Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2014, Vol. 6, No. 2

Smart Grid ICT Research Lines out of the European Project INTEGRIS

Josep M. Selga, Guiomar Corral, Agustín Zaballos, Ramon Martín de Pozuelo

Department of Engineering, La Salle-University Ramon Llull

Quatre Camins 2, 08022, Barcelona (Spain)

Tel: (+34) 932902400 E-mail: jmselga@salleurl.edu, guiomar@salleurl.edu, zaballos@salleurl.edu, ramonmdp@salleurl.edu

Received: April 8, 2014 Accepted: June 15, 2014 Published: June 30, 2014

DOI: 10.5296/npa.v6i2.5439 URL: http://dx.doi.org/10.5296/ npa.v6i2.5439

Abstract

The Smart Grid is an example of a cyber-physical system where the physical power grid is surrounded by many intelligent and communication devices that allow for an enhanced management of the power network itself. The Smart Grid may bring great benefits by massively introducing renewable energy sources in the power grid, reducing carbon emissions and improving sustainability. However, it may also bring big challenges regarding reliability, latency and even cybersecurity, since it opens the power system to at least the same threats faced by the Internet. In fact, vulnerabilities may be still larger, considering the novel, heterogeneous and distributed nature of the Smart Grid. Furthermore, cybersecurity is essential for its survival and feasibility, thus making the risks still more relevant.

Such Information and Communication Technologies and computer networks supporting the Smart Grid need to comply with very stringent requirements. They also need to efficiently integrate and manage in a single network a vast array of technologies which diverse link layer technologies, meshed and non-meshed Ethernet networks, different cybersecurity protocols, networking at different layers, cognitive systems and storage and replication of data.

The objective is to provide a system capable of providing adequate service to the wide array of applications foreseen for the Smart Grid but the complexity of the problem is impressive and it is not possible to focus all of its aspects in a single paper or even project.

The present paper presents these requirements, the solutions and results developed and tested in the FP7 European Project INTEGRIS, especially in the security domain, as well as the future challenges and research lines identified and some prospective solutions.

Keywords: Cyber-Physical systems, Cybersecurity, Cognitive Systems, Computer Networking, Heterogeneous systems, Homomorphic Encryption**,** Smart Grid, TRILL.

1. Introduction

The Smart Grid is a system of systems that includes not only the power system itself but also, as a fundamental building block, multiple diverse Information and Communication Technologies (ICT) which many times have not been integrated together in previous systems. The partial solutions that have been frequently applied, targeted only to specific aspects of the power system are no longer valid, if ever have been, given the many services to be provided and the high cost of deployment of many specific systems.

The Smart Grid (SG) [1] will only be possible with the massive deployment of ICT alongside with power installations and devices. Although it will provide a great benefit to the society, this will not come without important challenges yet to overcome and enormous risks in terms of cybersecurity [2] that have to be urgently abated. To this respect, there is a great consensus in that the cybersecurity threat is enormous and that security breaches can cause very important damages. Consequently, all the relevant Standard Developing Organizations (SDO) are working since several years to face such a big problem. In fact, it is urgent to solve it, given that the Smart Grid is critical to achieve the goals on reduction of carbon dioxide emissions and to allow the massive introduction into the Power Grid of Distributed Energy Resources (DER), specially the green ones. Furthermore, the ICT requirements of the different Smart Grid functions are very diverse and some of them are very stringent in terms of reliability and latency. Thus, the ICT system has to cope with all of them at the same time.

Many efforts are underway to tackle with the mentioned problems and among them we highlight here the recently finalized Europen FP7 project INTEGRIS: INTelligent Electrical GRId Sensor communications (http://fp7integris.eu) [3] [4], which specific objective was the achievement of an ICT system capable of providing service to all the functions (services) foreseen for the electrical distribution Smart Grid.

Despite that the mentioned project achieved its objectives, it also identified important challenges yet to be overcome by current state-of-the-art technologies. Thus, this is a main topic of the present paper besides introducing the Smart Grid ICT requirements and presenting the solutions developed and tested in the INTEGRIS project.

INTEGRIS creates Layer 2 (L2) networks that cover the distribution power system and extend the Primary Substation (PS) SG solutions and protocols to their surrounding distribution area without modifications or further specific protocol standardization. This is done by creating L2 heterogeneous mesh networks based on the TRILL [5][6][7] protocol, a set of QoS mechanisms, a multi-level cyber-security subsystem, a data replication subsystem and a context-aware intelligent subsystem, driving the whole system based on the data acquired from the other subsystems. This constitutes a novel and flexible ICT infrastructure based on mixing L2 technologies such as Power Line Communications (PLC) [8], Wireless, Fiber Optics, etc. glued together by means of the TRILL protocol. This has led to the

definition of a single specific device called “INTEGRIS device” (I-Dev) that incorporates all the INTEGRIS networking developments as well as room for hosting and running distributed SG functions. Moreover, the solutions provided by INTEGRIS use standard protocols whenever possible and emphasize on their coordination suggesting further potential improvements.

The paper is organized as follows: Section 2 introduces the ICT basic challenges of the Smart Grid. Section 3 introduces the ICT requirements of the Smart Grid. Section 4 explains the ICT architecture defined in the INTEGRIS project and shows some of the results emphasizing the computer networking and cybersecurity solutions as well as the cognitive and data replication systems defined in INTEGRIS to further improve the system. Section 5 identifies the challenges yet to overcome and propose some prospective solutions to them, nevertheless highlighting their limitations. Finally, Section 6 contains the conclusions.

2. Smart Grid ICT challenges

Power network technology has been exceptionally stable for long time, thing that is in contrast with the fast evolution of ICT systems. Nevertheless, nowadays this stability needs to be challenged due to the need to introduce flexibility in the grid in order to allow in it new actors (customers, producers, prosumers, Distribution System Operators (DSO), Transmission System Operators (TSO), service companies of many types, market operators, the Administration). DER improve its reliability. This evolution is something like the creation of an Internet of Energy with many actors of very different sizes and roles cooperating in it. The challenge is still more important in relation to the electrical distribution networks.

This evolution presents many operational problems that cannot be solved by current systems and technologies especially if they are used isolated. The difficulties come basically from the following reasons: (1) the energy flow will no longer be unidirectional to become bidirectional depending on the needs of the considered moment, fact that forces a tightly control of the voltage of the supply points, (2) the short-circuit power on the supply points will increase, (3) there will be need to introduce latency demanding electrical protection systems now only used in High Voltage (HV) systems into the distribution grid and (4) the introduction of renewable energies makes it complex the necessary balance between consumption and production of energy making it still more necessary to act flexibly and continuously on the demand.

Fortunately, the evolution and todays maturity of ICT systems makes it possible to cope with the mentioned problems, especially over the distribution grid where today ICT systems are scarcely deployed.

In practice, the Smart Grid will be an intimate superposition of the power system and a high performance ICT system, including heterogeneous communication networks to get access to all the network corners, offering a plethora of new functions with different requirements, some of them very stringent. The next section focuses on these ICT requirements of the Smart Grid.

3. Smart Grid ICT requirements

Many of the SG functions have very stringent requirements in terms of availability and latency [9][10][11], but these requirements have been only fully specified for the PS. Specific requirements for the Distribution SG still lack. Besides, the Distribution SG has trouble beyond those encountered by its HV counterpart because of its distributed, complex and partially underground nature, in addition to its partially meshed physical topology.

INTEGRIS considers that such stringent requirements defined for the PS can be relaxed a little bit in the context of distribution networks to those indicated in Table 1, which shows the functional classes and requirements set in the project. In that way, the already established smart grid ICT requirements for the PS are adapted to distribution networks. Table 1 is based on the analysis of standards IEEE1646 [9] and IEC 61850 [10] among others [11].

Table 1. Functional classes and requirements according to INTEGRIS Deliverables 2.2 and 3.2 [3]

Class of Service	Function class	Latency	Reliability	Integrity	Confidentiality
APF	Active Protection Functions	< 20ms	Very High (99.999%)	High	Low
CMD	Command & Regulations	< 2s	High (99.99%)	High	Low
MON	Monitoring & Analysis	< 2s	High (99.99%)	High	Low
AMS	Advanced Meter & Supply management functions	<5m <10s	Low (99%)	High	High
IEM	End to end info. Exchange and Depand Response management	<5m <5s	Medium (99.9%)	High	Low

From Table 1 we underline the low latency and very high reliability needed for APF, difficult to achieve with current technologies, but also the high reliability needed for CMD and MON, which are not easy to achieve in practice in a distribution grid environment.

Regarding cybersecurity, the parameters in Table 1 that affect it directly are Integrity and Confidentiality but also Reliability and Latency, due to the following reasons:

- Security mechanisms are related to the network operation in many ways. Security procedures may introduce delays and cause the unavailability of some devices thus denying the service.
- The very high reliability required for some functions implies that special care is to be taken to minimize Denial of Service (DoS) attacks to a minimum.

Regarding Integrity and Confidentiality, Table 1 reflects the well-known difference between control and office systems [2, 12], consisting in that Integrity is paramount in control systems while Confidentiality has to be higher in administrative systems. This is due to the fact that faults cannot be later recovered without consequences in control systems. An exception to this is the data coming from smart metering systems, where confidentiality is to be kept very high to prevent unauthorized eavesdropping of personal data.

Besides, other requirements that affect cybersecurity options are the following:

- The need for autonomous operation of different distribution areas.
- The current context in the different parts of the Smart Grid may change. The grid may be under attack or may suffer disconnections, or lack of resources.
- The typical long duration of the investments in power network assets (typically 40 years), which is in contrast with those for ICT infrastructures.

Besides other sources, [11] also suggests very low latency requirements for the control of DER and grid management, as can be seen in Table 2. Other identified SG qualitative requirements are the following:

- Many SG services assume an always-connected service without previous connection establishment.
- SG services are typically difficult to model as flows. They are more of a burst nature; used from time to time but expecting high performance when used.
- Some services operate directly over Ethernet (the so called "Goose" messages defined in IEC61850 series of standards).

Table 2. Communication requirements of SG technologies according to the U.S. Department of Energy [11]

Application	**Network requirements**				
	Bandwidth	***Latency***	***Reliability***	***Security***	***Backup Power***
AMI	10-100 kbps/node. 500 kbps for backhaul	2-15 sec	99-99.99%	High	Not necessary
Demand Response	14 kbps-100 kbps per node/device	500 ms – several minutes	99-99.99%	High	Not necessary
Wide Area Situational Awareness	600-1500 kbps	20 ms - 200 ms	99.999 - 99.9999%	High	24 hour supply
Distribution Energy Resources & Storage	9.6-56 kbps	20 ms – 15 sec	99-99.99%	High	1 hour
Electric Transportation	9.6-56 kbps, 100 kbps is a good target	2 sec – 5 min	99-99.99%	Relatively high	Not necessary
Distribution Grid Management	9.6-100 kbps	100 ms – 2 sec	99-99.999%	High	24-72 hours

Besides, electrical distribution networks have specific difficulties for deploying ICT systems because of their heterogeneity, partially buried and different depending on the country, and the convenience to operate autonomously in case of temporal disconnections.

