Semantic Integration of IEC 60870 into CIM

Yoseba K. Penya, Aitor Peña, and Oihane Kamara Esteban
DeustoTech, Energy Lab
University of Deusto, Bilbao (Basque Country)
{yoseba.penya, aitor.pena, oihane.esteban}@deusto.es

Abstract—The transition from distribution and transport power networks into the so-called smart grid vision must cope with many problems, one of them being the large amount of related standard protocols. Bringing them to work together in an standard fashion is the key to this goal. We focus here on the IEC 60870, the Spanish standard for high-voltage meter control and management. Applying the Semantic Web paradigm, we have mapped the IEC 60870 services to CIM in order to achieve interoperability. Moreover, we have enabled SPARQL (SPARQL Protocol and RDF Query Language) queries to retrieve the information from CIM-compliant meters and, as a proof-of-case we have implemented it with an IEC 60870 meter.

I. INTRODUCTION

One of the challenges the so-called smart grids must face is the unification (when possible) and untangling of the related protocol mess. As accounted in [1], the NIST (National Institute of Standards and Technology) originally identified 16 key smart grid standard protocols [2] and in a report from the EPRI (Electric Power Research Institute) to the NIST, the list increased to 77 items [3]. This drawback aggravates when it comes to the management of high-voltage (HV) meters due to historical reasons. For instance, the ANSI C.12 [4] rules in the USA whereas COSEM (Companion Specification for Energy Metering) [5] is the standard Europe-wide while Spain remains still loyal to the humble IEC 60870 [6]. Needless to say, these protocols are not interoperable.

With the emergence of the semantic web, the interoperability of protocols may be achieved in an easier and more feasible way. To be more specific, one of the basic pillars of the semantic pyramid is the concept of ontology, an information model that combines definitions of concepts and their relationships; OWL (Web Ontology Language) is the standard language to represent ontologies.

Aware of the opportunities that semantic models enable, the IEC has defined the OWL model of the CIM [7], [8], laying the foundations for many research projects that have extended the CIM to include related protocols [9], combined the CIM ontology with other protocols’ ontologies to achieve interoperability [10], etc. Still, there are some useful tools that have not being addressed so far in this domain, leaving a number of opportunities unexplored: the ability to create new knowledge from semantic sources (and their ontologies) by applying first-order logic or querying semantic persisted data (by means of SPARQL, SPARQL Protocol and RDF Query Language, the standard devised for this purpose).

Against this background, we advance the state of the art in two main ways. First, focusing on the IEC 60870, we show that in some cases a simple mapping suffices to achieve interoperability. Second, we go further and present, for the first time, an approach to apply SPARQL to CIM-compliant meter sources queried by means of semantic web services. We also show as a proof-of-case an implementation of CIM SPARQL to IEC 60870 meter data. This methodology aims at managing old proprietary HV meters as smart meters.

The remainder of this paper is organised as follows. Section II discusses related work. Section III introduces the IEC 60870 protocol. Section IV presents the mapping of the IEC 60870 services to CIM. Section V details the possible architectures to achieve the interoperability. Section VI focuses on the SPARQL querying of CIM-compliant meters. Finally, section VII concludes and outlines the avenues of future work.

II. RELATED WORK

Since smart grids have become a fashionable term, there has been a hectic research around many of their compounding parts and particular or global requirements [11]: evolution from classical design [12], protocol interoperability [13], integration of renewable sources [14], control and monitoring [15], metering [16], modelling of both transmission [17] and distribution systems [18], energy production scheduling [19]... the list of issues grows yearly.

