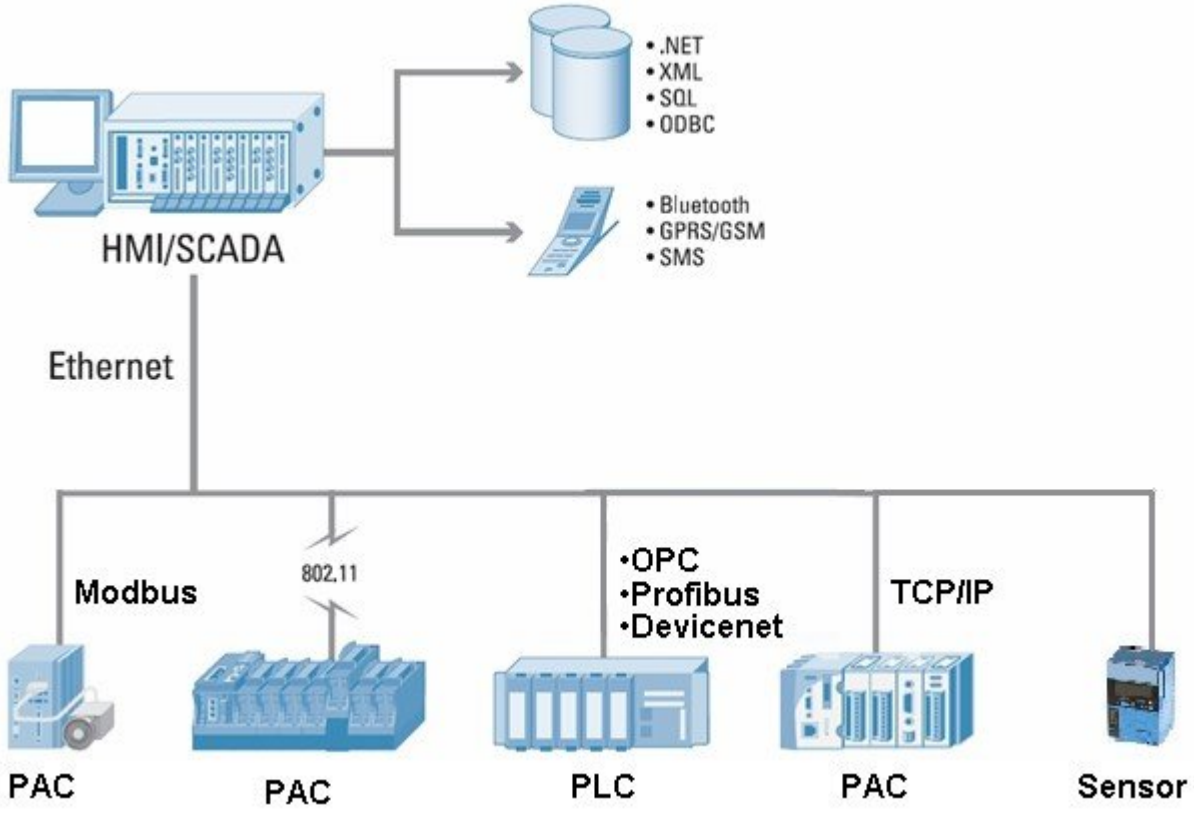
Безопасность Систем SCADA и АСУТП

СИСТЕМЫ УПРАВЛЕНИЯ АСУТП

Автоматизированная система управления технологическим процессом (АСУ ТП) — комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях. Большая часть этих систем была разработана в те годы, когда вопросы кибербезопасности имели низкий приоритет. Эти системы работали в изолированной среде, на базе индивидуального программного и аппаратного обеспечение, а так же устаревших коммуникационных технологий.

В отличие от старых систем, современные комплексы SCADA и АСУТП базируются на стандартных протоколах связи. Большинство контроллеров поддерживает адресные протоколы в IP среде. Стандартные операционные системы (Windows или UNIX) используется в операторских, которые в свою очередь имеют доступ к отдалённым системам контроля посредством частных каналов связи, предоставляемых телекоммуникационными компаниями.



В результате этого взаимодействия один из потенциальных доступов в систему обеспечивает сама коммуникационная сеть. Современные технологии кибератак ориентированы на обнаружение и использование различного рода узких мест в компонентах коммерческих системах. Способность операторов стратегических инфраструктур обнаружить возникающие угрозы и уязвимости в системе является необходимым условием для разработки эффективной стратегии безопасности и принятия контрмер.