From the above, it is clear that the Smart Grid requires a robust and flexible communications network, and that many current technologies are not capable of complying with the defined requirements, given that few technologies provide delays about a few milliseconds and guarantee very high reliabilities for the terminals service. This is still more complex because in many cases communication is formed by several hops, making it still more difficult to achieve a very low latency. Moreover, the low latency needs to be provided

also in case of failures so that the communications system needs to recover also in 20ms, a difficult target to achieve. A high reliability is also a challenge because, although it can be achieved with redundancy, this is not easy in practice for a distribution grid.

4. INTEGRIS ICT Architecture

4.1 Global view of the INTEGRIS architecture

There are many communications technologies available and applicable to the distribution SG but neither of them is able to completely reach the whole electrical distribution infrastructure that is partly located underground and partly aerial. The challenge is to combine the many available ICT technologies in a flexible, transparent, secure and efficient manner capable to fulfill the requirements (Tables 1 and 2) in all of its locations. Besides the required reliability and latency, there is the need to provide distributed applications and storage resources to host distributable SG functions, placing them close to the consumption points in an attempt of improving the data availability and latency of these functions.

INTEGRIS solves the problem by safely interconnecting the different communications, computing and storage resources needed in the Smart Grid in a single device called I-Dev. This I-Dev device acts as (1) an Ethernet bridge with high reliability to build adequate Field Area Networks (FAN) , (2) as a concentrator for the data collected by the surrounding Smart Grid devices, and (3) as the host for distributable Smart Grid functions and which enables the creation of novel and flexible ICT infrastructures called INTEGRIS Domains or I-Domains (see Fig. 1) by locating them over the power distribution network in places like PSs, Secondary Substations (SS), and Meter concentrations.

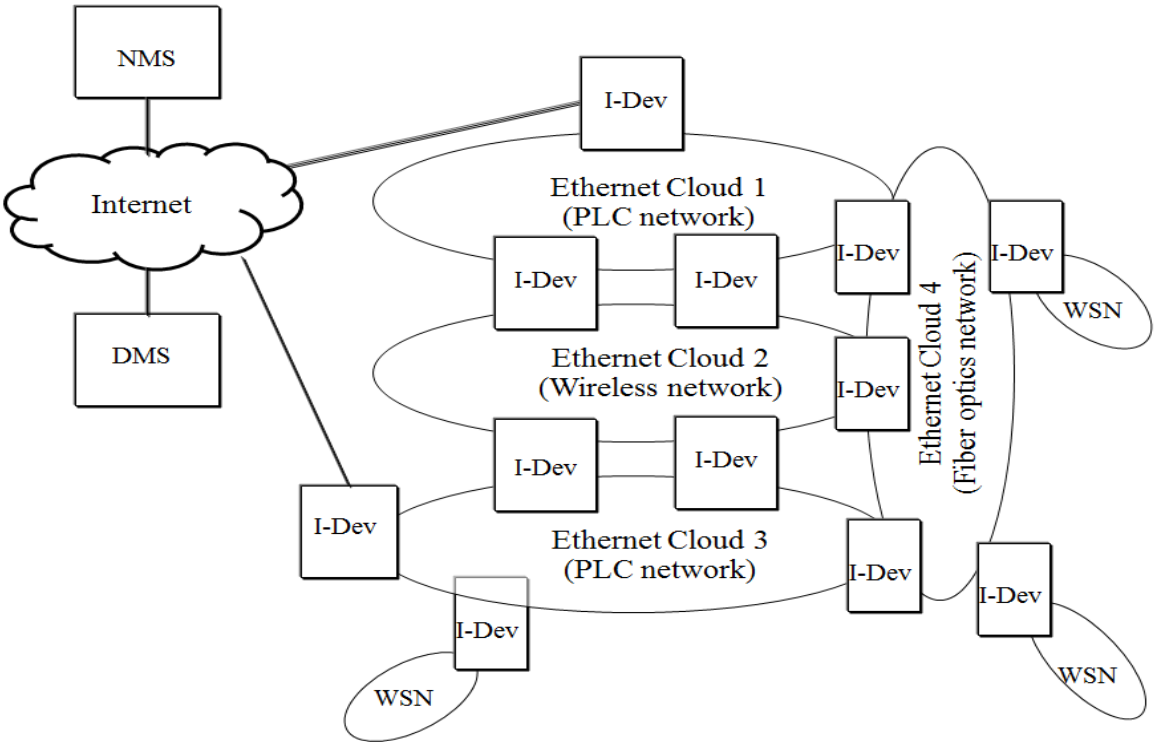

Figure 1. Example of a topology of an INTEGRIS Domain

The high reliability Ethernet bridge (I-Dev) is capable of integrating any L2 technologies with the only requirement being to show an Ethernet interface above them, although the specific L2 technologies integrated in the INTEGRIS field trials are PLC, Wireless and Fiber Optics. The integration is based on the TRILL [5, 6, 7] protocol that allows for creating mesh heterogeneous L2 networks. It also provides QoS mechanisms, a multi-level coordinated cybersecurity system and, finally, a cognitive system that drives the whole system based on inputs of the different subsystems (networking, QoS, cybersecurity and data replication subsystems) including cybersecurity metrics and actions. This cognitive system is based on the mature Learning Classifier System (LCS) architecture [13]. Its workflow imitates those of a living being: it receives inputs from the environment and then it takes decisions based on this knowledge, which gives this subsystem a certain degree of awareness. More specifically, an enhanced version of the extended classifier system (XCS) [14], a competent LCS, is deployed as the brain of the Smart Grid infrastructure.

The data collection can be performed either directly from sensors, through Remote Terminal Units (RTU) or by collecting data from surrounding Smart Meters as depicted in Fig. 2, where the internal architecture of the I-Dev is shown. This figure depicts the way the work has been shared among the INTEGRIS partners by assigning Fig.2 boxes to partners.

The hosting of distributed SG functions is made by providing extra computation and storage capacity; also by providing those functions a data replication system to reduce latency and improve reliability of data access, the possibility of encrypting/decrypting the stored data and a module that provides a Homomorphic Encryption (HE) [15] service.

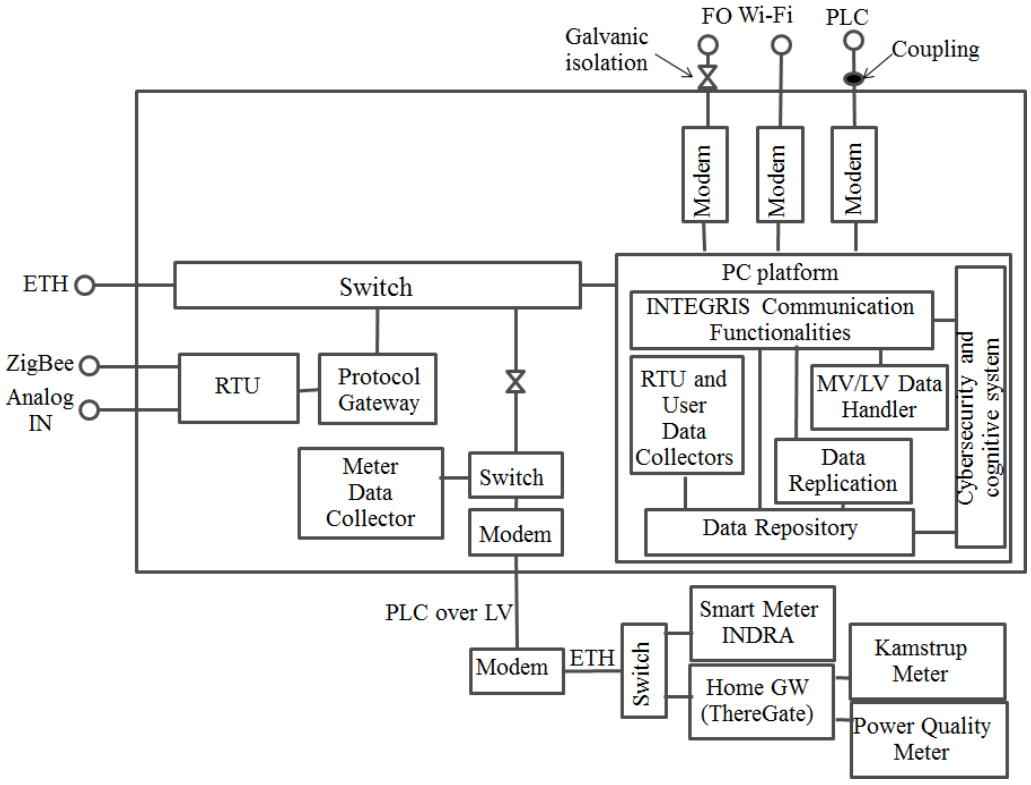

Figure 2. Internal architecture of the INTEGRIS Device

A group of I-Devs communicating directly among them at L2 forms an I-Domain so that, the Smart Grid in the INTEGRIS vision is formed by a collection of I-Domains. In fact, what is represented in Fig. 1 is an I-Domain, which typically may span over a Medium Voltage (MV) line and their Low Voltage (LV) spurs or over the distribution area around a PS.

The detailed functions that the I-Dev provides are the following:

- Networking and connectivity
  - High reliability, low latency bridge that allows the creation of meshed Ethernet networks among I-Devs, achieving efficient internetworking by means of TRILL.
  - Communication with other I-Domains.
  - Multi-connectivity with WAN networks to allow for the reliable connection to Control Centers such as SCADA, EMS, DMS, NMS or other I-Domains.
  - Multi-path capability for high reliability and low latency within the I-Domain.
  - Correct QoS policies application in agreement with the CoS of each packet/application and the output of the context-aware system.
  - Smart Grid cybersecurity protocols (L2 security, IPsec [16], IEC62351-6 [17], HE [15]) in a coordinated manner.
  - Apply context-aware cybersecurity policies based on the intelligent system.
- Data collection from its immediate surrounding devices (e.g., smart meters, RTUs, intelligent electrical devices and sensors) and operation over electrical actuators.
- Applications
  - Capability for hosting distributable SG functions as well as other applications.
  - Capacity to host the Data Replication algorithm for optimizing data access latency and reliability.
  - Capacity for hosting the cognitive system that drives the INTEGRIS system.
  - Service to store the data encrypted.
  - Service to work with some data in homomorphic encrypted form by the use of the Paillier system [18] that allows performing summations and multiplications directly over encrypted data.

Fig. 3 illustrates the protocol stack handled by the I-Dev. It shows that the I-Dev operates with the IEC 61850 protocol and that any other protocols for accessing data are translated to the mentioned protocol before storing the data in the I-Dev repositories. It is also relevant the enablement of GOOSE messages defined in standard IEC61850 in the whole I-Domain, so even outside of the PS.

