International Journal of Smart Grid and Clean Energy

Software defined utility: A step towards a flexible, reliable and low-cost smart grid

Ramon Martin de Pozuelo[a], Miguel Ponce de Leon[b], John Howard[c], Alan Briones[a], Jerry Horgan[b], Julia Sánchez[a]

[a] *Engineering Department, Universitat Ramon Llull (URL) - La Salle, Quatre Camins 30, 08022, Barcelona, Spain*
[b] *Telecomunications Software and Systems Group, Waterford Institute of Technology (WIT), Cork Road, Waterford, Ireland*
[c] *ESB Networks, 27 Lower Fitzwilliam Street, Dublin, Ireland*

Abstract

The Smart Grid relies in Information and Communication Technologies (ICT) but usually there is still a lack of integration in their deployment. They are designed as separated systems and managed that way too. In addition, the changes in the electric network are so complex and dependable on a very rigid hardware architecture. Based on the work done in the European project FINESCE, this paper presents the "Software Defined Utility "(SDU) concept, which advocates the migration of the utility infrastructure to software systems instead of relying on complex and rigid hardware based systems. This new approach provides a prospective view on the evolution of power systems that will benefit from software systems and high-speed data network infrastructures. More concretely, as a first SDU building block, the paper proposes a data storage and management system based on a hybrid cloud infrastructure to meet the storage requirements of electric utilities. In this regard, the following dimensions have been analysed: the most appropriate methodology to select where data resources should be allocated; security requirements and threads taking into account its deployment in a critical infrastructure like a Smart Grid.

Keywords: Smart grids, software defined networks, hybrid cloud, resource allocation, security.

1. Introduction

The relevance of Smart Grid has gained momentum in the last few years, although not all the parts of what this trend involves are equally deployed [1]. Actually, the Smart Grid is a system of systems that includes not only the power system itself but also multiple Information and Communication Technologies (ICT) that represent its fundamental building block. However, there are many times when they have not been integrated together in previous systems [2]. Partial solutions targeted only to specific aspects of the power system are no longer valid given the many services to be provided and the high cost of deployment of many specific systems [3].

It is clear that the energy sector requires integrated smart grid communications. The FINESCE project [4] developed an advanced optical network architecture to overcome the impediments of stringent electrical protection requirements; cyber security and legacy infrastructure. It also focused on validating and evaluating the novel "Software Defined Utility" (SDU) concept, which advocates the migration of the grid utility infrastructure to software systems as much as possible.

The Smart Grid and more concretely in the electricity distribution network, there is a huge amount of data collected and being processed continuously. Nowadays, it is handled by dedicated and highly expensive devices. Relying on the expertise and experience from the authors (with a joint perspective from utilities and academia), we advocated for the SDU concept where many of the functions that those devices do will rely on programmable commodity hardware, low-cost sensors, and high-speed and

Manuscript received April 5, 2016; revised October 18, 2016.
Corresponding author. Tel.: +34 932902475; *E-mail address*: ramonmdp@salleurl.edu.
doi: 10.12720/sgce.5.4.280-289

reliable IP-based communications underneath.

As fundamental pieces of this approach, there were some devices we defined as a single, yet distributable and interconnected, device (called FIDEVs, FInesce DEVices), which integrate the needed functions for it (scalable data storage system, identity management and access control, high-speed and reliable communication interfaces, Remote Terminal Units (RTUs) and Smart Meters data collectors, and support for Smart Grid functions).

Those FIDEVs are targeted to be placed at different electrical distribution network points (e.g. secondary substation) and interconnected, considering the following list of potential applications to be developed over FIDEVs architecture, such as remote electrical fault information recovery and remote access control, self-healing network functions, or distribute energy resources (DER) monitoring and control.

The rest of the paper is structured as following. Section 2 synthesise the trial undertaken in FINESCE for evaluating the SDU concept and the usage of interconnected FIDEVs as part of the deployment. Section 3 discuss about Smart Grid communication requirements and challenges, and proposes different solutions. Section 4 evaluates the usage of hybrid (public-private) cloud platforms for managing the data of the Smart Grid at distribution level. Section 5 reviews some security concerns in Smart Grid and list some of the security requirements that should be considered. And section 6 presents some conclusions and further work to be done continuing the development of the SDU concept.

