SCADA as a Service approach for Interoperability of micro-grid platforms

Van Hoa NGUYEN[1], Quoc Tuan TRAN[2], Yvon BESANGER[1]

[1] Univ. Grenoble Alpes, G2Elab, F-38000 Grenoble, France
CNRS, G2Elab, F-38000 Grenoble, France
[2] CEA-INES, 50 Avenue du Lac Léman, 73370 Le Bourget-du-lac, France
Email : van-hoa.nguyen@grenoble-inp.fr

***Abstract*— In the context of smart grid development, this paper considers the problem of interoperability of micro-grid platforms, particularly among research institutions. Various levels of interoperability are introduced with the respective requirements. The primary aim of the paper is to propose a suitable private hybrid cloud based SCADA architecture satisfying various necessities in the framework of interoperability of micro-grid platforms while maintaining security restriction conditions. Due to the limited time restriction of critical SCADA functions in the electrical grid (protection, real time control, etc.), only selected non-critical SCADA functions (back-up, data historian, etc.) are accessible to partners from the private cloud. The critical SCADA tasks functionality remains under control of local server, thus, a hybrid cloud architecture. Common Information Model (IEC 61970 and IEC 61968, CIM/XML/RDF) is proposed to be used as model for information exchange. The communication model is based on PaaS delivery model and OPC Unified Architecture (OPC UA) specifications are considered. OPC gateway is proposed as conversion between the old OPC Distributed Common Object Model (DCOM) protocol and the Simple Object Access Protocol (SOAP) for cloud.**

***Index Terms*— Smart Grid, Micro-grid, Interoperability, Hybrid Cloud Based SCADA, OPC UA.**

ACRONYMS

AMI	**A**dvanced **M**etering **I**nfrastructure
CIM	**C**ommon **I**nformation **M**odel
DCOM	**D**istributed **C**ommon **O**bject **M**odel
EMS	**E**nergy **M**anagement **S**ystem
HMI	**H**uman-**M**achine **I**nterface
IaaS	**I**nfrastructure **a**s **a** **S**ervice
IEC	**I**nternational **E**lectrotechnical **C**ommission
IP	**I**nternet **P**rotocol
LAN	**L**ocal **A**rea **N**etwork
MTU	**M**aster **T**erminal **U**nit
OPC	**O**pen **P**latform **C**ommunication
OPC UA	**OPC U**nified **A**rchitecture
PaaS	**P**latform **a**s **a** **S**ervice
RDF	**R**esources **D**escription **F**ramework
RTU	**R**emote **T**erminal **U**nit
SaaS	**S**oftware **a**s **a** **S**ervice
SCADA	**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
SOAP	**S**imple **O**bject **A**ccess **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
UML	**U**nified **M**odeling **L**anguage
WAN	**W**ide **A**rea **N**etwork
XML	e**X**tensible **M**arkup **L**anguage

I. INTEROPERABILITY OF MICRO-GRID PLATFORMS

A. Problem of interoperability of micro-grid platforms.

Facing the enormous growth of energy consumption and the demand of effective integration of renewable energy resources into the electric grid, the conventional unidirectional power grid has been being considered insufficiently adapted [1]. Defined as an electrical network equipped with informatics technologies which dynamically optimizes performance, minimizes network losses, efficiently integrates distributed generations (renewable energy resources), the new generation "Smart Grid" is believed to increase reliability and to improve the energy efficiency of the whole system [2]. The integration of communication and information technologies allows smart grid to enable the exchange of data and to consider the actions of all factors in the electricity system in a communicative and interactive way, in order to act on demand and to adjust in real time the production and the distribution of electricity according to their urgency [3], [4].

The growing number of smart grid research and development projects around the world has led to a significant portfolio of demonstrators and advanced networking features. According to [3], there are 459 projects and demonstrative platforms smart grid in Europe (2002 to 2014) with an investment of around 3.15 billion €. Notably, we can mention Secure Interoperable Open Smart Grid Demonstration Project [4], JRC Smart Electricity Systems and Interoperability[5], Irvine SG Demonstration [6] and GreenLys (http://greenlys.fr). The collaboration and information

exchange among research and industrial institutions is become more and more necessary to efficiently exploit the research infrastructures and to rapidly transfer new developments. To achieve that purpose, interoperability among their infrastructures, especially micro-grid platforms, is identified as a top priority.

Usually installed in laboratories or research centers as demonstrating and experimental platform, a micro-grid (as defined in [7]) often focuses on a particular aspect of the grid, particularly interested by the institution, while the other aspects, for example customers or business model, play a very insignificant role. It is therefore judicious to improve collaboration among research and industrial institutions**, to efficiently exploit the existing platforms and to complement the missing infrastructure with available assets from other partners.** As a consequence, it is necessary to implement a certain degree of interoperability among the platforms.

The IEEE defined interoperability as the "**capacity of two or more networks, systems to externally exchange and readily use information securely and effectively"** [8]. Interoperability among micro-grids will allows the research institutions to exchange meaningful information, get access to shared resource pool and eventually, locally or remotely borrow the partner infrastructure for research activities. Interoperability among partners is imperative when facilities from several platforms are needed for an application (hardware-in-the-loop co-simulation, for example). Connecting interoperable platforms requires much less time and resources than constructing new necessary experimental modules. The mutual understanding and control of technological means provide also the possibility to realize multi-site research projects, for example: coupled platforms, long distance energetic management, etc. Such inter-platforms applications can be considered as a complex system of systems, in which a common understanding of their components and how they interact must be mutually shared [9]. **Interoperability of micro-grid platforms allows users to exchange, to process meaningful information among the energetic systems, automation systems, to visualize and to control in real time the available experimental tools in the partner platforms.** It has a direct impact to the cost of installation experimental modules and integration processes. It also introduces the possibility to easily connect and integrate new platforms [10].

The most important aspect of interoperability is information exchange. Therefore, these questions should be answered: what information to exchange, how to formulate the message to achieve mutual comprehension, how to send the message and on which architecture? Several difficulties to the interoperability of micro-grid platforms can then be pointed out:

- Lack of a **suitable interoperability model**,
- Choice of **suitable communication protocols**,
- Possible differences in **security and confidential policies,**
- Necessity for a **common information model** and
- I**ntegration of SCADA architecture.**

In this paper, we aim to address the above issues in the context of interoperability among micro-grid platforms. A novel SCADA architecture based on the hybrid-cloud SCADA model with selected information model and communication protocols, which provides solutions for these issues, is proposed and discussed.

B. Necessity of SCADA architecture integration.

Several interoperability models for smart grid are introduced in the literature such as: GWAC [11], SGAM [12] and SGIRM [8]. The first two frameworks provide a general approach. On the other hand, SGIRM is oriented to applications and is based on the usage of interfaces. The fact that these existing models are interested mainly on interoperability among one power system of large scale makes their applications to micro-grid platforms appear to be complicated and redundant because a micro-grid is often specialized into one specific domain of the grid and does not necessarily contain all the domains of the smart grid architectural model [13]. The interoperability model SGIRM [8], introduced by IEEE, oriented to applications, is probably the best fit for implementing interoperability among micro-grids, in our humble opinion. However, the detailed level of SGIRM is still high, which introduces some certain difficulties to the implementation.

Besides, interoperability among micro-grid platforms of different institutions requires **harmonization of different security and confidential policies**. Serious consideration and agreement should be taken over which information to share and which application is accessible for the partners. A common information model is also imperative so that the exchanged information is comprehensive. It should also be done in a way that demands the least modification to the current infrastructure of each partner.

