DELIVERABLE

EU Project No.: 238868

SEESGEN-ICT

Supporting Energy Efficiency in Smart Generation Grids Through ICT

Thematic Network

ICT PSP Programme

REPORT ON TECHNICAL AND NON-TECHNICAL BARRIERS AND SOLUTIONS FOR MANAGING SMART GRIDS WITH DER

D2-3

Revision: Final R0

July, 2010

This is a Deliverable of WP2

Deliverable Leader: Geert Deconinck (KUL)

Authors:

Geert Deconinck (KUL)	**Parvathy Chittur Ramaswamy (KUL)**

Contributors:

Jianzhong Wu (CU)	**Jerzy S. Zielinski (UL)**
Rune Gustavsson (BTH)	**Marina Lombardi (ENEL)**
Fritz Swartzlaender (SAP)	**Sotirios Hadjimichael (PPC)**
Matthias Stifter (ARSENAL)	**Jochen Koszescha (ECPE)**
Diana Moneta (ERSE)	**Maher Chebbo (SAP)**

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	X
C	Confidential, only for members of the consortium and the Commission Services	

Revision History

Revision	Date	Author	Organisation	Description
R0	July 2010	Geert Deconinck	KUL	First issuing

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

NOTES:
For comments/suggestions/contributions to this Document, contact:
the Leader for this Deliverable at Geert.Deconinck@esat.kuleuven.be
or the Coordinator of SEESGEN-ICT at Giorgio.Franchioni@erse-web.it

For more information on the project SEESGEN-ICT, link to http://seesgen-ict.erse-web.it

INDEX

EXECUTIVE SUMMARY

Following the work of deliverable D2.2 which made a survey on the different ICT-approaches that can be applied for the better management of smart grids (namely voltage control, adaptive protection and grid reconfiguration), the current deliverable D2.3 looks at barriers that might prevent further deployment of ICT-based approaches in these applications, and identifies possible solutions.

Firstly, the **methodology that was adopted** in preparing this deliverable to identify barriers and solutions is described.

In this report, the **barriers to the implementation of ICT in smart grid applications** have been broadly **classified** into two classes, namely, the **technical barriers** and the **non-technical barriers.** The technical barriers have been evaluated on the basis of ranking. Bandwidth of the communication channel, latency supported by the communication channel, dependability, flexibility and security of the communication channel deployed, scalability, standardisation, interdependency of the power system & ICT, control paradigm, controllability of the current power system, testing facility and cost are the parameters that have been evaluated based on a ranking showing the significance of the parameter in behaving as a barrier for the deployment of ICT in the three exemplary applications of voltage control, adaptive protection and grid reconfiguration. **Latency** supported by the communication channel**, dependability, security** of the communication channel deployed**, interdependency** of the power system & ICT, and the need for **testing facilities** are the parameters that have **a rank of 5** which means that they are a **very important barriers** to be overcome especially for the power system protection applications of adaptive protection and grid reconfiguration.

The list of non-technical barriers are to some extent more general than the scope of this work package alone, but they are nevertheless mentioned as an enumeration, in order to be taken up at the project-wide level. The **problem of ownership** for the various aspects of the distribution system, the lack of eagerness to use new **open technology** for critical applications, the lack of clarity in the **regulatory aspects** of the smart grids, the fewer **return on investment** in rural areas, very vaguely defined **communication architecture,** lack of **consumer education** and hesitation to invest by the **vendors** are some of the non-technical barriers, for the deployment of ICT in smart grids, identified in this report**.**

The report identifies several elements that can contribute to solving the barriers. Sticking to **quality-of-service**, use of **open standards** and **cyber security** standards, conducting **more research** on the various **control** paradigms for each of the three intra-grid control applications, improving the **controllability** of the communication system with more **sensors** and **control knobs, simulation and testing** of the **complex systems** in **real time, design innovation** to help curb the cost**,** regional and national **demonstration** of the communication technologies, a well defined **regulatory framework** will all act as solutions for overcoming the technical and non technical barriers for the implementation of ICT in smart grids.

1 INTRODUCTION

SEESGEN-ICT work package (WP) 2 considers how Information and Communication Technology (ICT) can be used for a better management of smart grids in which many Distributed Energy Resources (DER) are integrated.