2. FINESCE SDU Trial Deployment

FINESCE is the Smart Energy use case project of the Future Internet Public Private Partnership Programme. It aims at defining an open infrastructure based on Information and Communications Technology (ICT) used to develop new solutions and applications in all fields of Future Internet related to the energy sector. To accomplish this goal a cloud-based environment is proposed, providing high scalability, fast provisioning, resilience and cost efficiency, while facilitating the deployment of applications and services for utilities.

One of its trials deployed in Ireland was focused on the development of SDU concept. In that sense, the first step proposed was establishing a distributed storage system that provides high-availability and reduces the latency in acquiring data from the local sites of the utility while offering a secure solution to share data information with external stakeholders.

Relying on the data network infrastructure of the utility, the SDU Trial interconnects different FIDEVs (FInesce DEVices) placed at different sites of ESB and WIT in Ireland and FUNITEC lab in Barcelona. FIDEV is a platform built on commodity hardware, in which different software subsystems on top provide communication and data concentrator functionalities. To mention some of those subsystems, it incorporates a TRILL [5] protocol interconnection between and other FIDEVs. It provides Layer 2 routing functionalities, together with a simplified communication network management, a more efficient use of the network throughput, and the possibility to directly use different protocols on top of it, such as IEC 61850.

FIDEV is defined in FINESCE project as an upgrade of the communication part of IDEVs (Integris DEVices) defined in FP7 INTEGRIS [6], adapting the concepts developed in INTEGRIS into the FIWARE ecosystem of Generic Enablers (GEs) and cloud approach. These GEs will provide a secure interface with the distributed storage system and seamless interfaces to data management for the managers (in this case, a network manager from ESB). Among these new functionalities, it incorporates seamless interaction between FIDEVs private distributed storage system and FIWARE Lab Cloud. In this sense, the system will be formed by a set of separated INTEGRIS FIDEV's testbed devices (physical or virtualised) that will constitute a private Cloud, plus public cloud storage capabilities by means of FIWARE Lab. Data can reside in any of both clouds and be moved from one to another according to the decision of their owners.

What is proposed, as one of the main components in which a Software Defined Utility system, is providing a flexible data management system that will allow to maintain ESB generated data locally

replicated and also in the cloud (through FIWARE Lab), when needed.

The scenario (Fig. 1) deployed in this trial wanted to show a novel ICT infrastructure for Smart Distribution Grids that allow for the flexible movement of SG data and applications from local systems to FIWARE Lab Cloud and protect them by the use of the security GEs developed in FIWARE.

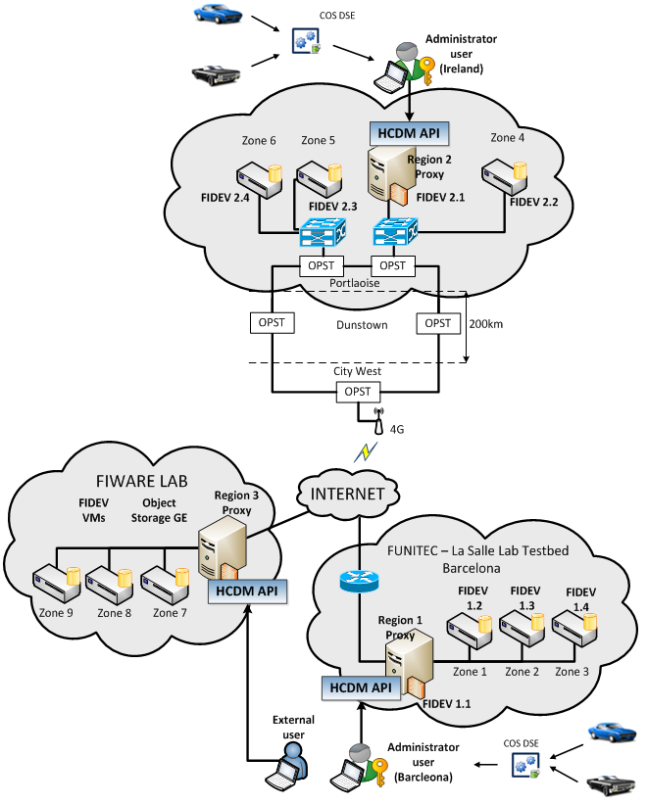

Fig. 1. FINESCE Software Defined Utility trial scenario.

