**Основные понятия:**

ПУ — пункт управления.

КП — контролируемый пункт (RTU, remote terminal unit).

ОИК — оперативно информационный комплекс.

ЦППС — центральная приемо-передающая станция (CTS, central transceiver station).

ТС — телесигнал.

ТИ — телеизмерение.

ASDU — блок данных, обслуживаемый прикладным уровнем.

APDU — протокольный блок данных прикладного уровня.

COT — причина передачи (cause of transmission).

GSM-устройство — это устройство приёмо-передачи, использующее сети операторов мобильной связи.

SMS — служба коротких сообщений.

**Введение**

В реальных условиях организация взаимодействия между ПУ и КП для целей обмена телемеханической информацией не всегда бывает возможна с использованием физических линий связи, например в следствии территориальной удаленности КП от некоего географического центра, или же построение физических линий связи становится экономически нецелесообразным.

Так как зоны покрытия базовых станций операторов сотовой связи постоянно расширяются, то в качестве альтернативы проводным линиям связи для обмена телемеханической информации возможно использовать мобильную радиосвязь. В частности, если объем передаваемых данных не велик, то удобной оказывается служба коротких сообщений, описанная в стандарте GSM 03.40.

Максимальная длина одного текстового сообщения в стандарте GSM 140 байт (1120 бит). Таким образом при использовании 7-битной кодировки (латинский алфавит, цифры) возможно отправлять сообщения длиной до 160 символов. Для поддержки других национальных алфавитов (в частности русского) используется 2-байтовая кодировка UCS2. Таким образом, SMS, написанное кириллицей, не может превышать 70 символов. Также возможна отправка SMS, которое состоит из нескольких частей (concatenated SMS), теоретически до 255 частей. Для рационального использования доступного объема SMS необходимо применять компактный и практичный формат обмена телемеханической информации. Текстовый формат сообщений дает возможность представить набор телесигналов и телеизмерений в свободной форме, которую оператор может оценить наглядно.

Одним из достоинств использования SMS технологии, является то что функцию хранения и доставки сообщений берет на себя SMS-центр.

Процесс получения телемеханической информации от КП, поверх существующих сетей сотовой связи средствами SMS, и дальнейшую ее передачу в ЦППС с использованием протокола IEC 60870-5-104 можно разбить на несколько этапов:

*Первый этап*

Получение SMS

Разбор SMS

Cинхронная запись сообщений на диск

*Второй этап*

Обслуживание очереди входящих сообщений

Сборка ТИ и ТС в ASDU в форме ascii-hex

Организация отправки ASDU с применением механизма транзакций

*Третий этап*

Непосредственная передача телемеханической информации в ЦППС средствами протокола IEC 60870-5-104.

**Подробности реализации**

*Список утилит*

iecinit

smsget, smsdrop

quemngr, asdusend, asduconv, sockwrite

iecproxy, ieclink, ginterrog

*Библиотеки вспомогательный функций*

io\_utils

sms\_utils

sms\_parsers

*Список конфигурационных файлов*

iecenv

rtu\_list.conf

cts\_list.conf

*GSM-устройство*

Модем Teleofis RX100-R4.

**Подготовительный этап**

**iecinit**

iecinit — основной скрипт инициализации, запускается как демон с использованием утилиты start-stop-daemon. Отвечает за старт всех дочерних процессов (экспорт переменных окружения?).

iecinit читает конфигурационный файл cts\_list.conf и для каждой записи вида   
cts\_name ip\_address port, запускает отдельный экземпляр программ quemngr и iecproxy в фоне, которые взаимодействуют с конкретной ЦППС. При первом запуске создает структуру каталогов для данных дочерних процессов.

Задает параметры конфигурации GSM-устройства с помощью AT-команд и утилиты stty:

* Разрешает сырой ввод-вывод символьного устройства
* Устанавливает режим кодирования USC2
* Определяет область памяти для хранения SMS
* Переводит GSM-устройство в режим PDU (Protocol Data Unit)
* Запускает фоновый процесс smsget для опроса GSM-устройства на наличие новых SMS.