Figure 1 illustrates different layers in the context of interoperability between two micro-grid platforms, represented on the SGAM interoperability stack [9]. From the top layer, a harmonization of communication policies between two operational bodies should be done. Both parties should agree upon the confidential aspects of the exchanged information and which applications and functions are accessible to the other party. This leads to the second layer of functions. Interoperability at this level requires a communication between two parties about their cartographies of experimental applications and research infrastructures. This is necessary for the efficient cooperation of both parties. This information is used to plan for multi-site projects and applications, such as co-simulation or long distance control, etc.

From a more technical point of view, interoperability requires that both parties share a common information model or at least a conversion interface, so that the exchanged information is understandable to the other side. In communication layer, synchronization of communication protocol is necessary to guarantee the good emission and reception of information. The component layer concerns the physical elements of the communication. The choices in these three layers are strongly influenced by the popular communicational standards and should be open for an

eventual integration of more partners into the network. The architecture, on which these three layers are organized, should allow the seamless and reliable integration of SCADA systems while offering enough security measures to protect against cyber-attacks.

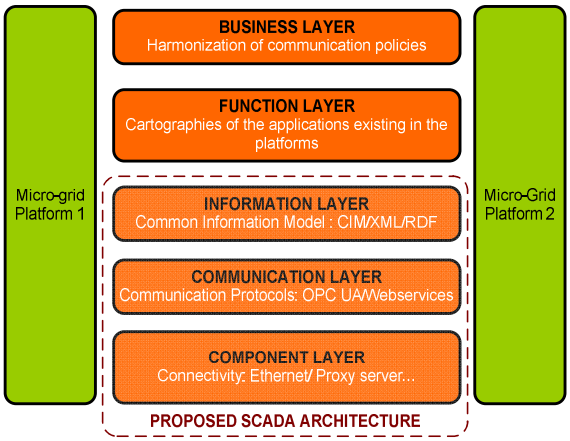

Figure 1: Different layers and necessary tasks for interoperability of micro-grid platforms, represented on SGAM stack.

Efficient interoperability among micro-grid platforms needs to be done in all layers (as classified in GWAC model [11] and SGAM model [9], or represented in Figure 1). While interoperability at application layer and above requires an exchange of information on platform cartographies and possible experiments, the **integration of SCADA systems of partner micro-grid platforms** requires a secured and distanced access to shared resources (data and control of the platforms)**.** In this context, the cloud based SCADA concept offers great flexibility and significant lower cost, but also provokes additional security aspects. Due to reliability and security issues of an electrical grid (response time, availability, etc.), critical control and protection tasks should be executed by the local PLC/RTU and the exchanged information should be selected and moderated.

C. Necessity of a common information model.

The communicational infrastructure assures an informative connection among different platforms. However, they do not specify how data should be organized in devices in terms of application. In order to exchange meaningful information, to mutually understand the transferred message and to use that information to operate, it is imperative that all partners use the same standardized information model. A standardization approach promotes also the possibility of further integration of new partners into the network. **IEC 61850** [14] and **IEC 61970** [15] **/IEC 61968** [16] **(Common Information Model/ CIM)** are recognized as two most important standards in the actual development of smart grid [17].

Another important issue preventing interoperability of micro-grid platforms is the **difficulty to exchange information on the architecture and topology of the infrastructure.** Interconnection architecture of a micro-grid platform is often changed according to necessary experiment. This information should be communicated to the partner platforms. Classical approaches, consisting of exchange separated measured dynamic values, demand prior manual communication of interconnection architecture to partners. It becomes a time-consuming task when there are many partners with difference in their data formulation or when there is a change in system topology or a reconfiguration of system interconnection. It is possible to easily exchange this kind of topology information in recent information models, using object oriented approaches, such as IEC 61850, CIM or eventually the OPC UA abstract data model.

The standard-based configuration of each micro-grid platform is therefore the key perquisite for a successful and secure interoperability. In this paper, we propose a SCADA architecture considering the possibilities of integrating Open Platform Communication (OPC) within cloud and PaaS to provide OPC based SCADA applications. Due to the timely restriction of critical SCADA functions in the electrical grid (protection, real time control, etc.), only selected non-critical SCADA functions (back-up, data historian, etc.) are accessible to partners from the private cloud. The critical SCADA tasks functionality remains under control of local server. CIM/XML/RDF is selected as the mean for model exchanges. We will give some insights to the usage of CIM over OPC UA, serving in the context of interoperability of micro-grid platforms. OPC gateway is proposed as conversion between the old OPC Distributed Common Object Model (DCOM) protocol and Simple Object Access Protocol (SOAP) for cloud. The communication model is based on PaaS delivery model and OPC Unified Architecture (OPC UA) specifications are then considered. The proposed architecture solves all the currently identified obstacles toward interoperability of micro-grid platforms.

In the following section, a novel SCADA architecture, based on hybrid cloud concept and PaaS delivery model, is proposed and discussed. The model is tweaked to cope with the security and reliability risks, while keeping the benefits of using cloud. In the third section, a brief state of art on information models in smart grid is presented, where CIM is introduced and compared to other existing models. We will give some insights to the usage of CIM over OPC UA, particularly the mapping of CIM semantics to the UA abstract model, serving in the context of interoperability of micro-grid platforms. Finally, we provide some requirements for the types of OPC-based applications should be available for partners in the collaboration network. This contribution should demonstrate that the proposed architecture provides a seamless support of communication, to successfully implement interoperability among micro-grid platforms.

II. NOVEL HYBRID CLOUD-BASED SCADA ARCHITECTURE FOR INTEROPERABILITY OF MICRO-GRID PLATFORMS

Interoperability in technical layers requires a secured and distanced access to shared resources (data and control of the platforms) which implies an **integration of SCADA architectures of partner micro-grid platforms**. Due to the possible distance among partner platforms, the classical

central approach is no longer suitable and new architectural approaches with ICT integration are required. In this section, we discuss firstly the concept of cloud-based SCADA and then, we apply this novel concept to the problem of interoperability of micro-grid platforms. A hybrid cloud-based SCADA architecture is finally proposed, in that purpose.

A. Cloud-based SCADA concept

The cloud is the concept of using remote network based servers to store and handle information. This information can be accessed through network connection. Cloud computing also offers three service delivery models: SaaS, PaaS and IaaS [18], [19].

IaaS, PaaS and SaaS are classified by the level of control the users can have access to. IaaS gives the users control over the infrastructure and applications deployed on the cloud. PaaS delivery model allows users to deploy the applications, but does not allow users to get full control of the underlying infrastructure or to get access to restricted data. SaaS delivery model, on another higher level of security, allows users to use the applications running on the infrastructure, though a client interface, such as web browser. The operator, however, has complete control over the infrastructure [20].

In the context of current development, SCADA services require security, reduced costs and uptime. Cloud based SCADA can solve critical issues related to uptime and redundancy while offering great scalability and flexibility [21]. One most important advantage of cloud-based SCADA compared to classical system is the much **faster speed of disaster recovery (DR) efforts**. Depending on the level of data exposure to public, cloud-based SCADA systems can be classified as **Public, Community** or **Private**. When SCADA applications are entirely deployed on-site and run on intranet, the system is considered as a private cloud-based SCADA. The access in this case is restricted to local level and may be granted a certain cooperators to create a community. When SCADA applications are entirely run in the cloud with remote connectivity to a control network, the architecture is considered as public and requires access authentication. The delivery models (SaaS, PaaS or IaaS) are chosen according to the needs of the operators and the security restriction.

