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 INTER-STAKEHOLDERS SERVICE MONITORING IN SMART GRIDS

D3-3

Revision: R3
October, 2010

This is a Deliverable of WP3

Deliverable Leader: Rune Gustavsson (BTH)

Authors:

Rune Gustavsson, Shahid Hussain, Björn Ståhl (BTH)	
Pekka Koponen (VTT)	
Evangelos Rikos (CRES)	

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	Aug 2010	R. Gustavsson	BTH	First issue
R1	Sep 2010	R. Gustavsson	BTH	Overall Revision
R2	Oct 2010	G. Franchioni P. Koponen	RSE VTT	Overall Revision
R3	Oct 2010	P.Koponen R. Gustavsson	VTT BTH	Added Conclusions

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This deliverable contains original unpublished work except where clearly indicated otherwise.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 rgu@bth.se
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

List of Abbreviations

BMS	Business Management Systems
DER	Distributed Energy Resources
DG	Distributed Generation
DS	Distributed System
EC2	Elastic Cloud Computing
EiMS	Electricity infrastructure Management Systems
IaaS	Infrastructure as a Service
IKT	Information and Knowledge Technologies
OPC	OLE for Process Control
PaaS	Platform as a Service
PLC	Programmable Logic Controller
RES	Renewable Energy Sources
RTU	Remote Terminal Unit
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreements
VPN	Virtual Private Network
XML	Extensible Markup Language

INDEX

Executive summary

The general objective of WP3 is to explore emerging IC Technologies addressing issues related to the monitoring of Energy Efficiency in smart grids. At the level of single grid, monitoring of energy production, transmission and distribution is mainly facilitated by various automation systems comprising plant, network and energy management systems, SCADA (Supervisory Control and Data Acquisition) systems, local automation systems etc. However, the network automation systems do not themselves meet the monitoring requirements of future Smart grids. Firstly, the hierarchical integrated architecture does not easily encompass integration of Distributed Energy Resources (DER) and Renewable Energy Sources (RES). Secondly, present and legacy SCADA systems have some well-known vulnerabilities and scalability barriers. Thirdly, SCADA systems do not easily support customer empowerment. In the next future, these information management systems should also be able to support the new business processes and have a view of effects of inclusion of e.g. DER.. The interactions between SCADA systems and ICT supporting the emerging functionalities needed to Smart grids have to be taken into consideration.

In order to deal with automation systems of the energy infrastructure allowing DER integration, we have thus to design and implement ICT solutions supporting new energy based business processes, including data management. In short, future Smart grids will be composed of three main interacting infrastructures:

- Automation, control and management systems of the physical energy infrastructure (EiMS) Electricity infrastructure management Systems.
- Business Management Systems (BMS)
- Other Information Management Systems (ICT)[1].

Present EiMS architectures do not support **coordination** between relevant sets of stakeholders. It is a fact that design and implementation of business cases in Smart grids typically involve new stakeholders such as active users, prosumers, aggregators and integrators, as emphasized by several EC funded projects. These stakeholders interact with each other in a energy services network based on the electrical and communication infrastructures, strongly interlaced..

To allow for setting up and monitoring coordination between identified stakeholders in business cases based on energy based services the use of the mechanism of the **Service Level Agreement** (SLA) is deemed promising. SLAs are well known mechanisms in areas such as Telecom, but novel for use in future Smart grids.

The importance of ICT as a mean to coordinate new stakeholders is stressed in a recent report from European Technology Platform Smartgrids: **Strategic Deployment Document (SDD)**, April 2010, Deployment Priority #4 ICT.

The work in SEESGEN-ICT Work Package 3 is described in the following two deliverables:

[1] ICT (Information and Communication Technologies). Sometimes it is interpreted as IKT (Information and Knowledge Technologies). In this report the intended interpretation is Information Management Systems, a combination of traditional ICT and IKT.

- The already delivered D3-2, dealing with ICT for data management and inter-stakeholders service monitoring in Smart grids
- The present D3-3, Report on technical and non-technical barriers and solutions for inter stakeholders service monitoring in smart grids with DER.