2.1. Objectives

Several reasons could arise in the mobility of the applications and information from the public cloud to local storage and vice versa. They range from application latency improvement (placing apps closer to data when necessary) to the confidentiality of the data (when the data is too sensitive to be stored in the public Cloud), through the low capacity of local resources (and using the public Cloud when more storage resources -and more flexible and dynamic ones- are required). However, it will make DSO infrastructure ready to interact with the Cloud in a very gradual incorporation of the novel functionalities.

The objective of this trial was to assess the benefits of using a distributed architecture of these devices into the Smart Distribution Grid infrastructure (e.g. locating one of them into each substation), in order to simplify its communications and show the benefits of a "Software Defined Utility" approach in which FIDEV platforms could be basic management elements.

More concretely, first objective is to investigate networking alternatives to the Optical Packet Switch and Transport (OPST) architecture and TRILL protocol deployed. In order to create a virtual network for each FIDEV over fibre, within the IEC 61850 context, some virtual networking technologies were investigated. Virtual Extensible LAN (VXLAN), NVGRE: Network Virtualisation using Generic Routing Encapsulation and SDN / Openflow were studied as alternative solutions while still conforming to IEC 61850 and being installed with legacy substation relay technologies.

Second objective is to integrate the flexible interoperation of the FIWARE Lab public Cloud with the

distributed FIDEVs storage system, acting as a Smart Grid private Cloud, to allow moving DSO data between them.

And the third objective is to analyse the level of security required in that environment and validate if the software tools used can provide a good solution to secure the data to be hosted in the FIWARE Lab public Cloud and again to allow a flexible collaboration among clouds.

3. Substation Communications

One of the requirements that the new generations of Smart Grid are bringing is the advanced management by means of real-time monitoring of the energy parameters at several points of the electric network. Furthermore, the massive amount of data generated by the Smart Grid in different contexts (RTUs, IEDs, smart meters, sensors, electrical vehicle charging points, etc.) should be handled adequately in order to take the required action as fast as possible at a specific location. Hence, in order to move the collected data to the point where can be processed and it is valuable, the data communications network becomes a critical piece of the smart grid and should be correctly integrated. An ICT environment able to efficiently encompass the communications requirements of the Distribution Smart Grid and providing a distributed architecture capable of integrating in a more flexible way the different elements of the Smart Grid is needed. This flexibility and high-speed data movement requirement is fostering the adoption of IP in the DSO environment, and electric utilities are looking for solutions that can gradually introduce IP interoperability and management functionalities. FINESCE project evaluated the deployment of high-speed optical network between substations and the usage of TRILL layer 2 protocol to transport the data between FIDEVs, which worked as data concentrators in each substation.

In today's times, virtually all Ethernet networks are switched networks, meaning that they employ switches to allow users to send and receive data at the same time without collisions. That is also the case of the communications networks in the Smart Grid, in which high availability and low latency requirements are especially critical. TRILL protocol eliminates the problems associated with using the Spanning Tree Protocol in a data network. Spanning Tree restricts all traffic to a loop-free tree and in doing so creates blocking conditions that require the over provisioning of links. TRILL allows to provide a fully meshed network where all links are available on all paths, eliminating the need to over-provision links and improving the utilization of data networking equipment. Its objective is to preserve the benefits of STP but, at the same time, optimizing the usage of bandwidth and having redundancy and load balancing. While still operating at the link layer (level 2), TRILL uses some concepts of network layer protocols such as IP. As a matter of fact, TRILL is an adaptation and extension of the IS-IS routing protocol to the Ethernet addressing and frames.

FINESCE project tested an implementation of TRILL protocol in C code over the FIDEVs, in order to interconnect them, maximizing the usage of the links between the different facilities of the SDU trial scenario and improving the availability of the data collected there.