The deliverable D2.2 made a survey on the different ICT-approaches that can be applied for the better management of smart grids. They fall in three categories.

- **Voltage Control**: Voltage control in the smart distribution grid will not only be based on the local measurement of electrical quantities, but also on the exchange of values concerning these quantities among the different control points in the distribution grid. Using such information, the controller at the distribution system operator or elsewhere can use DER to contribute to the reactive power management in the grid, and as such improve the energy efficiency.
- **Adaptive Protection**: In distribution grids with bidirectional power flows adaptive protection is required in order to deal with the direction of short circuit currents and to ensure selectivity. Communication among protection devices can ensure reaching these goals but puts stringent requirements to the involved ICT.
- **Reconfiguration**: Smart grid management may imply the reconfiguration of the topology of the distribution grid – if sufficient hardware (switches, breakers,…) is available – in order to better handle the load and generation in the grid due to a large amount of unpredictable DER and faults. Such reconfiguration can be applied pro-actively before emergency conditions occur, or reactively after an alarm triggers. This latter reactive approach also relates to 'self-healing' distribution grids. Proactive and reactive actions are commanded by controllers, based on information provided via different sensors in the grid, and communicated to the former.

The current deliverable looks at barriers that might prevent further deployment of ICT-based approaches in these applications, and identifies possible solutions.

It is useful to recall that these three applications are representative for the applications that are absolutely required in a smart grids context where many DER are deployed.

These applications – in contrast to their current counterparts – heavily rely on a reliable ICT infrastructure to be effective and efficient. Without dependable ICT, the power system at distribution level would not be able to evolve to a smart grid with many DER incorporated [1].

Such ICT infrastructure needs to be able to deal with an enormous amount of data (due to grid management applications and end user applications such as charging electric vehicles) and hence needs to be scalable, available, responsive and cost-effective by being based on open interoperable standards.

1.1 Methodology to identify barriers and solutions

This document has been developed in an iterative way, as follows.

In a first step a plenary brainstorming has been performed by all work package partners in order to identify the barriers to a wide deployment of ICT approaches for intra-grid management applications in their overall scope in its full width and to some depth.

In a second step, the work package coordinator has structured these barriers into technical and non-technical barriers. The technical barriers were further clustered into themes.

All work package partners provided a priority ranking to these themes in a third step. This allowed us identifying to which extent the themes play a role for the intra-grid applications.

The fourth step was based on feedback from the partners on the prioritised barriers in order to identify solutions.

Finally, a consolidated text was circulated and agreed among the work package participants.

2 TECHNICAL BARRIERS HINDERING THE IMPLEMENTATION OF ICT-BASED INTRA-GRID MANAGEMENT APPLICATIONS

2.1 Identification and ranking of Barriers

The following list enumerates the barriers and ranks the issue for the different intra-grid applications on a 5-grade scale (1=not an important barrier at all … 5 = a very important barrier to be overcome for this application to be deployed). This has been based on a survey and discussion round by the project partners.

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
1.	Bandwidth of the communication channel	The bandwidth is the bits per second that can be transmitted via the communication channel. Is there a huge demand on bandwidth requirement for any of the three exclusive intra-grid management applications that are dealt herewith? If so, is this requirement a barrier because not all the communication mode have the same bandwidth?	**Rank: 3** **Comments:** For all three functions, the information needed for the real-time control is not enormous e.g. P,Q,V, I and switch gear status, and bandwidth is related to transmission speed. So for all real time control functions, the bandwidth requirement is less and is well within the capabilities of the presently available communication technologies. Hence bandwidth requirement is not a crucial barrier for the implementation of ICT in any of the three exemplary topics of grid control.		

