The Management System of INTEGRIS
Extending the Smart Grid to the Web of Energy

Joan Navarro[1], Andreu Sancho-Asensio[1], Agustín Zaballos[1], Virginia Jiménez-Ruano[1], David Vernet[1] and José Enrique Armendáriz-Iñigo[2]
[1]*La Salle – Ramon Llull University, 08022 Barcelona, Spain*
[2]*Universidad Pública de Navarra, 31006 Pamplona, Spain*

Keywords: Web-based Services, Intelligent Agents, Distributed Databases, Security, Smart Grids.

Abstract: The recent growth experimented by the Internet has fostered the interaction of many heterogeneous technologies under a common environment (i.e., the Internet of Things). Smart Grids entail a sound example of such situation where several devices from different vendors, running different protocols and policies, are integrated in order to reach a common goal: bring together energy delivery and smart services. Latest advances on this domain have led to effective architectures that support this idea from a technical perspective, but fail at providing powerful tools to assist this new business model. Hence, the purpose of this paper is to present a novel unified and ubiquitous management interface, driven by an intelligent system, that uses the advantages featured by the Web of Things to manage the Smart Grid. Therefore, this work opens a new path between the Internet of Things and the Web of Things resulting in a new concept coined as the Web of Energy.

1 INTRODUCTION

The ever growing set of features provided by the Internet has led into a standard communications framework that eases the deployment and development of distributed and heterogeneous applications. Such evolution has driven a rising interest in connecting several gadgets to the Internet, ranging from mobile phones to home appliances, including special systems such as traffic lights or embedded devices. This has led to a new form of distributed system, referred to as the Internet of Things (IoT), that consists in (1) uniquely identifying every object in the network, (2) using the Internet as the communications infrastructure, and (3) providing a lightweight interface to rapidly access everywhere.

Recent advances on Smart Grids have explored the feasibility of considering the electricity distribution network as a particular case of the IoT (Guinard et al., 2011; Zaballos et al., 2011). Certainly, this specific domain poses appealing challenges in terms of integration, since several distinct smart devices (also referred to as Intelligent Electronic Devices or IEDs) from different vendors—often using proprietary protocols and running at different layers—must interact to effectively deliver energy and provide a set of enhanced services and features (also referred to as smart functions) to both consumers and producers (prosumers) such as network self-healing, real-time consumption monitoring, and asset management (INTEGRIS, 2011). Although the latest advances on the IoT field have definitely contributed to the physical connection of such an overwhelming number of smart devices, several issues have arisen when attempting to provide a common management and monitoring interface for the whole Smart Grid (INTEGRIS, 2011; Aman et al., 2013).

Indeed, integrating the heterogeneous data generated by every device on the Smart Grid (e.g., wired and wireless sensors, smart meters, distributed generators, dispersed loads, synchrophasors, windmills, solar panels, communication network devices) into a single interface has emerged as a hot research topic. So far, some experimental proposals (Guinard et al., 2011) have been presented to face this issue by using the Web of Things (WoT) concept to access a mashup of smart devices and directly retrieve their information using reasonably thin protocols (e.g., HTTP, SOAP) (Guinard et al., 2010).

However, the specific application of these approaches to real-world environments is fairly doubtful because (1) they may open new security breaches (Zeng et al., 2011; Bou-Harb et al., 2013) (i.e., end-users could gain access to critical equipment), (2)

Navarro J., Sancho-Asensio A., Zaballos A., Jiménez-Ruano V., Vernet D. and Armendáriz-Iñigo J..
The Management System of INTEGRIS - Extending the Smart Grid to the Web of Energy.
DOI: 10.5220/0004950203290336
In *Proceedings of the 4th International Conference on Cloud Computing and Services Science* (CLOSER-2014), pages 329-336
ISBN: 978-989-758-019-2

there are no mature electric devices implementing *WoT-compliant* standards available in the market (INTEGRIS, 2011), and (3) industry is averse to include foreign modules (i.e., web servers) on their historically tested and established—but poorly evolved—proprietary systems (Gungor et al., 2013).

Therefore, the European project INTelligent Electrical GRId Sensor Communications (INTEGRIS) (INTEGRIS, 2011) has explored a new way to overcome these issues and, thus, provide a management interface for the Smart Grid inspired by the WoT. More specifically, the aim of INTEGRIS is twofold: on the one hand, it implements an ICT infrastructure—based on the IoT paradigm—to handle the Smart Grid security, storage, and communications requirements (Navarro et al., 2012). On the other hand, it uses a cognitive-inspired intelligent multi-agent system to manage the whole Smart Grid and link it with end-users using a WoT-based approach, which results in a new bridge between the IoT and WoT.

