ПРИГЛАШАЕМ ПОСЕТИТЬ СТЕНД НАШЕЙ КОМПАНИИ
НА МОСКОВСКОЙ МЕЖДУНАРОДНОЙ ВЫСТАВКЕ
«НЕФТЬ И ГАЗ» / MIOGE – 2012
25–29 ИЮНЯ, МОСКВА, ЭКСПОЦЕНТР,
ПАВИЛЬОН №2, ЗАЛ №2, СТЕНД 23В10

vira realtime

автоматизация и связь

## НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ:

- Разработка, проектирование и поставка «под ключ» АСУ ТП
- Разработка и производство программных средств для систем диспетчерского контроля и управления
- Распространение продукции фирмы Motorola на территории Российской Федерации

## УСЛУГИ:

- Проектно-изыскательские работы
- Разработка и производство аппаратных средств АСУ ТП
- Разработка прикладного и системного программного обеспечения
- Строительно-монтажные работы
- Пусконаладочные работы
- Обучение эксплуатационного персонала
- Гарантийное и послегарантийное обслуживание
- Поддержка партнеров

## ОБЛАСТИ ВНЕДРЕНИЯ:

- Газовая промышленность
- Нефтяная промышленность
- Нефтехимическая промышленность
- Энергетика
- Коммунальное хозяйство
- Тепло и водоснабжение
- Транспорт

## КОНТАКТНАЯ ИНФОРМАЦИЯ:

НПА ВИРА РЕАЛТАЙМ
г. Москва, Щёлковское шоссе, 77
Телефоны: (495) 723 75 59
Телефон/факс: (495) 662 56 92
http:\\www.rlt.ru

MOTOROLA

*Авторизованный дистрибьютор*

## ПРОДУКЦИЯ:

**Шкафы РЛТ-ТМ, ЩОПС**
Шкаф РЛТ является программируемым интеллектуальным устройством, используется в качестве аппаратуры телемеханики в составе автоматизированной системы диспетчерского контроля и управления.

**Блок-контейнеры**
ПКУ, Связи, ДЭС, КТП
Антивандальные, модульные здания, размещаемые в составе трасс нефтепроводов, газопроводов, предназначены для размещения в них аппаратуры, приборов и других элементов системы телемеханики, связи и электроснабжения, в том числе ДЭС.

**Система обнаружения утечек**
Система обнаружения утечек (PAS, Чехия и ООО «Энергоавтоматика») служит для защиты трубопроводов с жидкообразной и газообразной средой, а также их смесью.

**Контроллеры Motorola**
Контроллеры Motorola предназначены для решения широкого круга задач, которые необходимы для работы в сложных системах диспетчерского контроля и управления.

**ПО «Сириус-ИС», «Сириус-Скада», «Сириус-ВИН», «АРМ диспетчера»**
Представляют собой комплекс программ для построения:
- систем автоматизации локальных промышленных установок
- систем управления сложными, территориально распределенными промышленными объектами
- систем автоматизации научных исследований

# Аутентификация удаленных контроллеров в системах диспетчерского контроля и управления, использующих стандартные телемеханические протоколы

В статье проанализированы потенциальные угрозы, возникающие ввиду отсутствия механизмов аутентификации удаленных контроллеров в SCADA-системах при использовании стандартных телемеханических протоколов. Предложена процедура проверки подлинности удаленных контроллеров телемеханики в SCADA-системах на примере протокола МЭК-60870-5-104. Описана конкретная реализация предложенной процедуры.

ООО «НПА Вира Реалтайм»

## Введение

Системы диспетчерского контроля и управления (СДКУ; англоязычный термин – SCADA Systems) широко используются в нашей стране и во всем мире для управления технологическими процессами в различных отраслях промышленности: в нефте- и газодобыче, на трубопроводном транспорте, при переработке и распределении нефтепродуктов, в химической промышленности, электрических сетях, водохозяйстве и др.