In D3-2 the roles of SCADA systems, as the ICT supporting the control and the monitoring of the Network, and of SLA, as the mechanism to manage business, were discussed. The fundamental concepts of SLA monitoring, including service level data and data models, tied to the Smart grid functionalities were presented and discussed. Uses cases from the EC funded projects FENIX an ADDRESS were analyzed with the view to a possible SLA approach . Specifications of ICT supporting SLA monitoring were given.

In this deliverable D3-3 a set of **technical** and **non-technical** barriers are identified and addressed. Technical barriers are in general of two types. The first type is typically a list of barriers more or less generic but technology dependant, e.g., performance, scalability, interoperability, and so on. However, design and implementation of future smart grids face new barriers not directly connected to specific technologies. To identify and possibly bypass these barriers presuppose controlled development and experimentation on future emerging architectures and configurations., c.f., the SDD document [15]. In D3-3 we introduce a model of **co-evolution** to support a progressive **structured engineering approach** of designing, implementing and assessing pilots towards future Smart grids, enabling identification of **emergent barriers** as well as **potential solutions** to handle those in a sustainable way.

To that end, in D3-3, we have taken as a starting point experiences by WP3 partners of ongoing works in implementing pilots of future Smart grids. These pilots, essentially related to the EC funded project INTEGRAL, have typically been developed re-using well known infrastructures, e.g., web services, and configuring those with suitable tools, meeting the requirements of the pilot at hand. The following three pilots have been assessed:

- Pilot I: Business oriented, using web services as a platform
- Pilot II: EiMS oriented, using an OPC platform
- Pilot III: ICT Security oriented, using a VPN tunnel

The D3-3, after having summarized these pilots, lists some **inherent barriers** of those technologies as well as of Automation systems. Basically none of those pilots could have been developed from scratch, due to costs and lack of resources, unless the pilots could be integrated from standard components. This entails that a generic ICT architecture is not practical or effective, whilst a pragmatic architecture supporting integration of pilots from components could be.

Use of standard components or platforms in configuring new applications in a cost effective way and implementing SLA functionalities is a salient feature of **Cloud computing**. The example of **Amazon Elastic Compute Cloud (EC2)** is proposed as a web service that provides resizable compute capacity in the cloud. Amazon EC2 changes the economics of computing by allowing stakeholders to pay only for capacity that is wanted and actually used (as fixed by the SLA).

In the implementation of the above pilots, three kinds of **Platform as a Service** (PaaS), using here the terminology of Cloud Computing, have been used.

Disclaimer: The purpose of D3.3 is not to give a comprehensive tutorial on all technologies relevant to classical and future Monitoring. Rather, to give a motivation and background to our choice of dealing with the monitoring of Service Level Agreements as the mechanisms to coordinate different service processes among the Smart grids stakeholders. Selected summaries of EU projects have the same purpose. For more details we refer to the original sources. Lastly the notations used in this deliverable are not generic. Different interpretations (meanings) might exist. These ambiguities are mostly due to that the area of Smart grids and related technologies and methods are revolving. An example is the above definition of ICT.

1 Introduction

SEESGEN-ICT Work Package 3 (WP3) considers how Information and Communication Technology (ICT) can be used for monitoring of smart grids, allowing stakeholder dependant views on business processes, as well as supporting Energy Efficiency and customer empowerment when a large amount of Distributed Energy Resources (DER) is integrated.

The deliverable D3.2 *ICT for Data Management and Inter-Stakeholders Service Monitoring in Smart Grids* some different ICT-approaches that can enable increased Energy Efficiency and supporting User Empowerment are discussed.

To meet the stated requirements, design and implementation of Future Smart grids needs reassessment of classical monitoring tasks to ensure:

- Flexible grouping of stakeholders
- Flexible empowerment of users

To that end we introduced in D3.2 the concept of **Service Level Agreements** (SLAs) and related monitoring challenges. The concept is quite new in the energy sector, whilst is more consolidated for applications in the deregulated telecom market and in outsourcing of resources like in Cloud Computing.

