ ТП зарубежных государств. Гарбук Сергей Владимирович, Комаров Андрей Андреевич, Салов Евгений Игоревич (Режим доступа: http://www.securitylab.ru/analytics/398184.php).

6. Безопасность АСУ ТП и контроль привилегированных пользователей (Режим доступа: http://www.anti-malware.ru/node/11899).

7. Практическая демонстрация типовых атак и 0-day уязвимостей в SCADA и PLC-контроллера. Волобуев П., Миноженко А., Поляков А., DigitalSecurity 2011г.

8. 6 шагов к информационной безопасности АСУ ТП. Ли Ницель (Режим доступа: http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp).

9. Безопасность промышленных систем в цифрах v2.1. Г. Грицай, А. Тиморин, Ю. Гольцев, Р. Ильин, С. Гордейчик. Москва, 2012г.