Оборудование и программное обеспечение (ПО) для таких систем поставляют многие фирмы – как известные промышленные гиганты, так и более скромные по размерам компании. Исторически сложилось так, что обмен информацией между пунктом управления (диспетчерским пунктом) и удаленными контроллерами телемеханики, играющий крайне важную роль в работе всей системы, не стандартизован. Это приводит к тому, что каждый крупный производитель разрабатывает и использует в своих системах свой собственный протокол обмена информацией, который по лицензионным соображениям не может быть использован другими участниками рынка. Небольшие компании, не имея достаточных ресурсов для проведения полного цикла разработки, часто применяют протоколы с ограниченной функциональностью и сомнительной надежностью, что сказывается на качестве работы всей СДКУ и приводит к обоснованным претензиям со стороны заказчика.

С другой стороны, даже применив оборудование и ПО известного производителя, заказчик оказывается привязан к этому производителю на многие годы, поскольку из-за несовместимости по протоколу связи невозможно заменить ПО или оборудование какой-то части системы на продукцию другого производителя – нужно менять всю систему целиком, что на крупных промышленных объектах практически неосуществимо.

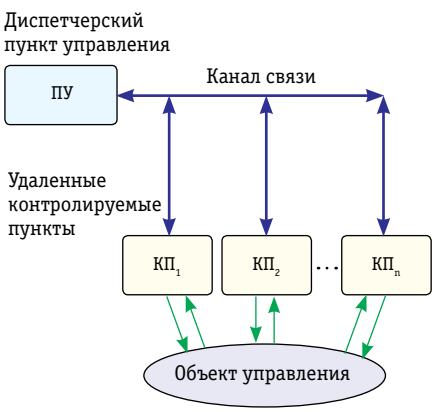


Рис. 1. Типовая СДКУ с пунктом управления и удаленными контролируемыми пунктами

Выходом из создавшегося положения могла бы стать разработка и принятие международного стандарта, регламентирующего информационный обмен в SCADA-системах. А до тех пор пока такого универсального стандарта нет, пользователи пытаются применить для своих нужд открытые общепринятые протоколы (стандарты «де-факто»), или появившиеся в последнее время отраслевые стандарты: Modbus, DNP3.0, IEC 101/104 и т. п.

В качестве примера можно привести решение ОАО «АК«Транснефть» – крупнейшего оператора магистральных нефтепроводов России – впредь использовать в своих системах диспетчерского управления только стандартные протоколы информационного обмена, а именно протоколы МЭК семейства 60870-5-101 (104).

Эти протоколы были разработаны Международной электротехнической комиссией для использования в энергетических отраслях промышленности. Имеются соответствующие Российские стандарты: ГОСТ Р МЭК 60870-5-101-2006 и ГОСТ-Р МЭК 60870-5-104-2004. С некоторыми ограничениями эти

протоколы можно применять и в других отраслях, прямо не связанных с энергетикой.

Применение открытых стандартных протоколов в СДКУ позволяет конечному заказчику не стать заложником ценового диктата какой-то одной компании-производителя. Появляется возможность использовать на своих объектах оборудование и ПО альтернативных поставщиков без опасений получить «нестыковку».

При всех достоинствах такого подхода есть в нем и серьезный недостаток: весьма облегчается умышленное вмешательство посторонних лиц в работу систем телемеханики. Причина – открытость протокола обмена и отсутствие каких-либо механизмов проверки аутентичности (подлинности) удаленных контроллеров в этих протоколах. Представим ситуацию, когда злоумышленник, пользуясь удаленностью контролируемых пунктов (КП) от центра управления (и от любых населенных пунктов вообще), подменяет в канале связи реальный контроллер телемеханики фиктивным, передающим в Центр сфабрикованную информацию. Это может вызвать неадекватную реакцию диспетчера и – как следствие – привести к аварии на объекте.

Поскольку многие из СДКУ используются для контроля объектов, заключающих в себе потенциальную угрозу для человека и окружающей среды, вопросы обеспечения безопасности их работы выдвигаются на первый план.

### Потенциальные риски

Потенциальные угрозы, возникающие ввиду отсутствия механизмов аутентификации удаленных контроллеров в SCADA-системах, можно разделить на две группы (см. рис. 1).

1. Подмена пункта управления (ПУ). Выдача несанкционированных команд удаленному контроллеру, прямое вмешательство в технологический процесс и вследствие этого нарушение нормальной работы системы.

2. Подмена контроллера на контролируемом пункте (КП). Передача в Центр сфабрикованной информации, не отражающей текущего состояния контролируемого объекта, для того чтобы вынудить диспетчера произвести какие-то действия, или наоборот – не предпринимать каких-то необходимых действий.