Due to reliability and security issues of an electrical grid (response time, availability, etc.), critical control and protection tasks should be executed by the local PLC/RTU and the exchanged information should be selected and moderated. The applications in this scenario are directly connected to the local control network and data analysis is done on the cloud. This architecture is similar to the PaaS model and can be considered as a **hybrid cloud-based SCADA**. Figure 2 represents different elements of a simple hybrid cloud-based SCADA system. Significant differences exist among the mentioned cloud-based SCADA architectures. They are mostly involved the level of data exposure to public (hence cyber-security problem) and performance reliability criteria.

Compared to a traditional approach, cloud-based SCADA systems offer several considerable advantages:

- **Scalability:** a cloud-based SCADA system is easily adapted to the actual needs.
- "Real-time" and historical **data access from everywhere**, with proper access authentication. .
- **Better collaboration**: the ease of information access at different levels of the system/project enables all partners to work together more efficiently.
- **Ease of upgrading and expanding** the system: Once the system is upgraded, it is instantly available to everyone with access authentication.
- More **efficient disaster recovery**.
- **Cost** for maintaining and expanding/upgrading system is much lower.

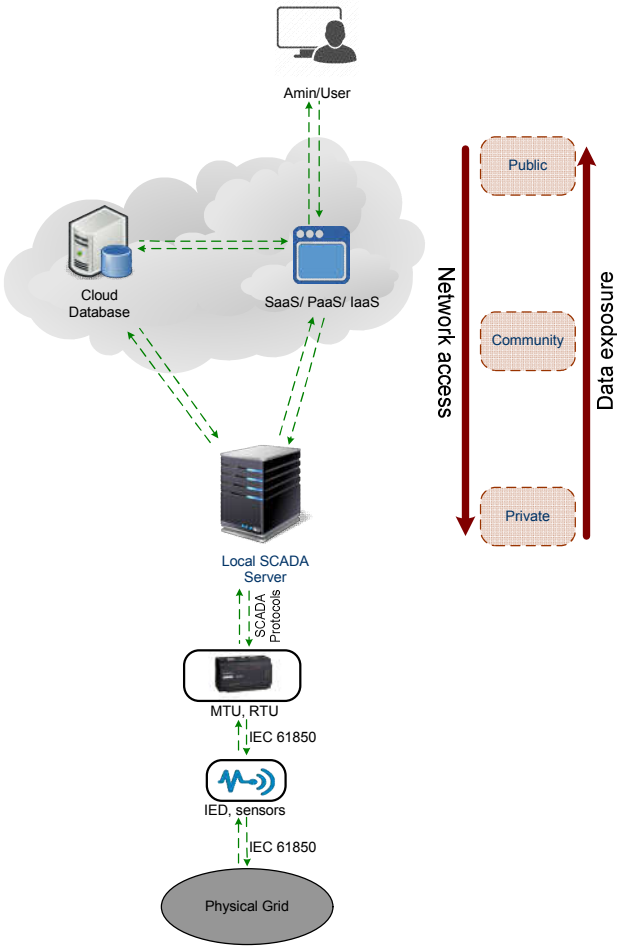

Figure 2: Simple hybrid cloud-based SCADA architecture

Cloud-based SCADA offers many attractive benefits; however, it also introduces some potential risks. This is especially sensible when some critical data is concerned. The most significant risks to be considered are Cyber-security and reliability:

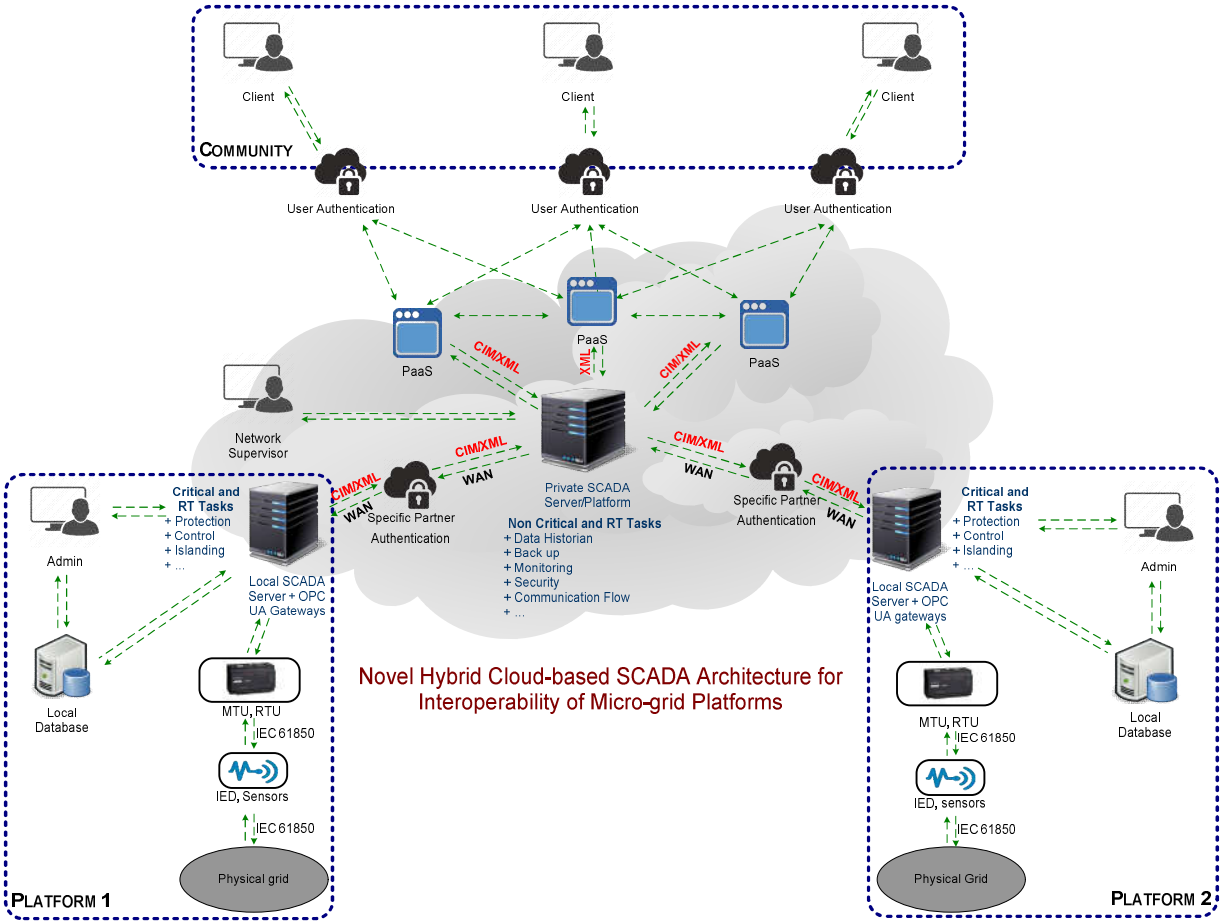

Figure 3: SCADA as Service approach for interoperability of Micro-grid Platforms.

