Многофункциональный встраиваемый контроллер

Часть 1

Александр Елисеев (г. Вильнюс, Литва)

В статье рассматривается контроллер «M2M ассистент», созданный на основе платы ARMGeoSpyder3. Контроллер выполняет ряд функций, необходимость в которых возникает при разработке систем удалённого мониторинга и управления через Интернет. Описаны архитектура программного обеспечения контроллера и взаимодействие с внешними устройствами и службами.

Введение

Устройство «M2M ассистент» (см. рис. 1) разработано для демонстрации возможностей платы ARMGeoSpyder3.1 (см. рис. 2). Подробное описание платы приведено в [1]. Плата оснащена набором интерфейсов, позволяющим реализовать типовые функции в сфере удалённого мониторинга и управления (M2M) и локальных применениях. Контроллер «M2M ассистент» можно рассматривать как основу для различных приложений, где компактность кода, небольшое число параметров и удобный доступ к настройкам (см. рис. 3) сокращают время освоения.

Рис. 1. Сборка «M2M ассистент» без корпуса

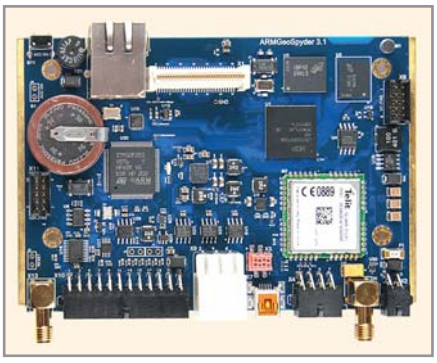

Рис. 2. Плата ARMGeoSpyder 3.1

Важным достоинством контроллера «M2M ассистент» является возможность полной смены программного обеспечения через Интернет по беспроводному каналу связи.

На данный момент «M2M ассистент» уже применяется в различном оборудовании, промышленных механизмах и установках, например, в блоках управления механизмами ангарных ворот (см. рис. 4). Промышленные ангарные ворота имеют в длину несколько десятков метров, приводятся в движение синхронной работой нескольких двигателей и снабжены десятками датчиков, предотвращающих аварийные ситуации и предупреждающих о необходимости технического обслуживания приводов и тяговых элементов. Минимизировать риски аварий и отказов таких ответственных объектов, как ангарные ворота аэропортов, позволяет «M2M ассистент», который может посылать речевые сообщения о нежелательных изменениях в работе механизмов, отображать на дисплее позицию датчиков, делать записи в журнал событий для прогнозирования износа и т.д.

Ниже представлен список функциональных возможностей контроллера «M2M ассистент»:

- повышенная надёжность функционирования за счёт встроенного контроля;
- возможность работы от аккумулятора с интеллектуальным зарядным устройством, гибким управлением потреблением и экономичным режимом сна;
- одновременная работа в сети Интернет через проводной и беспроводной интерфейсы, маршрутизация между интерфейсами;
- организация виртуальных каналов для обеспечения защищённой связи через Интернет;
- встроенный web-сервер с технологией CGI и SSI и защитой по спецификации SSL;
- встроенные FTP-сервер и клиент;
- встроенный DNS-клиент;
- встроенный клиент точного времени (протокол SNTP);
- встроенный почтовый клиент (протокол SNMP);
- встроенный агент SNMPv2, отвечающий спецификациям RFC1213 и RFC1471–RFC1473;
- встроенный сервер NAT;
- шлюз к внешним устройствам через простой протокол M2M с возможностью перепрограммирования внешних устройств;
- шлюз к облакам Google через механизм Google Fusion Tables;
- командно-диагностический интерфейс, работающий по протоколам VT100 и Telnet;
- работа в качестве прозрачного ретранслятора между удалённым клиентом Telnet и собственными портами RS-232;
- работа в режиме прозрачного доступа к встроенному модему GSM;
- унифицированное редактирование всех параметров по SMS или по TCP;
- возможность автоматической проверки наличия обновления собственного ПО и скачивания с удалённых серверов в Интернет;
- расширенная функция Over-the-air programming (OTA), когда перепрограммируется не только само устройство, но и все присоединённые к нему по локальной сети внешние устройства;
- менеджер команд и событий по TCP, SMS или звуковому каналу GSM;
- проигрыватель звуковых файлов как в GSM-канал, так и на внешние громкоговорители;
- конфигурируемый голосовой оповещатель;
- три независимых телеметрических регистратора внешних и внутрен-