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
2.	Latency supported by the communication channel	How much latency can the communication channel support? If there is a stringent requirement on latency then it will be a barrier for the implementation of that particular intra-grid management application for example the adaptive protection and grid reconfiguration when deployed during emergency have stringent requirement on latency.	**Rank: 2** **Comments:** Usually the latency of communication to the generators or from the measurements devices is lower than the time constant the generators need to change the given set point. For example, the Broad band over power line (BPL) deployed by PPC can easily meet the latency requirement for the voltage management application.	**Rank: 5** **Comments:** Adaptive protection is very latency sensitive and needs small response times. The time scale is in ms, hence response time should be as low as possible. Fault measurements and protection units are geographically closely located to achieve low response time but still communication over greater areas require adequate latency. For example the BPL technology deployed by PPC suffers in places where they have long lines. The latency is good only when line length is approx. 10km or less.	**Rank: 3** for non-protection application **Rank: 5** for protection application **Comments:** If the reconfiguration is for non-protection application like load balancing or loss minimization, then small latency won't be a problem but if the reconfiguration is for supply restoration or protection of the power system then latency is critical.

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
3.	Dependability of the communication channel	a. Availability of the communication channel b. Reliability of the communication channel	**Rank: 5** **Comments:** The communication channel is indispensable to realize voltage management with the integration of DG and demand.	**Rank: 5** **Comments:** The requirement on availability and reliability of the communication channel is indispensable to realize adaptive protection since it deals with the safety and protection of the electrical network.	**Rank: 5** **Comments:** The requirement on availability and reliability of the communication channel is indispensable to realize grid reconfiguration for both normal and abnormal operating condition.
4.	Flexibility of the communication technology deployed	a. Can it support an additional application other than what it is initially designed for to meet the growing complexity? b. Can it support physical mobility? For eg. wireless communication supports mobility and hence is flexible.	**Rank: 2** **Comments:** The communication network should be shared among other services consequently, QoS (quality of service) policies are needed but still new applications will automatically fit it as they emerge.		

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
5.	Security of the communication channel	a. Cyber security b. Physical security For example, how important is the cyber security for the application of adaptive protection? If the Cyber security is critical then it is a barrier for the implementation of the adaptive protection application because not all communication channels / control systems are equally robust against cyber attacks.	**Rank: 5** **Comments:** Based on ENEL that has implemented voltage management application, the large deployment on field of new access points is critical especially from a physical point of view. According to PPC, in Larrisa project the usage of WiFi for most of the applications (even after deployment of state-of-the-art protocols), there are concerns on security because of the easy access to WiFi equipment and the open frequency that one can jam quite easily. Thus both cyber security and physical security requirements are stringent since all these real-time control functions will directly impact on the security and reliability of the power system.		
6.	Scalability of the communication channel	If the application is scaled up to large systems, does any bottleneck become apparent?	**Rank: 3** **Comments:** It depends on the number of the involved points in the grid. With a large number of points, the scalability of the communication network is critical but a distributed architecture of the system can mitigate this aspect. If the network grows, then the throughput should also increase slowly and may be the communication processing capability for hierarchical and interconnected controller should increase faster but for most of the communication technologies available this increased requirement on bandwidth is not a problem. For example, according to PPC the BPL system that they have deployed in the Larrisa project has abundant bandwidth to handle the increase in bandwidth requirement.		

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
7.	Standardization of the telecommunication mode deployed	a. Is there a lack of standardization / protocol to be used for a particular communication channel for a particular application? b. Heterogeneity of hardware used	**Rank: 4** **Comments:** The standardization is extremely important for all new technologies since it provides a provider-independent platform on to which a power company can connect devices from different makers in the best quality and price. For example, the BPL technology deployed by PPC has a problem since it is not standardized. Still, lack of standardization does not avoid good and practical solutions, even if it does not promote interoperability and homogeneous solutions. Also, there are already work going on to frame the standards for example, IEEE is very close to a standard for BPL.		
8.	Interdependency of the Power system & ICT	• The failure of one infrastructure will affect the operation of the other • Lifetime of electronic hardware (5-15yr) is smaller than lifetime of Electric Power System assets (+30 yr) • Reliability/ availability of power grid is not matched by some telecommunication means (for example wireless communication).	**Rank: 5** **Comments:** PLC will be influenced by power system failure directly whereas wireless communication will be influenced by the terrain. According to ENEL, their past experiences have demonstrated that electric faults can have serious consequences on communication infrastructures. ICT for voltage management must work with grid operating and ICT for adaptive protection and grid reconfiguration must survive in grid failure conditions.		