**Первый этап**

В unix используется принцип «все есть файл». GSM-устройство в unix-подобной операционной системе обычно представлено файлом символьного устройства в каталоге /dev, например /dev/ttyUSB0 или /dev/ttyS0. Для записи и чтения данных из файла устройства используются стандартные средства оболочки:

dev=/dev/ttyUSB0

exec 3<$dev 4>$dev

printf '%s\r\n' "$AT-cmd" >&4

read <&3 reply

Данные команды используются в библиотеке shell-функций io\_utils, предоставляющей более удобный интерфейс для взаимодействия с GSM-устройством.

**Smsget**

smsget — программа, периодически опрашивающая GSM-устройство на наличие новых SMS, посредством стандартных AT-команд:

AT+CMGL=4 — получение списка всех доступных SMS

AT+CMGD=i — удаление из памяти устройства SMS с индексом i.

Список SMS представляет собой набор записей вида

+CMGL: 4,1,"",127

07919740430900F0040B919740324334F90008817050104140216C041F044004380431043E04400020003200380020041D043504380441043F044004300432043D043E04410442044C0020043200200437043E043D04350020004E00200031002000320033003A00340039003A00300030002000320036002D00310030002D0032003000310037

Данная SMS записана в формате PDU. Вся служебная информация такая, как адрес отправителя, кодировка, штапм-времени получения сообщения SMS-центром, номер части составной SMS, а так же текст сообщения находятся в теле TPDU (Transfer Protocol Data Unit).

Smsget использует библиотеку shell-функций sms\_utils с помощью, которой декодирует и склеивает отдельные части составной SMS, если таковые имеются.

После декодирования TDPU работа с SMS строится по такому алгоритму:

1. smsget сравнивает телефонный номер отправителя, с номерами из rtu\_list.conf. Если номер отсутствует, сообщение удаляется.

2. Если номер оказался валидным, smsget запускает дочерний фоновый процесс   
smsdrop $dev $comaddr $dcs $scts $data, где

dev — модель устройства, отправившего SMS;

comaddr — общий адрес ASDU;

dcs — кодировка текста сообщения (UCS2, GSM);

scts — метка времени получения сообщения SMS-центром;

data — текст SMS в кодировке $dcs.

3. smsget ожидает окончания работы smsdrop, и в зависимости от кода завершения, либо удаляет сообщение из памяти GSM-устройства (код возврата 0 или 2), либо считывает его повторно (код возврата 1).

4. Если процесс smsdrop завершился успешно, то синхронно записанный им файл db\_archive/$comaddr/tempfile с набором значений телемеханики, процесс smsget копирует в каталог входящей очереди work/drop каждого экземпляра quemngr, который был запущен ранее iecinit, с именем его собственного inode. После этого smsget уведомляет каждый процесс quemngr о наличии нового сообщения в каталоге work/drop активацией FIFO триггера.

**smsdrop**

smsdrop принимает на стандартном вводе SMS, проверяет его на соответствие формату, конвертирует полученное SMS в набор значений для помещения в ASDU и синхронно записывает его на диск во временный файл var/smsdrop/msgsync.

Каждое значение описывается следующей совокупностью полей:

1. Общий адрес ASDU (rtu address).

2. Общий адрес объекта информации.

3. Идентификатор типа.

4. Значение объекта информации.

5. Описатель качества (если таковой используется).

6. Метка времени.

Пример

130 6 30 0 not\_used 27600:40:14:29:4:3:18

130 1 36 32 not\_used 27600:40:14:29:4:3:18

…

В поле «Описатель качества» вместо not\_used можно задействовать следующий набор набор битов OV — переполнение (Overflow), SB — подстановки вручную (Substituted), NT — не актуальное значение (Not topical).

Также smsdrop\_\* сохраняет полученный набор значений в виде отдельного файла в базу архивных сообщений на диске, для возможности отслеживания хронологии событий, если это потребуется. Помимо этого каждое полученное значение, но уже без меток времени, сохраняется на диске в виде отдельного файла в базе активных значений для возможной процедуры общего опроса.

В зависимости от результата обработки, smsdrop\_\* будет иметь следующий код завершения: 0 — обработка прошла успешно, 1 — синхронная запись сообщения на диск не удалась, 2 — неверный формат сообщения.

**Quemngr**

Quemngr — менеджер очередей, управляет очередью отправки полученных сообщений в ЦППС, а также сканирует каталог входящих сообщений при активации триггера ожидания (файл fifo).