The purpose of this paper is to present this multi-agent intelligent system that extends the WoT approach and implements the management system used in the INTEGRIS' real-world domain. This proposal, which leads in a new form of the WoT coined as the Web of Energy (WoE), is targeted to provide a secure, context-aware, and uniform web-based novel environment to effectively manage, monitor, and configure the whole Smart Grid. Moreover, conducted developments proof the feasibility and reliability of our approach and encourage practitioners to further research towards this direction.

The remainder of this paper is organized as follows. Section 2 reviews the related work and justifies the proposal. Then, Section 3 details the reference architecture for the Smart Grid and Section 4 introduces how it is integrated into the Web of Things. Finally, Section 5 concludes the paper.

2 RELATED WORK

Service composition, heterogeneous devices interaction, and a close contact with the real-life demands are some of the features that have positioned Smart Grids as an appealing landscape for deploying the latest advances concerning the IoT and WoT. Over the last years, practitioners have directed their efforts on enabling communications between distinct types of devices spread across the different network facilities that compose the Smart Grid (Zaballos et al., 2011). Certainly, the IoT and the WoT approaches have promoted such advances in the sense that IEDs are no longer considered as isolated entities but referred to as gears of a complex and heavily coupled distributed system (Guinard et al., 2011; Guinard et al., 2010). While the IoT has provided a mature approach to enable hardware communication on the Smart Grid (Zaballos et al., 2011; INTEGRIS, 2011), management, monitoring, and grid configuration requirements envisage the need of using either centralized Network Management Systems (NMSs) (Gungor et al., 2013) or WoT-based approaches (Guinard et al., 2011; Priyantha et al., 2008).

Although centralized NMSs are rapid to deploy and easy to maintain, their lack of scalability, single point of failure exposure, and bottleneck effect vulnerability make them unfeasible for real-world applications (Aman et al., 2013). These issues are driving system designers to explore distributed solutions for the Smart Grid domain such as the Representational State Transfer (REST) and Web Services (Guinard et al., 2010). On the one hand, RESTful strategies (Cubo et al., 2012; Luckenbach et al., 2005) are targeted to ease the development of scalable services and applications by (1) uniformly identifying every smart object through a unique Uniform Resource Identifier (URI), (2) using HTTP stateless communications, (3) representing resources through standard human readable formats (e.g., XML), and (4) using simple parsing algorithms—typically embedded on tiny web servers—to interact with every IED (Guinard et al., 2011; Duquennoy et al., 2009). On the other hand, strategies based on Web Services pursue the same goal but implement some advanced facilities (e.g., UDDI server, WSDL, security) rather than using light weight protocols (Guinard et al., 2010; Priyantha et al., 2008).

Despite the aforementioned benefits featured by Web Services and RESTful frameworks, the established electric industry is still far from widely adopting them as a standard solution for the Smart Grid domain (INTEGRIS, 2011). In addition, both solutions may incur in some critical security issues that are not affordable in this domain (Zeng et al., 2011; Bou-Harb et al., 2013). Therefore, in the INTEGRIS project we have split the Smart Grid into two isolated layers: a lower layer that encompasses IEDs' communications following the IoT schema—described in (Navarro et al., 2012)—, and an upper layer—herein presented—that covers prosumers interactions with the grid following the WoT approach. To successfully bridge both layers and meet the stringent security and scalability constraints demanded by the Smart Grid (Aman et al., 2013; Navarro et al., 2012), we have implemented a multi-agent intelligent system that (1) is aware of all heterogeneities of the lower

layer (Zaballos et al., 2011), (2) predicts future situations (Gama, 2010), (3) builds a comprehensive system model (Navarro et al., 2012), and (4) delivers it to a uniform interface for user interaction using a RESTful approach. The following section reviews the key parameters to be extracted from the lower layer and presents the internals of this cognitive-inspired intelligent subsystem.

3 A REFERENCE MODEL FOR SMART GRIDS

Actually, splitting the ICT system that holds the ambitious requirements of Smart Grids (Aman et al., 2013) into the two aforesaid layers enables (1) providing an extra security barrier by hiding electric-devices and grid topology from unauthorized end-users, (2) building scalable mechanisms to collect data from IEDs, (3) addressing the electric functions (e.g., voltage monitoring) separately from user-driven functions (e.g., power flow management) and communication issues (i.e., overlay networks (Zaballos et al., 2011)), (4) integrating heterogeneous protocols and technologies, and (5) providing a uniform management interface (INTEGRIS, 2011). The purpose of this section is to present the architecture that supports this idea and announce the key parameters used to link both layers.