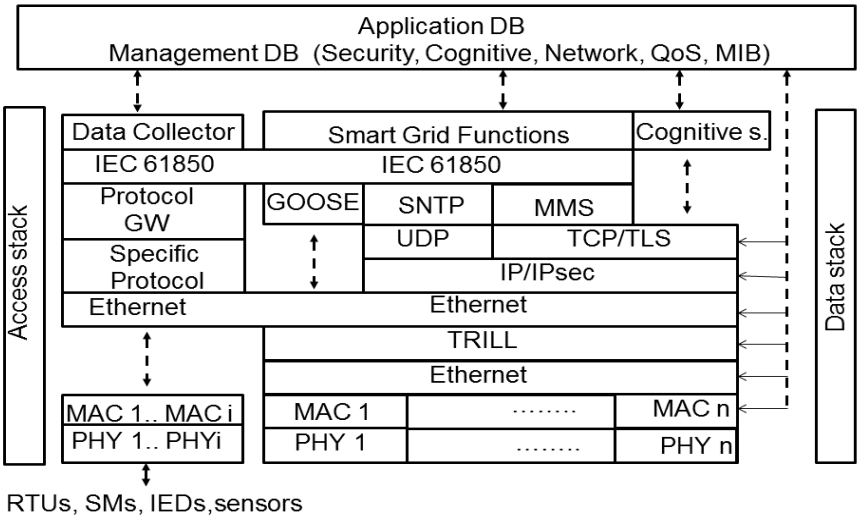

Figure 3. Protocol stack of the INTEGRIS Device

I-Devs contain a cognitive system [19] that drives the whole I-Domain by collecting data about the system performance (flows, latencies, network connectivity, cybersecurity performance and threats). With the obtained global view, the I-Devs correct the deficiencies and adapt to the current situation. Fig. 4 represents how this cognitive system acts as a broker on the INTEGRIS system by balancing the interests of the different subsystems.

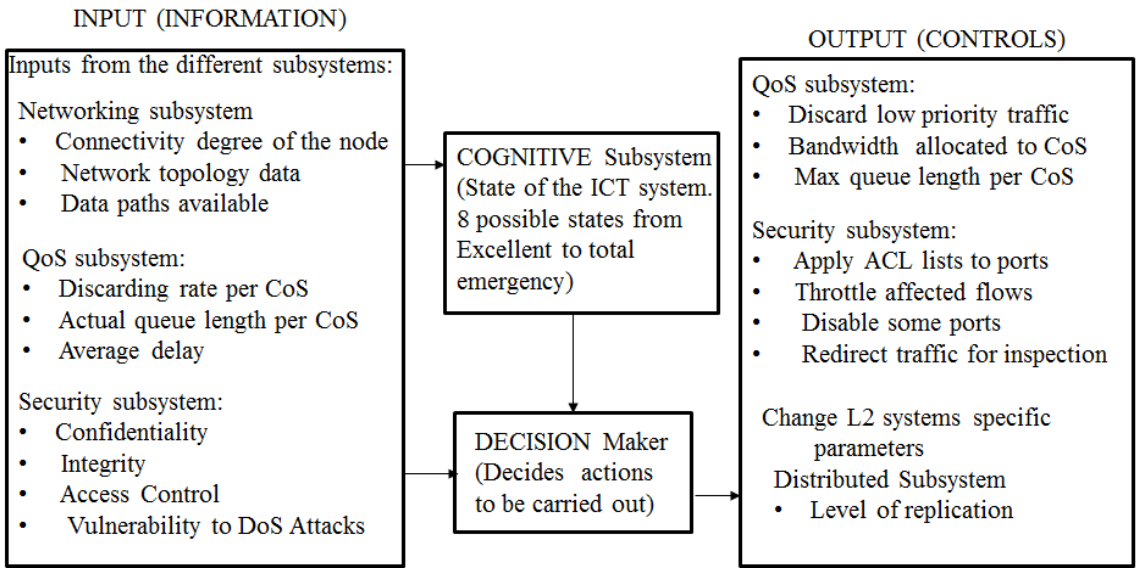

Figure 4. The cognitive system as a broker within INTEGRIS

The system needs first to be trained by an expert but then the Reinforcement Learning and generic algorithm modules adapt the system to the changes in the environment up to a certain extend. This system has been applied in INTEGRIS to control the communications system but not to manage the power system itself, which is a future research line of interest.

All these mechanisms have been developed and tested satisfactorily in the field in Spain (Barcelona) and in Italy (Brescia), as well as in the laboratories of La Salle-Universitat

Ramon Llull in Barcelona and in the University of Tampere in Finland.

4.2 Comparison of Layer 2 networking solutions

INTEGRIS creates FAN networks of heterogeneous link technologies at the MAC layer by means of the TRILL protocol, which is located in devices called I-Devs, which are scattered over the distribution grid. These networks span over portions of this grid creating L2 areas (I-Domains), where routing is based on the MAC addresses of the different devices.

Other alternatives to TRILL at L2 are the Spanning Tree Protocol (STP), the Rapid STP (RSTP) [20] or Shortest Path Bridging specified in IEEE 802.1aq [21]. The reasons to choose TRILL over the other options have been the following:

Regarding RSTP the basic reasons were three [5]:

- TRILL makes no assumptions about physical topology. It manages any network, let it be a mesh or a tree, while RSTP requires a tree and does not manage mesh networks.
- TRILL enables optimal paths and effective use of parallel paths within the defined electrical distribution area. This is not the case for RSTP.
- RSTP uses only one path so it is much affected by failures. Thus, it is necessary to wait for the network to recover in case of failure, with recovery times up to a few seconds. Although there are new versions protocol versions that claim much better recovery times, nevertheless these enhancements are usually proprietary solutions.

In fact and unfortunately, current ICT technologies have big difficulties in meeting the latency requirements either at layer 2 [22] or at layer 3 [23]. This includes any protocols that could be chosen for INTEGRIS like TRILL. Later we comment on the limitations of TRILL.

Regarding IEEE 802.1aq by the time of the INTEGRIS implementation its standardization was not enough advanced and was not an option. Nevertheless it is very similar to TRILL and is based also on the IS-IS [24] routing protocol, so that some limitations will be similar in both protocol. The possible advantages of IEEE 802.1aq over TRILL may come from the management complexity. This is something to consider in the future.

TRILL uses RBridges [5] that combine the advantages of bridging and routing, which are very convenient for the distribution SG, as we have already seen. Others are the following:

- It can transparently interconnect dissimilar L2 technologies maintaining optimal paths, even parallel paths, and presenting an Ethernet interface to the upper layers.
- It coexists with standard bridges, so legacy networks can be upgraded slowly, by replacing bridges one at a time.
- It does not require network configuration as routers at L3 do.
- It allows interconnection of IP nodes within a distribution area but without relying on IP end-nodes to do anything new.
- It works for any L3 protocol.

For all these reasons, TRILL was the chosen protocol in INTEGRIS.

4.3 Results and details of the Computer networking protocols

The tests undergone with the TRILL protocol show its correct functioning regarding the added delay, which is less than 1ms in the implementation made in INTEGRIS, but also its slowness in recovering upon a failure. To this respect, Fig. 5 represents four samples of the results of the undergone recovery tests of the TRILL protocol in front failures in a simple scenario formed by two I-Devs interconnected by two links, as represented in the same Fig. 5. One out of the two links carries data while the other does not. Such tests measured the delay in seconds for the TRILL to detect the loss of adjacency in case of disconnecting each of the links. The test also measured the recovery delay once the link was re-connected. In the case of disconnection of the data carrying link the represented time is the one over which data are lost. In the figure, it can be seen that the minimum adjacency recovery delay is never below 1 second, a normal result if we consider that the TRILL standard defines timers with a precision of only seconds. Despite of this, the tests undergone with timers adjusted to lower levels have only achieved a minimum recovery time of 1s despite implying a great increase in control traffic. As a conclusion, we may say that this is an essential limitation of TRILL that needs to be faced in the future.

Another limitation coming from the IS-IS [24] routing protocol on which TRILL roots is that it only considers parallel paths of equal length, thing that is a limitation for creating parallel paths and for load balancing.

The commented alternative of using protocol IEEE 802.1aq [21] instead of TRILL to our opinion would have similar limitations, at least regarding multipathing, because it is also based on the IS-IS protocol. Nevertheless, it is a research line yet to explore.

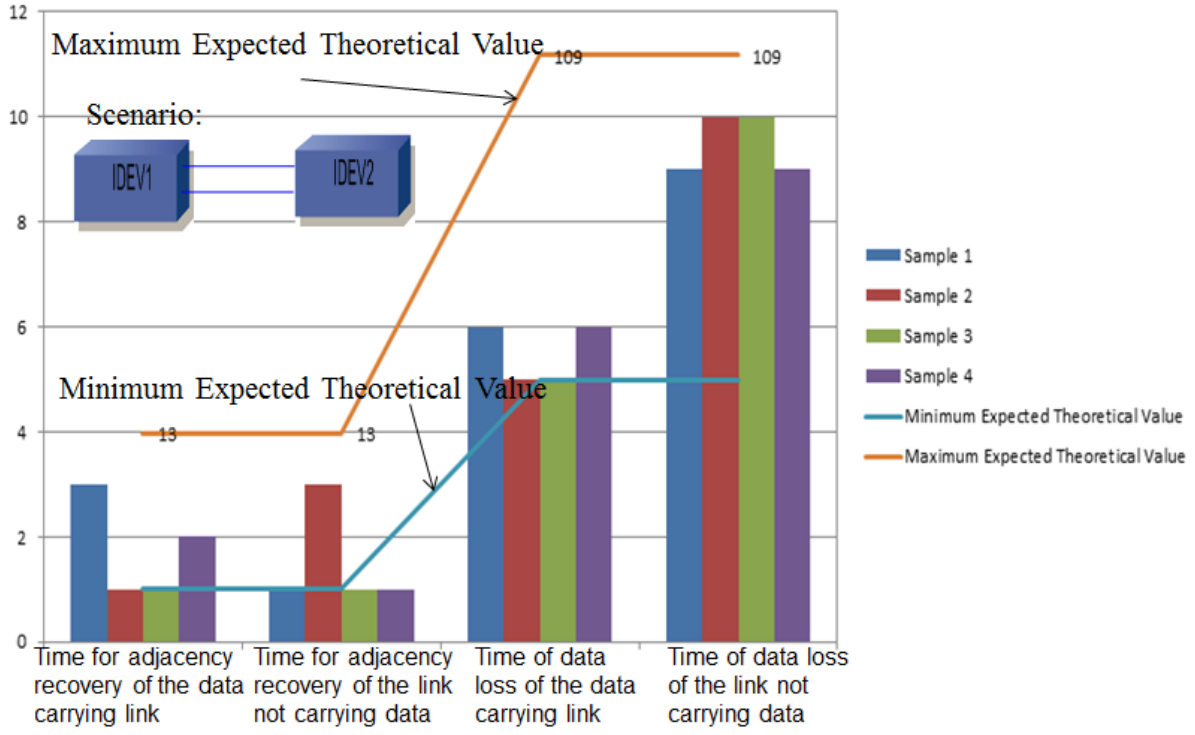

Figure 5. Results of the TRILL recovery tests in a simple scenario

4.3.1 Summary of TRILL limitations

As a result of the carried tests, here we list the detected TRILL limitations for the Smart Grid context. The first is a fundamental TRILL limitation. Others are implementation limitations.