Communication protocols are not an exception, taking into account the huge amount of related specifications and their lack of interoperability, as we pointed out in the introduction. There have been some interesting new directions explored lately within this domain, especially those focusing on the bidirectional integration of two smart grid protocols. In general, all of these works intend to place one of the targeted protocols as the basis, and then, they map the functionalities of the other through some kind of middleware layer, similar to the protocol tunneling achieved in other network domains [20]. This verge of research has recently turned to semantic technologies in their search for tools to accomplish interoperability. For instance, the appearance of the UML model [21] of the CIM standard [7] has been highlighted as the reference ontology [22]–[24] to be extended in order to include the rest of related protocols [1], [8], [16], [25]–[28] (approach envisioned and backed by the IEC [29] and the EPRI [30]–[34], starting by CIM’s sort of semantic ancestor in the USA, MultiSpeak. This methodology has also been promoted by the Technical Committees developing the involved protocols, as is the case of DLMS/COSEM, where the DLMS Users Group itself has led a study to integrate this protocol into CIM [9].
Further from this integration issue, there is another research direction that foresees the smart grid as a constellation of domain ontologies that must be mapped and brought together for collaboration [35]. The problem of this approach is not only the overcoming of smart-grid related drawbacks but also the ontology mapping challenge [36]–[38]: finding and expressing the equivalences between ontologies or their optimal alignment, achieving the actual communication, integrating diverse sources of data [39], [40], etc. Worth mentioning are the special efforts invested on integrating the IEC 61850 and the CIM [10], [41]–[43], both of them main pillars of the smart grid vision [29].

III. IEC 60870

The IEC 60870 is the standard adopted by the Spanish Transmission System Operator (TSO) for the management of high-voltage meters. It provides two types of frames depending on its length (fixed or variable). The first group is used to transmit acknowledge messages (ack, i.e. operation successful), error codes or information on the status of the communication. The second group carries questions and answers along with the pertinent data. Fig. 1 shows the schema of fixed and variable length frames (each cell representing a single byte).

<table>
<thead>
<tr>
<th>Fixed length</th>
<th>Var. length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Start</td>
</tr>
<tr>
<td>Op. Code</td>
<td>Length</td>
</tr>
<tr>
<td>Address</td>
<td>Length</td>
</tr>
<tr>
<td>Checksum</td>
<td>Start</td>
</tr>
<tr>
<td>End</td>
<td>Op.Code</td>
</tr>
<tr>
<td></td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td>ASDU</td>
</tr>
<tr>
<td></td>
<td>Checksum</td>
</tr>
<tr>
<td></td>
<td>End</td>
</tr>
</tbody>
</table>

Fig. 1. Fixed and variable length frame content.

The meaning of each field is explained next:

- **Start**: It indicates the head of the frame. In fixed length frames, this field is set to 0x10 whereas in variable length frames, it is assigned the value of 0x68. In the latter case, this field appears twice in the frame due to security reasons.
- **Operation Code**: This field determines the objective of the frame.
- **Address**: It defines the MAC address of the target meter. This field comprises 2 bytes sent in little endian format.
- **Checksum**: Allows to check the integrity of the received data.
- **Length**: Specifies the amount of bytes of the frame. In variable length frames, this field appears twice due to security reasons.
- **ASDU (Application Service Data Unit)**: It is a field whose length depends on the amount of data to be sent. It contains a byte specifying the type of ASDU (cdt), the address of the target (including meter id and an application layer address), and the data to be transferred.
- **End**: Similar to Start, this field signals the end of the frame. In both fixed and variable length frames its value is set to 0x16.

The Spanish standard for meter management is, more accurately, an implementation based on the IEC 60870-5-102 that specifies the communication protocol between registers or accumulators and meters. It presents three layers, namely physical, link, and application (taking the OSI Model as reference).

- **Physical layer**: The IEC 60870 foresees three approaches to access the meters, one direct and the other two remote (via GSM modem or TCP/IP, depending on the device model and its features). We focus here on the remote GSM alternative since all meters have a GSM modem attached. Therefore, the physical connection is performed through AT-HAYES commands.
- **Link layer**: This layer is dedicated to establish a communication session between the meter and the external querier by the assignment of an unique session id that lasts until the communication is closed. The vehicle to exchange data in this layer is the frame. The IEC 60870 specifies their type and order, being usually grouped in question-answer pairs, except for the session-open and session-close frames that receive a fixed length frame with Op.Code 0x10 (ack) in case the operation was successful. The connection in this layer is established as follows: the querier sends a fixed length frame with Op.Code 0x40, the meter responds with a 0x0B, then the querier replies with an Op.Code 0x40 and, if the connection is successful, the querier receives an ack frame.
- **Application layer**: The protocol enables non-password protected operations (i.e. non critical) such as inquiring the meter and vendor id, reading current date and time, official work-schedule dates (holidays and vacations), contracted power, consumed active and reactive power (accumulated and stored since the last reading), and so on. Password protected functions include all meter configuration operations that could lead to a deceitful or defective data retrieval such as changing date and time, modifying contracted power, holidays, password, or reading the meter’s configuration information (since this information contains the password).

