

Каналы технологического управления. Универсальность и безопасность

С.Е. РОМАНОВ, В.А. ХАРЛАМОВ

ЗАО «Юнител Инжиниринг»

Россия

Romanov@uni-eng.ru

КЛЮЧЕВЫЕ СЛОВА

Унификация, безопасность, технология, связь, качество.

1 ВВЕДЕНИЕ

В докладе обосновывается необходимость комплексного подхода к обеспечению современных требований по унификации оборудования и принципов построения каналов, а также обеспечения информационной безопасности в отрасли.

В настоящее время необходимо рассматривать механизмы воздействия на характеристики каналов технологического управления мер по реализации «универсальных» систем связи и информационной безопасности, обеспечить защиту каналов технологического управления от преднамеренного или случайного вмешательства.

Рядовые задачи обеспечения информационной безопасности отличаются от задач обеспечения безопасности технологической информации тем, что здесь важно не только не допустить искажения/поражения информации, но и обеспечить её верную доставку с заданным или требуемым качеством (с сохранением времени доставки, надёжности и безопасности передачи в темпе технологического процесса). Стандартные методы обеспечения информационной безопасности могут негативно сказаться на качестве передачи технологического трафика.

2 УГРОЗЫ ТЕХНОЛОГИЧЕСКОЙ СВЯЗИ

2.1 Проблемы

Технологические каналы и сети связи являются составной частью систем РЗ и ПА, телемеханики, автоматики и диспетчеризации.

Ограниченный набор параметров, характеризующих свойства технологических каналов и сетей связи в прошлом:

- Скорость передачи (время доставки),
- Надёжность,
- Безопасность

в настоящее время расширяется за счёт введения требований по:

- Унификации применяемых технических и сетевых решений, и
- Информационной безопасности (ИБ).

Необходимость реализации новых требований в рамках целевых программ, как правило, рассматривается независимо от их влияния на совокупность параметров технологических каналов.

Поскольку специалисты по информационной безопасности или корпоративной связи имеют малое представление о том, что такое PLC, SCADA, УПАК и другое специальное оборудование, что такое специальные каналы передачи информации, они уверены, что технологические сети изолированы не только от сетей общего пользования, но и от внутренних

сетей предприятия: в них применяются специфическое оборудование, ПО и специальные протоколы, а, следовательно, поразить технологические системы невозможно.

При этом, если ранее нормировка параметров надёжности и безопасности доставки информации в технологических системах связи выполнялась по отношению сигнал/шум или вероятности ошибки в канале, и соответствующим образом выбирались алгоритмы и протоколы передачи и приема, то в настоящее время специалистам приходится учитывать механизмы воздействия на технологические системы, как самих мер по реализации «унифицированных» систем связи и ИБ, так и обеспечивать их защиту от преднамеренного или случайного вмешательства, что раньше не учитывалось:

- Под «унификацией» систем и каналов связи, прежде всего, понимается использование одинакового оборудования, систем управления и протоколов передачи, не предназначенных для специальных целей;
- Задачами ИБ является обеспечение неискажённой передачи информации к правильному адресату;
- Наблюдается рост числа ложных и излишних срабатываний не из-за природных, а техногенных причин.

2.2 Унифицированная аппаратура и программы управления

Место специализированных модемов, приемо-передатчиков и коммуникационных серверов в технологических сетях заняли мультиплексоры и маршрутизаторы, представляющие собой специализированные компьютеры с управляющей системой собственной разработки на базе ОС Linux/Unix, режис QNX или DOS. Структура мультиплексоров и маршрутизаторов, как правило, является модульной: в состав включаются аппаратные и программные подсистемы для решения специальных задач. Для работы с мультиплексором или маршрутизатором используется графический интерфейс GUI человек-машина HMI, реализованный, как правило, на базе ОС Windows или Linux/Unix. GUI/HMI выводит на экран показания функционирования аппаратуры, обеспечивает возможность её конфигурации, а, иногда, ведёт запись отчётов, статистики и архивов. Общаются мультиплексоры и маршрутизаторы между собой и источниками-приёмниками информации по стандартным протоколам, в последнее время чаще по Ethernet. Очень редко выпускаются промышленные версии мультиплексоров и маршрутизаторов: чаще для обычных мультиплексоров и маршрутизаторов выпускаются более стойкие к внешним воздействиям, вибрациям, электромагнитным помехам, температуре, влажности и пр. отдельные модули.

Мультиплексоров и маршрутизаторов в сети всегда несколько – их количество зависит от масштаба технологической системы связи, и они могут быть расположены во внутриобъектовой и межобъектовой сети связи или системной и государственной сети связи, редко - на отдельном канале связи.

В соответствии с правилом, что наибольшее число уязвимостей безопасности обнаруживается в самых распространённых и известных/доступных продуктах, в специализированных компьютерах (мультиплексорах и маршрутизаторах) чаще всего поражается локально или дистанционно по каналам Ethernet GUI/HMI интерфейс на базе ОС Windows или Linux/Unix.

