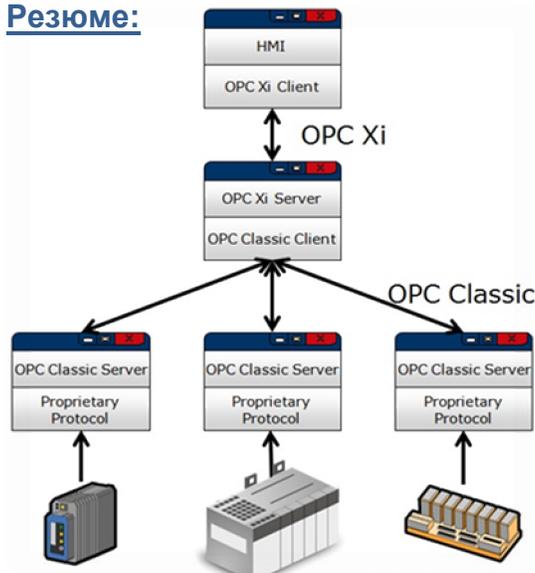




# Обеспечьте Кибербезопасность своих АСУ ТП основанных на OPC!

## Резюме:



OPC Classic это индустриальный протокол связи между различными приборами, контроллерами и ПК в промышленных системах управления. Этот протокол широко применяется для связи между полевым оборудованием различных производителей и Машинными Интерфейсами (HMI); Системными Архиваторами (Data Historian), передачи данных в корпоративные сети.

В этой статье компания **МОДКОН** предлагает рассмотреть два различных метода защиты систем контроля применяющих технологию OPC Classic:

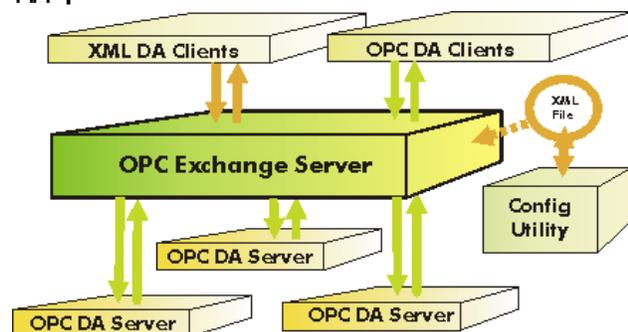
- I. Сегментация сети с выделением участков использующих OPC и защищённых по периметру брандмауэрами.
- II. Оптимизация функций протокола и их адаптация в операционной системе.

Оба метода защиты доступны к использованию в агрессивной среде индустриальных систем контроля

## OPC Classic – Ведущая технология в мире промышленной интеграции.

OPC Classic был разработан в 1996 (ранее назывался OLE) с целью взаимодействия систем управления различных производителей друг с другом. Сегодня OPC превратился в ведущую в мире технологию для интеграции различных модулей и систем автоматизации.

Не один промышленный протокол связи не добился такого широкого признания как OPC Classic. Этот протокол одновременно используется на всех уровнях АСУ ТП, соединяя Машинные Интерфейсы (HMI) с серверами, полевым оборудованием и отдалёнными терминалами (RTU) проникая через все уровни одновременно поддерживая связь индустриальных систем (DCS) с корпоративными сетями (ERP).





# Обеспечьте Кибербезопасность своих АСУ ТП основанных на OPC!

Причина такой популярности OPC проста – это единственный, по настоящему универсальный интерфейс для связи между различными модулями промышленных устройств, программного обеспечения и приложений, разных производителей и в независимости от используемых протоколов связи в АСУ ТП.

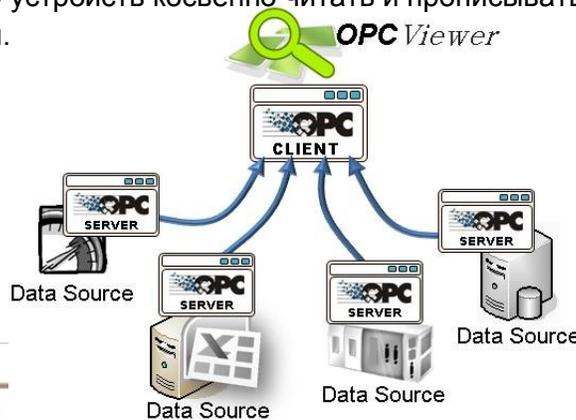
Перед разработчиками OPC стояла конкретная задача – разработать специальные драйверы, способные поддерживать связь, например одного HMI с более чем 200 производителями PLC и DCS. Добившись успехов в этой области, они сосредоточили свои усилия на оптимизации OPC Драйверов своего продукта таким образом, что бы в дальнейшем осуществить связь между OPC Серверами и производителями систем управления.