Given that the underlining data network communication between FIDEVs was based on layer 2 fibre communication infrastructure of the ESB, WIT investigated a distinct number of virtual networking overlay technologies such as Virtual Extensible LAN (VXLAN) [7], Network Virtualisation using Generic Routing Encapsulation (NVGRE) [8], Link Aggregation Group (MC-LAG) [9] and opened up the opportunity to look at SDN / OpenFlow [10] as an alternative to using TRILL.

Using overlay virtual networks for communications enables scale-out, resilience, and Equal-cost multi-path (ECMP) forwarding. This eliminates the need for Multiprotocol Label Switching (MPLS), virtual local area networks (VLANs) and Virtual Routing and Forwarding (VRFs) when securely separating traffic across the data plane. The underlying network's responsibility is merely to forward the overlay traffic. This will keep its use within the utility requirements for a Software Defined Utility.

VxLAN is a network virtualization technology that allows VLAN-Id to be re-used and applied per user instance. NVGRE is an alternative to TRILL (and VxLAN), which transports Ethernet frames tunnelled in GRE. NVGRE was found to be very similar to VxLAN but potentially more accessible to existing networking equipment through the usage of GRE as the underlying technology. However, ECMP was

considered an issue on some equipment / configurations as it could not provide efficient bandwidth utilisation. GRE does not use TCP/UDP and therefore provides limited ECMP hashing capability.

MC-LAG is a method of inverse multiplexing over multiple Ethernet links, with MC-LAG adding node-level redundancy to the normal link-level redundancy that a LAG provides. As part of the investigation we found that MC-LAG is not standardised in the networking world and thus could not be considered as an alternative in the IEC 61850 context.

With Software Defined Networking (using Openflow) the routing can become simpler, however the controller elements and management can become more complex. In this case we wanted to look at how OpenFlow could control the fibre wavelengths chosen to be used by the FIDEV device.

Making a comparison between TRILL vs VXLAN (NVGRE) vs OpenFlow it was found that:

- TRILL provides L2 bridging with L3 features (an underlay). It provides a mechanism to provide L2 bridges between network segments, but instead of using a single network gateway, multiple (localised) gateways can be provided by using Route Bridges and therefore providing better path optimisation. However, it was also noted that the standard was starting to drift amongst network vendors with support being dropped by Arista and Cisco evolving towards Fabric Path.
- VXLAN provides L2 over L3 (an overlay) with east-west scaling. It provides L2 links by encapsulation over Layer 3, which is very similar to NVGRE. However, it only provides for a single gateway, which can cause network inefficiencies and sub-optimal path selection. There are a few work arounds, such as using Cisco HSRP or VRRP, but these are not as efficient as using the nearest L3 hop. Additionally, IBM have adapted VxLAN to support their DOVE controller to try and address this L3 inefficiency.
- OpenFlow provides control plane automaton. OpenFlow is separate to the Data Plane and makes decisions based on pre-defined policies, as do switches and routers through configuration. However, OpenFlow maintains a view of the whole network and operates in a centralised fashion and therefore determines path selection etc based on a centralised view of the network and the policy versus a switch or routers view of its adjacencies.

Or to put it another way, TRILL and VxLAN only provide a piece of the networking solution (enabling devices to communicate at L2 with varying levels of efficiency) whilst introducing more technologies to be dealt with. They operate within the network and make decisions based on the level they see it at, i.e. what is my next hop to get closer to my destination (like following sign-posts within a maze) versus OpenFlow which can view the whole network simultaneously, along with the policy definition / configuration, and therefore make more optimal decisions (like being in a helicopter above the maze guiding someone below).

OpenFlow therefore provides a much richer control plane and therefore a fuller networking solution and enables the continued use of the existing data plane without needing to introduce underlay or overlay technologies. Control plane automaton is certainly the direction we wanted to go in, with OpenFlow (1.3) [11] supporting a number of significant features:

- MPLS (Push/Pop).
- VLAN (Push/Pop).
- Provider Backbone Bridges (PBB) (Push/Pop).
- IPv6.
- Differentiated Service Code Point (DSCP) re-writes.
- Slicing - multiple output queues per port.
- Address Resolution Protocol (ARP) matching.
- Virtual ports (LAGs / tunnels).
- Explicit Congestion Notification (ECN).