Совершенно понятно, что любой из этих сценариев может быть осуществлен только при наличии у злоумышленника физической возможности вхождения в канал связи между КП и ПУ. Однако, учитывая удаленность многих КП и безлюдность территории их размещения, такая возможность не представляется слишком уж невероятной.

С другой стороны, при использовании TCP/IP-сетей связи во многих современных СДКУ такую подмену удаленного устройства можно осуществить, просто изменив настройки сетевого оборудования, не выходя из офиса.

Поэтому, при всей важности охраны инфраструктуры связи, совершенно необходимо предусмотреть алгоритмические методы защиты SCADA-систем от подобных угроз. Сформулируем задачи, которые должны решаться этими методами для противодействия таким угрозам:

Удаленный контроллер, или RTU (от англ. Remote Terminal Unit – удаленный терминал), должен иметь возможность убедиться, что контролирующая станция – действительно «та самая», которой и позволено управлять.

Контролирующая станция должна иметь возможность проверить, что удаленный контроллер, с которым установлена связь, – настоящий, а не сфальсифицированный.

Другими словами, встает задача взаимной аутентификации ПУ–КП в системах диспетчерского контроля и управления. Особенно актуальна эта задача, естественно, в больших, территориально распределенных системах.

Здесь необходимо сделать два замечания. Во-первых, в каких-то конкретных случаях достаточно проводить только один из этапов проверки, скажем, только аутентификацию контроллеров (см. ниже). Во-вторых, такая очевидная мера защиты, как шифрование информационного обмена, во многих случаях по разным причинам невозможна и в рамках данной статьи не обсуждается.

### Методы аутентификации

В настоящее время задача взаимной аутентификации субъектов (устройств), взаимодействующих по открытым каналам связи, хорошо изучена и продолжает разрабатываться в разных направлениях. Из множества существующих методов аутентификации (см. например, [*1*]) в современных компьютеризированных системах диспетчерского контроля и управления, использующих микропроцессорное оборудование, наиболее естественно применить криптографические технологии, основанные на механизме так называемой «аутентификации с запросом и подтверждением», или CRAM (от англ. Challenge-response authentication mechanism).

В этом механизме широко используются так называемые «хэш-функции» – специально сконструированные процедуры, позволяющие получить из произвольного текста некий код, «однозначно» идентифицирующий этот текст:

H = Hash (message).

Длина кода H фиксирована и для разных функций может составлять 128 бит, 160 бит, 256 бит и более. Считается, что практически невозможно подобрать другой текст так, чтобы он имел тот же самый хэш-код. Затраты времени, которые понадобились бы для такого подбора, превышают все разумные пределы даже при использовании самых современных компьютеров. Другое важное свойство хэш-функций – однонаправленность, то есть невозможность восстановить исходное сообщение по его хэш-коду.

Примеры широко известных хэш-функций: MD4, MD5, SHA-1, ГОСТ Р 34.11-94 и т. п. Последние две функции в этом списке являются национальными стандартами в области криптографической защиты в США и России соответственно.

Суть процедуры CRAM в простейшем случае состоит в следующем:

- Сервер посылает клиенту уникальный, заранее неизвестный запрос (server_challenge).
- Клиент, зная пароль доступа (secret_password), вычисляет хэш-код

Hash_code = Hash (server_challenge || secret_password)

и отправляет этот код в качестве ответа (response) серверу, тем самым подтверждая, что он знает пароль.

‣ Сервер вычисляет ожидаемое значение хэш-кода и убеждается, что клиент ответил правильно.

Здесь важно то, что пароль должен быть известен обеим сторонам: как серверу, так и клиенту, чтобы они могли вычислить хэш-код одинаково.

Приведенная процедура рассчитана на тот случай, когда канал связи клиент – сервер не защищен от подслушивания. Сам пароль в открытом виде никогда не передается по каналу. Невозможность восстановить пароль по подслушанному запросу и ответу обеспечивается стойкостью использованной хэш-функции к взлому. Предполагается, что при использовании качественной хэш-функции взлом возможен только путем полного перебора всех паролей (brute-force attack), что практически неосуществимо за разумное время, если длина пароля составляет не менее 128 бит (16 байт).