From our real-world experiences collected during the INTEGRIS project, we have found that dividing the Smart Grid into these logical layers poses some critical difficulties arisen from the fact that typically, IEDs are closed devices that do not allow implementing custom developments (e.g., security or information-exchange protocols)—as novel experimental devices do (Guinard et al., 2011). Therefore, we proposed a new device coined as I-Dev (Navarro et al., 2012) that behaves as a frontier between these two layers and implements (1) a communications subsystem that allows heterogeneous network coexistence, (2) a security subsystem that provides a reliable and secure low layer communications infrastructure, (3) a distributed storage subsystem that smartly stores all data generated by IEDs, and (4) an intelligent cognitive-inspired subsystem that is aware of all events arisen from any subsystem of the network.

In order to avoid the bottleneck effect and thus deploying a scalable ICT infrastructure, two distinct roles have been assigned to I-Devs: the Perception Action Agent (PAA) and the Domain Management Agent (DMA). Therefore, the whole Smart Grid is spread into several regions (e.g., low voltage substations) referred to as I-Domains (Navarro et al., 2012), where in each I-Domain a DMA and several PAAs interact with deployed IEDs using the IoT approach (Zaballos et al., 2011).

As depicted in Fig. 1, PAAs—placed in the bottom layer—(1) gather information from their associated IEDs, (2) report their findings to their assigned DMA, and (3) execute the commands ordered by it as a result of a collaborative decision between all DMAs in the Smart Grid. Hence, I-Devs behaving as DMAs bridge the bottom layer and the top layer while ensuring scalability and a safe isolation between both sides. Likewise, the upper layer is committed to interface with the management side of all the smart functions provided by the Smart Grid (e.g., supervisory control and data acquisition (SCADA), advanced distributed automation (ADA), distributed energy resource (DER), automatic meter reading (AMR), advanced metering infrastructure (AMI), NMS, or quality of service) taking benefit from the ubiquitous features provided by the WoT approach.

As the lower layer has been broadly addressed in (Navarro et al., 2012; Zaballos et al., 2011), the remainder of this section is devoted to (1) summarize the functionalities of every subsystem running in any I-Dev and (2) specify the key monitoring and configuration parameters to be delivered to the herein proposed upper layer.

3.1 Distributed Storage Subsystem

Smart Grids intrinsically generate vast amounts of heterogeneous information (i.e., every IED may have its own proprietary data format) that need to be effectively stored in order to be later processed by the aforementioned smart functions. In this context, data are generated at different points of the grid and need to be reliably replicated in order to afford site failures and boost their availability through a distributed storage system. Typically, classical relational databases are unable to handle neither the dynamic nature, nor the scalability requirements, nor the stringent computing and storage capabilities of smart devices (Aman et al., 2013). Hence, we developed our own distributed storage architecture running a custom replication protocol that smartly placed data to optimize the performance of smart functions being executed at the I-Devs layer. This replication protocol is aimed to provide a consistent view of any datum—stale but consistent versions are useful for non critical functions such as average consumption monitoring—at any situation. To achieve this commitment data is replicated and partitioned following a hierarchical hybrid approach between state-machine and synchronous primary copy replication that attempts to