- **Reliability**: Cloud connection relies on bandwidth availability and reliability. Vital information to safety and control functions is particularly important to the operation and functionality of the grid. We can therefore consider the dependency on internet connectivity as a risk and an obstacle to a reliable cloud-based SCADA.
- **Cyber-Security**: The cloud comes up with a secured system of data supervision and access authentication. However, cyber-attack may happen to the server or eventually to the data link (which is often out of the internal network). From a risk analysis perspective, it is important to consider and moderate which information to put on the cloud. For example, reports, analytics and configurations are suitable, but control data is very sensible. The operator should decide which information would be suitable to put on the cloud and risk analysis in case of accidental information leak should be taken beforehand.
- **Performance** of the functions that demand high **bandwidth** and low **latency** would also be affected in cloud-based SCADA. For this reason, the hybrid cloud-based SCADA appears to be the most suitable for the cooperation of electrical grid operators.

Due to the possible sensitive nature of the exchanged data among research institutions, the implementation of cloud-based SCADA should include a strict consideration of the aforementioned risks. In the following, we adapt the architecture to achieving cloud-based benefits while limiting the associated security and reliability drawbacks.

B. Adaptation of the architecture to the problem of interoperability among micro-grid platforms.

1) Architecture description

In order to enable the interoperability among micro-grid platforms, the problems mentioned in Figure 1 should be properly addressed and suitable technical solutions should be deployed respecting the agreement of harmonization of communication policies among partners. We propose in this section the SCADA architecture (Figure 3), which allows a secured and meaningful communication among the platforms and provides the ability to easily integrate new partner platforms to the networks.

The architecture represents the three lower layers of Figure 1. We adopt the hybrid cloud architecture and the PaaS delivery model. The local SCADA server supervises and controls its components via the corresponding industrial Ethernet. The physical components of both platforms are

connected to their MTU, RTU via standardized protocols (IEC 61850, IEC 60870 or DNP over TCP/IP, etc. Bulk data from the grid comes from sensors and is transmitted in different intervals (from miliseconds to several hours).

Two main issues of putting SCADA system to cloud is security and reliability. In this approach, the critical SCADA task is solely located on-site and is controlled by the local SCADA server, PLC or RTU, etc. This classical way ensures a low latency (as the communication is done via LAN) and strong protection (the information exchange is local) for these critical tasks. On the other hand, Markovich discussed in [21] that the cloud SCADA server is expected to address the following types of applications:

- Large scale transfer and storage of data
- AMI, MDMS, DMS, volt/VAR optimization, and outage management.
- Visualization, reporting, and access to remote users.
- Real-time energy usage and power pricing information to users though web portal.
- Virtual power plant.
- Migrating High Performance Calculation (HPC) to the cloud

These applications are delivered via the PaaS model. SaaS model can also be considered as an alternative. The proposed architecture is therefore based on the architecture of a hybrid cloud-based SCADA(Figure 2).

The interoperability of partner micro-grid platforms is actualized through a common private SCADA server. Data of the shared applications is transferred from the local service to a common private platform (Figure 3). It can be a physical SCADA server or a virtual PaaS/SaaS based server. This server communicates with local SCADA server in the platforms with WAN network. Ethernet with TCP/IP and Webservice protocols is the simplest and probably cheapest choice for implementation. However, according to the requirement of bandwidth and latency, other options can be considered (wireless network, satellite communication, etc.). As the communication interfaces are identified, an analysis on their data characteristics and requirements can be done. The data classification table 5.1 in [8] defined some requirements for general types of application (monitoring, control, protection, AMI, etc.) such as reach, latency, etc. for intra-platform of one smart grid of large scale. This classification can be adapted for the inter-platform WAN interface. It is however necessary to adjust the details according to the situation.

The results of this analysis provide a base for selecting communication protocols to these connections. From the data requirements of one interface, a set of suitable communication protocols should be chosen from various existing standards for interoperability in smart grid[1]. When there is more than one solution, the cost factor should be taken into account. The availability of security measures is also an important factor to the decision. In case that no existing standard satisfies the data requirements, it is necessary to adapt the data characteristics at the application level.

In this architecture with PaaS delivery model, the SCADA application is running on-site and is directly connected to the platform control network. The **critical functions of the SCADA server is isolated at local platform** and only selected non-critical information is transferred to the common cloud SCADA server that provides visualization, reporting and limited access to a range of applications, to remote authorized users and partner institutions. This (physical or virtual) common cloud SCADA server should be **private** (for the partner network), located at a partner platform or a site ,agreed by the partners, to provide optimized latency for the possible applications and is **strictly moderated** by a common council and technical staff, in charge of the interoperability within the network.

Using PaaS delivery model, it is also possible to remotely demand to launch a certain function (setting values, starting simulating, etc.) and visualize the result, provided that the demander is allowed by the platform owner. This property is very important **in the context of interoperability among micro-grid platforms of research institutions**, because it enables the **possibility to make experiments on the shared resources,** without having to come to the platform in person.

During the implementation of the proposed architecture, it is important to determine which applications are suitable to access from the cloud. In our specific context of interoperability among micro-grid platforms, these applications are decided according to the confidential policies and agreement of the partners. SCADA system is dependent upon the bandwidth and latency of the network connection. Losing functionality to real-time monitoring and control for a few minutes or even seconds may cause damage on the platform. Therefore, the critical tasks should only be accessed from the cloud after a **strict risk evaluation** (a bandwidth and latency test, at least). These criteria should be considered:

- Performance fluctuation
- Latency and latency variability
- Effect of network inaccessibility to the platform and data.

For each application, the response time cannot deviate from the requested value more than a defined difference.

[1] The tools provided by IEC (Smart Grid Standards Map – http://smartgridstandardsmap.com) and by the Smart Grid Mandate M/490n project (http://cencenelec.eu) can be a great help in standard selection.

Also, the total traffic of active applications and the dedicated gateway for protocol conversion cannot exceed the overall bandwidth the connection. These requirements need to be met in both WAN connection to the cloud SCADA server and the LAN connection in local platforms. If the involved risk is too high, only non-real-time applications should be available from the cloud. Each situation has to be evaluated on its own terms [22]. The data should also be alternatively stored in the local data base.

The proposed approach eliminates the two most important risks of cloud-based SCADA: security and reliability. Firstly, since the **critical functions are processed on-site by the local SCADA server**, as in classical approach**, the issues of latency and bandwidth is eliminated**. The system, on the other hand, can benefit the aforementioned advantages of the hybrid-cloud architecture and PaaS delivery model. Secondly, as for the security issue, the common cloud server is actually **private for the partners in the network and is strictly moderated**. It is not open for public and can only by accessed after a successful user authentication. A partner in the network can choose to grant access to a certain part of its platform to a specific partner and not the others. An additional partner authentication is required before access to more important functions is given. These two authentications can be separated (user is not associated to the institution) or be associated (the system will auto-detect the institution that the user belongs to and check for its right of access). **The above reasons make this architecture suitable for implementing interoperability of micro-grid platforms.**

It is important to note that even though the cloud server is private, the communication link, if shared with the public network, can still be attacked. If there is no dedicated private communication link to connect the partners, the data may still be sniffed while traveling though the intermediate servers (for example, while using the public Ethernet network). This risk, however, will always be there, whenever we decide to exchange information without a dedicated private link, no matter what architecture the system is. Additional security control needs to be implemented to make sure that the exchanged data among the partners is carried out in a secure manner.

