ДЕНИС ЗОЗУЛЯ
Менеджер по продукции
Control and Industry Solutions,
ООО «Феникс Контакт РУС», г. Москва

ЗАЩИТА ПРОМЫШЛЕННЫХ СЕТЕЙ В СИСТЕМАХ АВТОМАТИЗАЦИИ

Автоматизация опасных объектов требует соблюдения комплекса мер для обеспечения безопасности технологических процессов, таких как резервирование оборудования и систем электропитания, искробезопасность и взрывозащита, а также повышенная надежность компонентов.
Системы автоматизации строятся с применением современных сетевых технологий. Но промышленные сети так же уязвимы, как и офисные, и в отличие от них защите промышленных сетей не всегда уделяется должное внимание.

Специфика промышленных решений информационной безопасности

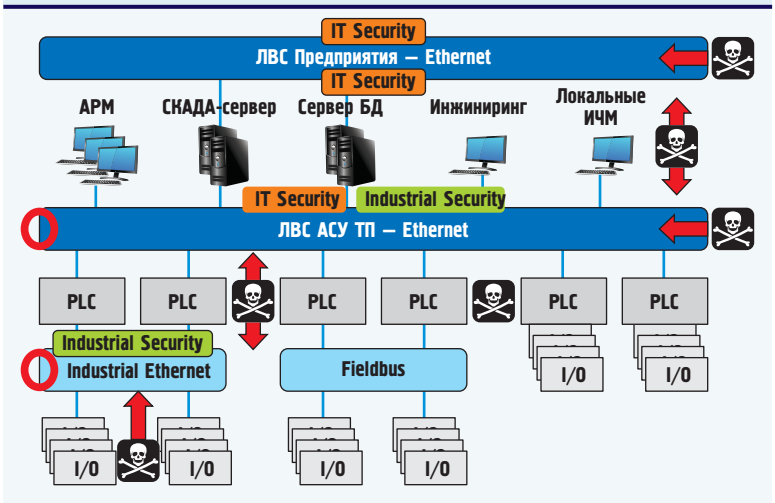
Почему же защите промышленных сетей не всегда уделяется должное внимание. Ответ прост: специалисты в области АСУ ТП не имеют должной квалификации в области информационной безопасности (ИБ), а специалисты в области ИБ не имеют полного представления о технологиях и специфике промышленных систем. Поэтому современные системы АСУ ТП обладают множеством уязвимостей, которые необходимо принимать во внимание и по возможности устранять.

Системы защиты информации и сети должны иметь промышленное исполнение, работать при низких или высоких температурах, сильных вибрациях, быть устойчивыми к наводкам, иметь компактные габариты. Промышленные решения должны быть необслуживаемыми, т.к. устанавливаются они один раз, а обновление ПО, плановые перезагрузки и прочие сервисные действия не предусмотрены. Промышленные системы работают круглые сутки без перерыва и должны обеспечивать безотказную работу.

Квалификация обслуживающего персонала в области информационных технологий не всегда достаточна для правильной настройки сетевого оборудования защиты. Поэтому промышленные решения должны быть, во-первых, просто настраиваемыми любым инженером АСУ ТП по заранее созданным пошаговым инструкциям, а, во-вторых, замена оборудования должна производиться в считанные минуты без дополнительной настройки нового устройства простой установкой карты памяти с конфигурацией из неисправного устройства в новое.

Офисные решения предназначены для защиты данных, персональной или коммерческой информации, промышленные — для обеспечения безопасности технологического процесса и безаварийной работы системы.

Архитектура современных АСУ ТП и карта уязвимостей промышленных сетей



Угрозы в промышленных сетях

Рассмотрим угрозы безопасности технологического процесса, пути их возникновения и возможные последствия. Промышленные Ethernet-сети используются на всех уровнях АСУ ТП — как на уровне связи систем управления между собой (средний уровень), на уровне коммуникации со СКАДА-системами (верхний уровень), так и на уровне распределенной автоматизации (нижний уровень). Сеть любого уровня может нести в себе угрозу безопасности технологического процесса. Поэтому необходимо обеспечивать защиту на любом уровне системы АСУ ТП.