The meter stores, every fifteen minutes, the current load consumption data in a cyclic buffer (i.e replacing older data by newer information) whose capacity depends on the vendor and the model of the device (the average is about three months worth of data). As any simple meter control and management protocol, the IEC 60870 offers basic meter management services and load data querying (absolute, relative,
and accumulated values). All services that access private or sensitive data are password protected.

IV. IEC60870 INTEGRATION INTO CIM

The first step to achieve interoperability between CIM and, in this case, IEC 60870 is to carefully analyse the services offered. Some protocols include an advanced data model (e.g. DLMS/COSEM [9]) that require extending some of the CIM classes to reflect such structure, but this is not the case of the IEC 60870: a direct mapping between services suffices. The strategy is simple and consists on taking one by one each of the IEC 60870 services, looking for the equivalent in CIM and performing the conversion at frame level. In this way, every frame arriving from an IEC 60870 meter will be transformed into a CIM message by a wrapper (the different architectures and modalities we address will be discussed later in section V). For the sake of simplicity and due to space constraints, we will illustrate this process with the most popular service in a meter: querying and retrieving active power consumption values. Mapping the rest of IEC 60870 services into CIM messages follows the same strategy.

According to the CIM specification [44], a meter is handled as an end device and, therefore, is represented using the CIM MeterAsset class, which is a subclass of EndDeviceAsset. CIM also defines the message interface of a special profile, namely the MeterReadings profile, that contains all the functions to be used with a meter; we have completed it with the CIMTool, adding all necessary classes. This profile foresees several forms to retrieve load consumption values from a meter: periodic reads, manual, on-request, historical meter data access; we have selected the on-request modality as the equivalent for the IEC 60870 absolute integrated consumption retrieving service (Op.Code 0x189).

As aforementioned, this information obtained from the Op.Code 0x189 frames is recast into a MeterReading message (the actual format and schema can be found in [44]). This message specifies, among others, the identity of the meter or meters, the reading values (as IntervalBlocks for the periodic reads or single Readings for the rest), and their respective qualities and time-stamps (as well as other important information specified within the ReadingType class, such as interval length of the measure, type, unit, etc.).

V. INTEGRATION ARCHITECTURES

Now, there are different approaches to design the wrapper that translates IEC 60870 frames into CIM messages and vice versa. The first decision to be taken is the nature of that wrapper. We have selected a SOA-based architecture (against proprietary ad-hoc wrappers) in order to achieve an open and scalable solution. In this way, taking into account the aforementioned connection variants of the IEC 60870 (direct, via GSM, or via TCP/IP), we envision three different approaches for enabling SOA management on IEC 60870 meters, as follows:

- **Embedded SOA wrapper**: It implies connecting directly to the meter and managing all of its inputs and outputs. The accomplishment of this goal may be difficult due to a possibly hazardous environment and the need to invest on an embedded lightweight platform (which will have limited storage capacity as well) that may not be allowed by the Utility that owns the meter.

- **Remote SOA wrapper**: This alternative consists of a remote machine that, via GSM or TCP/IP, queries and stores the meter data in a database (avoiding in this way
the problem of storage limit) and offers simultaneously decoupled access to that database (e.g. through SOA). The database could even be placed as a cloud computing service [45], if needed. This architecture is illustrated in Fig. 4. As pointed out in [32], the database is not a CIM database, but a database implementing a CIM messages interface.

- Remote real-time SOA wrapper: In a similar vein to the previous one, the remote machine acts as a transmitter of the CIM requests, translating and delivering via GSM or TCP/IP to the meter and vice versa for the responses. This strategy still suffers from the limited storage problem (though it could be solved by querying the meter on a regular basis). This architecture is depicted in Fig.5.