The current deliverable identifies barriers that might prevent the wide deployment of ICT-based approach in the above applications and proposes possible solutions including possible further R&D developments, as needed.

2 Methodology to identify barriers and solutions

This document has been developed in an iterative way, as follows. In the first step a plenary brainstorming was performed involving all work package partners in order to identify the barriers to a wide deployment of ICT approaches. The results of this effort are similar lists as those provided by SEESGEN-ICT WP2 and which are presented in D2.3. A summary of those findings is given in Section 2.1. The barriers and solutions thus identified are naturally a compilation of existing experiences by partners. However, since design and implementation of future Smart grids will require mechanisms and processes entailing identification of further emerging barriers and research of new suitable solutions, we propose in this deliverable a complementary **system engineering approach** (named **co-evolution** mechanism) as a second step towards identifying emergent barriers and proposing solutions towards pilots of future Smart grids.

2.1 Barriers of different kinds and solutions

Deliverable D2-3, issued by WP2, deals with the barriers to the deployment of ICT based solutions related to functions of the Electricity infrastructure Management System (EiMS) identified as crucial tasks.

A. Voltage Control

B. Adaptive Protection

C. Reconfiguration

Of course, relevant tasks related to EiMS, other than those above identified by WP2, are of importance, as, for example, local balancing and demand management. However, for the objectives of the present Deliverables, i.e. from a SLA point of view, the selected tasks are sufficient and fulfil a first approach to barriers identification, also for what concerns the monitoring issues treated in WP3.

The barriers are herein listed and ranked with respect to the above functions. More details including justification of the ranking are provided in D2-3.

The scale of ranking is: 1=not an important barrier at all … 5 = a very important barrier to be overcome for this application to be deployed.

#	Description	Ranking		
		A	B	C
1	Bandwidth of the communication channel	3	3	3
2	Latency supported by the communication channel	3	5	3
3	Dependability of the communication channel	5	5	5
4	Flexibility of the communication technology deployed	2	2	2

5	Security of the communication channel	5	5	5
6	Scalability of the communication channel	3	3	3
7	Standardization of the telecommunication mode deployed	4	4	4
8	Interdependency of the Power system & ICT	5	5	5
9	Control Paradigm	3	3	3
10	Suitability of present SCADA	5	5	5
11	Controllability of the current power system	4	4	4
12	Testing facilities	3	5	5
13	Cost effectiveness of the communication technology deployed	4	4	4

Table 3.3_1 Ranking of barriers related to tasks A, B and C (From D2.3)

A list of 10 recommendations to overcome those barriers and thus contributing to solutions is also included in D2.3.

In monitoring of SLAs we typically have to rely on **services** provided by the EiMS and BMS and supported by the ICT, specifically when dealing with business processes depending on DER. This entails that we presuppose that, e.g., those monitoring services can be supported by the functions identified above in D3-2. The investigations and results of D3-2 are thus also very valid for success of monitoring of SLAs.

A second step in identification of barriers is presented in this deliverable and is based on findings from ongoing and planned EU projects such as INTEGRAL (http://integral-eu.com/), KIC InnoEnergy. (http://www.innoenergy-initiative.com/) and ADDRESS (http://www.addressfp7.org/).

Basically, we propose an **engineering approach** of **co-evolution** as described in the following Figure 3.3_1. In fact, we argue that future Smart grids are examples of **Socio-technical-economic systems** with the following three main components of requirements:

- **Social aspects**, including societal goal (regulatory constraints) as well as user requirements
- **Technical aspects,** including energy systems, ICT systems and their interconnections
- **Economic aspects,** including business models, cost of investments and cost of ownership

In most of contemporary investigations, identifications of barriers and enablers are restricted to only one or two of the above aspects. That approach, however, makes it difficult to assess and address the important interplay between the components. To enable a process of co-evolution we have suggested in the INTEGRAL project **drivers of regulatory frameworks and experimental environments** enabling controlled experiments to assess, e.g., **context dependant** ICT solutions.