- TRILL inherits the timers of IS-IS**.** According to RFC1142, most of these timers are to be set in seconds. This implies a normative limitation in the convergence time of IS-IS and TRILL so that it can never be below 1second. Future enhancements of TRILL and IS-IS will likely allow to reach convergence times of several hundreds of milliseconds. There are efforts to achieve delays of milliseconds [25].
- The current implementation of TRILL is not aware of VLANs. PyTRILL (The INTEGRIS implementation was made with Python language) transmits VLANS but does not manage them.
- TRILL can only establish an adjacency over point-to-point physical or logical links. Shared media like PLC and Wireless need SSH tunnels in order to create a valid adjacency between I-Devs.
- PyTRILL implements multipathing but not load balancing. This means that in case of loss of the path being used, TRILL will only send the messages on the other existing path after the detection of the broken path, something that takes time.

4.4 Cybersecurity protocols and architecture

The Smart Grid inherits the vulnerabilities of Internet plus the new ones coming from the different applications, requirements and actors interacting together in a Smart Grid. These vulnerabilities are many and, for this reason, this paper needs to limit its scope to the network issues avoiding dealing with Application and End terminals security.

Among the Smart Grid network specificities concerning security to consider, the strongest requirement is the need to continue securely operating even upon temporary communication disconnections due to communication network partitions. This fact forces the distribution of security servers and repositories to avoid the single point of failure issue.

In Chapter 3, the cybersecurity requirements of the Smart Grid have been detailed. From these requirements, it is possible to draw many conclusions for the design of the cybersecurity system and for choosing the correct options in the selected protocols. These conclusions and design lines for INTEGRIS are the following:

- Keep cybersecurity decisions close to the affected devices.
    - The stringent requirements in terms of latency and reliability defined in Table 1 mean that security decisions are to be kept as close as possible to the sensing and actuation points to avoid added delays. Therefore, security needs to be as decentralized as possible in the Smart Grid. In fact, this is done in INTEGRIS by placing them in the cybersecurity server and repository contained in the I-Devs.
    - The need to continue operating in case of occasional disconnections abounds on the convenience to take cybersecurity decisions as close as possible to the affected devices.

- Use Standards.
  - Rely as much as possible on proven existing standards, only complementing them when strictly necessary. This comes from the evidence that the first versions of most standards contained serious vulnerabilities that had later to be fixed.
  - From these standards, choose the right options for the Smart Grid.
- Use a common cybersecurity data repository for all the involved technologies. Distribute this repository, either as a whole or partially, in the I-Devs although having also a central repository where all the information is gathered and coordinated. The central cybersecurity repository is replicated in part in each I-Dev so that, in case of disconnection, the system continues to work for some time even allowing the inclusion of new L2 devices.
- The changes in the context situation of a given Smart Grid area lead to differentiated or adaptable security policies depending on that context and requires a context-aware security design. This is achieved in INTEGRIS by the definition of cybersecurity metrics that feed the cognitive system that together with other metrics (See Fig. 4) enables an improved cognitive system management.
- Use, whenever feasible, authentication based on Certificates. Specifically, secure servers (I-Devs) by using certificates.
- The convenience and even need to distribute some of the functions to be performed in the Smart Grid means that data is also to be protected when being used by the distributed applications. This leads to the use of HE, although this technique is still an open research area. In any case is something to explore.
- Implement known, relatively efficient, HE techniques as a service for SG applications in order to start a research line on this not yet mature but very promising technology.
- DoS is also an issue not only by itself but also because it may imply a reduction in application availability below the targeted requirements. The reduction of the DoS attacks needs to work at all the levels of the ISO hierarchy including L2.
- The high integrity needed means that all packets are to be protected by strong enough integrity hashes; at least, 64 bit long.
- The high confidentiality needed for Meter Data means that, at least for these data, it is necessary to strongly encrypt them both when being transmitted and when being stored in intermediate systems.
- The typical long duration of the investments in power network assets means that the horizon is about year 2054 and, since by that year it is expected that 3DES encryption will be broken, the Smart Grid cannot rely on 3DES.
- Adhere to the principle of the Trusted Computing Group (TCG) of using Trusted Platform Modules (TPM) to protect in-built software and hardware as well as storage of data, including the basic keying material. This is done in the I-Devs.

These statements lead to the multilevel distributed cybersecurity system specified for INTEGRIS that applies common standard protocols to each of the layers but selecting the right options to cope with the requirements.

This need to deal in SG with a large set cybersecurity standards is highlighted in NISTIR 7628 vol. 1 [26]. It also provides guidelines for cybersecurity implementation in SG and provides a logical security architecture of general nature with a detailed description of requirements and elements. Significantly, it contains interesting reflections regarding certificates and secret keys and seems to conclude that the use of certificates is more adequate for SG. Furthermore, a relevant standard listed in [26] is ISO-IEC62351-6 [17], because it is the cybersecurity standard of reference for IEC 61850 and, thus, for SG. IEC62351-6 mandates to apply security at the Layer 4 (TLS1.0 [27] with some restrictions) and above.

In agreement with all the above, the cybersecurity architecture of INTEGRIS incorporates IEC62351-6 and TLS and uses certificates to authenticate the end-devices connected to the network and the I-Devs themselves. So that an I-Dev can only create a connection with another I-Dev if this other I-Dev has a valid certificate.

It could be argued that protecting at Layer 4 could be enough since this may provide confidentiality, integrity and device authentication for user data and because many commercial systems rely on this. However, protecting SG only at L4 leaves the network open to cybersecurity attacks. This may produce DoS and eavesdropping of network management messages and, thus, prohibiting the users from accessing the service and this is against the high reliability expected in SG. For this reason, SG really urges multilevel security.

As a consequence, INTEGRIS protects the Smart Grid at all levels, including Layers 2, 3 and 4 while protection above these levels, albeit important, is to be done in the end devices but with some implications in the intermediate ones, as it will be seen in the next sections. This is the case when applying HE [15], implemented in INTEGRIS in a limited form.

L2 protection is done by using the security mechanism already specified in the standards for each technology operating at this layer (PLC, Wi-Fi, WiMAx and Ethernet). At L2, there is a broad range of cybersecurity protocols, typically one for each technology. Because of this, the landscape is complex and it is necessary to analyze each technology and to define the correct settings for each of them. An important one is IEEE 802.11i [28], which defines the Robust Secure Network Architecture (RSNA) and IEEE 802.1X [29] for key management. IPsec is the reference standard at L3. It is a convenient and proven protocol to protect networks and for this reason, INTEGRIS uses it. In fact, IPsec is even mandatory in IPv6, networks that are very promising for the Smart Grid. Fig. 6 depicts the cybersecurity network protocols considered in INTEGRIS and their position in the network.

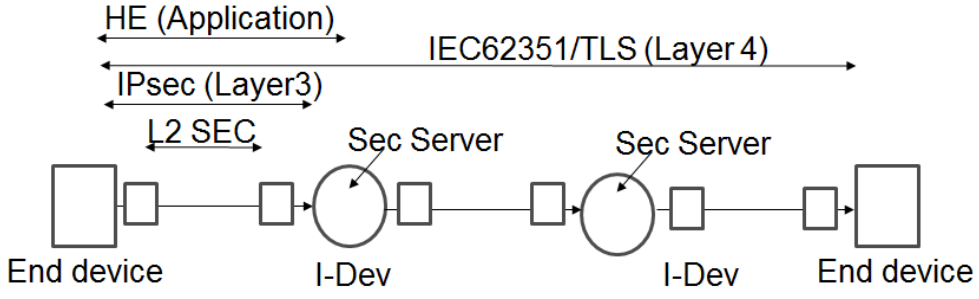

Figure 6. INTEGRIS Cybersecurity network protocols

Now it is of paramount importance to choose correctly the options of the considered standards to make them compatible with the Smart Grid requirements. Table 3 shows the selection made in INTEGRIS for the purpose. The reasons for this selection of options is contained in subchapters 4.4.1.and 4.4.2.

Table 3. Setting of options and parameters in the chosen protocols made in INTEGRIS

Protocol	Mode	Key management	Encryption	Integrity
IPsec	ESP in tunnel mode [30]	IKE in Main mode [31]	AES [32]	SHA-2 [33]
IEC62351/ TLS1.0		TLS_DH_RSA_WITH_AES_128_SHA [17]	AES	Mandatory Hash SHA-2
Layer 2 802.11i [28]	RSNA	802.1X [28] [29]	AES	AES (CCMP) [28]

It is also necessary to protect the data when stored and when being used by the Smart Grid functions.

Finally, the global cybersecurity architecture of INTEGRIS is depicted in Fig. 7.