Fig. 5. Remote real-time SOA architecture.

VI. CIM SEMANTIC QUERYING

Any of the architectures presented in section V enables the interoperability of CIM and the IEC 60870 protocol. Still, this goal would have been accomplished in an easier way if we had performed the mapping simply using the CIM model expressed in UML. Instead, we chose to use ontologies since semantic models do present a number of advantages [16] that allow to go further from mere syntactical interoperability. The Semantic Web paradigm comprises methods and technologies devised to make information readable and understandable to machines. To this end, RDF (Resource Description Framework) expresses knowledge in the form of triples (subject, object, predicate) in XML (eXtended Mark-up language). RDF Schema defines the structure of the knowledge, OWL classifies the resources based on description logic and SPARQL allows querying RDF data stored persistently in knowledge bases.

Therefore, performing the mapping with the CIM ontology (and not with the UML model), we can address CIM-compliant meters as RDF databases whose information can be retrieved by SPARQL queries. The three architectures presented in section V are compatible with this approach: all CIM messages must only be embedded or transformed into CIM RDF messages as presented in Tab. III.
application wants. The SPARQL query processor searches for sets of triples that match the given triple patterns, binding the variables in the query to the corresponding parts of each triple and returning the pertinent information in the form of a set of bindings or an RDF graph. Tab. VI shows a SPARQL query to retrieve the load consumption from a CIM compliant meter and Tab. III presents an extract of the response that a CIM compliant meter may generate. In our case, the SPARQL query was received by the remote server (as proof-of-case we implemented the second database SOA architecture), whose database was continuously receiving and recording IEC 60870 meter data. The answer was then mapped into a CIM SPARQL response and sent back to the querier.

\begin{verbatim}
PREFIX mr: <http://iec.ch/TC57/2011/>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>

where {
  ?meterDhs a mr:MeterReading;
  mr:MeterReading.MeterAsset ?meterAsset;
  mr:MeterReading.valuesInterval ?valInt;
  ?valInt a mr:DateTimeInterval;
  mr:DateTimeInterval.beginDate ?beginDate;
  mr:DateTimeInterval.endDate ?endDate.
  ?meterAsset mr:Asset.serialNumber ?serialNum;
  ?intBlock a mr:IntervalBlock;
  mr:IntervalBlock.IntervalReadings ?intRead;
  mr:IntervalBlock.ReadingType ?rdnType;
  ?rdnType mr:ReadingType.kind ?rdnKind;
  mr:ReadingType.unit ?rdnUnit;
  ?intRead rdf:type mr:IntervalReading;
  mr:IntervalReading.value ?val;
  mr:IntervalReading.ReadingQualities ?rq.
  FILTER regex("^\d{4}\d{2}\d{2}\d{2}\d{2}\d{2}$")
  FILTER (?beginDate ≤ "2010-11-30T00:00:00"^^xsd:dateTime & ?endDate ≤ "2010-11-30T09:30:00"^^xsd:dateTime).
}
\end{verbatim}

**TABLE II**

**SPARQL QUERY.**

**VII. CONCLUSIONS AND FUTURE WORK**

One of the most pressing challenges smart grids have to face is the harmonisation of the involved standard protocols. For instance, if we focus on high-voltage meter management, depending on the country we may find the supremacy of the ANSI C.12 (e.g. in the USA), or the DLMS/COSEM (e.g. almost all over Europe). We deal here with achieving interoperability with the IEC60870 protocol, the standard for this purpose in Spain.

In this paper, we have illustrated first how to achieve semantic interoperability with CIM when the source protocol does not use a data model (or it is very simple). Moreover, we have shown how to further explode the opportunities that the semantic web paradigm offers by enabling SPARQL queries of CIM-compliant sources and, as a proof-of-case, we have implemented this approach with data of IEC 60870 meters.

Further works will concentrate on the problem of query federation problem [16] (how to answer to queries like: what is the current consumption of all the meters placed within neighbourhood). We will also investigate the way to apply C-Query ([46] Continuous Query, a real time SPARQL variant to query real-time RDF stores) to our model in order to define a real-time management framework of CIM-compliant meters.
REFERENCES