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
9.	Control Paradigm	What is the best paradigm: central, distributed or co-ordinated control? Can the usage of any particular one control paradigm be a barrier for the implementation of the intra-grid management applications?	**Rank: 3** **Comments:** Central control will be a barrier for implementation of voltage management. Distributed and coordinated control is a paradigm for the voltage management.	**Rank: 3** **Comments:** There are consensus that the adaptive protection has to have distributed or coordinated control paradigm which calls for strong ICT support.	**Rank: 3** **Comments:** Coordinated control paradigm which calls for strong ICT support suits the grid reconfiguration application. The usage of distributed control paradigm poses a barrier in the context of grid reconfiguration.
10.	SCADA	What are the features lacking in SCADA that prevents the use of SCADA for implementing the intra-grid management applications in smart grid? Is lack of real time capabilities for communication and computation a barrier? Is centralized nature of SCADA a barrier for any of the applications, if so for which application & why?	**Rank: 5** **Comments:** We need consistent and accurate system information for power system operation. SCADA is highly performing but real-time measurements are very limited currently. The desired distributed control is a different approach from the current centralized SCADA operation. In future there may be more real-time information available but how to acquire, filter and aggregate such information is very challenging.		

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
11.	Controllability of the current power system	Only very few control knobs (hardware) like switches, few OLTC transformers are available at low voltage levels for controlling the power system	**Rank: 4** **Comments:** The control and communication systems are rendered useless without the availability of control elements / hardware.		
12.	Testing facilities	a. Lack of testing facilities for complex (because of non-linear increase of control problems) **combined** ICT/Electric Power System. b. Simulation environments are needed but no realistic data is available at large scale	**Rank: 3** **Comments:** According to the industries like ENEL and organization like ERSE, till now field test activities have been sufficient to understand the requirements.	**Rank: 5** **Comments:** There is a lack of test facilities to evaluate the impact of reverse power flow and unintended islanding. Development of a model for altered network topology is a huge challenge.	

Issue	Characteristic	Description / Key words	Ranking for voltage management	Ranking for adaptive protection	Ranking for grid reconfiguration
13.	Cost effectiveness of the communication technology deployed	What will be the cost of the primary communication technology deployed for the particular intra-grid management application? Will there be a need for a back up communication? How effective should the back-up communication be? Hence what will be the total cost involved and whether the cost involved will be too huge that it will become a barrier?	**Rank: 4** **Comments:** Depending on the degree of automation (for example, tap changer only vs. coordinated control) the costs can be crucial to the deployment. Deployment of total back up for all the communication could be too expensive.		

Table 1: Ranking of barriers

2.2 Quantitative aspects

Once the most important features of communication channels are identified, it is possible to define the ICT requirements according to the specific function that DG units are intended to provide, i.e., voltage control, generation curtailment, etc.

This however can then become very application-specific.

For such a scope, it is useful to quantitatively define the different ICT requirements in the smart grids context according to suitable reference ranges.

The data transfer rate can be classified as:

- High = greater than 100 kbit/s;
- Average = between 5 and 100 kbit/s;
- Low = between 1 and 5 kbit/s.

The reference sets for what concerns the latency are:

- Low = between 5 and 60 s (in some applications it could be even higher).
- Average = between 0.5 and 5 s;
- High = less than 500 ms (anti-islanding signal should be transmitted within 200-300 ms).

The application priority is usually quantified as a reciprocal ratio among the different users of the communication channel, and so the priority cannot be defined as an absolute value.

The availability of the communication channel, which is clearly related to the relevance of each application, can be defined as follows:

- High = greater than 99.9%;
- Average = between 90% and 99.9%;
- Low = between 80% and 90%.

Finally, the reliability of the communication channel can be quantified in terms of Bit Error Rate (BER), as indicated below:

- High = information loss smaller than 0.01%;
- Average = between 0.01% and 0.1%;
- Low = between 0 .1% and 5%.

As an example – which was elaborated in deliverable D2.2 of this project – table 2 summarizes the ICT requirements as a function of the different services requested to the DG units. It identifies the ICT requirements for the grid management [2].