Для конечного пользователя значительное преимущество использования OPC имеет минимальная и очень простая конфигурация при достаточно сложной архитектуре всей системы. Другими словами, при интеграции могут использоваться команды с именами элементов (или целых групп) вместо того что бы постоянно определять местонахождения функции или команды (например, 40156 или %MW7:5), так как это работает у других производителей.

В результате использование OPC экономит время во время настроек и конфигурации, по сравнению с использованием традиционных протоколов связи.

В результате, сегодня редко встречаются предприятия или промышленные объекты, на которых хотя бы частично не используется OPC.

Технология OPC основана на архитектуре Клиент/Сервер. OPC Сервер это программное обеспечение, опрашивающее OPC устройства (например, PLC; DCS; RTU или SCADA Контроллеры), использующие собственные протоколы (например MODBUS или PROFIBUS). Затем Сервер позволяет мультимедийный доступ к этим данным по средствам COM, что в результате позволяет каждому из OPC устройств косвенно читать и прописывать данные в таблицах других OPC пользователей.





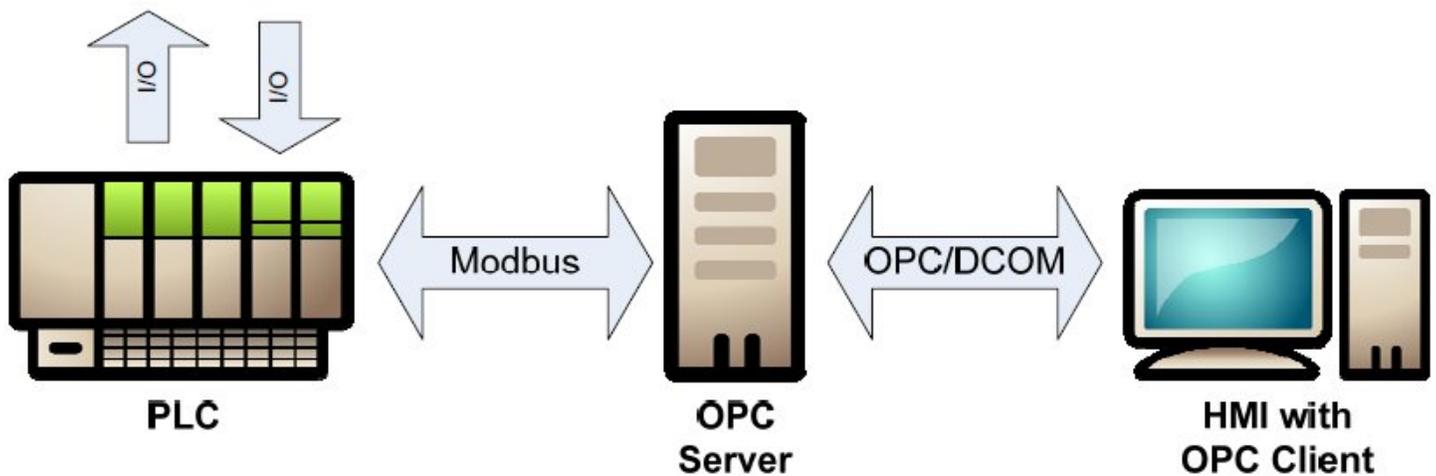
## Обеспечьте Кибербезопасность своих АСУ ТП основанных на OPC!

OPC Клиент это приложение, отвечающее на запрос OPC Сервера, формирующее в структуру своего ответа запрашиваемые данные. Машинный интерфейс (HMI) может быть OPC Клиент, тем самым позволяя передачу данных на следующий уровень SCADA к OPC Серверу. В то же самое время Машинный Интерфейс (HMI) может быть и OPC Сервер по отношению к полевому оборудованию и контроллерам, одновременно запрашивая у них все необходимые данные. В результате гибкость данной технологии позволяет обмен данными между OPC клиентами.

Что бы проиллюстрировать архитектуру Клиент-Сервер, представьте себе три основных компонента системы контроля уровня жидкости в резервуаре:

- **ПЛК на базе MODBUS** для обработки логических алгоритмов и функций контроля.
- **Платформа OPC Сервера** поддерживающая протокол MODBUS.
- **Машинный Интерфейс (HMI)** для управления операторами системой контроля.

