УДК 681.518.5

ЗАДАЧА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИЕРАРХИЧЕСКИХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Карасевич А. В.
ГВУЗ «Национальная металлургическая академия», г. Днепропетровск

Структура управления, оптимально выбранная для выполнения заданных целей, в сочетании с комплексом 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).

Рассмотрим комплексно автоматизированную систему, так как она является отличным примером автоматизации с использованием полного набора подсистем и обратной связью для воздействия на объект управления (рис. 1).

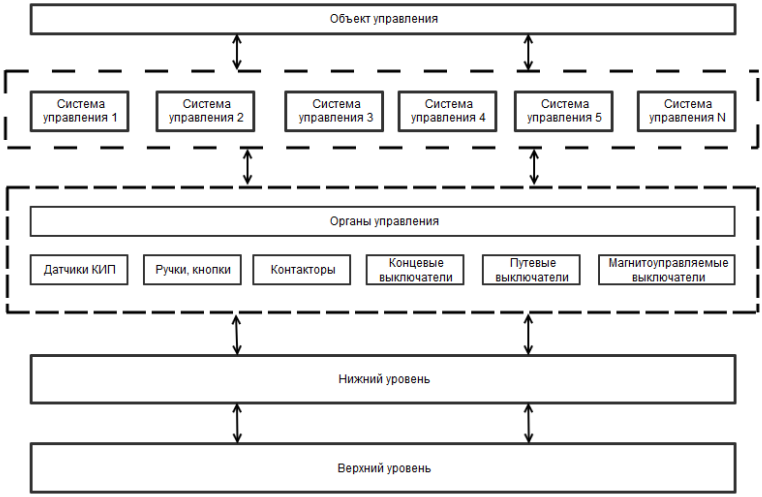


Рис. 1. Комплексно автоматизированная система

Современная АСУ состоит из устройств первичного формирования, автоматического извлечения и передачи, логической и математической обработки информации, устройств для представления полученных результатов, выработки управляющих воздействий и исполнительные устройства. В последнее время кроме этих классических функциональных блоков добавляется система контролирующая работу одного или нескольких функциональных блоков. На рис.1 показано как все 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 АСУТП. На волне этого много исследовательских лабораторий, центров, институтов начали заниматься анализом уязвимостей систем АСУТП. Большинство этих исследований касается кибератак, 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.

Комплексная система, контролирующая работу остальных функциональных блоков, на данный момент отсутствует, зато есть готовые решения от различных корпораций, с разной функциональной нагрузкой. 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 автоматизацииAllenBradley.

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.

Например, можно привести такую ситуацию по системе автоматического управления загрузкой шихтовыми материалами (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.2).

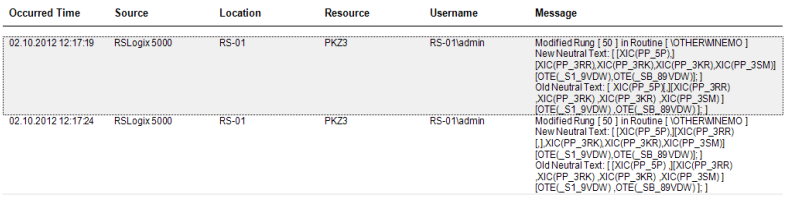
Рис. 2. Последствия исключения проверки заданного материала

Расследование происшествий существенно усугубляется отсутствием фиксирования 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 AllenBradley,поэтому рассмотрим детальнее программное предложение AssetCentre RockwellSoftware. Данный продукт предназначен для контроля 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.3, он иллюстрирует реальную проблему, произошедшую 2 октября 2012 года на доменной печи №3, о которой было написано выше.



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)];]

Рис. 3. Пример отчета изменений в логике нижнего уровня

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

Данная подсистема появилась в ноябре 2011 года и легко внедрилась в существующую АСУ ТП и САУ приводами доменной печи. 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 критическими, 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 эксплуатации АСУТП ПАО «ЕВРАЗ – ДМЗ им. Петровского», изображенную на рисунке 4.

Рис. 4. Усредненное количество изменений в системах АСУ в месяц, зафиксированных в дежурном журнале

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.

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. Но 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 установить шунт на датчик, реле или замкнуть контакт физически и главное, что 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 выдавать какие-нибудь команды из верхнего уровня. То есть, таким образом, мы частично уменьшаем человеческий фактор в лице специалистов, которые работают непосредственно с нижним или верхним уровнем. При этом, никаким образом нельзя получить данные о том, что будет происходить непосредственно на механизме которым управляем.

Таким образом, на рассмотренном примере видно, что сложные иерархические АСУ чувствительны к несанкционированным вмешательствам в функциональность своих элементов.

Возникает задача определения факта, и локализации такого вмешательства.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Парк Дж., Маккей С. Сбор данных в системах контроля и управления. Практическое руководство: - М.: ООО "Группа ИДТ", 2006. – 504 с.
2. Нестеров А.Л. Проектирование АСУТП. Методическое пособие. Книга 1. - СПб.: Издательство ДЕАН, 2006. – 552 с.
3. Нестеров А.Л. Проектирование АСУТП. Методическое пособие. Книга 2. - СПб.: Издательство ДЕАН, 2009. – 944 с.

4. Федоров Ю.Н. Справочник инженера по АСУТП. – М.: Инфра–Инженерия, 2008. – 928 с.
5. Гарбук С.В., Комаров А.А., Салов Е.И. Обзор информационной безопасности АСУ ТП зарубежных государств. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/analytics/398184.php.
6. Аникеенко В.В. Безопасность АСУТП и контроль привилегированных пользователей. [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/node/11899.