Однако наибольшую опасность представляет собой поражение аппаратного и программного ядра специализированных компьютеров – процессоров и их дисковой системы, поражение возможное дистанционно и локально, немедленно и отложено. Связано это с тем, что ОС Linux/Unix или DOS, используемые в коммуникационном оборудовании, как правило, очень старые, имеют открытые каналы/порты связи/поражения, не имеют никаких средств обеспечения безопасности, и одновременно имеют уязвимости в настоящее время известные очень широко. Результатом поражения процессора может быть, как полный отказ в обслуживании, так и изменение функциональности или содержании передаваемой информации.

В исследуемых в 2011-2012 годах системах обнаружены уязвимости в продуктах RuggedCom, Selta и SEL. В 2012-2013 годах обнаружены и продемонстрированы уязвимости

платформы ABB FOX515/512, доступные не специально подготовленному инсайдеру без специальных технических средств (с обыкновенного ПК).

Время устранения таких уязвимостей обычно превышает один-два года, чаще из-за старости ОС и средств разработки их устранение невозможно вообще.

2.3 Унифицированные решения ИБ

В типовой унифицированной корпоративной-технологической сети можно выделить несколько обособленных зон – корпоративную, административную, бизнес, исполнительную, телемеханизации, автоматизации, диспетчеризации, релейной защиты и противоаварийной автоматики, управления. По крайней мере, четыре последние из которых относятся к технологическому сегменту (каналы телемеханики и данных для нужд РЗА и ПА относятся к их зонам).

Рядовые задачи обеспечения ИБ в типовой унифицированной корпоративно-технологической сети отличаются от задач обеспечения безопасности в технологическом сегменте тем, что в технологических зонах важно не только не допустить искажения/поражения информации, но и обеспечить её верную доставку с заданным качеством (нормированными временем доставки и надёжностью передачи).

Поскольку стандартные методы обеспечения ИБ, например, из ГОСТ Р 34.10 и ГОСТ Р 34.11 (далее ГОСТ Р 34.10/11), основаны на введении информационной избыточности в передаваемые сообщения или сеансы связи, они неминуемо и негативно скажутся как на скорости передачи, так и на надёжности и безопасности передачи технологического трафика. Особенно в таких приложениях, как АСУ ТП, РЗА и ПА. Здесь стандартные методы обеспечения ИБ применяться не могут.

Поскольку в унифицированных системах технологические зоны являются составной частью единой системы связи, возникает противоречие требований ИБ и технологий реального времени.

2.4 Технологические каналы и протоколы в унифицированных системах

Унифицирование свойств и характеристик современных корпоративно-технологических систем не позволяет использовать ряд специальных технических решений по построению технологических каналов связи. Вместо этого тем или иным способом производится адаптация унифицированных решений для нужд технологий реального времени, функционирующих теперь в более тяжёлых условиях.

Типичным и наиболее ярким примером можно считать увеличение числа случаев ложного/излишнего срабатывания систем РЗА при селективных помехах или точечных/единичных воздействиях техногенной природы. Фактически 100% современных алгоритмов передачи сигналов команд РЗ и ПА подвержены воздействию преднамеренных помех с той или иной, обычно низкой степенью устойчивости. Это касается не только аналоговых, но и цифровых каналов связи – меняются лишь механизмы воздействия (например, ошибки адресации или синхронизации в цифровых системах, асимметрия передачи).

2.5 Архитектура унифицированной сети и канала

Происходит это на фоне того, что унифицируется (упрощается и технически ухудшается) структура ВЧ аппаратуры, возрастает число производителей, использующих старые негодные способы передачи информации. В цифровых системах технологической зоны используются модифицированные связные протоколы и стандарты: E1 -> G.709, Ethernet -> IEEE 802.3 - не самые удачные решения, как с точки зрения технологии реального времени и ИБ, так и для передачи критичной инфраструктурной информации.

Поскольку аппаратные унифицированные решения используются и в технологической зоне, на них должны располагаться некоторые специальные требования, например, по параметрам и способам резервирования. Чаще всего это приводит к умножению всего на два (оптических трактов, мультиплексоров и т.д.). А конфликт невозможности разделения зон обслуживания и ответственности между службами технологической зоны и зоны корпоративной связи приводит к дополнительной параллельной установке для служб

технологической зоны облегчённых унифицированных решений технологической связи. А это уже приводит к умножению всего на три. Но сохраняет вероятность поражения функционирования технологической зоны со стороны зоны корпоративной связи через программы и интерфейсы управления и GUI/HMI локально и дистанционно.

2.6 Универсальность и безопасность вместо унификации

ИБ в технологической зоне нужна не только для защиты конфиденциальных данных, а прежде всего для обеспечения непрерывности производственного процесса, невозможности остановить производство. Для чего необходимо перенести риски поражения из локально-дистанционной программно-сеть-связной плоскости в плоскость физического уровня: физически разделить зоны корпоративной и технологической связи, сделать обязательным для совершения какого-либо действия личное присутствие.