Машинному Интерфейсу (HMI) необходимо иметь доступ к контроллеру для того чтобы прочитать уровень воды в резервуаре, сравнить с установками оператора и выполнить необходимые функции контроля над наливным насосом, задвижками и сигнализацией тревоги. Для интеграции всех перечисленных функций необходимо запросить у ПЛК данные по протоколу MODBUS (соблюдая архитектуру запроса Сервером Клиента) и преобразовать их в OPC для отображения Машинным Интерфейсом (HMI). Когда обработанная информация возвращается обратно в ПЛК, так же необходимо выполнить все преобразования OPC<->MODBUS соблюдая архитектуру - Клиент/Сервер и при этом «поменяться ролями» - OPC Сервер, ранее запросивший данные у OPC Клиента, становится OPC Клиентом ожидая сформировать ответ на запрос OPC Сервера (ранее выполняющего роль OPC Клиента). Такой «обмен ролями» выполняется при каждом сеансе связи.



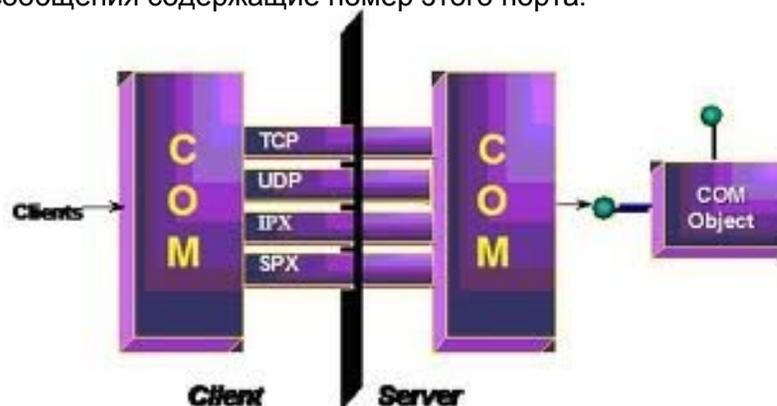


## Проблемы Кибербезопасность OPC Classic!

Не смотря на то, что многие производители систем контроля, системные интеграторы и даже пользователи SCADA очень рады использовать OPC Classic, эксперты в области безопасности сообщают о **серьёзных «пробелах» в безопасности этого протокола.**

1. OPC Classic был разработан на базе технологии DCOM в 1996 году (в то время вопросов кибер атаки не существовало). Основной задачей было широкое использование этой технологии. Этот фактор один из основных проблем безопасности. **Принцип технологии основан на динамическом назначении коммуникационных портов.**

Каждый, кто хоть немного знаком со структурой TCP (и UDP), понимает масштабы рисков связанных с динамическим назначением портов. Речь идёт о специальном номере, встроенном в каждое передаваемое по TCP или по UDP сообщение, а не о физических Ethernet портах. Например, протокол MODBUS использует порт №502, а HTTP использует порт №80 и редко их кто-то меняет. В таких случаях очень просто определить защиту – брандмауэр блокирует все сообщения содержащие номер этого порта или наоборот пропускать только сообщения содержащие номер этого порта.



Одна из уязвимостей протокола OPC Classic это отсутствие возможности использовать фиксированный номер порта. Вместо этого они динамически назначают новый номер порта при каждом открытии сеанса связи OPC Клиентом. Подключившись к OPC Серверу OPC Клиент запрашивает номер TCP порта, который должен быть использован для этой сессии. Затем производится новое соединение и снова отправляется запрос на номер свободного порта.

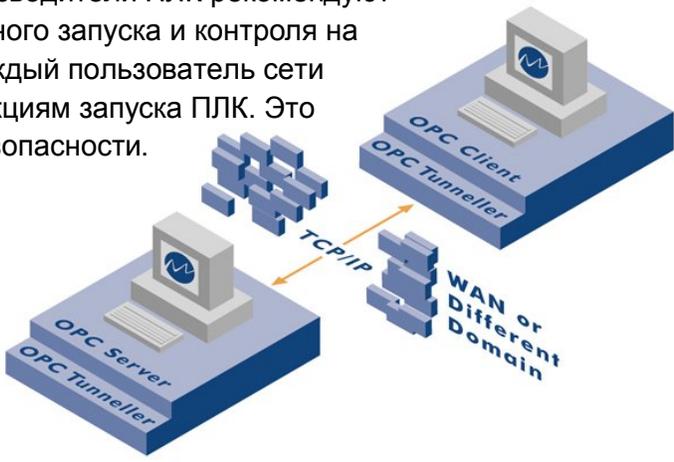
OPC Серверы используют любой порт в диапазоне между 1024 и 65535. По этой причине протокол OPC сложно и почти невозможно защитить с помощью стандартных брандмауэров, так как при настройках останется открытым весь диапазон используемых протоколов. Словами специалистов ИТ это «огромная дыра», которую могут использовать злоумышленники для нанесения кибер атаки.