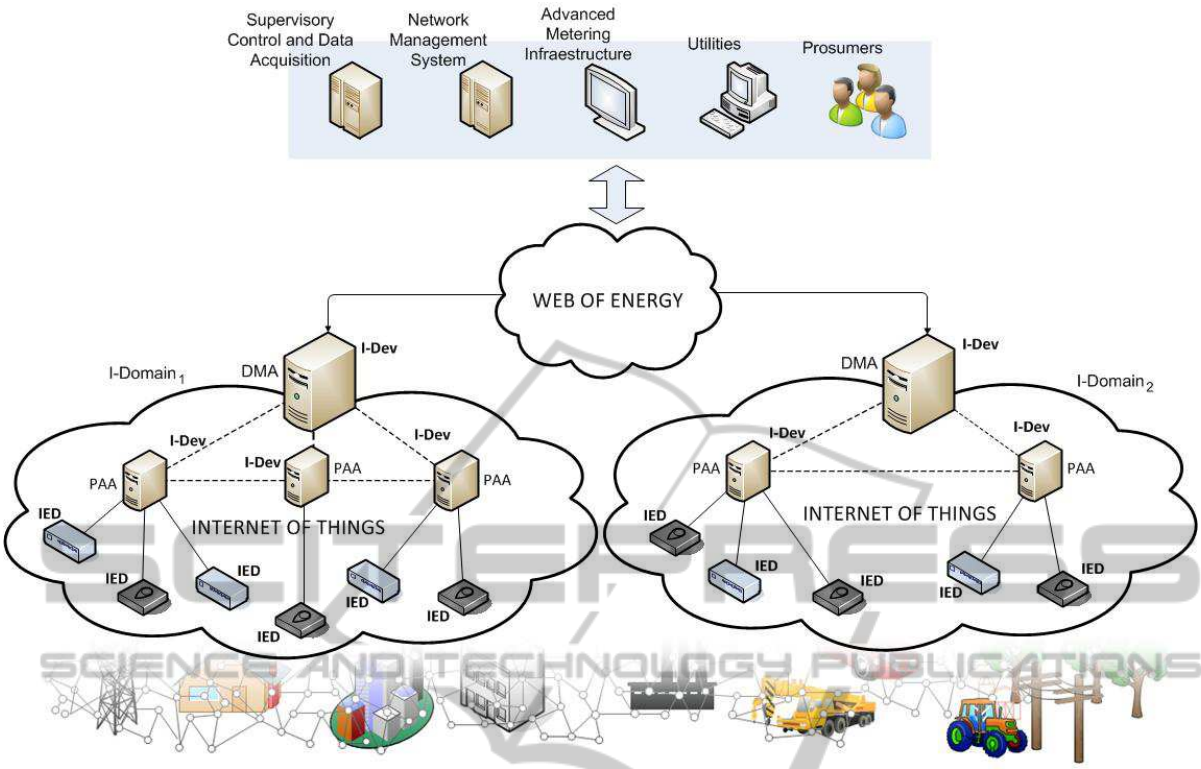

Figure 1: Deployed reference architecture for Smart Grids.

keep system scalability by epidemically updating data across I-Devs (Navarro et al., 2012). This strategy converts the storage infrastructure composed by I-Devs as a dynamic set of nested onion layers that store eventually consistent versions of data.

Manually configuring and monitoring this distributed system is unfeasible because (1) there is an overwhelming number of devices involved on the replication process, (2) there are several interdependencies with other subsystems, and (3) the system conditions may change abruptly. Therefore, we propose to deliver the following key performance metrics and configuration parameters to an intelligent system who is aware of the status of the whole Smart Grid, in order to get a reliable set of actions to be performed on the storage domain. Specifically, we need to track the amount of read/write operations, response time, replication depth, required consistency degree, and replication hierarchy layout (Navarro et al., 2012). The following subsection describes the communications and security subsystem and details which metrics are delivered to the intelligent system.

3.2 Communications and Security Subsystem

ICTs, trust management, and technological integration play an essential role when coordinating all IEDs to solve every smart function. However, they have to be carefully addressed since the electrical distribution infrastructure encompasses aerial and underground areas that current communications technologies are unable to reach (Zaballos et al., 2011). Current approaches in this domain rely on the Internet network to boost their performance but inherit the same threats and critical risks in terms of cyber-security (Bou-Harb et al., 2013). Therefore, communications and security in Smart Grids are crucial for the survival and feasibility of the global electricity distribution concept (Navarro et al., 2012). So far, very few standards concerning security (e.g., IEC62351, NISTIR7268) have been proposed to address the specific issues posed by Smart Grids, which still leaves the network and its links open to cyber-security attacks that may produce Denial of Service (DoS) and eavesdropping of critical network management messages. Cyber attacks in the communications network are aimed to bring the maximum damage, exploit the greatest benefits and take advantage of the network structure or from protocols vulnerabilities for malicious purposes (e.g., extended power outages and destruction of power equipment (Bou-Harb et al., 2013)). Latest advances on network resilience protocols (Chen et al., 2012) implemented on I-Devs permit them to sustain from temporal node

failures or disconnections as long as countermeasures can be activated.

However, these countermeasures may prevent other subsystems to behave properly (e.g., the distributed storage system may be unable to collect data from a given PAA) and thus drive the whole Smart Grid to a panic situation. Therefore, our proposal sends the following key communications and security metrics of every I-Dev to an intelligent system that owns a global view of the Smart Grid: connectivity—the number of links to the Smart Grid control center—, security performance—number of packet errors, number of encryption errors, number of unsuccessful access attempts, number of I-Dev reboots, number of network overload situations and other DoS attacks, and number of packet retransmissions—, quality of service performance—amount of flow rates, discarding probabilities and queue lengths—, and delay performance—average link delays. Then, the intelligent subsystem examines these parameters and selects the best security and communications action (e.g., isolating an I-Dev) in order to achieve the best Smart Grid overall performance.