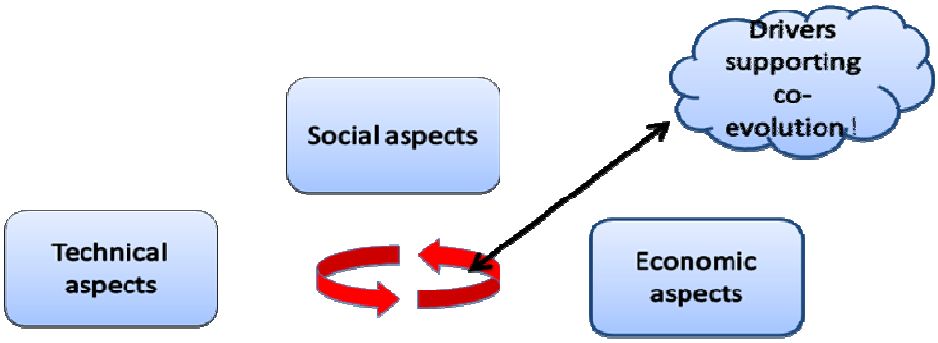

Figure 3.3_1 Main components and mechanisms supporting co-evolution of Smart grids

In this deliverable D3.3 we propose a structured approach to group these emerging barriers into technical and non-technical barriers that can be resolved by selecting and integrating suitable ICT platforms with corresponding EiMS and BMS systems. Furthermore, we suggest a state-based approach of monitoring SLAs (Section 4).

3 A generic and a pragmatic architecture for Smart grids

System architectures capture relevant **context dependant aspects** of the system under study. An architecture identifies the main components and their relationships complemented with, e.g., data models, data flow models, sequence diagrams and/or use models. Different perspectives of a system are captured by different architectures. Important perspectives are requirements, design, implementation and maintenance.

From the INTEGRAL project we borrow the following generic four-tiered architecture of a service-oriented future Smart grid. IICT stands for Integrated ICT system, due to the fact that different Smart grid solutions typically have different ICT components.