# Проблемы Кибербезопасность OPC Classic!

2. OPC Classic обладает чрезмерно расширенным и многоуровневым правом доступа. Это достаточно трудоёмкий процесс для самостоятельной конфигурации. По этому, часто поставщики SCADA рекомендуют не определять средства защиты. Например, производители ПЛК рекомендуют определить все средства отдалённого запуска и контроля на Анонимный вход. В результате каждый пользователь сети потенциально имеет доступ к функциям запуска ПЛК. Это серьёзная проблема для Кибербезопасности.



3. OPC Classic чаще остальных протоколов цитируется прессой, как протокол подверженный кибер атакам. За последние 10 лет половина вирус, червей, троянов и ИТ - Происшествий были зарегистрированы в среде DCOM RPC на разновидностях протокола OPC. Как обсуждается в профессиональных форумах, эта тенденция только растёт.

*.....«За последние несколько месяцев два из основных векторов кибер атак были направлены на Windows DCOM (Distributed Component Object Model) интерфейс службы RPC (Remote Procedure Call).... Это фаворит атак нынешних вирусов и само регистрирующихся червей. Наблюдается нарастающая тенденция в этой области.».....*

Благодаря усовершенствованным Операционным Системам за последние несколько лет, упомянутая проблема стала менее угрожающей. Но огромное количество червей и троянов, существующих в этой кибер среде, по-прежнему ищут слабо-защищённые системы OPC.





# Почему необходимо защищать системы OPC?

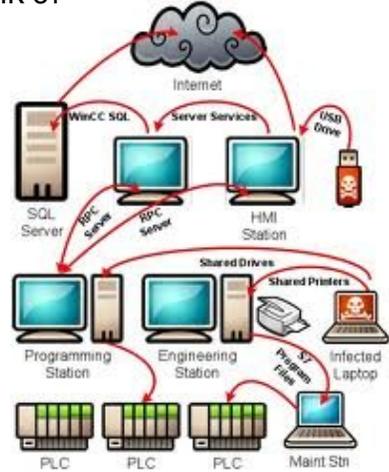
Этот вопрос часто возникает так как OPC Сети редко имеют прямое подключение к Интернету. К сожалению, даже если у Вас полностью изолированные сети, обеспечение надёжной защиты необходимо для безопасной эксплуатации всего комплекса АСУ ТП.



В Июле 2010 червь Stuxnet наглядно это доказал, что злоумышленники сфокусировали своё внимание на промышленных системах. В случае со Stuxnet, червь распространяется через USB ключи. Последний анализ показал, что Stuxnet был специально разработан для атаки на продукцию производства Siemens – WinCC; PCS7 и Step7. Stuxnet оказался способным выкрадывать информацию, обрабатывать её, видоизменять модификацию и логику контроллера, при этом скрывать исходные коды алгоритмов ПЛК от пользователей.



W32 это название мене известного вируса, но на прямую связанного с OPC. В 2009 году этот вирус проник через одного из отдалённых OPC Клиентов к OPC Серверу заразив по многоуровневую систему контроля. W32 вызывал сбои в работе ключевых OPC Серверов этой сети тем самым полностью парализовав работу всей системы SCADA.



## Защитите свой OPC Classic!

Хорошая новость в том, что первые две проблемы безопасность OPC (Чрезмерный Уровень Доступа и Динамичное распределение портов) теперь решаемы самими пользователями OPC если каждый запрос и ответ в среде OPC контролировать с помощью глубокой инспекции.

Для решения третьей проблемы OPC, а именно уязвимости технологии DCOM RPC, достаточно использовать хороший антивирус, ограничивающий на уровне системы управления эфирные окна сеанса обмена запросами и ответами между OPC Клиентами и Серверами. Этот способ значительно снижает возможность вирусов и червей использовать уязвимости этой технологии.

Если ваши OPC компьютеры не имеют антивирусной программы, обеспечивающей глубокую инспекцию протокола OPC, мы настоятельно рекомендуем этот как первый шаг. Представление подробной инструкции и рекомендации по детальной защите протокола OPC выходит за рамки этой статьи, но мы будем рады ответить на ваши вопросы и детально проработать необходимую защиту для ваших OPC Сетей.



Ещё одна новость! благодаря новым технологиям, разработанным в последнее время, стало на много проще создавать OPC защиту. Основываясь на международный стандарт безопасности ANSI/ISA-99, мы рассмотрим в следующей статье решения для обеспечения безопасности ваших OPC Classic систем.