2) Risk evaluation and security control

Security in electrical grid is a crucial factor because disruptions in these systems can lead to interruption of critical services and destruction of expensive equipment. Therefore, interoperability of the micro-grid platforms and research institutions should only be done within strict security consideration. Many problems derive from the fact that the classical SCADA systems were not designed to be connected to the outside network infrastructure and security aspects were not considered during the development phase. IEEE standard 1547-2030 [8] identifies and classifies the types of "intrusions" into a substation and discussed the methods for coping with them. Also, guidelines and security measures coupled with electronic controls are discussed in [23], [24]. The Risk Management Framework (RMF) [25] is recommended by NIST as a methodology to implement security control.

As mentioned above, the proposed architecture demands two kinds of authentications. The user authentication is required to grant access to the common cloud SCADA server, which provides some PaaS or SaaS applications. Then when access to a specific platform is necessary, a second authentication is required to check if the corresponding partner institution is authorized to access the local SCADA services. Besides authentication, several other means could be implemented to improve the security controls of the network.

In [26], the following components in SCADA system are determined as vulnerable:

- IEDs and RTUs
- LAN and firewall
- Communication network between substation and control center.
- SCADA LAN and firewall
- Corporate LAN and firewall
- Computer of vendor that can access the SCADA network for maintenance.

The security risks in the local front-end SCADA server (Figure 3) are mainly caused by the lack of cryptographic capacity. Extra payload and processing would induce unacceptable delays in sensitive applications [27]. Until recently, secure DNP3 and IEC 61850 introduced the ability to validate the authenticity of the messages [21].

Sharing the aforementioned security risks with the classical SCADA system, the proposed SCADA architecture is potentially vulnerable to attacks to the common cloud server. Some risks can be addressed:

- **Denial of Service** (DoS) and Distributed Denial of Service (DDoS) are the most probable attack to the proposed architecture. Their main goal is to flood the system with demand of service and to make the system unable to function as intended. In our architecture, the target of this kind of attack is the common cloud SCADA server. Even though the server is private to the partners of the working network, it is still open for the authenticated users to access from public. Therefore, this risk still exists. DoS attack in the server can cause unavailability to shared resources and disruption in communication over collaboration activities.
- **Data security**: as mentioned in last section, even though the common server is secured, the communication link and intermediate servers are

not. Especially when the network uses the public Ethernet.

To properly address these risks and enforce the security of the SCADA architecture, several solutions can be implemented:

- **DoS Detection**: The server must detect DoS attacks when they take place in order to apply appropriate counter measures. Several methods can be implemented to detect DoS attack through the packet content, attack pattern, etc. We can mention some popular and recent methods such as using flow entropy [28], [29], signal strength [30], sensing time measurement [31], transmission failure count [32] or signatures [30].
- **DoS mitigation**: This method is used once the attack has been detected, to protect the nodes and minimize the outage time. The DoS mitigation is often done over the two layers: network layer and physical layer. The action may vary from pushback, block or limiting the traffic from the attackers [30], [32]. The system can also actualize a reconfiguration to change the topology of the network in order to dedicate more resources to a victim or isolate and attacker [33]. Frequency hopping technologies [34] is recently developed as a more efficient DoS resistant data transmission [35].
- **Authentication**: This provides a preliminary process of identification, via the classical username and password procedure.
- **Authorization**: This is a mechanism to implement control access by user profile (normally attached their grades and to their institutions). The data and service are provided to the user according to his profile.
- **Notification**: The system must be capable to inform the operator of the platform when its shared data or its service are accessed through the collaboration network.
- **Data Encryption**: The cryptography algorithms are used to secure communication among between the cloud SCADA server to the local ones and to the end users. Both symmetric key encryption [33] and public key encryption [36] can be used.
- **Network security protocols**: for the communication to and from the cloud SCADA server, IPSec and TLS can assure a secure communication. On the other hand, for the communication of lower layers, the electrical grid requirements differ from the classical data network. Such new protocols as Secure DNP3, IEC 61850 and IEC 62351 are more suitable. They add a security layer to the end-to-end communication architecture.
- **Compliance check**: A compliance test runs checks across all the components in the system to ensure that they are up to standards of secure mitigation and protection.

The security measures and control ensure a secured data exchange and interoperability of the micro-grid platforms. The proposed architecture provides a common research infrastructure for the partners of the working network, offering the benefit of a cloud-based SCADA and PaaS delivery model while taking efficient measures against security and reliability issues. However, it does not specify the data to exchange for each application, as well as how the message should be formulated. In next section, we investigate the state of art of information models in smart grid, in order to suggest a suitable model which ensures that the exchanged data is mutually and correctly understood by all the partners of the project.

III. CIM/XML/RDF FOR INTEROPERABILITY OF MICRO-GRIDS

As stated above, information exchange is the core to interoperability. We are interested particularly in this section the questions: **what information to exchange and how to formulate the message to achieve mutual comprehension**. The communication protocols assure an informative connection among different platforms. However, they do not specify how data should be organized in devices in terms of the application. In order to exchange meaningful information, to mutually understand the transferred message and to use that information to operate, it is imperative that all partners use the same standardized information model. A standardization approach promotes also the possibility of further integration of new partners into the network. In this section, we investigate a state of art of existing information models in the development of smart grids. A brief introduction to CIM/XML/RDF is also presented

An agreement among the partner micro-grid platforms is important, not only on the common information model but also on the formulation of the models, the method and syntax to store and share their information. That allows exact and rapid comprehension of the exchanged messages. An information model should contain therefore, **not only a data storage model, but also information about system structure, in a synchronized format, syntax and semantics**. Traditionally, the exchanged messages were mostly separated dynamic signals and the information on system ontology is manually defined. It is actually possible to describe the latter information in current information models. As for smart grid, three information model standards are widely used: IEC 61850 [14], Multispeak (http://multispeak.org) [37] and Common Information Model (CIM) [15], [16], [38]. While **IEC 61850** focuses on station and field level, mainly on **communication within substation**; both Multispeak and CIM focus on interfaces between applications above station level. Whereas the main

interest of **Multispeak** is the **distribution** domain, **CIM** covers **transmission, generation and distribution** domains. Figure 4 gives a general view of the application domains of these information models.

It is necessary to note that CIM is transport independent while Multispeak use Simple Object Access Protocol (SOAP) messages over HTTP, TCP/IP socket connections to transfer data. Several works are underway to bring these two standards together [39], [40]. For IEC 61850 and CIM, there are semiautomatic approaches to create converters between their models, as in [41], [42]. Common Information Model (CIM) is officially adopted by the International Electrotechnical Commission (IEC) as electrical network information model. Currently maintained as a Unified Modeling Language (UML) model, CIM is organized in packages, each containing a set of classes with their structure, attributes and associations. CIM defines a common vocabulary and ontology for the electric power industry. It is mainly used in data exchange for EMS applications and energy markets.

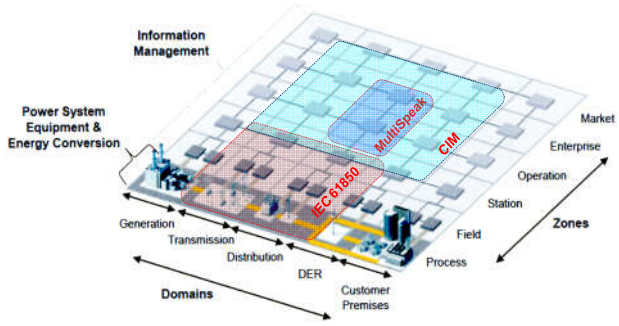

Figure 4: A simple representation of information domains on the smart grid plan of SGAM model.