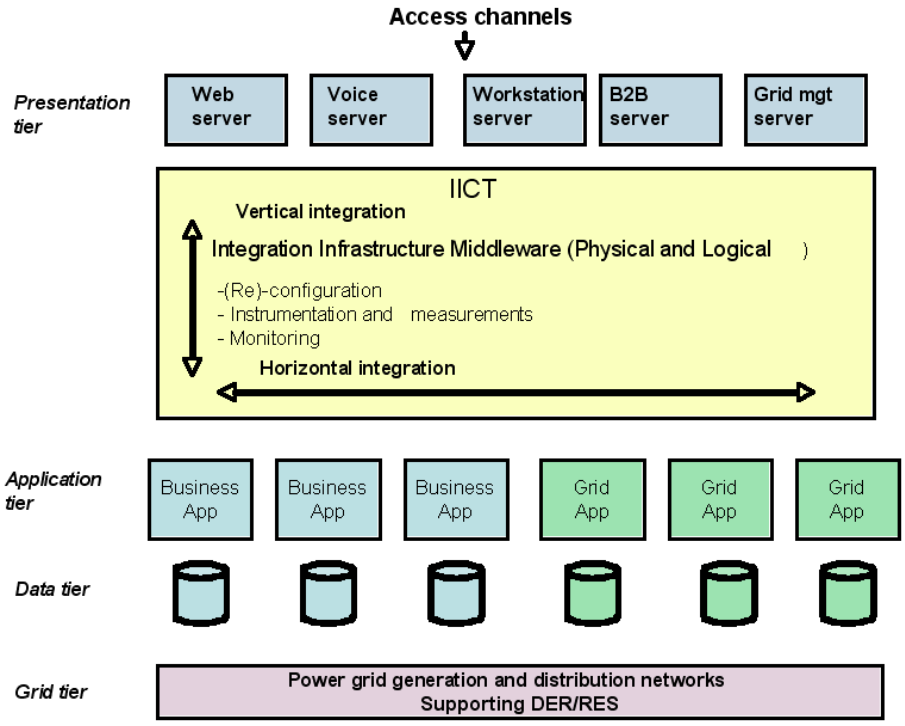

Figure 3.3_2 Generic architecture of service oriented Smart grids

A service oriented architecture for a **distributed system** highlights the ICT component providing the **communication** and partly the **coordination** functionalities of the **Distributed System** (**DS)** at hand. The integration of the ICT system with functional components, databases and HCI components is facilitated by middleware software. In a **vertical integration** we typically have traditional **stovepipe applications**. Difficulties of maintaining and integrating stovepipe type architectures led to the concept of **serve based systems** and service based architectures. A service-based system is **configured** from services using appropriate middleware. Horizontal

integration means **reuse** of services across old stove-pipes. The architecture in Figure 3.3_2 support system focuses on design and requirements tasks.

However, this generic architecture does not easily support implementations and maintenance or assessing performance of Smart grids themselves. That is, neither, how to address/compare barriers of generic ICT systems or how to compare different solutions in practice. Furthermore, implementation costs or cost of ownership is also difficult to estimate from this generic architecture.

In order to implement and assess **pilots** of future Smart grids such as the three Field tests of INTEGRAL (Section 5), the following supplementary and pragmatic architecture has been developed.

The focus of the pilots was to choose, from a set of standard industrial ICT platforms ~~e.g.,~~ web services to support the selected BMS. Given the focus of the pilot the relevant additional components of the EiMS, Functional system and SCADA system as well as the underlying Electrical infrastructure were selected. The pilot thus configured was then implemented and assessed. In the pilots implemented in the INTEGRAL project we made the following simplification: We focused on the top level on either the Energy Management system or the Business Management system since they typically demand different kinds of ICT support. In fact, the pragmatic architecture supports stakeholder involvements, rapid prototype development and structured assessments.

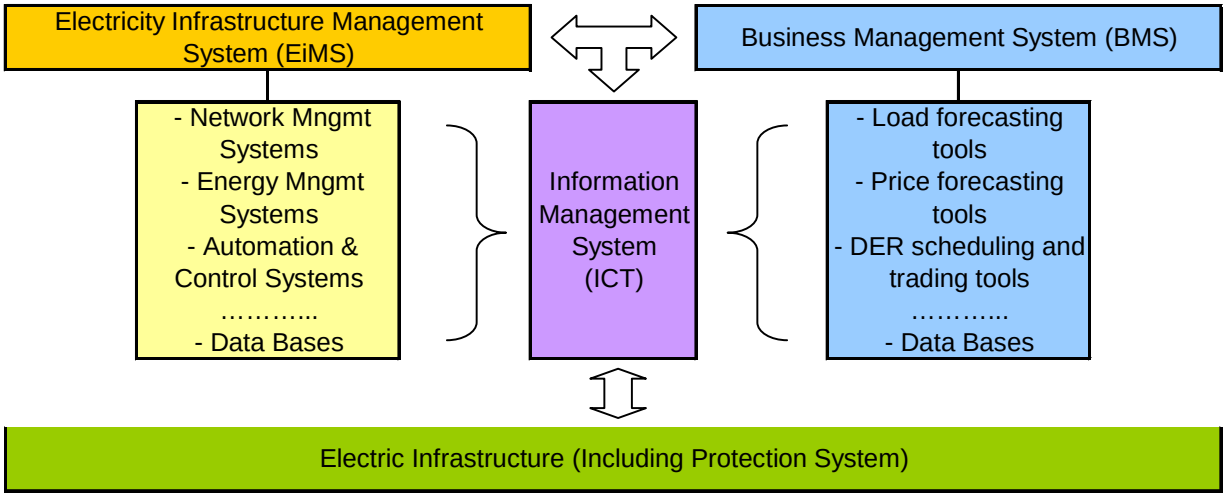

Figure 3.3_3 Components of the technical infrastructure of future Smart grids supporting ICT focused rapid prototyping