Структура рабочего каталога:

work/drop — очередь входящих сообщений. Сканированные сообщения из входящей очереди попадают во внутреннюю, только если их имя совпадает с собственным inode.

work/in — внутренняя очередь сообщений.

work/act — рабочая очередь на отправку. В данной очереди находятся сообщения, отправка которых осуществляется в данный момент.

work/df — очередь отложенных сообщений. Сюда помещаются сообщения, отправка которых не удалась, но через определенный тайм аут возможно повторная. Очереди с определенным тайм аутом представляют собой именованный определенным образом каталог, например 0h0m50s, 0h20m0s, 1h30m25s.

work/fail — каталог сообщений, отправка которых не удалась после определенного числа попыток.

При запуске quemngr, сканирует каталоги очередей и восстанавливает связанные с ними структуры данных, при наличии канала до ЦППС начинает немедленную отправку сообщений.

Все новые сообщения из входящей очереди помещаются во внутреннюю, которая уже повторно не сканируется. Quemngr поддерживает структуры данных, при перемещении сообщений из одной очереди в другую. Сообщения передаются по возможности одновременно, но с ограничением на количество (конкуренцию) процессов передачи. Таким образом можно управлять нагрузкой на ЦППС и предотвратить шквал передачи в случае приёма большого количества SMS. Сам quemngr передаёт данные опосредованно. Его основная задача: управление очередью и выдача команд на передачу сообщений.

Во время инициализации quemngr запускает сопроцесс asdusend, с которым он связан неименованными каналами. Если во внутренней очереди имеются сообщения, quemngr переносит их в рабочую очередь и оповещает asdusend, передавая ему на стандартный ввод идентификатор сообщения. На стандартный вывод asdusend асинхронно записывает номер сообщения и статус. Успешно переданные сообщения quemngr (статус 0) удалит из рабочей очереди, а с теми сообщениями передача, которых не удалась (статус 2 и более), поступит в соответствии с политикой повторной передачи: либо перенесет в отложенную очередь с отправкой через определенный тайм аут, либо сбросит в каталог work/fail для последующего анализа и обработки вручную.

**asdusend**

Asdusend — сопроцесс quemngr, который на каждое передаваемое сообщение из рабочей очереди инициирует процедуру его передачи в ЦППС. Получив на стандартном вводе идентификатор сообщения, asdusend делает следующее:

1. Записывает на стандартный вывод номер сообщения со статусом 1, уведомляя quemngr о возможности передачи следующего сообщения из внутренней очереди.

2. Запускает два дочерних процесса asduconv и sockwrite, которые связаны между собой неименованным каналом, и осуществляющие передачу сообщения в iecproxy.

Статус завершения sockwrite вместе с индетификатором сообщения записывается на стандартный вывод.

**Asduconv**

Asduconv — программа для преобразовния телемеханической информации в текст ASCII HEX (список строк длиной до 492 символов). Asduconv имеет один ключ -c с помощью, которого задается причина передачи (3 - спорадическая передача, 20 — общий опрос). На стандартный ввод или в виде файла ей передается набор значений, формат которых был описан выше. Данный набор сортируется по общему адресу, затем по типу и адресу объекта. Если адреса объектов информации будут преимущественно по порядку, то при формировании ASDU указывается адрес и значение первого объекта информации, а далее перечисляется только последовательность значений оставшихся объектов информации, в классификаторе переменной структуры бит SQ = 1. Иначе в каждом объекте информации указывается собственный адрес, а бит SQ = 0. После того как список ASDU сформирован, он передается на стандартный вывод, разделителем ASDU служит перенос строки (LF).

Например, на ввод передаем набор значений с причиной передачи 3  
130 1 30 0 not\_used 27600:40:14:29:4:3:18

130 2 30 1 not\_used 27600:40:14:29:4:3:18

130 1 36 32 not\_used 27600:40:14:29:4:3:18  
на выходе имеем две сформированные ASDU в виде ASCII HEX  
1E020300820001000000D06B680E9D031202000001D06B680E9D0312

2401030082000100000000004200D06B680E9D0312.

**Sockwrite**

Sockwrite — простая программа, принимающая на стандартном вводе текст, который записывает в указанный через ключ -s unix сокет. Sockwrite получив от asduconv сформированный список ASDU и отправив его iecproxy, закрывает свой конец unix-сокета через системный вызов shutdown(fd, SHUT\_WR) и ждет окончания передачи. Iecproxy сообщает о статусе передачи в ЦППС короткими служебными сообщениями:

«<» передача прошла успешно (sockwrite завершается с кодом 0).