Сетевой шторм

Не все угрозы в сети связаны с умышленными действиями. Порой сбой в сетевом оборудовании может привести к серьезным неполадкам в сети. Например, для резервирования топологии очень

Межсетевые экраны FL MGUARD

часто используется стандартный алгоритм RSTP, который по факту не является промышленным и отказоустойчивым.

Сбой сетевого интерфейса на каком-либо устройстве может привести к развитию сетевого шторма, лавинообразному росту уровня широковещательного трафика в сети. Многоадресные посылки в сети с инфраструктурой без поддержки его фильтрации также приводят к росту широковещательного трафика. Определенный уровень широковещательного трафика влечет за собой отказ RSTP, и в сети начинается шторм.

При сетевом шторме происходит полная потеря связи между системами, контроллерами, серверами и рабочими местами оператора. Система управления может зависнуть или потерять связь с подсистемами, а это приводит к аварийному останову технологического процесса или, в худшем случае, к полной потере контроля над процессом.

Сетевой шторм может образоваться в самой сети АСУ ТП, прийти из сети предприятия или любой смежной сети. Поэтому необходимо произвести комплекс мер защиты всей системы в целом. Инфраструктура сети должна поддерживать функции фильтрации или ограничения, иметь возможность настройки управлением потоком данных. В этом случае паразитный трафик будет выведен на безопасный уровень, не приводящий к сбоям сети.

Все современные серии коммутаторов Phoenix Contact поддерживают функцию защиты от сетевого шторма, обеспечивая максимальную безопасность сети. Все точки соединения различных подсетей должны разделяться межсетевыми экранами, которые полностью отсекают паразитный трафик и ограничивают доступ неавторизованного персонала. Промышленные межсетевые экраны FL MGuard от Phoenix Contact блокируют нежелательный трафик, а также позволяют ограничивать пакеты, применяемые для DDoS-атак, которые не только затрудняют нормальную коммуникацию между системами, но и могут вывести из строя систему управления в целом.

Неавторизованный доступ

Главная уязвимость промышленных систем — это возможность неавторизованного доступа к системе управления. Очень часто сама сеть управления опасным процессом распределена по всему объекту. И даже если доступ к центральному управляющему контроллеру закрыт физически, то сетевой доступ к нему, подчиненным системам, рабочим местам и серверам СКАДА можно получить из любой точки сети. Если сеть предприятия подключена к промышленной без межсетевого экрана, то к системам управления возможен доступ извне. Контроллер можно перепрограммировать, остановить выполнение программы, изменить установки или передать сигнал управления. Если в общей системе работают несколько подсистем различных производителей, то сервисные инженеры могут получить доступ к смежной системе и выполнить нежелательные действия.

Рассмотрим способы защиты системы автоматизации от неавторизованного доступа. Во-первых, необходимо разделить сети верхнего, среднего и нижнего уровней межсетевыми экранами. Так мы ограничиваем доступ к локальным системам извне. Для получения доступа к данным системы, передачи команд или программирования системы в межсетевом экране настраиваются правила доступа с различным уровнем.

В стандартных межсетевых экранах правила доступа статические, но часто необходимо обеспечивать временный доступ к системе без дополнительной перенастройки межсетевого экрана. Решения информационной безопасности MGuard поддерживают функцию пользовательского межсетевого экрана. Данная функция позволяет создать динамические права временного доступа к определенным частям системы АСУ ТП. Для доступа необходима аутентификация на самом межсетевом экране по заранее созданным учетным данным на самом устройстве или RADIUS-сервере.

Заключение

Информационная безопасность АСУ ТП — новая и перспективная тенденция в современных системах автоматизации. Внедрение системы защиты — это инвестирование в безопасность людей, экологии и защита от финансовых потерь из-за сбоев в работе сетевой инфраструктуры или неавторизованного доступа к системам управления.

ООО «Феникс Контакт РУС»
119619 Москва,
Проектируемый проезд 5167,
д. 9, стр. 1
Тел.: +7 (495) 933-8548
Факс: +7 (495) 931-9722
info@phoenixcontact.ru
www.phoenixcontact.ru