From Figure 3.3_3 it follows that we can design and implement the technical infrastructure as an Electricity infrastructure Management Systems (EiMS) interacting with a Business Management System (BMS) and coordinated by an ICT system (Section 7.1). The EiMS is consisting of Management Systems, Automation & Control Systems (SCADA) and Databases. The BMS is consisting of specific ICT system enabling implementation of distributed smart BMS

and Databases. Since there are overlapping functionalities between the SCADA systems and BMS specific ICT systems depending on the intended pilot, this conflict has to be resolved. The benefit is an increased reusability of ICT solutions across context. For example, web-services is often the choice of ICT platform in business related pilots.

In general, ICT systems enable design and implementation of smart **distributed information processing** systems. The components of an ICT system are:

- Functional components and data bases
- Communication components
- Coordination components

Again we observe a terminological overlap between ICT systems and Automation systems (including SCADA), due to the fact they support different processes.

In certain cases, some functional elements could be modeled and implemented as **agents** to implement some form of intelligence – adaptation. There are, of course, other AI technologies than agents, that could be used to implement intelligent behavior. However, this is beyond the scope of this deliverable.

Agents are characterized by:

- **Adaptive behavior** enabled by a knowledge base and a pattern-based rule base. Behavior is created by pattern matching of facts (beliefs) in the knowledge base with received messages. The term “intelligence” refers to this **flexible behavior** compared to a fixed determined algorithmic behavior of deterministic input-output (or failure). The control of the pattern-matching can be programmed allowing flexibility,
- **High-level communication language** where messages consists of a tuple message_type (content) coordinated by a **dialogue** model.
- **High-level coordination** between agents taking into account agent capabilities and coordination principles.

Agent technologies have some **inherent barriers** due to the flexibility gained by decoupling the algorithmic control. The term **brittleness** refers to that scope of the agent competence is defined by the scope of the rule set and the pattern matching implying that the results of agent computations could be wrong – out of scope. However, there is **no generic solution** to handle this barrier in a semantically correct way. Methods to address brittleness are out of the scope of this deliverable.

In summary: **intelligence** in software intensive systems could be entailed by modeling **components as agents** and/or by programming **flexible interfaces** between components. A modern introduction to relevant AI technologies is given in the book [1].

The Communication and Coordination components constitute an example of ***Infrastructures as a Service* (IaaS)** in **the Cloud Computing** terminology.

Challenges of ICT systems include design, implement and maintain an *information management system* that support different stakeholders views on energy based business models and ensure:

- Balancing Intermittent production
    - Voltage control and massive introduction of DER
- Meeting societal goals of Energy Efficiency
- Meeting customer requirements

- Meeting economic goals
- Managing interactions with SCADA systems

4 Monitoring states of Smart grids

From Figure 3.3_3 we derive that future smart grids can be modelled as an integration of a EiMS with a BMS supported by an ICT system. We advocated in D3.2 introduction of sets of SLAs between stakeholders as a mean to monitor the performance of sub systems as well as the overall system.

Monitoring SLAs entails that we assess if parameter values are within pre-assign limits and take appropriate actions if some threshold are passed. Introduction of system states is a natural way to model and implement this behaviour.

As an example: In INTEGRAL we have identified the following states of the full system of Figure 3.3_3.

- Normal
- Critical
- Emergency
- Loss of service (energy)
- Black start

Those states could also be applied to the subsystems (EiMS, BMS or ICT). Challenges include:

- Model the states (referring to a proper set of SLAs)
- Model transition between states. Specifically, Black start --- normal!
- Model actions and responsibilities related to transition between states

The type of state is dependant of context, i.e., stakeholders, sub-systems and **monitored criteria**. Thus the type of state can be inferred from the relevant set of SLAs.

The system (SYS) of Figure 3.3_3 can be modelled as the triple:

SYS = (EiMS, BMS, ICT)

This entails that SYS has at most 3x5 = 15 states. A reduction of the number of states is dependant on the context and has to be investigated into further details.