Also with OpenFlow there are flow message attributes that could be used in the SDU context such as:

- Cookie
- Priority
- Buffer_id

All these factors have pointed towards a usage of OpenFlow as a viable alternative in the SDU environment.

4. Hybrid Cloud for Smart Grids

In FINESCE project we advocated for a Software Defined Utility (SDU) concept where many of the functions that those devices do will rely on programmable commodity hardware, low-cost sensors, and high-speed and reliable IP-based communications underneath. For building up this concept we started to develop a storage system adapted to the requirements of the Smart Distribution Grid (e.g. very low latency, high-availability, data processed in spread locations, etc.), and can handle properly the data generated at the costumer (smart meter), aggregator or substation level. At the end, we aimed at establishing a distributed storage system that provides high-availability and reduces the latency in acquiring data from the local sites of the utility while offering a secure solution to share data information.

One of the objectives of FINESCE was to investigate in the usage of hybrid cloud for managing the the data generated by the Smart Distribution Grid environment. A private cloud was considered to store recent gathered data generated (smart meter data, electric vehicle charging stations, etc.), but there is not always enough storage capacity to keep all the historical data. Then, a public cloud is used to respond less restrictive queries or to handle peak demands, using an outsourcing burst. In the case of outsourcing burst, there is only an additional expense on demand when the private cloud cannot provide all the services, being the necessary additional resources provided by the public cloud [12].

Concretely, Software Define Utility trial (SDU) specifies data gathering from utility and data replication between nodes located in two different environments, in public and private clouds, creating a hybrid cloud. These nodes have the ability to replicate information through them and aim to store information in several allocations to have access from anywhere, regarding the cyber-security aspects, and allowing the users with the corresponding permissions to access the system.

However, the crucial factor for economic savings in IT by using a hybrid cloud is the optimal allocation of resources. If we imagine a scenario with different services to be allocated in more than one cloud, the distribution of these services is not trivial. Besides, a high time response is a detriment of the Quality of Service (QoS) offered by the cloud [13]. The fact of choosing a particular location without a defined strategy may entail not the best choice for a resource distribution to fulfil the defined requirements or can represent a cost much higher than the optimum cost [14]. It is necessary to design a set of rules that mark preferences, priorities and limits of cost, time, etc. in order to obtain the best possible location for services or data in a particular scenario [15]. In order to analyze the behaviour of the cloud and help to determine the best place to store the Smart Grid data, a table (Fig. 2) was created to characterize the cloud depending on the service provided and a set of objective metrics. This table was created thanks to the joint feedback of experts from different perspectives (Academia, DSOs, ICT industries, etc.) working in FINESCE project.

In the vertical axis, the table provides a set of metrics classified in different categories: Computation, Storage and Network. The Miscellanea category is added to complement this classification, including economic, elasticity, scalability or security aspects. So, the importance of several metrics on a cloud is qualitatively defined depending on which action is being carried out, with a weight of 1 (low importance), 2 (medium importance) or 3 (high importance). It is important to emphasize that the assigned colors, red (1), yellow (2) or green (3), were defined through a process of cross opinion between different stakeholders involved in the project. The boxes in blue were subsequently modified in a second iteration, analyzing the contributions and opinions from other partners and cloud service providers.

The horizontal axis defines a set of processes and operations that are performed in a cloud, in order to characterize the behavior of the cloud. Depending on the type of services mostly used, and therefore the type of cloud demanded by the user, this table can determine which metrics should be selected if we want to evaluate and grade the available clouds where the user can allocate resources. If we want to use it in a more fine-grained view, before doing one of the specific operations, Fig. 2 can be consulted in order to select which metrics should be taken into account to evaluate in which cloud to allocate a resource.