Уязвимость Систем АСУТП

УЯЗВИМОСТЬ В БЕЗОПАСНОСТИ

Системы SCADA и АСУТП обычно разрабатывались в соответствии с самыми жесткими международными требованиями в части безопасности. Тем не менее, уровень их безопасности уже не соответствует сегодняшним требованиям. Подробный анализ потенциальных угроз и их возможных последствий вызывает ряд серьезных вопросов, касающихся безопасности и требующих решения следующих задач:

- **Связь с внешним миром.**
- **Взаимозависимости.**
- **Сложность.**
- **Унаследованные системы.**
- **Доступность системы.**
- **Автономность.**
- **Доступность информации.**

Связь с внешним миром. Современные системы SCADA и АСУТП как правило связаны с корпоративными сетями, которые функционируют на базе стандартных операционных систем и имеют доступ в Интернет. Несмотря на то, что эти современные “удобства” повышают эффективность работы предприятия, они параллельно создают дополнительную уязвимость, так как не обеспечены требуемыми для промышленных систем контроля средствами безопасности.

Взаимозависимости. Из-за высокой степени взаимозависимости между секторами инфраструктуры, сбой в одном секторе может распространиться на другие секторы системы. Кибер - террористы могут воспользоваться этой взаимозависимостью для организации волны разрушений и таким образом увеличения общего экономического ущерба.

Сложность. Требования к контролю в режиме реального времени требует непрерывного доступа к системам большого количества пользователей, а также связи с корпоративными бизнес сетями. Различие в принципах построения систем ИТ и АСУТП, а также отсутствие понимания специалистами каждой из этих двух структур специфики второй технологии, приводят к проблемам в координации безопасности сетей между этими двумя ключевыми группами.

Унаследованные системы. Хотя старые системы АСУТП рассчитаны на работу в автономном режимы, они, как правило, не имеют структуры паролей и администрации безопасности. Более того, в этих системах не предусмотрены средства защиты протоколов, чем и обуславливается их уязвимость.

Уязвимость Систем АСУТП

Доступность системы. Даже ограниченное подключение к Интернету подвергает АСУТП всем существующих угрозам взаимосвязанных компьютерных сетей, вирусов, червей, троянов, хакеров и кибер - террористов. Многочисленные каналы управления, использующие беспроводные или специально выделенные линии (VPN), проходящие по коммерческим телекоммуникациям, также мало защищены от дублирования передаваемых данных. Эти вопросы особенно критичны в областях промышленности, расположенных на взаимосвязанных предприятиях и системах контроля имеющих удаленный доступ на территории или за её пределами.

Автономность. До сих пор не найдено приемлемой альтернативы вместо использования корпоративных сетей для вспомогательных модулей и подсистем (типа Архиваторов; серверов истории и Базы Данных). Зарубежные производители комплексов АСУТП не всегда считаются с государственными интересами тех стран, в которых используются их системы. Ещё одной проблемой являются договора технической поддержки дистрибьюторами и третьими лицами.

Доступность информации. Техническая Спецификация и Руководства по эксплуатации комплексов АСУТП являются общедоступными, в том числе и для хакеров, которые скачивают их из Интернета и используют для своей технической подготовки. Злоумышленники не обязаны быть экспертами в системах контроля, что бы нанести необратимый ущерб критическим инфраструктурам государства.

Подробная информация о различных типах систем АСУТП и их уязвимости для кибертеррора расположена на сайте www.modcon.ru

Кого должна беспокоить защита АСУТП

Защита используемых в промышленности систем АСУТП это общая задача владельцев критических инфраструктур, руководителей промышленных объектов и государственных служб безопасности, ответственных за обеспечение безопасности предприятий и населения.

Для обеспечения зашиты от кибертеррора необходимо принятие всеми заинтересованными сторонами следующих мер безопасности:

- ***Владельцы предприятий***, заинтересованные в обеспечении безопасность своих систем АСУТП, представляют свои отчёты правительству и тем самым привлекают государственные инвестиции.

- ***Государственные, региональные и городские органы*** сотрудничают, обмениваются информацией по вопросам безопасности, уязвимости и угрозах в промышленности, с целью определения необходимого бюджета, создания фондов и базы данных по проблемам в безопасности инфраструктур, а так же организации исследований, разработок и периодической инспекции общими усилиями.

- ***Промышленные организации, проектные институты и технические отделы***, обеспечивающие координацию между несколькими секторами, а так же содействующие в преодолении организационных сложностей сотрудничают в части разработки стандарты и принципов руководства для каждого конкретной отрасли.