	Transfer rate	Latency	Priority	Reliability	Availability
Inject energy surplus into the grid	×	×	×	×	×
Produce maximum power	×	×	×	×	×
Peak shaving (generation curtailment)	✓	✓✓	✓	✓	✓
Anti-islanding	×	✓✓	✓✓	✓✓	✓✓
Voltage and reactive power regulation	✓	✓	✓✓	✓	✓
Support island operation	✓	✓✓	✓✓	✓✓	✓✓
Ensure correct operation of power system	✓	✓✓	✓✓	✓✓	✓✓

Table 2: ICT Requirements based on the functions assigned to units DG (□□ High, □ Medium, □ Low)

Another example is Table 3 that shows the minimum latency requirements that have been defined by the “Network of Energy and Communication” [4].

Type of task	Min. latency	Frequency
Command and reply	2 sec	1-30 per day
Status information - failure - status of operation	 1 sec 5 sec	 <1 per day 1-30 per day
Transmit set points (P,Q)	2 sec	1-30 per day
Readings of measurements	2 sec	Every 5-10 sec
Readings of counter	2 sec	1-30 per day
Daily profile (P,Q – 96 quarter hourly)	20 sec	1-2 per day
Transmit parameter	10 sec	1-30 per day
Protection error event protocol	1 min	<1 per day

Table 3: Minimum latency requirements of communication in distribution networks

A very detailed set of requirements can also be found in the document[1] of the OpenSG users group (OpenSG = open smart grids).

[1] http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Forms/DispForm.aspx?ID=220&RootFolder=%2FUtiliComm%2FShared%20Documents%2FSG-NET%20PAP%20work-in-progress&Source=http%3A%2F%2Fosgug.ucaiug.org%2Fdefault.aspx

3 NON-TECHNICAL BARRIERS

The following list of non-technical barriers are to some extent more general than the scope of this work package only, but they are nevertheless useful to mention as an enumeration, and to be taken up at the project-wide level.

There exists a **problem of ownership** for the various aspects of the distribution system between the end users, DNOs, suppliers and energy service companies. There is no clear consensus on who pays for what.

The communication network usually is not controlled / owned by electric utilities and hence this means that the operation of the distribution grid **rely** on other businesses that are service based. Hence the reliability of the distribution network also depends on the reliability of the participating communication companies. A standardized communication service for grid operation is neither defined at regulatory level.

Traditional grids have been **centrally controlled** by the electric utilities but as the smart grids emerge there is emergence of different new stakeholders. The old electric power utilities do not want to lose control of the electric grid and this poses a barrier to the implementation of more and more communication technologies in the electric distribution systems. Responsibilities for outages and maintenance will have to be clearly identified.

Utilities are not eager to use new **open technology** for critical applications for distribution grids since the service levels are not yet justified and the communication companies are not able to demonstrate service guarantees at a reasonable price. Nevertheless, **interoperability** is a *condition-sine-qua-non* for broad take up.

Though some tariffs and infrastructure investments are regulated, the **regulatory aspects** of the smart grids are not yet clear. Owner of the infrastructure is not always the grid operator and different countries have different laws. Regulatory and policy-setting bodies have not yet provided the regulations that will ensure that the investments in new technologies will not lead to losses [5]. Also, the public and the private sectors are not treated equally. Finally, before investing in new services, all involved parties ask for clear and stable rules.

Rural areas present less return on investments even if most of the voltage problems are due to DER in those areas.

So far, stakeholders have not developed and endorsed a clearly defined **communication architecture** that will meet the requirements of the modern grid or the transition plan needed to achieve such architecture.

Regional and national demonstrations of communication technologies are lacking to **create interest**, excitement and the societal, political and economic stimuli that will accelerate their deployment.

There is not yet the **consumer education** to create interest and motivation among the consumer groups. Consumers can realize substantial benefits when the modern vision is achieved. Currently these benefits are not clear to the consumer and these new services are developing without including customers requirements and needs.

Vendors who supply sensors, IEDs, DER, and other end-use devices are **hesitating to invest** in these products until universal standards are adopted.

4 SOLUTIONS

The following elements contribute to solving these barriers.