In general, CIM is used for two primary objectives:

- **Exchanging data between applications**: in this case, the messages use CIM Semantic and are formulated into XML serialization. Extensible Markup Language (XML) [43] is used as message format in IEC 61850, CIM and Multispeak. XML is a meta-language that allows the description of data structure. In XML, the data is encoded as plain text and is platform independent. However, a basic XML document cannot denote any link between two elements that is not inheritance relation.
- **Encapsulating entire power system models**: In case of exchanging topology data of the system or of networks, XML hierarchy becomes insufficient. The Resource Description Framework (RDF) [44] is a XML schema that provides the possibility to define other relationships between XML nodes. The combination XML/RDF allows a set of objects to be expressed as XML while retaining their relationships and class hierarchy.

In the scope of this paper, we suggest to use **CIM/XML/RDF** as information model, due to its generality and platform/protocol independence. Another reason is that the information exchanged among partner micro-grid platforms will be generic and will mainly focus on application layers because of the confidential issues and the distance among platforms (some critical tasks, i.e. protection, is only available at local place). This choice is also supposed to provide the possibility of extending the network with external platforms using other data models by adding a data adaptation step at the interfaces with those platforms.

CIM/XML/RDF ensures the possibility to exchange static and dynamic data as well as the current state of electrical networks in a standardized way, which leads to a seamless semantic data exchange among components in a platform and among partners in the working network.

CIM is a platform and transport independent model. In order to successfully apply CIM, it is necessary to setup a suitable communication protocol. For an efficient collaboration among research and industrial institutions, there are scenarios in which a user needs to demand remote access to certain applications or experiments in partner platform. Therefore, the chosen communication protocol for interoperability of micro-grid platforms should be able to handle the classical SCADA functionalities and also to do WAN communication. The legacy Open Platform Communication (OPC) protocol[2] is widely accepted in industrial and research platforms and provides a certain degree of interoperability within the local network. To extend the functionalities beyond the local network and to reach interoperability among different platforms, the OPC Unified Architecture (OPC UA) has been developed and standardized (**IEC 62541** [45]).

The OPC UA comes up with an abstract data and information model – the address space – which is adapted to the domain of application. In the electrical domain, CIM provides the necessary information and semantics to develop the according UA address space. On the other hand, OPC UA provides the necessities to make CIM applicable in term of communication of data payloads [46], the capacity to generalize measured data into model and to communicate beyond the local network. The OPC UA plays also the role of a gateway, to converse the legacy DCOM protocols, popularly used in local OPC-based application, to XML and SOAP, adapted for the communication inter-platforms.

This combination of CIM and OPC UA allows the provision of OPC-based applications (EMS, HMI and SCADA) in the PaaS delivery model and brings CIM semantic to the OPC UA communication – a final brick to the proposed architecture.

[2] http://www.opcfoundation.com

IV. OPC UA AND CIM IN PAAS DELIVERY MODEL

In previous sections, a novel hybrid-cloud based SCADA architecture was proposed to actualize the interoperability of micro-grid platforms and CIM/XML/RDF was chosen as the information model. We consider in this section the OPA UA protocol and its mapping with CIM, to investigate the possibility of delivering SCADA applications to users via the PaaS model. In general, CIM provides the utility domain specific models which are mapped to the UA address space and use the UA protocol to deliver services. This section consists of two main ideas: firstly, the mapping CIM – OPC UA to bring CIM semantic to the OPC UA protocol; secondly, the delivery model for OPC based applications via PaaS and its requirements.

A. OPC UA and CIM

1) OPC Unified Architecture

OPC UA is developed by the OPC foundation[3] as successor to the classic OPC protocol. OPC UA maintains the server-client-architecture, but replaces the three different OPC servers (Data access – DA, Alarms and Events – AE and Historical Data Access - HDA) with only one OPC Unified Architecture server, which simplifies semantics and overall implementation [18]. OPC UA also provides the platform for interoperability among the existing OPC specifications beyond local network, using web services. OPC UA is standardized by the IEC 62541 standard series [45].

OPC and OPC UA are used for the exchange of real-time plant data among control devices. OPC specifications are based on Microsoft Distribution Component Object Model (DCOM) to provide a certain degree of interoperability among devices from different vendors. OPC UA, on the other hand, is based on the open technologies such as XML and Web services SOA [18].

The UA also comes with a generic information model [47], using object-oriented techniques, which is a basis for domain specific information model. The communication of OPC UA relies on nodes, described by their attributes, connected by references and grouped into classes [48].

The data of a UA server can be published in either binary or XML format. Several Web service security standards can be used in OPC UA communication: WS-Security, WS-Trust or WS-Secure Conversion. In the context of OPC standards, the UA can be considered as a top level standard providing platform-independent and service based communication, in contrary to platform-dependent and component-based approach of the others [48].

In general, the major improvements of OPC UA to its predecessors can be summarized:

- Platform independent
- Capacity to exchange data beyond local network
- The generic UA information model

The OPC UA protocol provides the necessities to make the CIM applicable in terms of communication of data payloads [46]. To achieve that, the UA abstract data model – the Address Space – has to be completed with CIM information and semantics.

2) CIM to OPC UA

To use CIM model over OPC UA communication, it is necessary to fill the UA address space with CIM information and semantics. Using the fact that CIM model and UA abstract data model are both based on UML, in [46], [49], Rohjans introduced a two-step approach of how CIM semantics can be used to generate OPC UA address space. First step concerns the modification of the UML model of CIM to develop a platform specific model, which is the input for external generator creating an UA address space. In second step, Rohnjans introduced CIMbaT, an Enterprise Architect (EA) Addin, to semi-automatically generate an UA Address space. The procedure to implement CIM semantic to OPC UA server is represented on Figure 5.

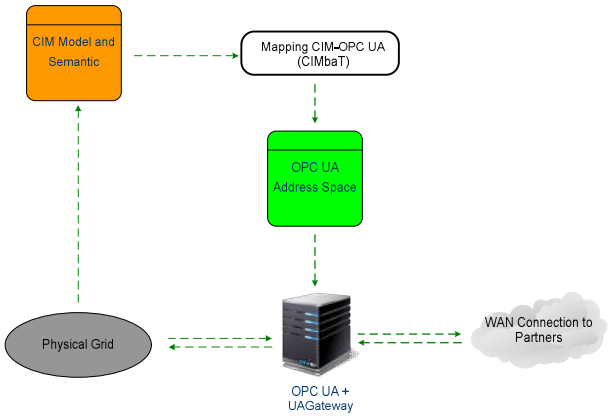

Figure 5: Procedure for implementation CIM over OPC UA.

The CIM – OPC UA mapping rules depend on the coordination with the IEC. The mapped elements will be written into a XML file. Some mapping rules of the attributes and hierarchies of CIM to OPC UA stereotypes are represented on Figure 6.

This mapping step allows the OPC UA server to run with CIM-based semantics. This combination leads to a highly interoperable infrastructure, enabling the seamless and meaningful communication among the applications, the DMS and the SCADA servers in the proposed architecture. It provides a strong support for interoperability of micro-grid platforms. To demonstrate the mapping procedure, Figure 7 represents an example of implementing CIM model to OPC

[3] http://www.opcfoundation.org

UA address space for a battery using Prosys[4] OPC UA simulation server and client.