Рис. 3. Дисплей пользовательского интерфейса «M2M ассистент»

Рис. 4. Блок управления воротами авиационного ангара с телеметрическим узлом на базе ARMGeoSpyder3

них сигналов и переменных с периодом выборки 1...10 000 с и возможностью записи на карту памяти microSD и передачи в Интернет;

- непрерывный регистратор сигналов в реальном времени с периодом выборки от 10 мс и сохранением данных в файлы размером до 2 Гб;
- регистратор координат, получаемых с модуля GPS/GLONASS/Galileo, с записью в файлы различных форматов и передачей в Интернет;
- настраиваемый графический интерфейс пользователя на базе 24-битного ЖК-дисплея с разрешением 320 × 240 пикселей;
- универсальный загрузчик образов Windows CE или Linux.

Данный перечень функций «M2M ассистент» не является полным и продолжает расширяться. Последние обновления бесплатно доступны на интернет-странице поддержки устройства.

Установка, конфигурация и обновление программного обеспечения

Программное обеспечение «M2M ассистент» записано в микросхему типа NAND Flash на плате ARMGeoSpyder3. Приложение полностью готово к работе менее чем через 1 с после подачи питания. Пользователь может выбрать для исполнения другой образ приложения, который находится на карте памяти microSD. Последняя содержит файловую систему FAT32 и все основные файлы с настройками, конфигурационные файлы приложений, файлы журналов, сценарии, папки web и FTP, исполняемые образы и др. Такое решение удобно для быстрой смены конфигурации и программного обеспечения в приборе, которое может быть сведено к простой замене карты microSD.

f [_none_] 1 945 440 k of 1 955 488 k free

f:*.*

Name	Ext	Size	Date	Attr
[BOOTLOGS]		<DIR>	03.04.2012 10:13	-a—
[FONTS]		<DIR>	03.04.2012 10:13	-a—
[GFTDATA]		<DIR>	03.04.2012 10:13	-a—
[GFTLOG]		<DIR>	03.04.2012 10:13	-a—
[GPSDATA]		<DIR>	03.04.2012 10:13	-a—
[HMI]		<DIR>	03.04.2012 10:13	-a—
[M2M]		<DIR>	03.04.2012 10:13	-a—
[SOUNDS]		<DIR>	03.04.2012 10:13	-a—
[SSL]		<DIR>	03.04.2012 10:13	-a—
[WEBPRIVDIR]		<DIR>	03.04.2012 10:13	-a—
[WEBPUBLDIR]		<DIR>	03.04.2012 10:13	-a—
APN	LST	165	23.01.2012 15:05	-a—
BOOT	BIN	1 000 992	08.04.2012 14:17	-a—
BOOTPARAMS	INI	16 022	06.04.2012 16:00	-a—
CODEC	INI	273	23.01.2012 15:05	-a—
GSM	json	3 188	23.01.2012 15:05	-a—
ID	TXT	20	23.01.2012 15:05	-a—
IOconf	json	5 132	23.01.2012 15:05	-a—
SLOG	json	2 384	23.01.2012 15:05	-a—

Рис. 5. Структура папок на карте памяти SD-платы ARMGeoSpyder3

На рисунке 5 приведена структура папок на карте microSD устройства. Файловая система «M2M ассистент» имеет разветвлённую структуру; в Приложении 1 к статье (www.soel.ru) приведены её основные элементы и файлы.