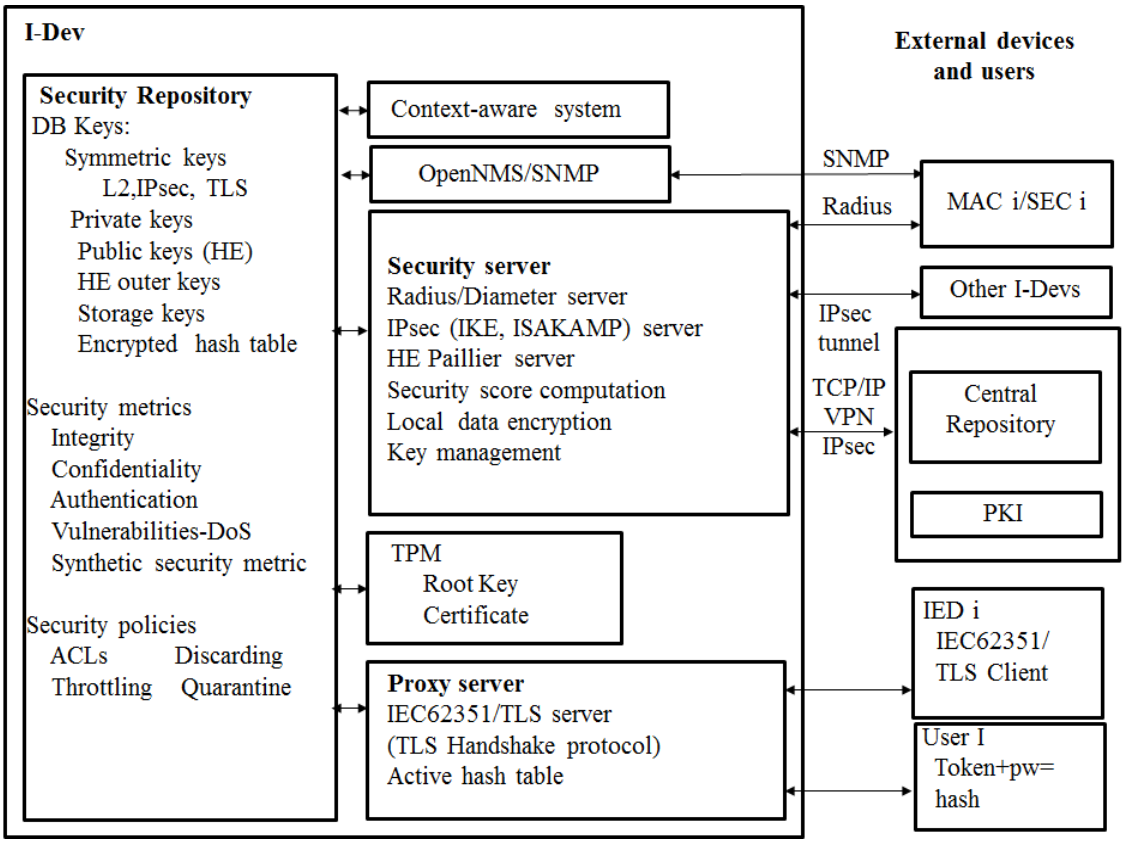

Figure 7. Data cybersecurity architecture of INTEGRIS

4.4.1 IPsec implementation options

As stated before, INTEGRIS uses IPv6 because it is a standard, convenient and proven protocol to protect networks. The chosen Smart Grid IPsc secure options are the following:

- Use Encapsulating Security Payload (ESP) [30] because ESP provides packet confidentiality by encryption, data origin authentication, data integrity and anti-replay.
- Use tunnel mode, which provides integrity and authentication for the entire IP packet (header plus payload).
- The combination of ESP and tunnel mode encapsulates the entire original IP packet with a new packet header added. This provides protection to the whole inner IP packet, including the inner header, although the outer header remains necessarily unprotected.
- For key management use Internet Key Exchange (IKE) Protocol [31] in Main mode to avoid dictionary or brute force attack against the hash.
- Encryption method: Use AES [32]. DES cannot be used because it is known to be vulnerable. 3-DES is believed that will be vulnerable by year 2054, leaving a too short time for the expected lifetime of Smart Grid assets.
- Hash function: Use SHA-2 for authentication given that SHA-1 is vulnerable to a collision attack [33], even though SHA-2 is not as widely used currently.

Finally, implementation should avoid defaulting to vulnerable states upon rebooting thus opening the door to DoS attacks as well as other known implementation pitfalls.

4.4.2. TLS implementation options

The State-of-the-Art regarding security in SG is in fact defined in the mentioned IEC62351-6 standard, which basically consists in applying security at the transport layer (TLS1.0 [27] with some restrictions) and above. For this reason, the cybersecurity architecture of INTEGRIS includes IEC62351-6 and TLS. It uses certificates to authenticate the end-devices connected to the network and the I-Devs themselves, so that an I-Dev can only create a connection with another I-Dev if this other I-Dev has a valid certificate.

In the case of IEC62351 the chosen secure options are:

- At the lower layers, IEC62351 mandates the use of TLS1.0, for which several vulnerabilities are known.
- The same standard IEC62351 already makes mandatory the use of a Message Authentication Check, deprecates non-encryption cipher suites and recommends 3DES and AES. Beyond that, INTEGRIS bets for using only AES.
- Besides, several shortcomings of IEC 62351 are known. First, IEC 62351 is currently unable to offer application layer end-to-end security if multiple transport layer connections are used [23] but such multi-hop connections are important for new Smart Grid use cases. To solve the problem, often a trusted intermediate is assumed. This assumption is a weakness in the overall system design that may not hold in some Smart Grid Use Cases. A possible solution [12] would be the introduction of security sessions for MMS connections in IEC 62351. This proposed extension of the current standard would provide end-to-end security for new use cases in SG scenarios.

4.4.3 Cybersecurity servers and repositories

The Security Server has the following functions:

- Radius [34] or Diameter [35] server to handle the security aspects of the L2 communication technologies surrounding the I-Dev.
- An OpenNMS server to monitor and control the mentioned L2 technologies.
- Key management, including both symmetric and asymmetric keys.
- Security score computation.
- Local data encryption.
- Homomorphic Encryption.

The security repository contains the following items:

- The I-Dev Certificate
- Security keys repository, which includes the encrypted key table and the encrypted hash table for user access control.
- The basic four security metrics (Integrity, Confidentiality, Authentication and Vulnerability level) and a synthetic security metric formed by combining them.
- The available security policies to apply depending on the network state as determined by the cognitive system and based on the following mechanisms: Access Control Lists, Discarding, Throttling, Quarantine, although others can be also applied.
- HE public keys

Finally, a central element hosts the Public Key Infrastructure (PKI) to manage asymmetric keys and the central security repository.

Last but not least, the security system collaborates with the cognitive system by contributing to the global optimization of the INTEGRIS system, by providing it with a synthetic cybersecurity metric for each I-Dev and I-Domain based on several partial metrics (Integrity, Confidentiality, Authentication and vulnerability to DoS attacks). The cognitive system, based on these metrics and others (See Fig. 4), issues a score and a set of corrective actions to be taken over the system.

4.4.4 Homomorphic encryption in INTEGRIS

HE is very desirable in the Smart Grid since it allows the data to remain always encrypted even when used by distributed applications. This enables the design of many new secure scenarios. The novelty of HE relies on the idea of working directly with encrypted information (math operations, algorithms), so that nobody is able to learn its real content.

HE has recently received a lot of attention since the first proposal of a Fully Homomorphic Encryption system (FHE) in year 2009 by Craig Gentry [15]. FHE allows for performing any mathematical operation over encrypted data while previous HE systems had several limitations.

Regarding FHE, the conclusion of INTEGRIS is that, at this moment, there is no feasible FHE algorithm that can work efficiently enough in practice. For this reason, its use in

INTEGRIS was discarded. On the contrary some partially HE systems, although still rather inefficient computationally compared to operating with raw data, can already be applied given the increasing power of computers. For this reason, INTEGRIS has dedicated efforts to find ways to apply existing HE systems to SG focusing on improving their efficiency.

From the several existing HE systems, INTEGRIS has focused on Paillier [18] because, due to its properties, it can be used in some Use Cases like the ones commented here. Paillier is a HE asymmetric algorithm based on public keys that provides the possibility to manipulate data securely with just the public key. It has the homomorphism property with respect to the summation and with respect to the multiplication by constants or flat texts.

Next subchapters describe the HE Use Cases defined in INTEGRIS and the implementation done in INTEGRIS.

4.4.4.1 The Use Cases

The designed Use Cases focus on collecting encrypted Smart Meter and RTU data and saving it encrypted in some place (the Cloud, a concentrator, the I-Dev…) in a way that the authorized actors can work with the data without having access to user specific data, preserving their customers' anonymity and protecting them from malicious attacks.

The Use Cases that could be implemented by using the limited HE system described here are (1) LV congestion and fault management, (2) LV network management and (3) End- User LV voltage monitoring. All of them are based on aggregation of Smart Meter readings and RTU measurements, gathering data like Smart Meter ID, contracted power, individual consumption readings, fault detection indications from RTU and Smart Meters, and RTU current measurements.

The operations needed to cope with the defined Use Cases are fortunately relatively limited because most of them are summations and comparisons and only a few are multiplications by constants. Table 4 shows the needed operations and the mechanisms implemented in INTEGRIS to achieve them.

Table 4. Operations needed by the Use Cases

Operation	Description	Implemented mechanism
Summation	Sum of values	Paillier HE system
Equality	Check whether two strings are equal or not	AES-128
Comparison	Check if one value is larger or smaller than another one	OPE

To cover all these functions, INTEGRIS implements HE plus Order Preserving Encryption (OPE), the latter in a similar way as described in [36].

The concrete operations that are to be performed are just summations to know the load of a given feeder, the consumption of a given area or transformer (real, historical evolution, contracted), and multiplications by constants to estimate costs of supplied energy. Summations in Paillier are performed by multiplying the two cyphertexts and the multiplications by constants are obtained by elevating the ciphertext to the power of this

constant using the known Pallier properties [18]. Comparisons are not using Paillier because some of them are to be done with letters, so they use an OPE system [36]. Equality check needs a deterministic encryption system like AES, since Paillier is randomized.

The different types of Encryption used in the system (ETE AES, IPsec, L2 encryption, Paillier, OPE and local encryption) are piled in layers like an onion, where in the interior there is the raw data and to the outside, the strongest encryption system being used. Table 5 depicts the different encryption layers of this kind of system used in INTEGRIS.

4.4.4.2 Homomorphic Encryption Implementation

The HE of INTEGRIS has been build following the ideas in [36] that consists in encrypting data several times an in different layers to cope with each of the mathematical operations to be performed. This fact allows running different queries on encrypted data while guaranteeing confidentiality. INTEGRIS has adapted this model to practical needs framed within a defined environment. It stores numbers twice in different encryption systems, one for performing equality check and the other for performing mathematical operations.

The applied encryption techniques for storing data are (1) random, to provide maximum privacy, (2) deterministic, to provide for equality check operations, (3) preserver of order, to maintain the relationships of order between the original texts although with even less security, and (4) homomorphic, to perform securely additions and multiplication on encrypted data.

The combination of concepts from each of the functions listed leads to a system that stores numbers more than once. This is an inefficiency of the system to be corrected as further techniques develop. The result is the scheme represented in Table 5, which shows the encryption performed depending on the type of data.

Table 5 shows the type of encryption performed on each type of data to get a given functionality. In the case of STRINGS, the outer layer provides randomness thanks to a random initialization vector while the inner layer, AES, provides deterministic encryption to allow checking for equality; but in the algorithm used in INTEGRIS, it is limited to a length of 16 bytes. In the case of NUMBERS, they are stored twice. On one hand, they are stored using an algorithm that maintains the order to make possible to execute comparison queries (larger than, smaller than, equal), protected by a randomized algorithm. On the other hand, the number is stored encrypted with Paillier to do sums and multiplications by constants.

Observe that Paillier does not need further protection while OPE, which is a weaker encryption scheme, deserves further protection.