3.3 Intelligent Subsystem

Although designing and modeling every subsystem of the Smart Grid separately eases the development process, we have observed that it is unfeasible to allow them running on their own (i.e., without considering the whole grid status) (Navarro et al., 2012). Considering the vast amount of data and distinct events continuously arisen from the grid, the management of such a system cannot fully rely on an expert. Therefore, we have chosen an intelligent multi-agent system to interprete the aforesaid key parameters of every subsystem in the grid in order to build a comprehensive model of the whole system. Specifically, this context requires an online learning scheme able to (1) put together the parameters of each subsystem, (2) rapidly adapt to the constant changes of the Smart Grid, (3) provide an accurate estimation concerning the whole grid status, and (4) come up with the best configuration at every subsystem to reach the optimal overall performance. To this regard, we have selected an enhanced version of the eXtended Classifier System (XCS) (INTEGRIS, 2011) that diligently meets these requirements as shown in what follows.

In fact, XCS, a cognitive-inspired algorithm, is targeted to evolve a population [P] of classifiers. At the end of the learning process, the population is expected to acquire a high quality model using these classifiers. Each one consists of a production rule—composed by an antecedent and a consequent—and

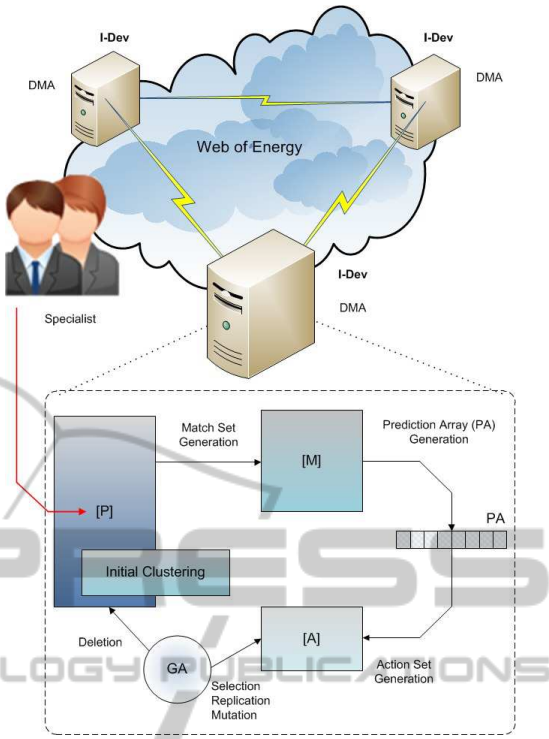

Figure 2: Intelligent subsystem learning architecture. DMAs use the Web of Energy to share their experiences collected at every I-Domain and build a global Smart Grid knowledge model.

a set of parameters that evaluate the quality of the rule. The antecedent part of the rule contains the input variables collected by PAAs from every subsystem and related to the environment (i.e., what the algorithm "senses"). Likewise, the consequent part contains the action predicted for the future status of the Smart Grid. The main parameters that evaluate the quality of every rule are (1) an estimation of the reward that will be received if the predicted status is triggered, (2) the expected error, (3) the experience of the classifier, and (4) the fitness of the classifier.

Thoroughly, XCS follows the online learning process depicted in Fig. 2 at the DMA: it starts with an empty population and it learns by sampling new training examples. This learning process creates the match set [M] containing all the classifiers that match with the current example (INTEGRIS, 2011). If [M] does not contain a minimum user-defined threshold of different actions, the system generates new ones arbitrarily. Then, the action to be proposed to the actuators (i.e., PAAs) is selected via a fitness-weighted average of all matching classifiers in [M], forming the action set [A]. All classifiers in [A] predict the same action and hence they share the evaluation payoff in a niching scheme. At the end of the iteration, a genetic algorithm is applied at [A] to discover new promising

rules, for instance ***if*** *data_response_time* $\in [10,100]$ *ms* ***and*** *... **and** reconnections* $\in [40,60]$ ***then*** *block I-Dev3*.

As the XCS is a reinforcement learning approach, training and scalability need to be properly considered: First, as it is unfeasible to manually label all examples of the training set, we have used an on-line clustering approach based on k-Nearest Neighbors (Navarro et al., 2012) to label them and thus let the system autonomously learn from the environment. Last, in order to meet the intrinsic scalability requirements of the Smart Grid, a unique centralized thinking unit is avoided by deploying a DMA and its associated PAAs on every I-Domian.