1. Stick to hard quality-of-service (**QoS**) of the ICT infrastructure for safety-critical applications, that is, to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. This is essential for safety-critical applications wherein the communication channel should have the ability of providing priority to safety-critical functions by allocating its resources for this purpose when there arises a situation of choosing among many different applications. Thus the heavy requirement on bandwidth, latency and dependability of the communication channel by the safety-critical applications namely adaptive protection and grid reconfiguration for protection applications can be met.

2. Use of **open standards** and not the proprietary solutions can help in overcoming the barrier of lack of standardisation of the telecommunication deployed thus enabling the choice of a provider-independent platform on to which a power company can connect devices from different makers in the best quality and price. Thus, with the adoption of open standards the flexibility of the communication technology deployed will also increase. Open standards can guarantee interoperability and extendibility between the various devices and manufacturers. The various standards that are available currently at the distribution grid level have been explained in [6] and are shown in a pictorial representation in Figure 1.

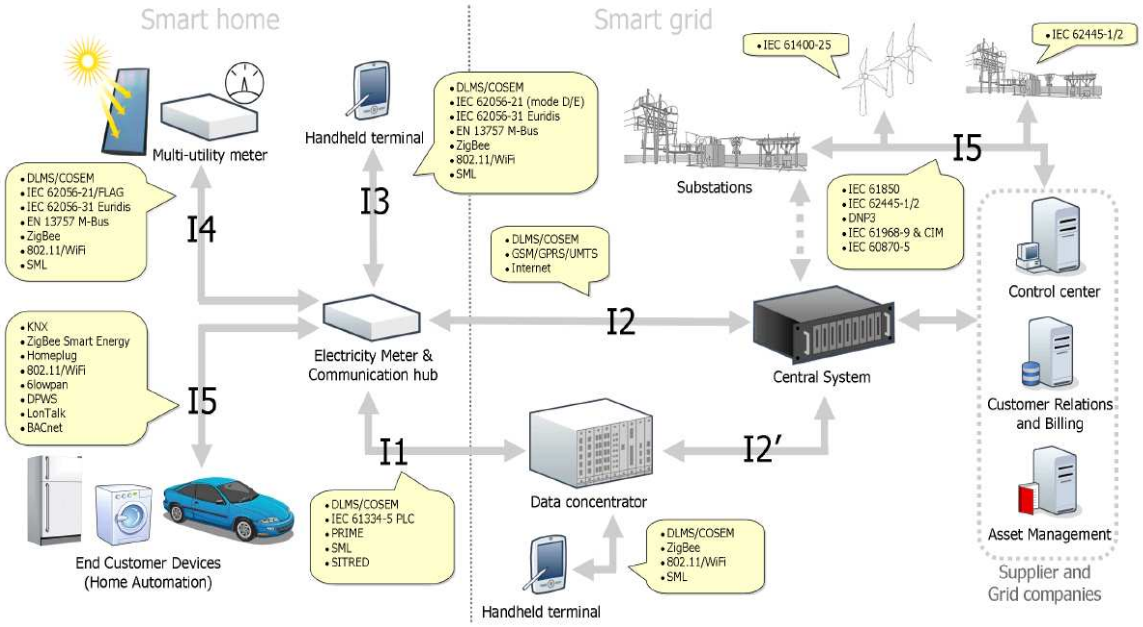

Figure 1: Placement of standards in the smart grid architecture [6]

Figure 2 shows the Seamless Integration Reference Architecture (SIA) from IEC TR 62357 “Power system control and associated communications – Reference architecture for object models, services and protocols”. Its focus on standards for implementing intra-grid management applications spans the range from the applications interfaces – defining the network data model and SCADA interfaces IEC 61970/61968 CIM – over the specific mapping and telecontrol protocols (IEC 60870) for exchanging measurements, conditions and states, down to the field device level changing the set points for the machines or the state of the switches using IEC 61850.