Обновление ПО на плате ARMGeoSpyder3 заключается в замене файла BOOT.BIN с исполняемым образом на новую версию. Несмотря на большое количество функций контроллера, размер двоичного исполняемого образа программного обеспечения «M2M ассистент» составляет чуть больше 1 Мб в сжатом виде. При таком размере полное обновление ПО даже по каналу GPRS-связи не вызывает трудностей. Файл можно обновить несколькими способами:

- загрузить с помощью FTP-клиента, подсоединившись к FTP-серверу устройства;
- послать команду по SMS, чтобы устройство само подключилось к удалённому FTP-серверу и скачало файл;
- послать команду по протоколу TCP на скачивание файла с удалённого FTP-сервера;
- загрузить файл средствами web-браузера, создав специальную страницу для встроенного web-сервера;
- непосредственно переписать файл на карте microSD.

При скачивании файла через Интернет контроллер выберет один из действующих каналов: GPRS или Ethernet. Предпочтение будет отдано каналу Ethernet. Если для обновления файла используется встроенный в устройство FTP-сервер, то он одновременно доступен и через GPRS, и через Ethernet по номеру порта 21. Доступ к FTP лучше защитить, и тогда устройство можно сконфигурировать на организацию канала VPN, который, в свою очередь, организуется либо через Ethernet, либо через GPRS.

Файл BOOT.BIN может быть сжат несколькими алгоритмами. Тип сжатия файла система определяет автоматически при загрузке. Кроме того, файл может быть зашифрован алгоритмом AES с длиной ключа 256 бит. Целостность файла проверяется контрольной суммой MD5. В случае повреждения файла система его не загружает, и в работе остаётся первоначаль-

ная версия «M2M ассистент», записанная в NAND Flash.

В контроллере предусмотрена возможность автоматической проверки на заданном FTP-сервере наличия файла BOOT.BIN. В устройстве задаются адрес FTP-сервера, режим доступа (активный или пассивный), параметры учётной записи, название файла и папки, в которой должен находиться файл.

Автоматическую загрузку файла BOOT.BIN можно запретить, изменив параметры в файле BOOTPARAMS.INI, который содержит все основные установки и параметры системы в текстовом формате <мнемоника переменной>=<значение> и комментарии, начинающиеся с символа <;>. Такое представление выбрано с целью упрощения редактирования файла. В случае утраты файла BOOTPARAMS.INI или его повреждения, система при загрузке создаст новую версию этого файла на карте microSD с установками по умолчанию. При включённом устройстве редактирование параметров в файле BOOTPARAMS.INI можно выполнить различными способами:

- через интерфейс RS-232 посредством терминальной программы по протоколу VT100;
- через Интернет или локальную сеть Ethernet по протоколу Telnet;
- через Интернет или локальную сеть Ethernet по протоколу HTTP с помощью встроенного web-сервера;
- через Интернет или локальную сеть Ethernet по протоколу FTP;
- через Интернет или локальную сеть Ethernet по протоколу SNMP;
- с мобильного устройства посредством SMS;
- с удалённого сервера посредством специального протокола.

По сути система не потеряет работоспособность, даже если карта microSD будет не заполнена, но при этом ряд служб не будет работать.

Формат файлов конфигурации JSON

При рассмотрении файловой системы «M2M ассистент» часто встречаются конфигурационные файлы с расширением JSON. Формат JSON широко применяется в интернет-технологиях и является стандартной нотацией описания объектов на языке JavaScript. Формат JSON используют для обмена командами и данными многие известные интернет-службы, такие как облачные сервисы Google, сайты погоды, обмена файлами и т.п. Поскольку контроллер тесно взаимодействует с Интернетом, поддержка файлов JSON вполне логична. Однако удобство данного формата побудило использовать его и для хранения локальных настроек программного обеспечения. С помощью формата JSON можно описать сложные структуры данных, при этом такой формат легко воспринимается зрительно, в отличие, например, от формата XML, который был создан для аналогичных целей.

В качестве положительных особенностей формата JSON можно назвать:

- краткость и наглядность синтаксиса;
- лёгкость редактирования;
- поддержку кодировки UTF8;
- наличие доступных в Интернете в интерактивном режиме средств проверки синтаксиса;
- наличие открытых библиотек на разных языках программирования;
- глубокую интеграцию с технологиями Интернета.