However, the distributed nature of this cognitive subsystem entails further concerns on how integrating all the knowledge to an accurate set of human-readable rules, which enables to think globally and act locally. The following section is devoted to detail how these rules are delivered across the upper layer of the herein presented WoT approach.

4 FROM THE IoT TO THE WoE

In fact, distributing the knowledge building layer of the cognitive subsystem (i.e., DMAs) to meet the scalability constraints posed by the Smart Grid definitively hampers the learning process. As shown in Fig. 2, refusing a centralized architecture forces locally collected rules at every I-Domain to be shared among all DMAs of the Smart Grid—the underlying hypothesis in rule sharing is that similar structures (i.e., I-Domains) require similar configurations (i.e., knowledge model)—, which may lead to some conflicting situations arisen from the fact that the cognitive subsystem is unable to reach 100% of accuracy (Navarro et al., 2012). Note that rules shared between I-Domains are those with a classification accuracy greater than a user-defined minimum threshold. Although the dynamics of this on-line learning architecture allow removing these conflicting rules without shutting down or reseting the affected DMA, a reliable decision process to conduct this action is mandatory.

Therefore, as depicted in Fig. 2, we have introduced a new role on the Smart Grid: the expert system; which is the combination of the aforesaid software entities and a specialist that owns enough experience related to the electricity domain. To this regard, this specialist is continuously analyzing the results provided by the intelligent system and thus, learning from the Smart Grid in order to supplement software suggestions by deciding which rules must be deleted from every DMA (also referred to as conflict resolution). Likewise, this expert can introduce new knowledge based on his expertise to the cognitive subsystem by forcing the usage of new rules. We have found (INTEGRIS, 2011; Navarro et al., 2012) that this expert system greatly enhances the performance of the intelligent system because it ensures that critical decisions are taken consistently.

However, the feasibility of this approach relies on a uniform interface that fits with the intrinsic distributed nature of the Smart Grid and enables its effective management. So far, existing preliminary solutions (INTEGRIS, 2011) achieve such commitment by using centralized management systems (e.g., SCADA) that are unable to fully integrate the long-term requirements and applications posed by the Smart Grid domain (Gungor et al., 2013). Hence, we have deployed a WoT-inspired infrastructure—coined as WoE—on top of the Smart Grid that links all I-Domains and permits a bidirectional communication between electricity domain (i.e., bottom layer in Fig. 1) and the application domain (i.e., top layer in Fig. 1).

To this concern, every I-Dev in the Smart Grid has been labelled with an URI, which enables specialists and all entities residing at the top layer of Fig. 1 using asynchronous communications to (1) incorporate new knowledge or erase existing rules that enter in conflict with previously discovered ones, (2) reset and manipulate the configuration parameters that control every subsystem—especially the cognitive one—, and (3) obtain accurate statistics from every DMA, and thus from the whole Smart Grid as depicted in Fig. 3.

More specifically, Fig. 3 depicts some of the web interfaces that integrate the heterogeneous framework found on the bottom layer of the Smart Grid—and linked using a IoT approach—to a uniform environment. The top left screenshot in Fig. 3 shows the configuration interface of the distributed subsystem (i.e., replication depth, cache size, number of layers (Navarro et al., 2012)) running at I-Domain 6. The top right screenshot in Fig. 3 shows the configuration of the communications and security subsystem running at I-Domain 3. Finally, the bottom screenshots in Fig. 3 are devoted to depict the two layers of the cognitive system.

The bottom left screenshot in Fig. 3 depicts the management interface of the intelligent subsystem running at I-Domain 9; first, it shows a list of three PAAs, below it depicts the predicted I-Domain status and the selected action in [P]. Additionally, the bottom right screenshot in Fig. 3 depicts the collected data at PAA 2 from I-Domain 7. In this way, specialists can monitor the (1) effects of applying a given ac-