Table 5. Layered Encryption Architecture

Operation	Equality	Comparisons	Summations
L1 of encryption	AES CBC IV (Random encryption)	AES CBC IV (Random encryption)	
L2 of encryption	AES (128 bits Deterministic encryption)	OPE (Order preserving encryption)	Paillier (Homomorphic encryption)
Type of data	STRING	NUMBER	NUMBER

5. Challenges and future research lines

As already said, INTEGRIS developments have been tested in the field and in the laboratory to check their practical performance level in comparison to the initial expectations and requirements. This process has thrown light with respect to the challenges yet to overcome. There are challenges in all the areas and they have been summarized in the following subsections.

5.1 TRILL results, challenges and prospective solutions

The use of TRILL in Smart Grids presents several limitations that have been shown in Section 4.3.1 and are also commented next with possible prospective solutions.

Recovery time upon a failure is still not enough for the APF traffic on the Smart Grid. Although several alternatives to improve IS-IS and TRILL recovery delays upon a failure have been proposed and compared, there is still the need to research on reducing recovery delays in IS-IS routing protocol to achieve effective convergence delays around 100ms. This effort is underway but has to be further pursued.

There exists a need to enable multipath over different cost paths (not just equal cost). This would greatly improve network availability and capacity. This can be possibly achieved by further IS-IS improvement.

It will also be necessary to consider complex link metrics. IS-IS protocol considers, as mandatory default, simple metrics like a fixed cost per link; but the links between RBridges in Smart Grids may be formed by underlying complex layer 2 technologies such as BroadBand PLC (BB PLC) or by wireless mesh networks that may be formed by several hops and may use different MAC and mesh protocols. It is very convenient that RBridges could take into account metrics including the effective transmission time and/or the number of hops interior to the link (BB PLC, Wireless mesh networks, etc.) either by using a mathematical model for each technology/interface or by really probing the link to determine the metric. For the purpose, the optional "Delay metric" contained in RFC 1142 [24] is an interesting option because the transmission time of one link between I-Devs, which may contain several internal hops, could be estimated or effectively measured.

5.1.1 Complementing TRILL with PRP

Another possible solution may be to consider the solutions standardized to get redundancy in PS. This is the case of the Parallel Redundancy Protocol (PRP) [37] and similar standards contained in standard IEC 62439, which may be useful for INTEGRIS as proposed by the authors in [38].

TRILL and RBridges [5] have many advantages over STP and routers but, although they are potentially faster in recovery time from failures, they are still not able to fully comply with the recovery times required by some Smart Grid application such as APF (4-20ms).

A possibility for improvement may come from the combination of TRILL and PRP [37], to better cope with the electrical distribution Smart Grid requirements. INTEGRIS analyzed 4

possible combinations [38]. From them we show in Fig. 8 the one that seems to be the better option so far.

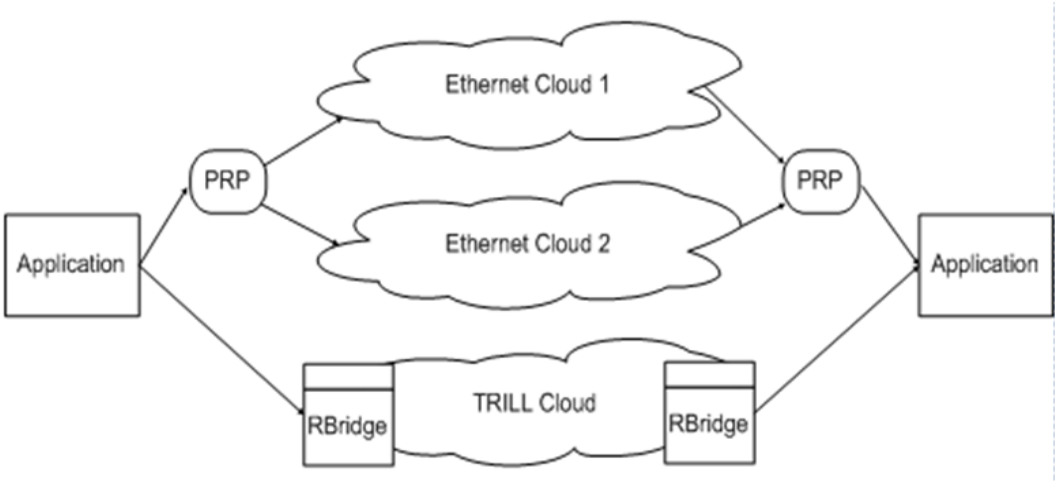

Figure 8. An interesting alternative for combining TRILL and PRP

The idea is to use the protocol most suited to each situation, either TRILL or PRP. If two I-Devs are connected to the same two L2 technologies, use PRP; otherwise use TRILL. This possibility is feasible because RBridges and bridges can coexist and because each L2 technology knows which I-Devs belong to it. In this case the I-Dev would switch from PRP to RBridge depending on the situation. This possibility complies with standards.

The whole stack of protocols for combining TRILL and PRP is shown in Fig. 9. In it, it can be seen that IEC 61850 services can run over MMS/TCP/IP, over UDP/IP in the case of Simple Network Time Protocol (SNTP) or even directly over Ethernet in the case of GOOSE messages. In Fig. 9, it can also be seen that there is the choice of using PRP when feasible or TRILL as the general case. This proposal can still be further improved as explained in [38].

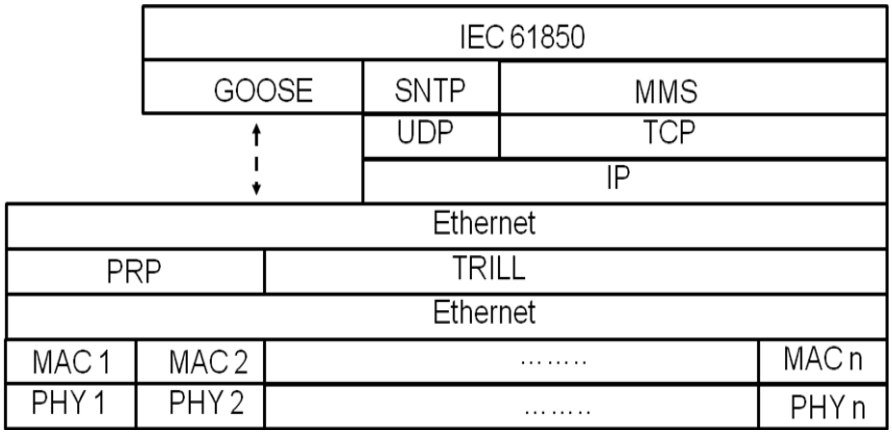

Figure 9. Stack of protocols for combining TRILL and PRP in the INTEGRIS project.

5.2 Cybersecurity challenges

INTEGRIS has only applied cybersecurity solutions to the four lower layers of the ISO stack and has also protected data when being stored, by using HE in some applications. We deem that the protection applied at the lower layers with the adoption of the mentioned options is enough to protect the data when being transmitted and when stored. Nevertheless, SG vulnerabilities are many and no system can actually be considered enough protected.

There are still DoS vulnerabilities at the lower layers, which have only been minimized but not eliminated. Care is to be taken to the future evolution of DoS attacks over L1 and L2 and to the design of the options to be used for each link technology.

The hierarchical cybersecurity servers and repositories defined in INTEGRIS needs more design to further reduce the introduced delays and by the security systems.

The HE is very promising but introduces great inefficiencies (In the case of INTEGRIS, Pailler HE system slows down computations by some 7 times). This means that research in improving its efficiency is an important research area.

The management of the cybersecurity system as a whole is also another challenge. This includes the management of keys, certificates, repositories, cybersecurity servers, policies and should be automated as more as possible.

End devices (RTUs, Smart Meters,..) have not been protected because it was not the INTEGRIS focus. Nevertheless, vulnerabilities and challenges exist at the terminal level and the current situation is that many terminals in the field are not using any cybersecurity protocols disregarding that networks are becoming more open as the time passes by.

5.3 Cognitive system challenges

The context-aware intelligent system used in INTEGRIS [19], which is not a standard component in a data network, is devised as a global system that perceives the general state of the network and decides the actions to perform, either directly or through other subsystems, in order to correct deficiencies and maximize the overall performance. The schema of the INTEGRIS cognitive system is shown in Fig. 10.

The solution integrated in INTEGRIS is based on XCS [14] due to (1) its incremental learning nature, which allows the system to directly learn from data streams, (2) the robustness of XCS to noisy data, (3) the transparency and generalization of the model produced by XCS, and (4) it has been tested in similar environments proving that it can perform properly in dynamic situations.

In order to improve the scalability of the cognitive system and reduce the number of attributes to speed up the learning process, the XCS scheme has been split in a 2-level hierarchic system: (1) the Perception-action agents (PAAs), and (2) Domain management agent (DMA). This is possible because the Smart Grid has also been divided into INTEGRIS domains, which are relatively small parts of the network meshed from the point of view of their communications network. This allows the system to learn in parallel.

PAAs are physically placed in I-Devs. PAAs are the simplest agents of the hierarchy and have a limited perception of their INTEGRIS domain. PAAs perceive the state of their PAA neighbors through the DMA as they only report to their corresponding DMA. Therefore, the DMA controls the whole domain. In this sense, the DMA can force a given PAA to apply any action. Occasionally, I-Domains share their rules in order to find the best control model.

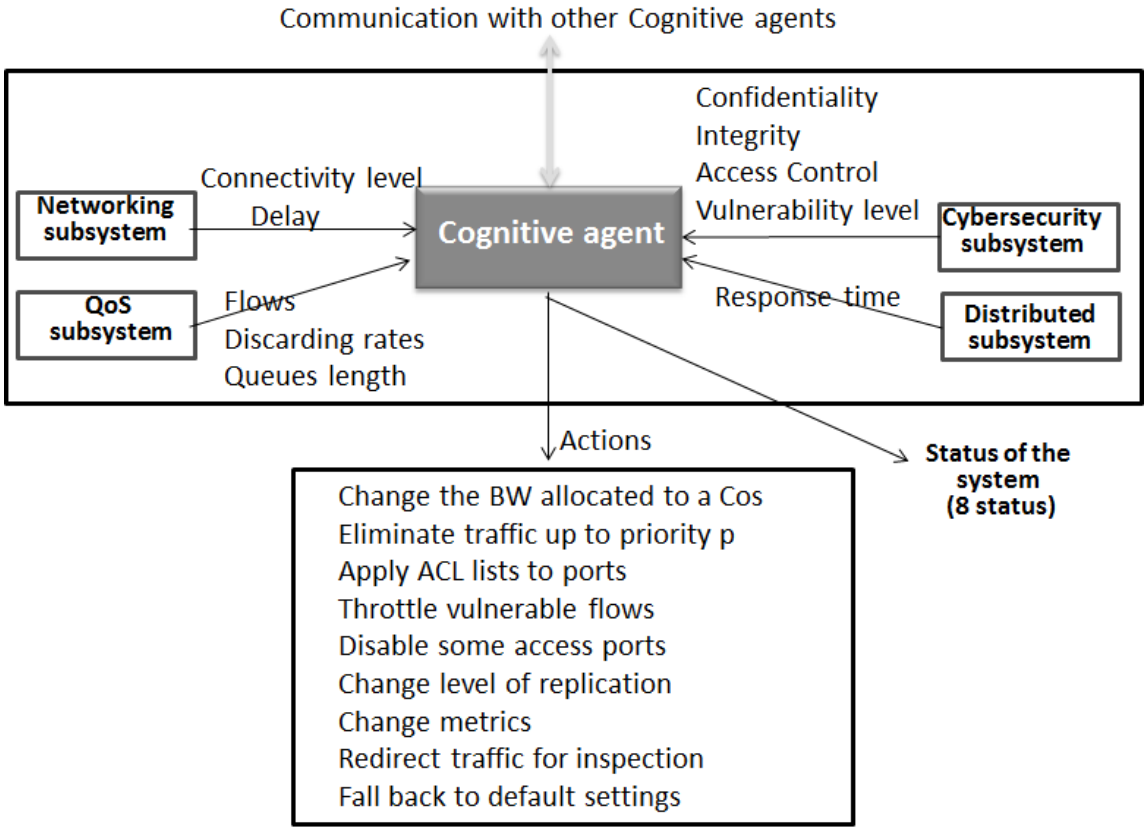

Figure 10. Schema of the principles of the context-aware intelligent system in INTEGRIS