В листинге 1 ниже приведён пример конфигурационного файла в формате JSON, встроенного в «M2M ассистент» сервера NAT, который осуществляет трансляцию пакетов интернет-протоколов из публичной сети во внутреннюю сеть в соответствии с правилами трансляции, указанными в файле.

Листинг 1

```
{
"NATPMAP": [
{
// Первая запись трансляции
"Protocol" : "TCP",
"IP" : "192.168.1.31",
"ExtPort" : 81,
"IntPort" : 80
},
{
// Вторая запись трансляции
"Protocol" : "TCP",
"IP" : "192.168.1.32",
"ExtPort" : 82,
"IntPort" : 80
},
{
// Третья запись трансляции
"Protocol" : "TCP",
"IP" : "192.168.1.33",
"ExtPort" : 83,
"IntPort" : 80
}
]
}
```

В данном примере представлено описание массива NATPMAP, содержащего три объекта. Объекты массива своих имён не имеют, доступ к ним осуществляется по индексу. Каждый объект массива здесь содержит четыре пары ключ/значение. Ключ Protocol может применяться со значениями TCP, UDP, ICMP. Ключу IP соответствует запись IP-адреса во внутренней сети, на который будет перенаправлен пакет, пришедший из публичной сети. Ключ ExtPort имеет значение номера порта-адресата. Ключ IntPort имеет значение порта, на который будут перенаправлены пакеты во внутренней сети. Комментарии начинаются с символов // и продолжаются только до конца строки. В целом имена ключей и наборы значений определяются приложением и должны быть описаны в спецификациях. Также строго должна выдерживаться структура данных.

Подключение к Интернету

Важнейшим свойством «M2M ассистент» является постоянное подключение к сети Интернет. Для этого используется сразу два канала связи – GPRS и Ethernet. Большое внимание уделяется надёжности поддержания связи. Для этого применяется несколько средств:

- контроль доступности корневых доменов Интернета;
- периодические посылки контрольных пакетов TCP;
- встроенный агент SNMP для удалённого контроля параметров сетевого стека;
- встроенный протокол RIP2 для обнаружения маршрутов.

Контроль доступности корневых доменов используется в канале GPRS. Это связано с тем, что существует повышенный риск соединения по GPRS без выхода в публичный Интернет либо разрыва связи с Интернетом. Недоступность корневых доменов указывает приложению на невозможность доступа к Интернету. Названия и количество корневых доменов в приложении пользователь может изменить в файле BOOTPARAMS.INI. Реакцией приложения на отсутствие связи с корневыми доменами может быль либо повторное установление связи по GPRS, либо сброс всего устройства.

Периодическая посылка TCP-пакетов может быть включена пользователем, если в его распоряжении есть удалённый сервер, распознающий специальный прикладной протокол приложения поверх протокола TCP. Этот подход позволяет более экономно расходовать интернет-трафик при контроле связи.

Встроенный агент SNMP является отдельной задачей внутри приложения, обслуживающей связь с удалёнными менеджерами SNMP. Поддерживаются протоколы SNMP v1 и SNMP v2 и стандартные информационные базы (MIB) согласно спецификациям RFC1213 и RFC1471-RFC1473. Это означает, что пользователь, подключившись удалённо к устройству через программу менеджера SNMP, может узнать практически всё о состоянии стека протоколов TCP/IP в устройстве: сколько данных по каждому интерфейсу было принято и отправлено, сколько данных было потеряно, какая в устройстве таблица маршрутизации, какие порты открыты, сколько установлено соединений и т.д. Кроме того, приложение снабжено специальной информационной базой (отдельный MIB-файл), предоставляющей доступ ко всем настройкам приложения из программ – менеджеров SNMP.

Протокол RIP2 служит для объявления устройством собственных маршрутов в сложной сети и для приёма информации о маршрутах с ближайших маршрутизаторов. В сетях с изменяющейся во времени топологией это может избавить от необходимости ручных настроек маршрутов в приложении.