Взаимная аутентификация осуществляется путем применения вышеуказанной процедуры в обоих направлениях. Имеется стандарт – Challenge-Handshake Authentication Protocol (CHAP), описанный в документе RFC 1994. Этот стандарт, например, используется PPP-серверами для идентификации удаленных PPP-клиентов.

### Аутентификация контроллеров при использовании стандартных телемеханических протоколов

Задача проверки подлинности удаленных контроллеров в SCADA-системах может решаться с помощью описанной выше процедуры CRAM. Однако эта задача осложняется тем, что в современных стандартных телемеханических протоколах, применение которых в некоторых случаях обязательно, отсутствуют какие-либо штатные процедуры аутентификации ПУ–КП.

Тем не менее реализация процедур аутентификации возможна на прикладном уровне, при условии согласования всех деталей между разработчиками ПУ и КП.

Для примера рассмотрим возможную реализацию процедуры аутентификации с запросом и подтверждением «поверх» стандартного телемеханического протокола МЭК-60870-5-104 (см. [*2*]).

Протокол МЭК-104. Это протокол типа ведущее устройство – ведомое устройство. Связь осуществляется по сети TCP/IP. Ведущее устройство устанавливает соединение с ведомым и инициирует передачу данных. Обычно первым действием является команда общего опроса для получения «среза» текущего состояния всех телеметрических параметров.

Предлагается несколько модифицировать эту процедуру. После активации канала командой “Start Data Transmission” и перед выдачей команды общего опроса (логично сделать это именно до опроса, хотя и не обязательно) ведущее устройство проверяет, то ли это ведомое устройство, которое должно быть.

Шаг 1. Ведущее устройство генерирует уникальный запрос, скажем, 64 случайных байта, и отправляет его ведомому устройству в виде 32 команд записи уставки с заранее согласованными адресами: в терминах протокола МЭК это команды типа 49 – «команда уставки, масштабированное значение».

Шаг 2. Ведущее устройство посылает ведомому команду «Ответить на запрос аутентификации». В терминах протокола МЭК это «Однопозиционная команда» (тип 45) по заранее оговоренному адресу. (Необходимость этого шага вызвана тем, что иначе ведомому устройству трудно отследить обновление всех 32 уставок, содержащих запрос.)

Шаг 3. Ведомое устройство вычисляет хэш-код (128 бит) от полученного запроса, объединенного с паролем (конкатенация строк), и формирует ответ-подтверждение ведущему устройству в виде 8 сообщений типа «Событие»: тип данных 35 – «значение измеряемой величины, масштабированное значение с меткой времени»; адреса переменных заранее согласованы.

Шаг 4. Ведомое устройство отправляет ведущему сигнал «Ответ на запрос аутентификации готов» в виде «события» с типом данных 30 – «одноэлементная информация с меткой времени».

Шаг 5. Ведущее устройство проверяет полученный хэш-код и в зависимости от результата выставляет флаг «Удаленный контроллер прошел идентификацию».

По соображениям безопасности эта процедура должна повторяться ведущим устройством для каждого ведомого устройства, с которым он работает, через случайные промежутки времени. Представляется, что делать это слишком часто нет необходимости. Разумными можно считать интервалы порядка 10–30 минут. При использовании высокоскоростных цифровых каналов связи вся процедура занимает доли секунды и практически незаметна для диспетчера.

Понятно, что вместо протокола МЭК можно использовать практически любой другой телемеханический протокол, переписав процедуру в соответствующих терминах и используя соответствующие типы данных для обмена запрос – ответ.

Здесь тоже есть одна проблема: для реализации этого механизма на практике требуется применение весьма производительных контроллеров телемеханики, которые к тому же имеют возможности программирования, достаточные для реализации всех описанных процедур.

### Механизм идентификации контроллеров на морском терминале КТК

Ниже в качестве примера кратко описана реализация этой идеи в SCADA-системе Каспийского трубопроводного консорциума (КТК). Система в числе прочего контролирует три выносных причальных устройства (ВПУ), расположенных в море на расстоянии нескольких километров от берега. Эти ВПУ полностью автоматизированы, необитаемы и являются необслуживаемыми.

В рамках проекта расширения и модернизации Каспийского трубопроводного консорциума проводилась замена программного обеспечения и оборудования SCADA-системы, в том числе и контроллеров, установленных на выносных причальных устройствах.