The system has been tested satisfactorily, not only in laboratories but also including field-testing [4]. The system works properly, but several aspects can be improved, which are the following:

- The cognitive system is based on the supervised learning paradigm. This fact implies that the system must be initially trained by an expert (although the Reinforcement Learning and the genetic algorithm modules finally tune the system). The unsupervised learning paradigm should be considered to increase the practical application field.
- It is essential to spend more time to learn from the interaction between the Smart Grid, the cognitive system and the expert. This will help tuning the metrics, the actors, the actions and the cognitive system itself.
- The possibility of including inputs from the Smart Grid applications into the cognitive system should be considered.
- The response time should be improved.

5.4 Data replication system challenges

Regarding the data replication system [4], INTEGRIS has proved the concept and its proper functioning. The improvement to consider in future is to supplement the existing data repository with automatic partitions.

Fig. 11 shows an example of the data replication system. A given I-Dev replicates data from its attached IEDs with a replication depth of 3. It uses an-epidemic update replication protocol to replicate data, as they are collected from smart meters to neighboring I-Devs. As the time goes on new versions of data (V) are propagated through neighboring I-Devs.

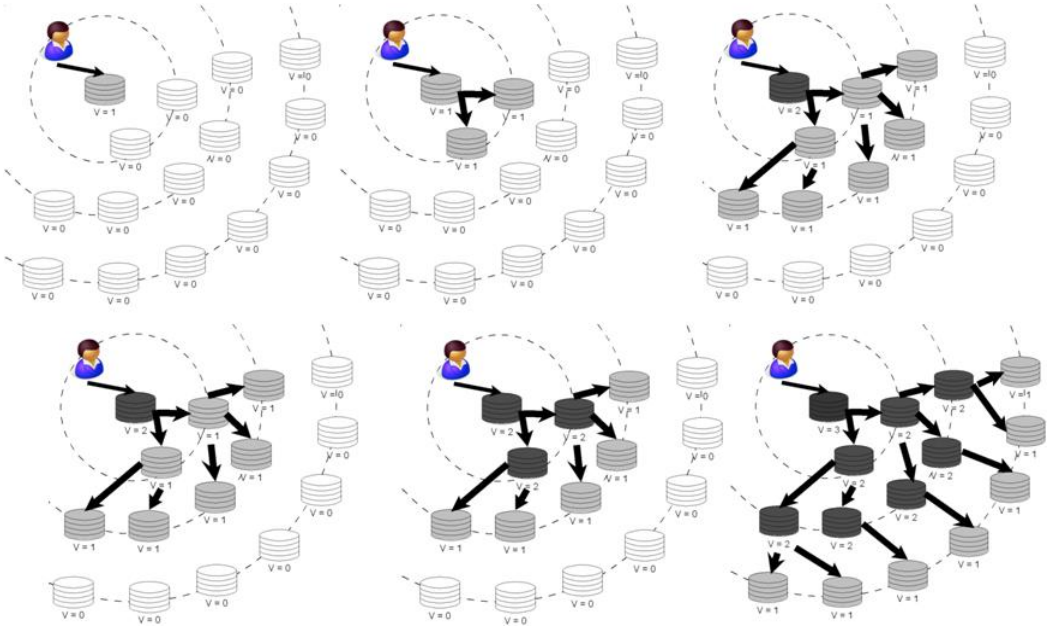

Figure 11. Data replication system in INTEGRIS with a replication depth of 3.

The data replication system contributes to achieving low latency for applications, approaching data to applications. Moreover applications can also move forward data, transferring from the centralized control (traditional operational mode) to the distributed I-Devs (INTEGRIS operational mode), as it is shown in Fig. 12.

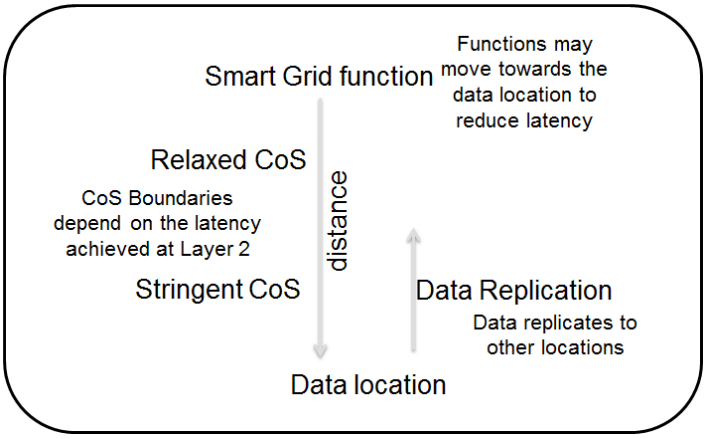

Figure 12. Representation on how the applications and data may move to better match the needed latency.

5.5 Communication technology challenges

The tests carried in the INTEGRIS project over the communication links and technologies, showed the limitations of PLC the level of noise on the power grid is high. This limitation affects the necessary latency guarantee although, in general, it is not enough to limit the transmission capacity below the needed one. The computations made in INTEGRIS showed that the links of the distribution Smart Grid might carry at most some 4Mbps quantity, which is always achieved when using Broadband PLC, which has a nominal capacity of hundreds of Mbps.

The latency issue can possibly be improved by acting on the PLC MAC Layer orienting it towards Smart Grid services. To this respect it is necessary to remind that the PLC standard IEEE P1901 [39] as well as others was designed for the in-home and access markets and not for the Smart Grid.

It is interesting to remind that PLC is convenient and even necessary for the Smart Grid because it has the capacity to reach to the underground parts of the grid which in Europe is around some 50%. Despite of this, the high reliability needed suggests the convenience to supplement the PLC network not only with radio and cabled systems owned by the DSOs as done in INTEGRIS but also with Telecom Operator services to form an integrated network thought for the Smart Grid with the potential of matching the needed reliability.

To this respect, our impression is that the proposed integration or interoperation of networks might be enabled by the use of virtualization of resources and networks. This is another line of research in La Salle-Universitat Ramon Llull issued form the INTEGRIS project. Fig. 13 shows this possibility with pictures.

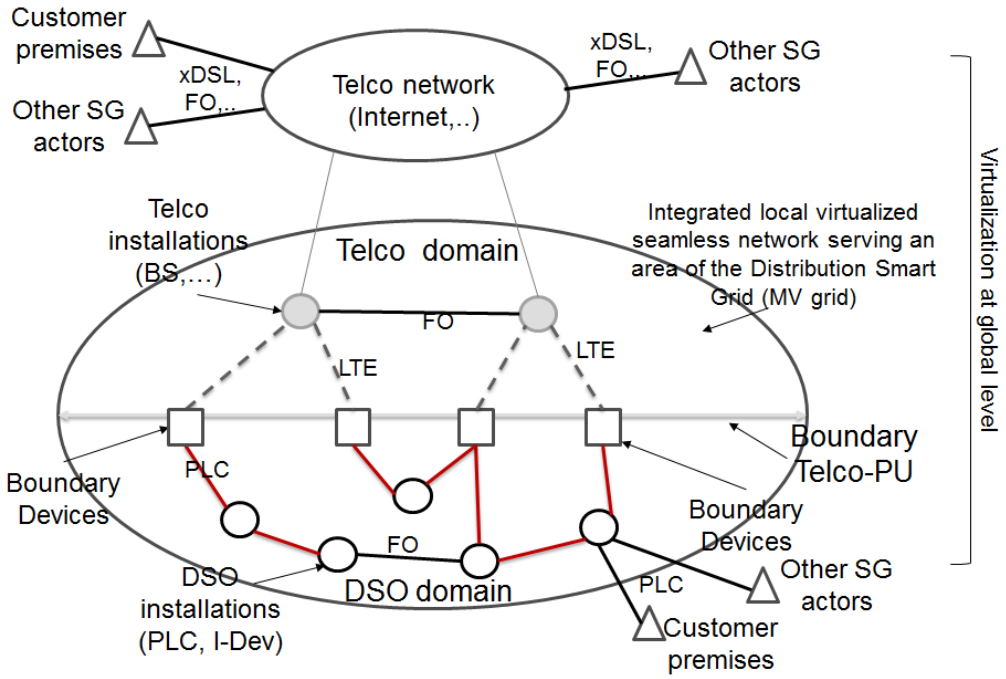

Figure 13. A possible integration schema between the Telecom Operator services and the DSO communication network including PLC.

6. Conclusion

This paper presents a complete ICT architecture especially designed to meet the distribution Smart Grid ICT requirements developed in the context of the European INTEGRIS FP7 Project. It also presents the requirements of these systems, some of the results, highlights the detected limitations of state-of-the-art technologies to meet the requirements and proposes some solutions to be tackled in the future in any case emphasizing computer networking and cybersecurity aspects.

The INTEGRIS Project has achieved its main goals by means of the creation of a single but replicable element, the I-Dev, to be scattered over the electrical distribution grid. The I-Dev integrates the many developments made in INTEGRIS and forms a mesh spanning the grid that enables the concept of distribution Smart Grid.

Decentralization of applications and also of communications leads to the convenience of integrating of both capabilities. This has been addressed by creating the mentioned single integrated device (I-Dev) that integrates all the developments and safely interconnects the different communications, computing and storage resources needed in the Smart Grid in a single device. Merging of information in the I-Dev is the crucial point of the development that enables many of the rest of developments and applications made. In fact, the merging of so many diverse developments is a novelty in the Smart Grid context.