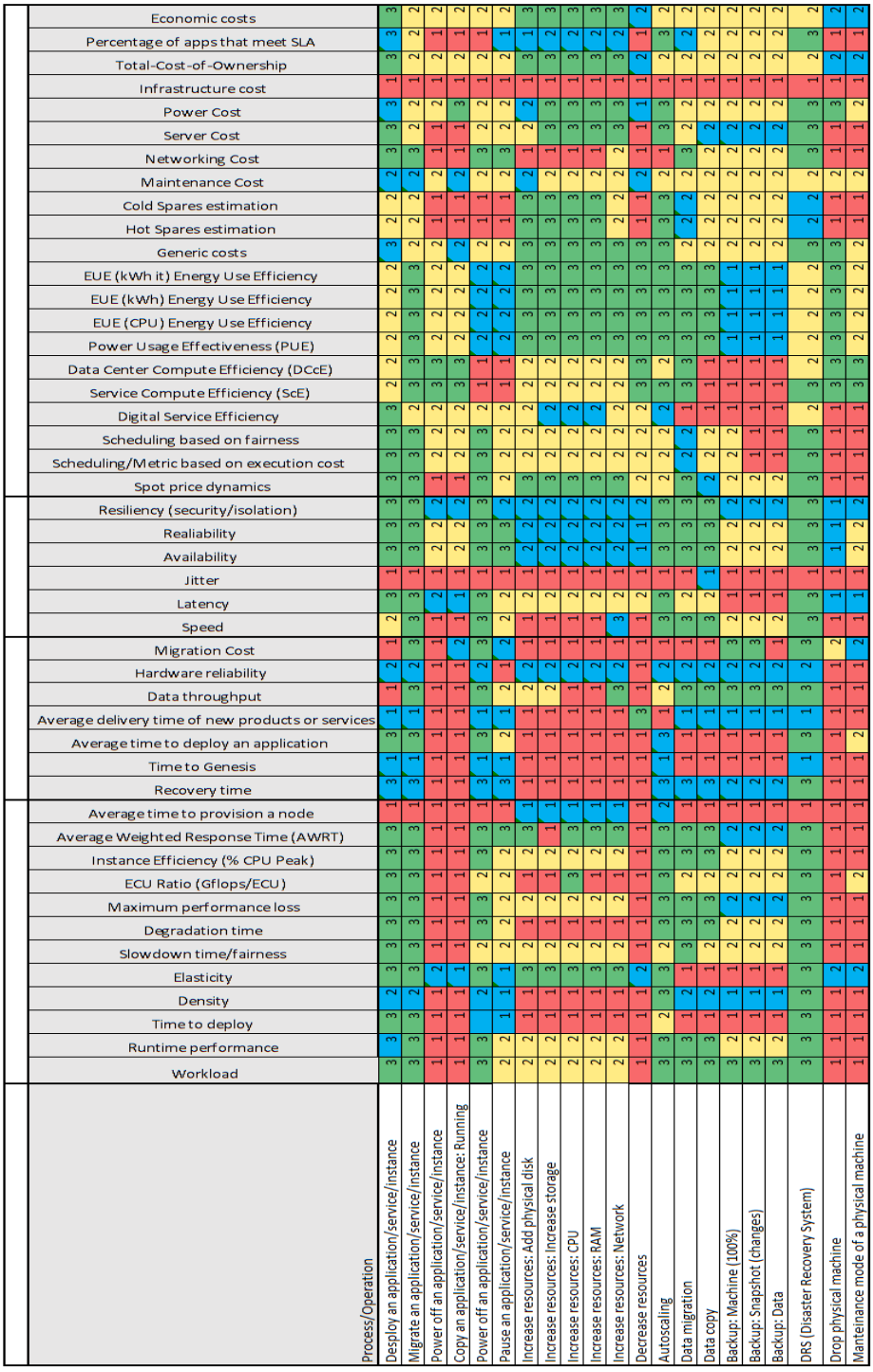

Fig. 2. Cloud metrics and evaluation.

After reviewing several similar studies [16], it was found that there is a tendency to follow a specific strategy to deploy services in the most suitable cloud. This strategy is based on using metrics to evaluate the location of services in one cloud or another. Some studies [17], [18] stand on the premise that the

placement of resources will always be cheaper in the private cloud than in public clouds. This is because it is supposed to have available resources in the private cloud (the investment to deploy the infrastructure has already been performed previously). Thereby, the proposal is to place all the services in the private cloud, which shall not assume any additional cost unless the operation itself, relying on a threshold value. Beyond this threshold, the resources should be placed in the public cloud due to peak loads and their associated cost on demand. To set this threshold, the use of metrics that help to mark the boundary of the private cloud usage is necessary.