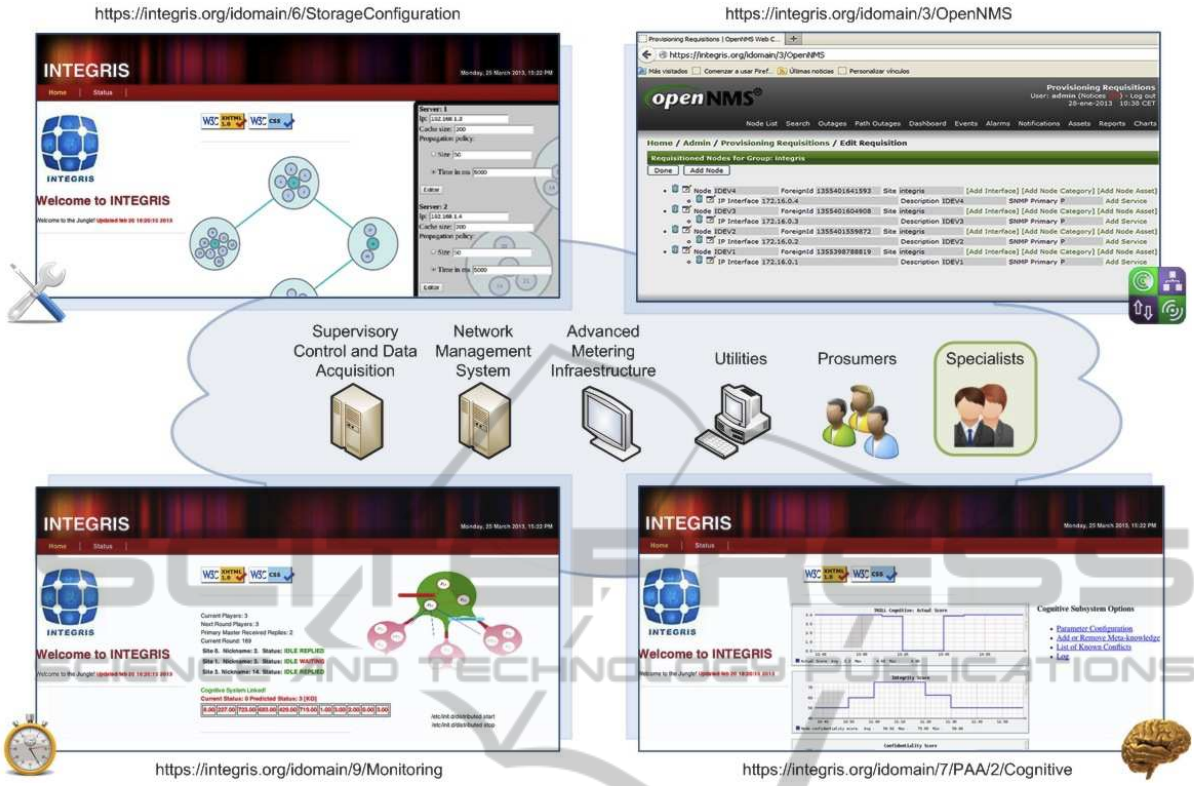

Figure 3: The Web of Energy. A uniform interface to support smart functions and manage the associated distributed, communications, security, and intelligent subsystems.

tion, (2) set of locally and globally collected rules, (3) parameters perceived at every PAA, and (4) training accuracy at a glance.

Thoroughly, the herein presented approach provides a uniform web-based interface referred to as WoE that safely isolates the electricity grid domain from its applications. More specifically, this system includes an ad-hoc distributed storage architecture to support the massive amount of data generated by the grid, that delivers these data through a secured communication network to a multi-agent—able to face the intrinsic dynamic nature of Smart Grids—intelligent subsystem that processes the events and changes arisen in this domain.

5 CONCLUSION

This paper presents a particular application of the WoT to the concrete scenario of power networks. We have conducted our experimentation over the system presented in (Navarro et al., 2012), where an IoT-based infrastructure enabled machine-to-machine interactions between small and resource-constrained devices on the Smart Grid domain. Thus, we have extended the IoT concept by providing a bidirectional human-to-machine interface—inspired by the WoT—that results in a ubiquitous energy control and management system coined as Web of Energy. This proposal combines the web-based visualization and tracking tools with the Internet protocols, which enables a uniform access to all devices of the Smart Grid.

In order to provide such an effective and reliable management interface aimed to address the heterogeneous nature of devices residing on the grid, we have deployed an intelligent subsystem devoted to (1) learn from the real-world events, (2) predict future situations, and (3) assist on the decision making process. This intelligence layer is composed by means of a multi agent system to meet the scalability requirements of the Smart Grid. Moreover, it builds a knowledge model in terms of production rules, implements its own apportionment of credit mechanism (i.e., uses reinforcement learning), and has an ad-hoc rule discovery technique based on a genetic algorithm. However, we have seen that the intelligent system is unable to cope with the complexities of the Smart Grid that hamper the optimal learning performance (i.e., 100% accuracy). Therefore, we have successfully

included the role of the specialist in the presented WoE approach. This entity is targeted to dynamically rectify the intelligent subsystem outcomes and improve the global grid performance. Note that the aforesaid WoE framework eases the specialists commitment considerably, in the sense that they are able to interact with the different modules that control the Smart Grid through a pervasive and user friendly web-based interface rather than traditional roughly command lines.