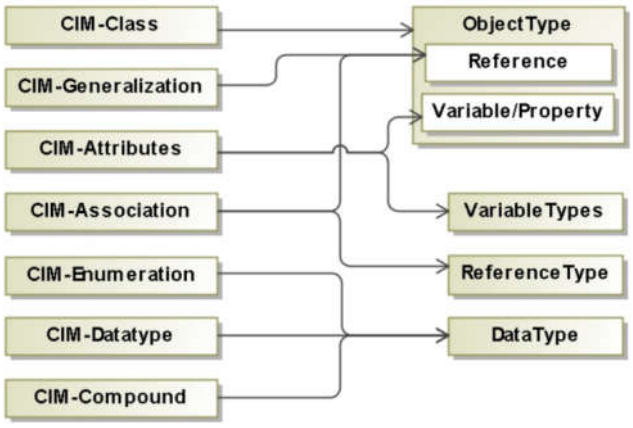

Figure 6: CIM to OPC UA mapping [46].

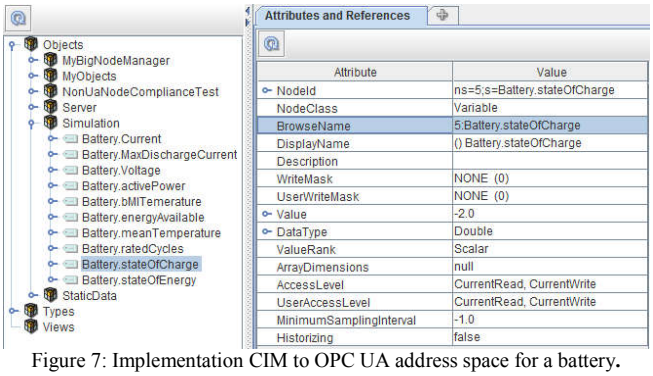

Figure 7: Implementation CIM to OPC UA address space for a battery.

B. Requirements for OPC-based applications via Cloud PaaS.

In the context of interoperability among micro-grid platforms, particularly in research and industrial infrastructures, there are scenarios in which a user needs access to an application of a remote partner platform. In electrical grid, several applications depend strongly on latency and bandwidth (such as control or protection). Accessing these applications via WAN connection may cause malfunctions to the system. Some requirements should be satisfied in order to enable access to a certain function via WAN network.

The system specifications must satisfy the defined requirements, in term of request response time T_{req} [ms], bandwidth P_{req} [Mbps]. As mentioned above, the electrical grid demands a strict requirement of response time and latency. For each application, the response time cannot deviate from the requested value more than a defined difference:

$$T < T_{req} + \quad T$$

[4] https://www.prosysopc.com

The OPC UA server is capable to communicate with both legacy DCOM protocol and WAN protocols, such as REST and SOAP. However, the devices dependent on OPC DCOM and unable to work directly with OPC UA must be connected to a dedicated OPC gateway. The bandwidth occupied by this gateway must be taken into consideration while evaluating the capacity of a server to provide service to a remote user. In general, the total traffic of active applications and the dedicated OPC gateway for protocol conversion cannot exceed the overall bandwidth the connection.

$$\sum P_{app} + P_{gateway} < P_{req}$$

These requirements need to be met in both WAN connection to the cloud SCADA server and the LAN connection in local platforms. Therefore, a test of communication and risk evaluation is necessary before implementing the architecture. This will help as an additional criterion to the decision of which services available to the partners, besides the security, confidentiality, communication and sharing policies of the institutions.

Moreover, the system specifications are required to satisfy the defined Service Level Agreement (SLA) in PaaS delivery model, in term of request response time T_{SLA} [ms], bandwidth P_{SLA} [Mbps] and number of concurrent users (n) [18].

V. CONCLUSION

In the context of strong development in smart grid, this paper considers the problem of interoperability of micro-grid platforms, particularly among research and industrial infrastructures. As there are more and more SG projects and platform, the necessity of collaboration and information exchange among research and industrial institutions appears naturally. It leads to the need of interoperability among their infrastructures, especially micro-grid platforms. Interoperability of micro-grid platforms allows users to exchange, to process meaningful information among the energetic systems, automation systems, to visualize and to control in real time the available experimental tools in the partner platforms. It is required to enable the collaboration and information exchange among research and industrial institutions and to provide a common support for multi-site R&D projects.

The hybrid cloud SCADA concept and the PaaS delivery model were used to propose a suitable architecture to resolve the problem of interoperability of micro-grid platforms. The architecture offers the benefit of a cloud-based SCADA and PaaS delivery model while taking efficient measures against security and reliability issues. CIM/XML/RDF was recognized as the suitable information model to ensure that the exchanged data is mutually and correctly understood by all the partners of the project. This combination allows the provision of OPC-based applications (EMS, HMI and SCADA) in the PaaS delivery model and brings CIM

semantic to the OPC UA communication, which completes the proposed architecture.

The contribution of this paper resides in the proposition of the novel SCADA as a service approach, which provides an infrastructure for interoperability among micro-grid platforms. Even though the security and reliability issues need to be carefully considered, we pointed out some measures to limit these issues while keeping the benefit of the PaaS delivery model. Secondly, this paper contributed to the usage of CIM over OPC UA, two important standards in the development of smart grid. A harmonization of these two information models will bring CIM semantic to the OPC UA communication, while the OPC UA protocol provides the necessities to make the CIM applicable in specific domain communication. The final contribution of the paper resided in the discussion of requirements for the integration of CIM and OPC UA to the PaaS model in the proposed architecture. This contribution enables a seamless and meaningful communication among partners of the collaboration network and provides a strong support for information exchange among micro-grid platforms. The proposed architecture provides a common research infrastructure with secured data exchange and interoperability for the partners of the working network.

ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions of C. Boudinet, T. Braconnier, A. Labonne and E. Ferre, to the development of the work presented in this paper.

REFERENCES

[1] M. James, *Smart Grid - Fundamentals of Design and Analysis*. Wiley - IEEE Press, 2012.

[2] ISE New England Inc, "Overview of the smart Grid - Policies, Initiatives and Needs," ISO New England Inc, Feb. 2009.

[3] F. C. Catalin, A. Miicea, V. Julija, M. Anna, F. Gianluca, and A. Elefherios, "Smart Grid Projects Outlook 2014," European Commission - Joint research centre, JRC Science and Policy Reports, 2014.

[4] T. Magee, "Secure Interoperable Open Smart Grid Demonstration Projet," Smart Grid Implementation Group, New York, NY 10003, Final Technical Report DE-OE0000197, Dec. 2014.

[5] H. Keith, "Status of the EV-Smart Grid Interoperability Centers in Europe and the U.S," in *EV-Smart Grid Interoperability Center Argonne National Laboratory*, Pacific Northwest National Laboratory at the University of Washington Seattle, Washington, USA 98105, 2014.

[6] A. Kamiab, "Irvine Smart Grid Demonstration (ISGD)," presented at the 2012 Smart Grid Program Peer Review Meeting, Southern California Edison (SCE), 2012, p. 10.

[7] S. Bacha, D. Picault, and B. Burger, "Photovoltaics in Microgrids: An Overview of Grid Integration and Energy Management Aspects," *IEEE Industrial Electronics Magazine*, pp. 33–46, Mar-2015.

[8] IEEE P2030 Working Group, *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*. 2011.

[9] Smart Grid Coordination Group, "Smart Grid Reference Architecture v3.0," CEN-CENELEC-ETSI, Nov. 2012.

[10] Smart Grids Task Force Expert Groups, "Final Report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids," European Standardizations Organizations, May 2011.