Связь с этими контроллерами осуществляется через промежуточ-

ный коммуникационный контроллер по УКВ-радиоканалу, не защищенному от прослушивания.

Используются контроллеры телемеханики Motorola ACE3600 и протокол информационного обмена берег – море MDLC (Motorola Data Link Communication). Протокол является закрытым, в нем применяется коммуникационный пароль. Все это затрудняет несанкционированное вмешательство в информационный обмен между пунктом управления и контролируемым пунктом. Однако в данном случае заказчик выразил желание усилить защиту.

Было принято решение использовать в данном проекте описанную выше процедуру аутентификации. Поскольку согласовать процедуру с зарубежным разработчиком ПО верхнего уровня SCADA не представлялось возможным, аутентификация была реализована внутри системы на уровне обмена береговой контроллер (FIU) – удаленный контроллер (RTU) (рис. 2).

Чтобы проверить канал связи, береговой коммуникационный контроллер периодически обменивается тестовыми пакетами с удаленными контроллерами. Было решено совместить обе процедуры и использовать этот же трафик для аутентификации устройств в системе. Теперь контроллер FIU периодически (точнее, со случайным интервалом 10–20 сек) передает одному из контроллеров RTU, установленных в море, запрос идентификации "SC" (Server Challenge). Запрос имеет длину 144 байта и содержит:

- счетчик (монотонно возрастающее длинное целое число);
- метку времени (с разрешением до миллисекунд);
- адреса отправителя и получателя (в терминах протокола MDLC);
- псевдослучайную компоненту 512 бит, сгенерированную встроенным ПО контроллера FIU.

Кроме того, к запросу добавляется 128-битовый код аутентификации сообщения, вычисленный на основе вышеуказанных полей и секретного пароля-ключа Key с помощью хэш-функции Hash (msg) – так называемый hash-based message authentication code (HMAC) – см. документ RFC 2104:

$$HMAC(Key, msg) = Hash(Key1 \| Hash(Key2 \| msg)),$$

где:
$Key1 = 0x5C5C...5C \oplus Key$,
$Key2 = 0x3636...36 \oplus Key$,
$\oplus$ – исключающее «ИЛИ»,
$\|$ – знак конкатенации строк.

Получив запрос "SC", удаленный контроллер, зная пароль-ключ, вычисляет ожидаемое значение HMAC и сравнивает его с полученным в пакете, тем самым убеждаясь, что отправитель знает пароль.

Убедившись в том, что полученный код HMAC совпадает с ожидаемым, удаленный контроллер RTU:

- модифицирует полученный запрос и создает сообщение "CC" (Client Challenge), имеющее аналогичную структуру и поля; в частности, заменяется псевдослучайная компонента;
- вычисляет новый код HMAC (Key,"CC"‖"SC"), используя пароль-ключ Key;
- отправляет то и другое в качестве подтверждения на берег в адрес FIU.

Береговой контроллер FIU, в свою очередь, вычисляет ожидаемое значение HMAC для модифицированного запроса и убеждается в том, что RTU знает пароль.

Таким образом, во внутренней базе данных FIU для каждого удаленного контроллера формируются флаги «свой – чужой». Эти флаги доступны ПО верхнего уровня SCADA, которое может информировать диспетчера об их изменении и тем самым предупреждать о возможной недостоверности информации, получаемой от удаленных устройств.

Описанный алгоритм представляет собой процедуру односторонней аутентификации удаленных устройств-источников телеметрической информации. Как видно из описания алгоритма, проверка подлинности береговых контроллеров FIU со стороны RTU тоже реализована, но сделано это по упрощенной схеме. Причин этому несколько:

- устройства FIU расположены на берегу на охраняемой территории;
- FIU не являются источниками команд для удаленных RTU, а служат только коммуникационными контроллерами в телеметрической сети связи;
- в данном конкретном проекте удаленный RTU не имеет ни одной потенциально опасной команды. Его роль сводится к измерению текущих параметров погрузки нефти на танкер и включению/выключению сигнальных устройств (сирена, мигающая лампа и т. п.).