В контроллере предусмотрено несколько сценариев применения с настройками для определения интерфейса выхода в Интернет (GPRS, Ethernet, VPN поверх Ethernet или GPRS). Если на обслуживаемом объекте нет порта Ethernet, то для выхода в Интернет устанавливается канал GPRS. Если сеть Ethernet имеет выход в Интернет, то для экономии трафика GPRS логично установить выход через Ethernet, но как только связь по Ethernet разорвётся, GPRS станет текущим каналом выхода в Интернет. Если включена VPN, она автоматически становится каналом выхода в Интернет, независимо от того, какой интерфейс был назначен. При работе через интерфейс Ethernet устройство поддерживает протоколы ARP, RARP и DHCP.

Канал связи через GPRS

В контроллере использован модуль GSM/GPRS Telit 865 DUAL, который, помимо стандартных для модулей GSM настроек, обладает большим набором собственных настроек, расширяющих функциональность модуля. При включении модуля и установлении связи программное обеспечение «M2M ассистент» производит установку настроек модуля посредством AT-команд. Все команды, посылаемые модулю, и ответы, получаемые от него, записываются устройством в отдельный файл на карте microSD с сохранением точного времени их поступления.

Список команд, посылаемых модулю при включении и инициализации, и т.н. сценарий инициализации находятся в файле GSM.JSON на карте microSD. Хотя этот файл в большинстве случаев содержит все необходимые настройки для инициализации модуля, иногда, в отладочных целях или с целью изменения функциональности, может понадобиться его модификация.

В листинге 2 показаны несколько первых записей сценария инициализации, который представлен в виде JSON-массива COMMANDS. В массиве может быть произвольное количество объектов. Каждый объект описывает одну команду. Команды исполняются последовательно сверху вниз. Объекты имеют следующий набор ключей: ключ DESCRIPTION используется для описания команды, т.е. является комментарием и может отсутствовать в объекте; ключ STRING имеет значение, соответствующее передаваемой AT-команде; ключ TERM имеет значение символа в шестнадцатеричной кодировке, завершающего AT-команду при посылке модулю (обычно это символ с кодом 0x0D, но иногда, например при отправке SMS, это может быть другой символ); ключ DELAY задаёт значение задержки в миллисекундах при ожидании ответа на команду и введён с целью быстрейшего установления связи по GPRS. В некоторых приложениях, например в охранных системах, желательна очень быстрая передача сообщений, и тогда установление максимального времени ожидания ответа не позволяет модулю продолжительно «зависать» на некоторых командах и удлинять таким образом время выхода на связь.

Листинг 2

```
{
"COMMANDS":
[
{
"DESCRIPTION": "Device ignores
DTR transitions",
"STRING": "AT&D0",
"TERM" : "0D",
"DELAY" : 1000
},
{
"DESCRIPTION": "DTE-Modem Local
Flow Control",
"STRING": "AT+IFC=0,0",
"TERM" : "0D",
"DELAY" : 1000
},
{
"DESCRIPTION": "Calling Line
Identification Presentation",
"STRING": "AT+CLIP=1",
"TERM" : "0D",
"DELAY" : 1000
},
```

При установлении связи по GPRS в GSM-модуль необходимо передать правильное название точки доступа (APN), а также логин и пароль. Название точки доступа зависит от оператора сети GSM и параметров роуминга. По понятным причинам невозможно предусмотреть все сценарии установления связи во всех существующих сетях GSM. Тем не менее, в устройстве предусмотрен файл APN.LST со списком параметров точек доступа, которые может встретить пользователь в своём регионе. Каждая запись в файле содержит уникальный номер сети GSM, название точки доступа, логин и пароль. Установив связь с определённым оператором, устройство получает от GSM-модема уникальный номер сети оператора, по которому в файле APN.LST находит параметры точки доступа. Если необходимой записи в файле не найдено, устройство посылает SMS по заранее заданному номеру с объявлением номера сети оператора, к которому оно подключилось, и другими параметрами. Получив такое SMS, пользователь имеет возможность послать в ответ SMS, содержащее необходимую конфигурацию точки до-

ступа, которая будет записана устройством в файл APN.LST. После этого контроллер попытается вновь установить связь по GPRS.