[11] The GridWise Architecture Council, "GridWise Interoperability context - Setting Framework," GridWise Architecture Council and Battelle Memorial Institute, Mar. 2008.

[12] Smart Grid Coordination Group, "SGAM User manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM)," CEN-CENELEC-ETSI, SG-CG/M490/K_SGAM usage and examples Version 3.0, Nov. 2014.

[13] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," Smart Grid and Cyber-Physical Systems Program Office and Energy and Environment Division, Engineering Laboratory, NIST Special Publication 1108r3, Oct. 2014.

[14] International Electrotechnical Commission, "IEC 61850 - Power Utility Automation." TC 57 - Power systems management and associated information exchange, 2003.

[15] International Electrotechnical Commission, "Framework for energy market communications - Part 301: Common information model (CIM) extensions for markets," TC57, Geneva, Switzeland, International Standard IEC 62325-301, Aug. 2014.

[16] International Electrotechnical Commission, "Application integration at electric utilities - System interfaces for distribution management - Part 11: Common information model (CIM) extensions for distribution," TC57, Geneva, Switzeland, International Standard IEC 61968-11, Mar. 2013.

[17] S. Stjepan, M. Ante, and K. Ana, "Utilizing standards-based semantic services for modeling novel Smart Grid supervision and remote control frameworks," presented at the 2012 IEEE International Conference on Industrial Technologies, 2012, pp. 409–414.

[18] P. Peniak, "Cloud Computing and Provisioning of OPC based applications," *Journal of Information, Control and Management systems*, pp. 65–71, 2014.

[19] M. Giriraj and S. Muthu, "A Cloud Computing Methodology for Industrial Automation and Manufacturing Execution System," *Journal of Theoretical and Applied Information Technology*, pp. 301–307, 30-Jun-2013.

[20] P. Mell and G. Timothy, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Recommendations of the National Institute of Standards and Technology Special Publication 800-145, Sep. 2011.

[21] D. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic, "Smart power Grid and cloud computing," *Renewable and sustainable Energy Reviews*, pp. 566–577, 2013.

[22] K. Birman, L. Ganesh, and R. van Renesse, "Running smart control software on cloud computing architectures.," in *Proceedings*, Ithaca, 2011.

[23] The Smart Grid Interoperability Panel, "Introduction to NISTIR 7628: Guidelines for Smart Grid Cyber Security," NIST Cyber Security Working Group, 2010.

[24] North American Electric Reliability Corporation, "Security Guideline for the electricity sector: physical security," NERC, 2011.

[25] P. Gallagher and G. Locke, "Guide for Applying the Risk Management Framework to Federal Information Systems - A security Life Cycle Approach," Joint Task force Transformation Initiative, NIST Special Publication 800-37 Revision 1, Feb. 2010.

[26] G. Bjorkman, "SCADA system architectures," Vital infrastructure, Networks, Information and Control Systems Management Project, Project report D2.3, May 2010.

[27] A. Sanchez-Lopez, E. Islas-Perez, A. Espinosa-Reza, and A. Quintero-Reyes, "Deploying SCADA to web services for interoperability purpose," presented at the Global Information Infrastructure and Networking Symposium (GIIS), Guadalajara, 2015, pp. 1–8.

[28] J. Meng and N. Wang, "A Network Instrusion detection method based on improved K-means Algorithm," *Advanced Science and Technology Letters*, pp. 429–433, 2013.

[29] S. Shin, S. Lee, H. Kim, and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection.," *Expert systems with applications*, pp. 315–322, 2013.

[30] D. Lin, "Network Intrusion Detection and Mitigation against Denial of Service Attack.," University of Pennsylvania, Department of Computer & Information Science, MS-CIS-13-04, Jan. 2013.

[31] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” presented at the 6th ACM Int Symposium on mobile adhoc networking and computing, 2005.

[32] S. Shapsough, F. Quaten, R. Aburukba, and F. Aloul, “Smart Grid Cyber Security: Challenges and Solutions,” presented at the International conference on smart grid and clean energy technologies, Offenburg, 2015.

[33] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” *Computer Networks*, pp. 1344–1371, 2013.

[34] C. Pooper, M. Strasser, and S. Capkun, “Anti Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques.,” *IEEE journal on Selected areas in Communication*, pp. 703–715, 2010.

[35] E. Lee, M. Gerla, and Y. Oh, “Physical layer Security in Wireless Smart Grid.,” *IEEE Communication Magazine*, pp. 46–52, 2012.

[36] M. Line, I. Tondel, and M. Jaatun, “Cyber security challenges in Smart Grids,” in *ISGT Europe*, Manchester, 2011.

[37] National Institute of Standards and Technology, “NIST Framework and Roadmap for Smart Grid Interoperability Standards,” U.S Department of Commerce, Jan. 2010.

[38] International Electrotechnical Commission, “Energy management system application program interface (EMS-API) - Part 301: Common information model (CIM) base,” TC57, Geneva, Switzeland, International Standard IEC 61970-301, Dec. 2013.

[39] International Electrotechnical Commission, “Application integration at electric utilities - System interfaces for distribution management - Part 14: Multispeak - CIM Harmonization,” TC57, Geneva, Switzeland, International Standard IEC 61968-14, Mar. 2013.

[40] G. McNaughton, G. Robinson, and G. Gray, “MultiSpeak and IEC 61968 CIM: Moving Towards Interoperability,” presented at the Grid-Interop Forum 2008, Atlanta, GA, 2008, p. 5p.

[41] T. Kostic, O. Preiss, and C. Frei, “Towards the formal integration of two upcoming standards: IEC 61970 and IEC 61850,” in *Proceeding of the Large Engineering Systems conference on Power Engineering*, 2003, pp. 24–29.

[42] Electrical Power Research Institute, “Harmonizing the international electrotechnical commission Common Information Model (CIM) and 61850 - Key to achieve Smart Grid Interoperability Objectives,” EPRI, EPRI1020098, 2010.

[43] T. Bray, J. Paoli, C. . Sperberg-McQueen, E. Maler, and F. Yergeau, “Extensible Markup Language (XML) 1.0 (Fifth Edition),” W3C, REC-xml-20081126, Nov. 2008.

[44] G. Klyne, J. Caroll, and B. Mcbride, “Resource Description Framework (RDF): Concepts and Abstract Syntax,” W3C, W3C Recommendation REC-rdf-concepts-20040210, Oct. 2004.

[45] International Electrotechnical Commission, “OPC Unified Architecture - Part 1: Overview and Concepts,” IEC TC 65/SC 65E, TR 62541-1:2010, Feb. 2010.

[46] S. Rohjans, K. Piech, M. Uslar, and J.-F. Cabadi, “CIMbaT - Automated Generation of CIM-based OPC UA-Address Spaces.,” presented at the IEEE International Conference on smart grid Communications, Brussel, 2011, pp. 416–421.

[47] W. Mahnke, L. Stefan-Helmut, and M. Damm, *OPC Unified Architecture*, Springer Berlin Heidelberg. 2009.

[48] S. Rohjans, M. Uslar, and J. Appelrath, “OPC UA and CIM: Semantics for the smart grid.,” presented at the Transmission and Distribution Conference and Exposition, 2010 IEEE PES, New Orleans, LA, USA, 2010, pp. 1–8.

[49] S. Rohjans, K. Piech, and W. Mahnke, “Standardized Smart Grid Semantics using OPC UA for Communication,” *Interoperability Bus. Inf. Syst.*, vol. 1, no. 6, pp. 21–32, 2011.