5. Security Concerns

Security issues, threats and vulnerabilities were especially taken into account because of the criticality of the environment that the cloud supports. The key to deliver secure services through the cloud resides in perfectly knowing all the identified problems associated and try to apply "security by design". However, not all implementations are perfectly developed and some problems are found with the API implementation used to storage data.

Table 1. Securityrequirements for smart energy use case

Security Issue		Problem Description	Priority	Reason	Impact				
					Very Low	Low	Moderate	High	Very High
Data Security	Data Leakage	Data is stolen and delivered without permission of the proprietary.	5	If a malicious user can access the system, user stored data could be compromised. This fact could derive in legal problems.					X
	Data Forgery	Data is modified by a malicious user and not detected.	6	Once the access is accomplished, if notifications of changes are not considered, a malicious user could modify user stored data.				X	
	Data Lost	Data is erased by a malicious user or a human error.	7	If a backup system is maintained, this could be an important but not critical problem since data could be restored.			X		
Network Security	Data Transaction	Data is delivered through the network and could be visible to malicious users if it is not encrypted. It depends on the sensibility of the data transmitted that this issue becomes more critical.	1	It is not necessary to access the system to obtain data under these circumstances. Therefore, it is considered that the most important aspect is that data transactions (data in transit) are encrypted.					X
	Commands execution	Many applications that can reside in IEDs could be sensitive to latency. A DoS attack to the network resources could affect its performance. It affects availability of the services.	8	Network resources have to be controlled because the access to data stored and applications in IEDs depends on them. It is considered that network will be designed to detect DoS attacks and avoid latency problems.				X	
Authentication		Access to IEDs and data storage has to be controlled and tracked to avoid wrong usage. It affects confidentiality, integrity and availability if a malicious user gets a user with rights granted.	2	It is very important to maintain control over the users that access data stored in IEDs and track the actions this users perform to avoid problems with data stored and IEDs functionality. If a wrong usage is detected and users are authenticated, the system can isolate the problematic user to avoid damage.					X
Authorization		Not all users have the same authorization	3	It is important to maintain isolated rights to access resources				X	

	policies to different zones, resources or stored data. Admin users, privileged users, guest users and third party users must be catalogued with different authorization rules.		because the system could have third-party users, guests/clients, administrators, etc and not all should have complete access. The system could be modified by users without complete knowledge or by malicious users if a good authorization policy is not applied.	
Identity Management (IdM)	The way to maintain a good connection between users and authorization rules is implementing a robust IdM.	4	Necessary to map users with their respective authorization rules and to maintain control over granted access to the system.	X

Therefore, this paper presents also another contribution beyond the state of the art as a result of the FINESCE project. Table 1 was developed jointly with Smart Grid experts from industry and academia, presenting a table with a set of the most important security issues that can affect the proposed infrastructure for the FINESCE's Smart Grid. The main goal is to establish an order of implementation priorities regarding the security aspects. Authors gathered this information from several utilities in order to establish these priorities by numbering them with numbers from 1 to 8 (1 being the highest priority and 8 the lowest). Utilities have to provide the impact level for every problem if the system is crashed down. In the Reason column of Table 1 is presented a brief explanation of the rationale behind the order and decisions of which aspects are more critical than others. More extensive information about it and how those requirements were tackled in the case of FINESCE project can be found also in [19], [20].

6. Conclusions

The work done together between the ESB, WIT and URL - La Salle and the results obtained from the trial have been used by the ESB to evaluate a novel "Software Defined Utility" approach, which consists on high-speed physical communications and flexible software infrastructure over it. FIDEVs would be the only elements of this wider approach, focusing the trial on the demonstration of a secure and distributed storage system that can easily migrate data from private infrastructure of the utility/DSO, to public cloud, in order to easily sell or offer this data to external stakeholders. This also provided a platform to manage distributed data among different substations, automatically replicating it in the different locations, which can help to evaluate the substitution of some very expensive electrical network devices by software platforms such as FIDEVs, low-cost sensors and high-speed communications underneath.