Подключение к Интернету внешних устройств по сети Ethernet

Благодаря интерфейсу 10/100Base-T, контроллер может быть подключен в локальную сеть Ethernet, получив статический или динамический адрес IP. Контроллер может играть роль маршрутизатора в локальной сети для перенаправления пакетов из локальной сети в Интернет через модуль GSM. Чтобы остальные узлы локальной сети могли автоматически распознать присутствие резервного канала, устройство поддерживает протокол обмена маршрутами RIP2. Информацию о маршрутах контроллер может также сообщать по встроенному протоколу SNMP.

Локальная сеть может состоять из одного или нескольких простых микроконтроллерных встраиваемых устройств с интерфейсом Ethernet, подключённых к «M2M ассистент» напрямую или через концентратор. Для такой конфигурации контроллер может предоставить возможность открытия доступа к web-, Telnet- и FTP-серверам этих устройств из Интернета через свой канал связи GPRS. Для этого в «M2M ассистент» встроен сервер трансляции сетевых адресов (NAT), который позволяет внешним устройствам выходить в Интернет через контроллер и при этом делает их видимыми пользователям сети Интернет по публичному адресу, полученному устройством, и определённым номерам портов, которые указаны в файле конфигурации NAT. Формат файла конфигурации приведён выше при описании формата JSON.

В листинге 1 в первом объекте массива показана конфигурация, когда порт 80 (обычно это порт встроенного web-сервера) устройства с адресом 192.168.1.31 в локальной сети становится открытым в Интернете с обращением через порт 81. В данном случае номера внутреннего и внешнего портов разные, поскольку порт 80 будет занят для web-сервера самого контроллера. Поэтому в web-браузерах после IP-адреса «M2M ассистент» надо указать номер порта 81.

Подключение через VPN

Виртуальная частная сеть (VPN) устанавливается поверх протокола IP и защищает обмен данными, который ведётся с устройством. Защита канала связи в публичной сети Интернет является острой необходимостью не только по причине умышленных деструктивных действий, но и для защиты от сканирования и широковещательных запросов. Для начала взаимодействия с устройством через VPN, необходимо провести сеанс авторизации. Все пакеты, приходящие на другие порты или без авторизации, устройством игнорируются.

Устройство может организовать канал VPN как через Ethernet, так и через GPRS. Это определяется настройками в файле BOOTPARAMS.INI. В текущей версии поддерживается протокол VPN PPTP. По данному протоколу контроллер способен подключаться к компьютерам с операционной системой Window XP, Windows 7 или к маршрутизаторам VPN.

При использовании GPRS, для организации свободного доступа к портам TCP/UDP устройства пользователи вынуждены приобретать у провайдера планы с получением публичного адреса IP для модема GSM. Рано или поздно такой адрес становится объектом постоянного сканирования и направленных передач большого объёма данных со стороны некоторых агрессивных узлов Интернета. Это создаёт избыточный трафик, который будет вынужден оплачивать пользователь устройства. Технология VPN позволяет этого избежать. Но покупка выделенной виртуальной частной сети у провайдера – дело дорогое. В этом случае «M2M ассистент» предлагает более экономичное решение. Чтобы его реализовать, пользователь покупает план без предоставления публичного адреса IP, а «M2M ассистент» настраивается на организацию виртуального канала с частной сетью пользователя, организованной на базе персонального компьютера или недорогого маршрутизатора с функцией VPN. При этом сохраняется свободный доступ к FTP, web, Telnet и прочим серверам в устройстве.

Web-сервер с SSI, CGI и SSL

Сервер web в контроллере «M2M ассистент» доступен как со стороны GPRS-соединения, так и со стороны интерфейса Ethernet. Web-сервер применяется для редактирования параметров устройства, выполнения команд, просмотра состояний, доступа к файлам и т.д. из web-браузеров компьютеров и мобильных устройств. Учитывая специфику работы в Интернете, web-сервер снабжён функцией базовой авторизации и шифрованием потока согласно спецификации SSL. Для большей гибкости пользователь может изменить порт web-сервера со стандартного 80-го на какой-либо другой.

