Протокол передачи данных DLMS.

В современных приборах учета (счетчики электрической энергии, тепла, воды, газа), как правило, для передачи даннях используют проприетарные протоколы. В результате чего, приборы учета разных производителей становятся несовместимыми, а это не только усложняет модернизацию систем, внедрение инноваций, но и лишает рынок систем учета энергоресурсов «свободной» конкуренции.

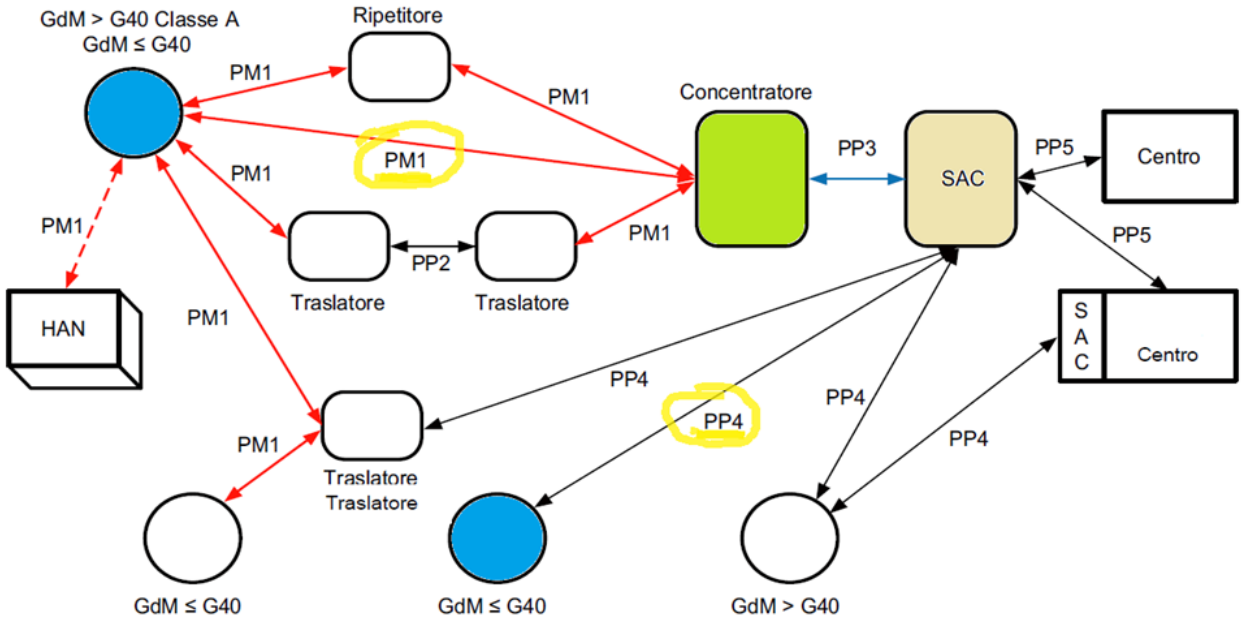
Решением данной проблемы является применение открытых протоколов, например, протоколов, соответствующих стандарту IEC 62056 (DLMS/COSEM).

Ссылки на опубликованные части серии публикаций

DLMS/COSEM – открытый протокол для обмела данными с приборами учета.

DLMS/COSEM это стек-ориентированный протокол базирующийся на концепцияхмодели OSI, регламентирующий обмен даннями между приборами учета и системами сбора данных, в основе котрого лежит клиент-серверная архитектура. Основополагающими спецификациями в этом стандарте являются DLMS и COSEM. Ниже приводится краткая характеристика этих спецификаций.

DLMS расшифровывается как Distribution Line Message Specification и представляет собой спецификацию прикладного уровня, которая не зависит от болем низких уровней и как следствие от коммуникационных каналов. Эта спецификация была разработана для стандартизации сообщений, передаваемых по распределительным линиям В последствии концепция DLMS претерпела изменения, а аббревиатура DLMS стала расшифровываться как Device Language Message Specification. Целью изменений стало обеспечение единой среды для структурного моделирования и обмела данными с приборами учета. В нынешнем виде, стандартом регламентируются: дистанционное считывание показаний с приборов учета, дистанционное управление, а также дополнительные сервисы для измерения любого вида энергоресурса (электричество, вода, газ, тепло).



В соответствии с DLMS, прибор учета представляет собой физическое устройство, состоящее из логических устройств. Каждое логическое устройство имеет уникальный идентификатор (в мировом масштабе), называемый логическим именем устройства. Информация, содержащаяся в каждом логическом устройстве, доступна посредством интерфейсных объектов. В свою очередь, доступ к интерфейсным объектам в рамках логического устройства осуществляется через объекты ассоциации. Объект ассоциации предоставляет информацию о ресурсах, имеющихся в логическом устройстве в зависимости от прав доступа.

Структурная модель RSE с двухточечнойпередачейдынных (*GPRS)*

Чтобы установить связь GPRS с Host, некоторые из определенных объектов Концентратор / Межсетевой шлюз поддерживаются для настройки в счетчике параметров сетевого подключения (например, APN, PPP Auth, IP-адреса и порта сервера) и для управления периодическими подключениями к host (например: callling_window); см. UNI / TS 11291-11-2 пар. 6 для справок;

В прикладном уровне счетчикиRSE клиентского/серверного приложения DLMS поддерживает следующие клиенты:

- Общественный: client_ID = 16, Нет аутентификации / шифрования, явная связь (требуется Application_Association), ограниченный набор данных OBIS;
- Управление (Host): client_ID = 1, требуется аутентификация и шифрование, предварительно установленная ассоциация;
- Установщика/Специалиста по техническому обслуживанию: client_ID=3, требуется проверка подлинности и шифрования, явная связь (требуется Application_Association);
- Гарант/Орган, выдавший документ: client_ID=48, требуется аутентификация и шифрование, предварительно установленная ассоциация;
- Радиопередача: client_ID = 32, доступный только с «многоточка», требуемая связь, аутентификация и шифрование;
- Сетевое взаимодействие: client_ID=64, доступный только с «многоточка», предварительно установленная ассоциация, проверка подлинности и шифрование.

Контроль безопасности передачи данных (SC):

- За исключением публичного клиента, передачи клиент-сервер аутентифицируются и шифруются на AES-128-GCM (спецификация NIST FIPS PUB 197 для ADVANCED ENCRYPTION STANDARD - AES)
- Для Установщика/Специалиста по техническому обслуживанию, требуется первоначальное подтверждение установления связи в соответствии с AES-128-GMAC (NIST – SP 800-38D)
- Тип APDU «общие-глобальное-шифрование» применяется к аутентифицированным / зашифрованным блокам данных (SC = 0x30) (см. Green BookDLMS 8-е изд., П. 9.2.7.2.3 / 9.2.7.2.4);
- Симметричный ключ (AES_KEY) используется как аутентификация (AK) и ключ шифрования (EK);
- Это список доступных симметричных ключей счетчика (AES_KEY) [128-битный ключ]:
- Управление: KEYC
- Установщик / обслуживающий персонал: KEYT
- Гарант / Полномочия: KEYS
- Механизм антиповторной атаки

В дополнение к средствам контроля безопасности в счетчике реализован механизм анти-повторной атаки

Более расширенное описание протокола DLMS можно скачать перейдя по ссылкам:
http://dlms.com/documents/Excerpt_GB8.pdf
http://dlms.com/documents/Excerpt_BB12.pdf