Для этого нет необходимости в удваивании аппаратного обеспечения – скорее наоборот, оно сократится - достаточно физически вывести из унифицированных решений сервисы технологической зоны.

С точки зрения технологической зоны унифицированные решения следует отнести к элементам и составным частям физической среды передачи, как к всего лишь одной из многих доступных возможностей и путей передачи информации.

В технологической зоне следует вернуться к принципам функционального резервирования – отказала или поражена одна из точек входа в множество сред передачи, надо использовать другую оптимальную пару (например, одна пара – ДЗЛ-синхронная оптика; другая пара – КСЗ-любая оптика, ВЧ; речевой канал – аналоговый-ВЧ/цифровой-оптика, радио и т.д.).

Из технологической зоны в корпоративную зону следует разрешить только однонаправленную связь, на физическом уровне блокировать обратную связь из корпоративной зоны в технологическую для мониторинга и управления.

В технологической зоне должна максимально использоваться однонаправленная связь. Много устройств с множеством точек входа в корпоративно-технологическую зону, широковещательная передача информации между устройствами и сетями с дистанционным управлением должны быть запрещены, так как приводят к лёгкому поражению всех зон унифицированной системы.

Поскольку одними из самых используемых каналов поражения унифицированных систем и сетей связи являются закладки и инсайд, в технологической зоне необходимо:

- Любые работы с программами и аппаратами привязывать к плановым остановкам основного производства на ремонт. Работы выполнять под надзором специалистов служб технологической зоны;
- Иметь для работы с оборудованием отдельный коммуникационный порт, физически изолированный от других портов. Причём при активации данного порта, чтобы исключить поражение системы во время сеанса, все другие порты связи с подключённым оборудованием и АСУ ТП должны быть отключены.
- Для исключения вероятности отложенного поражения из-за инсайда запретить оборудованию технологической зоны иметь встроенные носители информации: диски и флэш, а ещё лучше и ОС;
- Оборудование технологической зоны должно само уметь определять исправность или поражение унифицированной системы, как среды передачи, и уметь либо подключаться к другой исправной среде передачи, либо отключаться вообще.

В интересах ИБ протоколы и способы передачи, даже унифицированные, модернизируются. Для этого создаётся динамический ситуационный алфавит/словарь (в каждый момент времени может быть принята или передана только определённая информация).

Поскольку в технологической зоне без нарушения парадигмы РЗА и ПА использовать ГОСТ Р 34.10/11 затруднительно, а сами каналы РЗА и ПА относительно низкоскоростные, мощные вычислители успевают в темпе процесса выполнять сложное кодирование передаваемой информации без нарушения базы используемых протоколов и стандартов.

Так в рамках C37.94|G.704 компании ЗАО «Юнител Инжиниринг» удалось получить надёжность передачи сигналов команд РЗ и ПА не хуже 10^{-4} при наихудших безопасностях 10^{-40} и 10^{-77} при $BER=3 \cdot 10^{-3}$, и лучше 10^{-100} и 10^{-200} при $BER=10^{-6}$ при временах передачи 4-6 мсек по любым средам и каналам связи, включая IP/MPLS. Что превышает требования ГОСТ Р 34.10/11 (база кодирования более 10^{12} бит). И имеет более развитую систему диагностики качества и характеристик работы унифицированной среды передачи (например, контролирует задержку и вероятность ошибки канала).

Архитектурные решения зависят от того, в интересах какой конкретно службы внутри технологической зоны создаются каналы или сети связи.

На межобъектовом уровне должно быть все равно, через какую среду передавать информацию. Главное - обеспечить защиту от дистанционных атак, и влияния со стороны параллельно работающих сервисов. Проще всего это обеспечить при помощи технологии DWDM, если речь идёт об оптике, а более общее решение – создание или использование независимой среды передачи для каждого сервиса.

На внутриобъектовом уровне необходимо для каждого сервиса или службы создавать защищённые независимые кластеры, и при необходимости связи с другими кластерами использовать только однонаправленные связи, межсетевые разделительные однонаправленные экраны или защитные модули на базе анализаторов проходящего трафика на соответствие заданному словарю. Размещение экранов на границах каждого кластера, их группы и т.д. создаст многоуровневую эшелонированную оборону.

3 ЗАКЛЮЧЕНИЕ

Начатые компанией ЗАО «Юнител Инжиниринг» в интересах технологического и безопасности кластеров ТЭК России, работы по созданию комплексных решений, показали значительное снижение стоимости и сложности технических и проектных решений при повышении их привлекательности с точки зрения эксплуатации и привлечения к реализации российских производителей.

ЛИТЕРАТУРА

- [1] Positive Technologies, Безопасность промышленных систем в цифрах v2.1, Москва, 2012.
- [2] Digital Security, Безопасность SAP в цифрах, Москва, 2012.
- [3] Юнител Инжиниринг, Угроза безопасности ТЭК России, Москва, 2012.