Finally, we have demonstrated the feasibility of our proposal by running it on the real-world scenario defined by the INTEGRIS project (INTEGRIS, 2011). Our collected experiences show that this uniform management interface—depicted in Fig. 3—plays a key role in the process of development and standardization of current and new smart functions. Certainly, this paper encourages practitioners to conduct future work in this direction by defining new electric applications following this layered scheme.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union European Atomic Energy Community Seventh Framework Programme (FP7/2007-2013 FP7/2007-2011) under grant agreement 247938 for Joan Navarro, Agustín Zaballos by Generalitat de Catalunya for its support under grant 2013FI_B2 00089 for Andreu Sancho-Asensio, and by the Spanish National Science Foundation (MEC) (grant TIN2012-37719-C03-03) for José Enrique Armendáriz-Iñigo.

REFERENCES

Aman, S., Simmhan, Y., and Prasanna, V. K. (2013). Energy management systems: State of the art and emerging trends. *IEEE Communications Magazine*, 51(1):114–119.

Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., and Assi, C. (2013). Communication security for Smart Grid distribution networks. *IEEE Communications Magazine*, 51(1):42–49.

Chen, P.-Y., Cheng, S.-M., and Chen, K.-C. (2012). Smart attacks in Smart Grid communication networks. *IEEE Communications Magazine*, 50(8):24–29.

Cubo, J., Brogi, A., and Pimentel, E. (2012). Towards behaviour-aware compositions of things in the Future Internet. In *Proceedings of the 2nd International Workshop on Adaptive Services for the Future Internet and 6th International Workshop on Web APIs and Service Mashups*, WAS4FI-Mashups '12, pages 28–35, New York, NY, USA. ACM.

Duquennoy, S., Grimaud, G., and Vandewalle, J.-J. (2009). The Web of Things: Interconnecting devices with high usability and performance. In *International Conference on Embedded Software and Systems, ICESS '09, Hangzhou, Zhejiang, P. R. China, May 25-27, 2009*, pages 323–330, Hangzhou, Zhejiang, P. R. China. IEEE.

Gama, J., editor (2010). *Knowledge Discovery from Data Streams*. Advances in Database Systems. Chapman and Hall/CRC, Florida, USA, first edition.

Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., and Savio, D. (2010). Interacting with the SOA-Based Internet of Things: Discovery, query, selection, and on-demand provisioning of Web Services. *Services Computing, IEEE Transactions on,*, 3(3):223–235.

Guinard, D., Trifa, V., Mattern, F., and Wilde, E. (2011). From the Internet of Things to the Web of Things: Resource-oriented architecture and best practices. In *Architecting the Internet of Things*, pages 97–129. Springer Berlin Heidelberg.

Gungor, V. C., Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., and Hancke, G. P. (2013). A survey on smart grid potential applications and communication requirements. *IEEE Trans. Industrial Informatics*, 9(1):28–42.

INTEGRIS (2011). INTEGRIS FP7 Project INTelligent Electrical Grid Sensor communications. ICT-Energy-2009 call (number 247938).

Luckenbach, T., Gober, P., Arbanowski, S., Kotsopoulos, A., and Kim, K. (2005). TinyREST-A protocol for integrating sensor networks into the Internet. In *in Proc. of REALWSN*.

Navarro, J., Zaballos, A., Sancho-Asensio, A., Ravera, G., and Armendariz-Iñigo, J. E. (2012). The information system of INTEGRIS: INTelligent Electrical GRId sensor communications. *Industrial Informatics, IEEE Transactions on*, PP(99):1.

Priyantha, N. B., Kansal, A., Goraczko, M., and Zhao, F. (2008). Tiny Web Services: design and implementation of interoperable and evolvable sensor networks. In *Proceedings of the 6th International Conference on Embedded Networked Sensor Systems, SenSys 2008, Raleigh, NC, USA, November 5-7, 2008*, pages 253–266, St. Louis, Missouri, USA. ACM.

Zaballos, A., Vallejo, A., and Selga, J. M. (2011). Heterogeneous communication architecture for the Smart Grid. *IEEE Network*, 25(5):30–37.

Zeng, D., Guo, S., and Cheng, Z. (2011). The Web of Things: A survey (invited paper). *JCM*, 6(6):424–438.