- ***Коммерческие структуры, поставщики и системные интеграторы***, разрабатывающие и поставляющие программное обеспечение и оборудование для комплексов АСУТП удовлетворяют потребности владельцев и пользователей этих систем в области безопасности.

- ***Специализированные исследовательские центры*** изучают и разрабатывают решения по безопасности, а также средства защиты и определения уязвимости оборудования и программного обеспечения.

- ***Университеты и колледжи*** обеспечивают высококвалифицированные кадры для будущего поколения специалистов таким образом, чтобы удовлетворить нужды и запросы промышленности в части безопасности комплексов АСУТП.

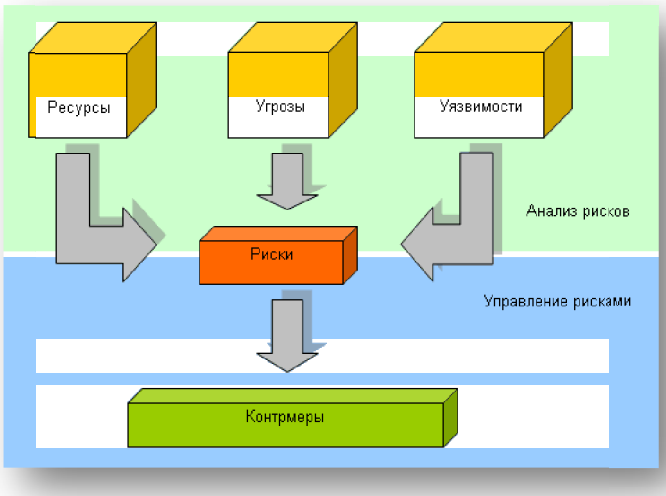
Принципы Защиты Систем Автоматики

Основные принципы для обеспечения защищённой Системы контроля.

Обеспечение Безопасности систем SCADA и АСУТП является сложной задачей, требующей комплексного подхода. Необходимо решать сегодняшние проблемы безопасности и в тот же самый момент быть готовыми к требованиям завтрашнего дня. Владельцы активов и операторы систем должны быть достаточно компетентными, чтобы управлять кибер рисками в эксплуатируемых системах.

Для выполнения этой задачи:

I. Необходимо применять различные средства безопасности, имеющие положительную практику эксплуатации и соответствующий уровень надёжности под многочисленными кибер атаками.
II. Пересмотр архитектуры системы управления и создание новой, соответствующей поставленным требованиям



Такая работа основывается на следующих основных принципах:

1. Создания видения, концепции и стратегии.
2. Определение наивысшей цели.
3. Определение средств для достижения этого видения, а затем выявление проблем, препятствующих достижению целей.
4. Порядок действий в случае успешной реализации предыдущего пункта. Ключевой набор таких действий определяет приоритеты.
5. Контроль над всеми процессами, привязанный к датам, так что в прогрессе достижения всех целей возможна корректировка отрабатываемых процессов.

Правительство и государственные службы играют решающую роль в этом процессе, поскольку инфраструктуры имеют ключевое значени для национальной безопасности. Кибербезопасность и её совершенствования должны сочитаться с другими приоритетами в инвестициях. Порой очень трудно оправдать расходы безопасности, не имея на это обоснованных «бизнес-кейсов».

Безопасность Промышленного Сектора

Видение Безопасности в Промышленности.

Наблюдая сегодняшнюю действительность кибер угроз, можно смело предположить, что в ближайшие 10 лет будут разработаны многоуровневые системы защиты для промышленных систем контроля критически важными объектами. Такие системы будут установлены и способны поддерживать непрерывную работу критически важных функций в течение и после кибер событий.

Важно отметить два определения
"Критические приложения" и "Соизмеримость с рисками"!

"Критические приложения" это те функции, потеря которых может непосредственно привести к долгосрочной остановке производства, серьезным экономическим потерям, ущербу окружающей среде, общественной угрозе, в том числе и гибели людей.

"Соизмеримость с рисками" это определение служит для определения технического уровня системы по отношению к вероятности кибер атаки и её последствий. Цель этого подхода заключается в повышении безопасности до уровня, при котором риск является приемлемым при достаточно низкой стоимости и предприятие продолжает функционировать и быть экономически эффективным. Оптимальная оценка рисков включает в себя как немедленные потери и косвенные последствия.