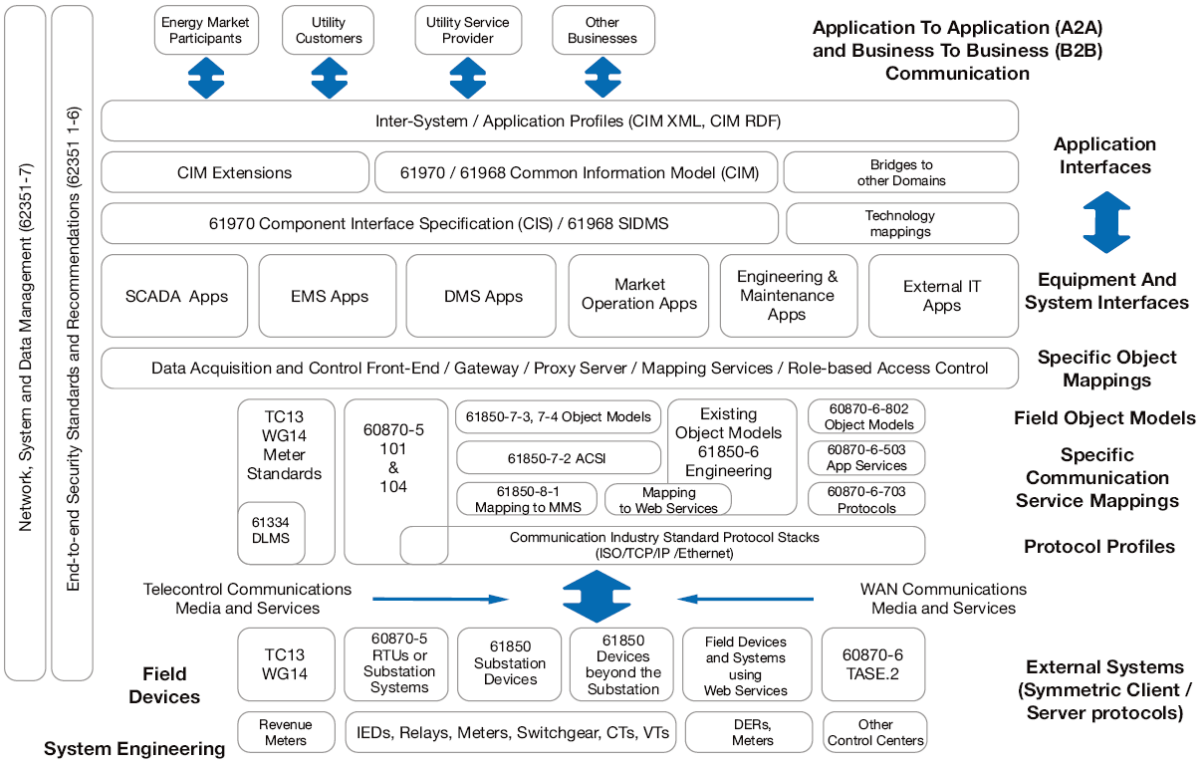

Figure 2: IEC TR 62357 Seamless Integration Reference Architecture (SIA) [7]

3. The use of **cyber security standards** will help in overcoming the barrier of threats to cyber security. The integrity of distribution control command is critical for distribution operations, avoiding outages and providing power to consumers reliably and efficiently. Integrity of outage information is critical for the safety-critical applications of adaptive protection and grid reconfiguration [8, 9]. This integrity of information can be achieved by the adoption of cyber security standards.

4. Make communication infrastructure at least temporarily **self sustained** in case of grid failure. Seeing both the systems as one and including them into control technology / SCADA / management systems will help in tackling the problems that will arise due to the interdependency of the electrical and the communication system.

5. Conducting more research on the effect of the various **control paradigms**, namely the central control, the distributed control and the co-ordinated control, on the grid stability will help in choosing the best paradigm for each of the three intra-grid applications.

6. For improving the controllability of the communication system more **sensors and control knobs** must be made available. The existing components can be retrofitted instead of being replaced. A clearly defined communication architecture will help to meet the requirements of the modern grid. Thus a clear specification of control algorithms and devices will improve the controllability of the communication system.

7. Increasingly **complex systems** and the interaction of components and systems – generating systems of systems- must be simulated and tested in real-time environments before they can be deployed. The deployment of local / regional controls must also be system wide integrated, that is, the impact on transmission system should also be simulated and tested. Clear specification of the methods, behaviour, effects, data acquisition, impact, implications, failures, communication, hardware / IEDs etc. should be made available by carrying out the tests.