While the network does meet utility requirements for distribution level systems and as the communications layer for the SDU, some issues regarding support for legacy differential protection requirements remain to be explored. Further testing has to be undertaken.

The work done in FINESCE represents only a first step of the whole concept of SDU, seeking a flexible, low-cost and easy-to-manage OT and IT infrastructure for the Smart Grid. A distributed storage built over a hybrid cloud system working at electric distribution level represents a powerful tool for managing the data generated by substations, smart meters and other sources (e.g. electric vehicle charging points) in real-time. Besides this, the requirements summarised in the paper give some guidelines of how to design this platform to meet the high level of security required in such critical infrastructure.

Acknowledgement

This work was carried out within the framework of FINESCE project, funded by the Future Internet Public Private Partnership Programme (FI-PPP) of the European Commission's 7th Framework Programme (ICT-2011, grant number 604677).

References

[1] Arnold GW. Challenges and opportunities in smart grid: A position article. *Proceedings of the IEEE*, 2011; (99)6:922-926.

[2] Zaballos A, Vallejo A, Selga JM. Heterogeneous communication architecture for the smart grid. *IEEE Network*, 2011; (25)5:30–37.

[3] Josep MS, Guiomar C, Agust ń Z, Ramon Mart ń de P. Smart Grid ICT research lines out of the european project INTEGRIS. *Network Protocols and Algorithms*, 2014; (6):2.

[4] FINESCE Project website. [Online]. Available: http://www.finesce.eu/

[5] Eastlake D, Banerjee A, Dutt D, Perlman R, Ghanwani A. Transparent Interconnection of Lots of Links (TRILL). *IETF RFC 6325*. 2011.

[6] Selga JM, Zaballos A, Navarro J. Solutions to the computer networking challenges of the distribution smart grid. *IEEE Communications Letters*, March 2013; (17)3:588-591.

[7] Sridhar T, *et al*. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. (2014). [Online]. Available: https://tools.ietf.org/html/rfc7348

[8] Garg P, Wang YS. NVGRE: Network Virtualization using Generic Routing Encapsulation. (2015). [Online]. Available: http://tools.ietf.org/html/rfc7637

[9] IEEE 802.1AX-2008 - IEEE Standard for Local and metropolitan area networks – Link Aggregation. Technical Report, IEEE, 2008.

[10] McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Turner J. OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 2008; 38(2): 69-74.

[11] OpenFlow 1.3 [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf

[12] Genez TAL, Bittencourt LF, Madeira ERM. On the performance-cost tradeoff for workflow scheduling in hybrid clouds, In *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, IEEE Computer Society, 2013:411-416.

[13] Li S, Zhou Y, Jiao L, Yan X, Wang X, Lyu MR. Delay-Aware cost optimization for dynamic resource provisioning in hybrid clouds, In: *Proc. of IEEE International Conference on Web Services (ICWS)*, June 27-July 2, 2014:169-176.

[14] Chu HY, Simmhan Y. Resource allocation strategies on hybrid cloud for resilient jobs. [Online]. Available: http://ceng.usc.edu/~simmhan/pubs/chu-usctr-2013.pdf

[15] Shifrin M, Atar R, Cidon I. Optimal scheduling in the hybrid-cloud. In: *Proc. of* IFIP/*IEEE International Symposium on Integrated Network Management*, 27-31 May 2013:51-59.

[16] Mazhelis O. Role of data communications in hybrid cloud costs. In: *Proc. of 37th EUROMICRO Conference on Software Engineering and Advanced Applications*, 2011:138-145.

[17] Malawski M. Cost minimization for computational applications on hybrid cloud infrastructure. *Future Generation Computer Systems*, 2013; (29):1786-1794.

[18] Zhang H, Proactive workload management in hybrid cloud computing. *IEEE Transactions on Network and Service Management*, 2014; (11)1:90-100.

[19] Sanchez J, Corral G, Mart ń de Pozuelo R, Zaballos A. Security issues and threats that may affect the hybrid cloud of FINESCE. *Network Protocols and Algorithms*, 2016.

[20] Howard J, *et al*. FINESCE D5.7 Trial Results. [Online]. Available: http://www.finesce.eu/Results.html, last access 08/04/2016.