Цели Системы Безопасности

Современные системы SCADA и АСУТП являются основным элементом в управлении сложными производственными процессами. Ущерб, нанесённый в результате кибер атаки, имеет негативное воздействие на активы, общественную и национальную безопасность, а так же безопасность окружающей среды. Владельцы активов и критических инфраструктур должны чётко и однозначно понимать все имеющиеся риски и быть способными управлять ими, обеспечивая кибер надёжность своих систем. Государство и правительство так же играют важную роль в этих усилиях, поскольку последствия этих риски могут иметь негативные последствия для общества и национальной безопасности.

Следующий список содержит краткое описание каждой из задач:

- ✓ **Измерения и оценка степени безопасности.** Компании должны тщательно понимать их текущий уровень безопасности, чтобы определить степень уязвимости, а так же какие меры необходимы для их устранения. Для этого необходимо иметь возможность мониторинга состояния безопасности системы управления в режиме реального времени.

- ✓ **Разработка и интеграция защитных мер.** Защитные меры могут быть разработаны и применены, тем самым снижая уязвимость системы, потенциальные угрозы и их последствия. Существующие решения безопасности, разработанные для устаревших систем, серьёзно ограниченны в возможностях конфигурации оборудования. Со временем они будут заменены или модернизированы. Новое поколение комплексов АСУТП имеют встроенные в систему, многоуровневые средства защиты, обеспечивающие единую безопасность всей структуры.

- ✓ **Обнаружение вторжений и построение стратегии реагирования.** Инструментарий Кибер вторжения становится все более сложным, тем самым делая уязвимой любую систему. Этот требует использование таких средств безопасности в промышленности, которые позволят автоматическое реагирование и принятие срочных мер по исправлению ситуации в ответ на попытки вторжения.

- ✓ **Отработка функций по поддержанию безопасности.** Поддержание активной кибербезопасности систем в долгосрочной перспективе потребует серьёзных ресурсов и тесного сотрудничества между всеми сторонами. Владельцы активов и пользователи должны будут взаимодействовать по всем направлениям, в том числе и с правительством, для устранения препятствий на пути прогресса и создания единой политики, которая ускорит устойчивый технологический прогресс всей отрасли.

- ✓ **«Безопасность» уже на стадии дизайна.** Системы SCADA и АСУТП должны быть защищёнными уже на стадии их разработки. Владельцы активов и пользователи промышленных системам АСУТП должны настаивать на выполнение конкретных требований, с тем чтобы поставщики обеспечивали поставку надёжных и защищённых систем.

Все перечисленные цели обеспечивают логическую основу для стандартизации единых усилий промышленности, правительства и других заинтересованных сторон.

Выводы и Заключение…

Задача №1 - Чтобы определить факторы риска и потенциальные опасности в системе АСУТП, необходимо использование единой методологии, а также профессиональная подготовка, наличие стандартов и глубокое понимание отраслевой практики. Для определения уровня безопасности систем необходимо использование единых согласованных принципов и требований. Эти требования должны серьезно анализироваться, чтобы база данных в данной сфере с годами пополнялась новыми сведениями.

Обмен информацией, связанной с кибер безопасностью, угрозами, рисками и уязвимостями требует наличия особой практики, инструментария, учебных материалов, которые стали появляться только в конце 2008 года. Механизмы обмена новейшей и востребованной информацией, это одна из основ кибер безопасности.

Задача № 2 - Требуется серьёзная профессиональная подготовка, средства и новые методы для обеспечения безопасности систем. Специально разработанные учебные курсы помогут владельцам активов в повышении своей информированности и создания культуры безопасности, связанной с системами SCADA и АСУТП.

Уязвимости в системах, появившиеся в результате связи между производственными и корпоративными сетями, требуют обеспечение защиты этих интерфейсов. Широкое использование беспроводной связи и удаленного доступа создало дополнительные риски, которые так же должны быть устранены при условии сохранения эффективности системы и всех её составляющих.

Требуется периодическое тестирование систем контроля, для определения:

1. Степени защищённости системы.
2. Технического состояния используемых средств защиты и их технического обслуживания.
3. Эффективности обнаружения, изоляции и автоматического реагировании на кибер - атаки.

Использование описанных в данной статье принципов анализа безопасности и защиты систем SCADA и АСУТП позволит обеспечить кибер устойчивую архитектуру систем для их успешного применения в промышленности.

MODCON SYSTEMS LTD.
Leaders in Analysis, Measurement and Automation
Перовская улица 61/2, стр. 1, Москва 111394
www.modcon.ru moscow@modcon-systems.com Тел: +7 (495) 9891840 Факс: +7 (495) 9891840 (9)