8. Design innovation and economy of scale for sensors, use of existing communication infrastructure (xDSL, internet), retrofitting of the existing components instead of replacing them etc. will help to curb the cost of the **deployment of communication** for achieving the intra-grid control.

9. Regional and national **demonstrations** of communication technologies should be carried out in such a way that they create interest, excitement and provide the societal, political and economic stimuli that will accelerate their deployment. Also, **consumer education** should be carried out to create interest and motivation among the consumer groups so that the consumers can realize the substantial benefits when the modern vision is achieved. In order for consumers to value investment in communication systems, they must have a stronger link to grid operators and energy providers.

10. Though some tariffs and infrastructure investments are regulated, the **regulatory aspects** of the smart grids should be made clearer. The infrastructure owner is not always the grid operator and different countries have different laws. Regulatory and policy-setting bodies should provide the regulations that will ensure that the investments in new technologies will not lead to losses.

5 CONCLUSIONS

In this report, the barriers to the implementation of ICT in smart grid applications have been broadly classified into two, namely, the technical barriers and the non technical barriers. The technical barriers have been evaluated on the basis of ranking. Bandwidth of the communication channel, latency supported by the communication channel, dependability, flexibility and security of the communication channel deployed, scalability, standardisation, interdependency of the power system & ICT, control paradigm, controllability of the current power system, testing facility and cost are the parameters that have been evaluated based on a ranking showing the significance of the parameter in behaving as a barrier for the deployment of ICT in the three exemplary applications of voltage control, adaptive protection and grid reconfiguration. Latency supported by the communication channel, dependability, security of the communication channel deployed, interdependency of the power system & ICT, and testing facility are the parameters that have a rank of 5 which means that they are a very important barriers to be overcome especially for the power system protection applications of adaptive protection and grid reconfiguration. The list of non-technical barriers are to some extent more general than the scope of this work package alone, but they are nevertheless mentioned as an enumeration, in order to be taken up at the project-wide level. Sticking to quality-of-service, use of open standards and cyber security standards, conducting more research on the various control paradigms for each of the three intra-grid control applications, improving the controllability of the communication system with more sensors and control knobs, simulation and testing of the complex systems in real time, design innovation to help curb the cost, regional and national demonstration of the communication technologies, a well defined regulatory frame work will all act as solutions for overcoming the technical and non technical barriers for the implementation of ICT in smart grids.

6 REFERENCES

1. The European Electricity Grid Initiative (EEGI) Roadmap 2010-18 and Detailed Implementation Plan 2010-12, ENTSOE and EDSO, May 2010, available from http://www.smartgrids.eu/documents/EEGI/EEGI_Implementation_plan_May%202010.pdf
2. Sistemi di communicazonie richiesti da una rete di distribuzione MT con elevate penetrazione di GD by V. Prandoni et.al, CESI, Tech. Rep. A5059615, Rev. 00, 2005, in Italian.
3. IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, IEEE Power Engineering Society, February 2005.
4. Kommunikation als Schlüssel für künftige Effizienz der Netzführung by B. M. Buchholz et al., 11th Kassler Symposium Energy Systems Technology, Kassel, 2006.
5. Integrated Communications, Appendix B1, A systems view of the modern grid, conducted by the national energy technology laboratory for the US department of energy office of electricity delivery and energy reliability (NETL), February 2007.
6. De Craemer K. , Deconinck G., “Analysis of state-of-the-art smart metering communication standards,” IEEE Benelux Young Researchers Symposium 2010 in Electrical Power Engineering, Leuven, Belgium, March 29-30, 2010; 6 pages.
7. DKE, Deutsche Kommission Elektrotechnik, Die Deutsche Normungsroadmap, E-Energy / Smart Grid, VDE, 2010, www.dke.de
8. Draft NISTIR 7628, Smart grid cyber security strategy and requirements, The cyber security coordination task group, Annabelle Lee, Tanya Brewer, Advanced security acceleration project – Smart Grid, September 2009, 236P..
9. Z. Lukszo, G. Deconinck, M.P.C. Weijnen (Editors), “Securing Electricity Supply in the Cyber Age: Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure”, Series: Topics in Safety, Risk, Reliability and Quality, Vol. 15, Springer, 2010, 187 pages, ISBN 978-90-481-3593-6.