Страницы web-сервера могут генерироваться динамически специальными встроенными приложениями либо быть статическими с динамическими включениями (SSI). Контроллер выпускается с уже подготовленным набором статических страниц, предназначенных для редактирования параметров устройства (те же параметры хранятся в файле BOOTPARAMS.ini). Редактирование параметров на web-страницах приводит к их перезаписи в файле BOOTPARAMS.INI.

Страницы редактирования параметров содержат включения динамического содержания, которые отмечаются специальным тэгом следующего вида:

```
<!-#internal_var_form
VARIABLE={мнемоника переменной}>
```

Встретив такой тэг на статической странице HTML, web-сервер, прежде чем отправить страницу браузеру, подменяет тэг на код HTML, представляющий значение переменной и элемент её редактирования. Таким образом, тэг

```
<!-#internal_var_form
VARIABLE=PRT1BDR>
```

будет заменён фрагментом кода HTML

```
<input type="text" size="32"
name="value" value="115200">.
```

Данный фрагмент кода HTML представляет поле текстового ввода шириной 32 символа со вставленной текстовой строкой 115200 (в данном случае это установка скорости первого порта RS-232). Тип поля ввода (text, radio, textarea...) изменяется автоматически web-сервером по определённым правилам в зависимости от содержания параметра. Каждое поле ввода находится в форме ввода, содержащей код кнопки ввода и скрытый параметр:

```
<input type="submit" name="Btn"
id="COMMNM" value="Update">
<input name="param" type="hidden"
value="COMMNM">
```

После того как пользователь отредактирует содержимое поля ввода и нажмёт кнопку Update в браузере, web-серверу будет отправлен запрос HTTP следующего вида:

```
POST
http://192.168.1.32/set_variable
HTTP/1.1
Host: 192.168.1.32
Connection: keep-alive
Content-Length: 37
Cache-Control: max-age=0
Referer:
http://192.168.1.32/pp652.HTM
.
. [Остальные заголовки запроса
браузера]
.
value=115200&Btn=Update&param=PRT
1BDR
```

В данном запросе применяется метод POST, а к «M2M ассистент» производится обращение по адресу 192.168.1.32. Получив такой запрос, web-сервер устройства однозначно идентифицирует, какой тип операции необходимо произвести (Update), с какой переменной (PRT1BDR) и с каким значением (115200). Выполнив операцию, web-сервер вернёт страницу, указанную в заголовке запроса HTTP ключом Referer. Так работает механизм редактирования параметров через web-сервер устройства. Перечень всех мнемоник переменных, доступных через динамическое включение internal_var_form, можно найти в файле BOOTPARAMS.INI.

Помимо редактирования параметров, web-сервер имеет специальные виды SSI, позволяющие создавать элементы просмотра состояний цифровых и аналоговых входов, просматривать и изменять состояния выходов и проводить другие действия. Файлы встроенного web-сервера находятся на карте microSD контроллера в папке WEBPUBLDIR. В данном случае страницы беспрепятственно доступны для всех пользователей сети. Одновременно контроллер может поддерживать до десяти независимых сессий с web-сервером. В публичных сетях для защиты web-сервера от несанкционированного доступа применяется т.н. алгоритм базовой аутентификации. Файл USERS.TXT с реквизитами доступа при базовой аутентификации хранится в папке WEBPRIVDIR устройства.

Процедуры аутентификации часто бывает недостаточно, чтобы защититься от нежелательных воздействий. В таком случае контроллер предоставляет возможность шифрования канала связи с web-сервером по спецификации SSL. Чтобы перевести web-сервер в режим использования SSL, достаточно все страницы web-сервера перенести из папки WEBPUBLDIR в папку WEBPRIVDIR на карте microSD. Страницы, оставшиеся в папке WEBPUBLDIR, по-прежнему будут доступны без аутентификации и шифрования. Сертификаты SSL, необходимые web-серверу, находятся в папке SSL на карте microSD. Устройство содержит демонстрационные сертификаты. При подключении устройства в рабочее окружение пользователь должен записать собственные сгенерированные сертификаты или сертификаты, приобретённые в центрах сертификации.

Продолжение следует