From the main master lines of the INTEGRIS developments listed in the text, here we highlight here the following: (1) to cope with the stringent Smart Grid ICT requirements, (2) to allow the easy deployment of distributed applications over the grid, (3) to follow existing standards as much as possible, (4) to extend the Primary Substation protocols to its surrounding distribution area by creating an IEC61850 centric system that allows to consider the defined area as a virtual substation from the communications point of view.

The paper introduces the many developments integrated in the I-Dev including (1) fast and easy networking at layer 2 based on the TRILL protocol allowing the use of IEC61850 as is in the distribution grid, (2) creation of a multilevel cybersecurity system rooted on a distributed system of servers and repositories, (3) distributed Smart Grid functions, and (4) a cognitive system that drives the INTEGRIS ICT system.

It also focus on the advantages of applying TRILL to the Smart Grid from which we extract the following, (1) it makes no assumptions about physical topology, (2) it can transparently interconnect dissimilar layer 2 technologies maintaining optimal paths, even parallel paths, (3) it coexists with standard bridges, so legacy networks can be upgraded slowly, by replacing bridges one at a time, (4) it does not require network configuration.

Regarding cybersecurity we may summarize that the main contributions of INTEGRIS mentioned in the paper are (1) the creation of a common cybersecurity server and repository which is distributed to each I-Dev, (2) the coordination with a cognitive system to achieve system wide optimization and (3) the introduction of HE techniques in the Smart Grid that permits the user to work with his data without decrypting them, thus opening the door to multiple scenarios that can take advantage of this paradigm.

Despite that the project has allowed to proof the validity of this concept, several limitations, sometimes fundamental limitations of state-of-the-art technologies, have been detected and they are exposed in the paper. Among them, we summarize here the following:

- Difficulties of the current networking technologies to achieve recovery times upon a failure on the order of tens of milliseconds or to easily allow for alternative mechanisms to avoid failures affecting applications.
- Limitations in the flexible load balancing over redundant paths of state-of-the-art technologies.
- Need for PLC systems with less and more predictive latency and more oriented to the Smart Grid services.
- Efficiency limitations of current HE techniques. Also the limited protection provided by OPE techniques so far.
- Nonexistence of a framework for the inclusive integration of telecom operator services together with DSOs telecom solutions.

All of them constitute future research lines by its own right. More specific related research lines out of the INTEGRIS project are the following:

- Explore the possibilities of improving reliability by combining TRILL with some principles of the PRP protocol.
- Explore the use of virtualization techniques to facilitate the creation of multi administrative domain networks.
- Improve the knowledge on the system behavior by testing it by the use of the context-aware intelligent system under different metrics and actions.
- Explore the use of unsupervised cognitive learning techniques as opposed to the supervised ones.

Acknowledgements

The research leading to these results has received funding from the European Union - Atomic Energy Community 7th Framework Programme for the INTEGRIS Project (no. 247938). In addition, we would like to thank La Salle (Universitat Ramon Llull) for their support.

References

[1] Arnold G. W., “Challenges and Opportunities in Smart Grid: A Position Article”, Proceedings of the IEEE, Vol. 99, Num. 6, pp.922-926, June 2011. http://dx.doi.org/10.1109/JPROC.2011.2125930

[2] Yan Y., Qian Y., Sharif H., Tipper D., "A Survey on Cyber Security for Smart Grid Communications", IEEE Communication Surveys&Tutorials, Vol.14, No. 4, Fourth Quarter 2012. http://dx.doi.org/10.1109/SURV.2012.010912.00035

[3] INTEGRIS: Intelligent electrical grid sensor communications. [Online]. Available at: http://www.fp7integris.eu (last accessed March 25, 2014)

[4] Repo S., Della Giustina D., Ravera G., Cremaschini L., Zanini S., Selga J.M. and Järventausta P, "Use Case Analysis of Real-Time Low Voltage Network Management", IEEE Innovative Smart Grid Technologies (ISGT) 2011 Conference. http://dx.doi.org/10.1109/ISGTEurope.2011.6162669

[5] Perlman R., "Rbridges: Transparent Routing", Proceedings of IEEE INFOCOM 2004. http://dx.doi.org/10.1109/INFCOM.2004.1357007

[6] IETF RFC5556, Touch, J. and Perlman, R. "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement". s.l, May 2009, draft-ietf-trill-prob-06.txt. Link: http://tools.ietf.org/html/rfc5556 (last accessed March 31, 2014)

[7] IETF RFC6325, Touch R. Perlman, D. Eastlake 3rd, D. Dutt, S. Gai, A. Ghanwani "Transparent Interconnection of Lots of Links (TRILL): Base Specification". July 2011. Link: http://tools.ietf.org/html/rfc6325 (last accessed March 31, 2014)

[8] Galli S., Scaglione A. and Wang Z. "For the Grid and Trough the Grid: The Role of Power Line Communications in the Smart Grid", Proceedings of the IEEE, Vol. 99, Num. 6, pp.998-1027, 2011. http://dx.doi.org/10.1109/SMARTGRID.2010.5622060

[9] IEEE Std 1646-2004, "IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation", 2005. http://dx.doi.org/10.1109/IEEESTD.2005.95748.

[10] International Electrotechnical Commission, "IEC 61850-5:2013, Communication networks and systems in substations – Part 5: Communication requirements for functions and device models".

[11] U.S Department of Energy. "Communication requirements of smart grid technologies". October 5, 2010. [Online] Available: http://www.smartgrid.gov/sites/default/files/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf (last accessed March 25, 2014)

[12] Fries S., Hof H.J., Seewald M., "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments" AICT 2010 Fifth International Conference on Internet and Web Applications and Services, Barcelona, Spain. http://dx.doi.org/10.1109/ICIW.2010.28

[13] Holland J., "Adaptation in Natural and Artificial Systems". MIT Press, 1992. ISBN: 9780262581110.

[14] Butz M. V., Rule-Based Evolutionary Online Learning Systems – A Principled Approach to LCS Analysis and Design, ser. Studies in Fuzziness and Soft Computing. Springer, 2006, vol. 191. ISBN 978-3-540-25379-2.

[15] Gentry C., "A fully homomorphic encryption scheme". PhD thesis, Stanford, 2009 University. http://crypto.stanford.edu/craig (last accessed March 25, 2014)

[16] IETF RFC4301, Kent S., Seo, K., "Security Architecture for the Internet Protocol". December 2005. Link: http://tools.ietf.org/html/rfc4301 (last accessed March 31, 2014)

[17] International Electrotechnical Commission IEC 62351, Power systems management and associated information exchange - Data and communications security-Part 6: Security for IEC 61850, October 2006.

[18] Paillier P., "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". J. Stern, Ed., Advances in Cryptology - EUROCRYPT'99, Year 1999, vol. 1592, Lecture Notes in Computer Science, p. 223-238, Springer-Verlag. http://paillier-cryptosystem.googlecode.com/svn-history/r16/doc/Pai99pai.pdf (last accessed March 25, 2014)

[19] Navarro J., Zaballos A., Sancho-Asensio A., Ravera G., Armendáriz J.E., "The Information System of INTEGRIS: INTelligent Electrical GRId Sensor Communications", IEEE Transactions on Industrial Informatics, November, 2012. http://dx.doi.org/10.1109/TII.2012.2228869

[20] Standard IEEE 802.1w - 2001 Rapid Spanning Tree Protocol (RSTP). http://dx.doi.org/10.1109/IEEESTD.2001.93287

[21] IEEE 802.1aq-2012 - IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks--Amendment 20: Shortest Path Bridging. http://dx.doi.org/10.1109/IEEESTD.2012.6231597

[22] Yan Y. et al. "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges" IEEE Communications Surveys & Tutorials, no.99, pp.1-16 (2012). http://dx.doi.org/10.1109/SURV.2012.021312.00034

[23] Li H., Zhang W., "QoS Routing in Smart Grid" GLOBECOM, pp.1-6 (2011). http://dx.doi.org/10.1109/GLOCOM.2010.5683884

[24] IETF RFC 1142, "OSI IS-IS Intra-domain Routing Protocol", February, 1990. Link: http://tools.ietf.org/html/rfc1142 (last accessed March 25, 2014)

[25] Alaettinoglu C., Jacobson V., Yu H., "Towards Milli-Second IGP Convergence", Internet Engineering Task Force. Internet Draft. May, 2001. Consulted in November, 2012. Link: http://tools.ietf.org/html/draft-alaettinoglu-isis-convergence-00 (last accessed March 25, 2014)

[26] NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, The Smart Grid Interoperability Panel – Cyber Security Working Group, August 2010. Link: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf . (last accessed March 25, 2014)

[27] IETF, RFC2246," The TLS Protocol Version 1.0", January, 1999. Link: https://www.ietf.org/rfc/rfc2246.txt (last accessed March 26, 2014)

[28] IEEE 802.11i-2004 Standard for Information technology -Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements.

[29] IEEE Std. 802.1X-2010, "Port-Based Network Access Control", 5th, February, 2014. http://www.ieee802.org/1/pages/802.1x.html

[30] IETF RFC4303, IP Encapsulating Secutity Payload (ESP). December, 2005.

https://tools.ietf.org/rfc/rfc4303.txt (last accessed March 26, 2014)
[31] IETF RFC2409 "The Internet Key Exchange (IKE)", November, 1998. https://www.ietf.org/rfc/rfc2409.txt (last accessed March 26, 2014)
[32] Federal Information Processing Standards Publication 197 (FIPS PUB 197), Advanced Encryption Standard (AES), 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. (last accessed March 25, 2014)
[33] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), Secure Hash Standard (SHA), 2012. http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf (last accessed March 25, 2014)
[34] IETF RFC2865, Remote Authentication Dial In User Service (RADIUS), June 2000. https://tools.ietf.org/html/rfc2865 (last accessed March 26, 2014)
[35] IETF RFC3588, "Diameter Base Protocol", IETF RFC3588, September 2003. https://tools.ietf.org/html/rfc3588 (last accessed March 26, 2014)
[36] Curino C., Jones E. P. C., Popa R. A., Malviya N., Wu E., Madden S., Balakrishnan H., Zeldovich N., "Relational Cloud: A Database-as-a-Service for the Cloud". 5th Biennial Conference on Innovative Data Systems Research, CIDR 2011, pp 235-240 Asilomar, California. *http://people.csail.mit.edu/nickolai/papers/curino-relcloud-cidr.pdf* (last accessed March 26, 2014)
[37] IEC Standard 62439-3:2012, "Parallel redundancy protocol and high-availability seamless redundancy."
[38] Selga J.M., Zaballos A., Navarro J., "Solutions to the Computer Networking Challenges of the Distribution Smart Grid", IEEE Communication Letters, Vol. 17, Issue 3, Page(s): 588 - 591 2013. http://dx.doi.org/10.1109/LCOMM.2013.020413.122896
[39] IEEE Std 1901-2010, IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, December 2010.

Copyright Disclaimer