Уникальность запросов, которая требуется стандартом CHAP, обеспечивается в данном случае генератором псевдослучайных последовательностей, счетчиком запросов и меткой времени, присутствующими в каждом запросе. Это требует тщательной синхронизации внутренних часов всех контролле-

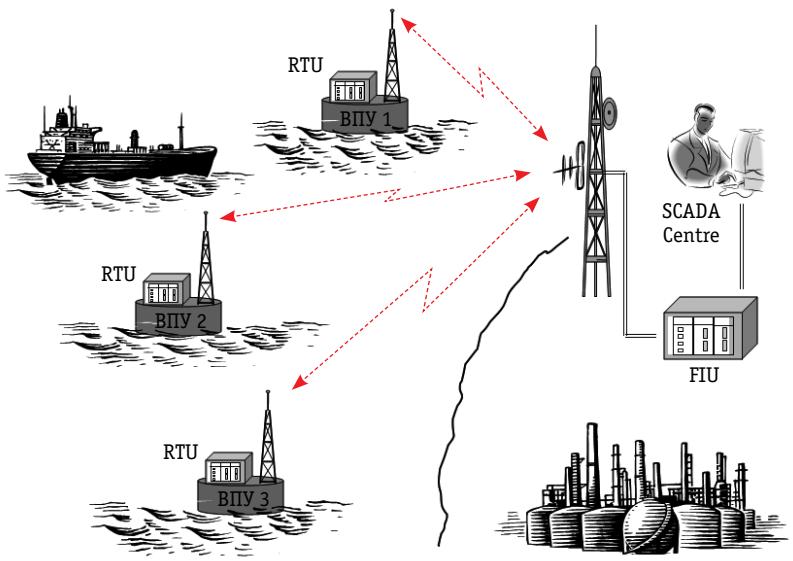


Рис. 2. Морской терминал КТК

ров, задействованных в процедуре аутентификации. Синхронизация времени реализована с помощью встроенного механизма контроллеров Motorola ACE3600, который обеспечивает точность до нескольких миллисекунд, чего более чем достаточно для данных целей.

Ключи-пароли, с помощью которых вычисляются коды аутентификации HMAC, должны периодически обновляться, причем синхронно во всей системе. Использование удаленной загрузки ключей по открытому каналу связи неприемлемо с точки зрения обеспечения безопасности всей процедуры. Вместе с тем частые выезды обслуживающего персонала «в море» для локальной загрузки ключей в удаленные контроллеры нежелательны по соображениям удобства эксплуатации системы.

Поэтому была реализована следующая схема:

- В контроллеры загружается файл, содержащий сразу 256 ключей.
- Каждый ключ представляет собой случайно сгенерированную последовательность 64 байт, то есть длина ключа равна 512 битам.
- При каждом вычислении кода HMAC от какого-то сообщения (message), прежде всего, на основании этого сообщения находится число i = i (message) в диапазоне от 0 до 255, которое используется как индекс в массиве ключей. Соответствующий ключ Key [i] используется для вычисления кода HMAC (Key [i], message).
- Поскольку сами сообщения-message генерируются случайным образом, то и ключи-пароли, используемые для аутентификации этих сообщений, выбираются всякий раз непредсказуемо.

Загруженный файл ключей используется в течение не более одного года, после чего он должен быть заменен другим файлом. В случае длительного присутствия на удаленных морских причальных устройствах неавторизованных лиц (ремонтные бригады сторонних организаций, группы экологов, контролеры и проч.) возможна внеплановая замена файла ключей-паролей в системе.

Следует еще раз подчеркнуть, что сам трафик телеметрической информации не шифруется. Ключи-пароли используются только в схеме опознавания «свой – чужой».

*Литература*

*1. Б. Шнайер.* Прикладная криптография. – М.: «Триумф», 2002.

*2.* ГОСТ Р МЭК 60870-5-104-2004. Национальный стандарт Российской Федерации. Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 104. Доступ к сети для ГОСТ Р МЭК 870-5-101 с использованием стандартных транспортных профилей. Официальное издание. М.: Госстандарт России, 2004.

А. Р. Стефанюк, канд. физ.-мат. наук, ст. н. с.,
Институт Проблем Управления РАН,
Д. Г. Конотоп, начальник отдела разработки ПО САУ,
ООО «НПА Вира Реалтайм»,
тел.: (495) 723-7559,
e-mail: info@rlt.ru,
www.rlt.ru