«-» передача не удалась (sockwrite завершается c кодом 2)

**Iecproxy**

Iecproxy — программа посредник между quemngr и ЦППС, в качестве дочернего процесса запускает ieclink, с которым связана неименованными каналами.

Проксирует запросы на передачу ASDU в ЦППС. Принимает через свой unix-сокет список ASDU в виде ASCII HEX текста, который записывает на стандартный ввод ieclink. Отслеживает статус переданых ASDU.

Уведомляет об отключении или востановлении канала до ЦППС процесс с pid, который она получает через перемунную окружения PID\_NOTIFY (в нашем случае это quemngr). Для этого использует пользовательские скрипты connect\_hook и disconnect\_hook.

Управляет прикладной процедурой общего опроса.

**Ieclink**

Ieclink — программа, реализующая канальный уровень протокола IEC104. В качестве аргументов принимает ip-адрес и порт сервера ЦППС. Устанавливает и поддерживает соединение (c помощью процедуры тестирования) с ЦППС.

Ieclink читает и пишет ASDU на стандартном вводе-выводе в виде текста ASCII HEX (разделителем ASDU служит символ переноса строки). Получив на стандартном вводе список ASDU, который завершается служебным символом «>», ieclink начинает отправку в ЦППС, дожидается передачи всех кадров на канальном уровне с подтверждением и записывает на стандартный вывод статус передачи.

Для уведомления iecproxy о событиях посылает на стандартный вывод короткие служебные сообщения «+» - соединение с ЦППС установлено, «-» - соединение с ЦППС потеряно (передача списка ASDU не удалась), «<» - передача списка ASDU прошла успешно.

**Ginterrog**

Ginterrog — программа, которая запускается iecproxy в качестве дочернего процесса в ответ на активацию прикладной процедуры общего опроса. Ginterrog формирует из базы активных сигналов, расположенных на диске в каталоге db\_active, список ASDU с причиной передачи 20 в виде текста ASCII HEX и записывает его на стандартный вывод.

**Rtupoll**

Rtupoll — скрипт, запускаемый по расписанию, опрашивает определенные КП из конфигурационного файла rtu\_list.conf. Механизм опроса зависит от возможностей устройств КП: это либо звонок с прерыванием через определенный тайм аут, либо посылка SMS определенного формата. Разделяет GSM-устройство установленное в системе вместе smsget, через файл блокировки device.lock.

Основные идентификаторы типов передаваемых сообщений, используемые в текущей реализации M\_SP\_NA\_1 (1), M\_ME\_NC\_1 (13), M\_SP\_TB\_1 (30), M\_ME\_TF\_1 (36).

**Основной сценарий работы для прикладной процедуры «Общий опрос»:**

1. ЦППС посылает команду общего опроса C\_IC\_NA\_1 с COT = 6 «активация». После подключения ЦППС периодически, через определенный тайм аут выполняет процедуру общего опроса или же по запросу оператора.

2. Iecproxy подтверждает прием C\_IC\_NA\_1 на прикладном уровне, дублируя его в направлении ЦППС с COT = 7 «подтверждение активации».

3. Если это первая процедура общего опроса после подключения, то iecproxy дожидается от quemngr отложенных сообщений, которые могли прийти во время отсутствия канала с ЦППС или же служебного сообщения об их отсутствии. Даные ASDU передаются в ЦППС с COT = 3 «спорадически». Статус передачи каждого отложенного сообщения передается quemngr.

4. Далее iecproxy запускает программу ginterrog, которая формирует список ASDU из базы текущих значений с COT = 20 «общий опрос», и начинает его передачу в ЦППС.

5. Закончив передачу последнего ASDU, iecproxy посылает команду C\_IC\_NA\_1 с COT = 10 «завершение активации».

6. Всю работу с канальным уровнем обеспечивает программа ieclink.

**Основной сценарий работы при установленном соединении:**

1. Все вновь пришедшие сообщения, находящиеся в рабочей очереди quemngr передаются в ЦППС с COT = 3 «спорадически».

2. В зависимости от статуса передачи они либо удаляются из рабочей очереди, либо переносятся в отложенную очередь с повторной отправкой через определенный тайм аут.