5 Coordination in Smart grids

High-level Coordination in future Smart grids will basically be of two types:

- Coordination of *resources*
  - Matching of supply-demand using a market model
  - Coordination of actions
  - Coordination in data management
- Setting up and monitoring *Service Level Agreements* (SLAs) between stakeholders. The focus of WP3.

Coordination of resources is applicable if we can abstract from constraints such as technical constraints and/or regulatory aspects. In INTEGRAL we have mainly focused on agent-based coordination of resources (PowerMatcher) or smart functions (agents).

High-level coordination could benefit from being modeled as agent based coordination. Two agent modeling environments are prevalent:

- JADE – a research based environment
  - A list of related environments:
    http://sharon.cselt.it/projects/jade/application-projects.htm
- JACK – a commercial environment
  - AOS – Autonomous Decision-Making Software: http://www.aosgrp.com.au/

For industrial maturity reasons, BTH and KTH will use the JACK environment for implementation and evaluation of agent-based coordination prototypes in the KIC InnoEnergy project [3].

Coordination and monitoring of the EiMS (Figure 3.3_3) is not the primary focus of WP3 but rather of WP2. However, it could be the situation that some monitoring tasks could be recast as services such as:

- Impact of disturbances in supply and demand on parameters of SLAs
- Impact of management of technical constraints on parameters of SLAs

6 Cyber security of Smart grids

Harnessing threats related to cyber security in a trustworthy manner might be the most critical task to address to enable successful uptake of future Smart grids by key Stakeholders.

In short: Inadequate cyber security is a large barrier in successfully deploying Smart grids.

With reference to Figure 3.3_3, cyber security relates to the ICT systems, the SCADA systems and the Protection systems and their interconnections. In a classic setting the Protection systems is focused on protection of EiMS processes. Also, there is a vast literature on security and integrity of ICT systems [.

In short, in Smart grids we have to monitor and protect Energy management processes, Business management processes and information management processes. That is, we have to detect vulnerabilities, specifically, when and how they are exploited. An exploit is a hostile attempt to take over a critical process at a selected critical point (interface). The critical interface is an access point to a system component allowing exploits.

There are several reports on SCADA vulnerabilities and exploits [8, 9] and also some recent discussions of vulnerabilities related to AMI-systems and empowerment of customers [10]. From a WP3 point of view monitoring of SLAs aiming at intrusion detection and/or Rule Based Access Control (RBAC) of tools accessing data [4, 5]. These mechanisms could be supported by proper SLAs and monitoring tools (Section 9).

A method to detect emergent vulnerabilities could be based on structured experiments following the approach of co-evolution (Section 2).

7 Some findings from assessments of pilots

The INTEGRAL project investigates the following three pilots or Field tests (Texts related to the Demonstrators are copied from the INTEGRAL home page):

- ***Demonstrator A*** This demonstrator, in The Netherlands, covers the day-to-day "normal" market trading and service operation conditions of DER/RES aggregations.
- ***Demonstrator*** *B* This demonstrator, located in Spain, covers the "critical" operating conditions such as stability of DER/RES aggregated grid-integrated clusters, cells, or micro-grids
- ***Demonstrator C*** This demonstrator, in France, covers "emergency" conditions including security aspects and will especially demonstrate the self-healing capabilities of DER/RES aggregations.

Implementing and assessing the three different business cases (Field tests) of INTEGRAL in a cost efficient way was possible by using and tailoring existing ICT infrastructures. In fact we have separately implemented and integrated:

- Web services as a IaaS – The "normal" business cases of Demo A
- OPC as a IaaS – The "emergency" conditions (self healing) of Demo C
- VPN as a IaaS – The "critical" situations of Demo B

IaaS stands for **Infrastructure as a Service,** a solution to deploy the Cloud Computing methodology (see D3.2) to share and save costs in development and use of infrastructures.

That is, we have implemented the three different ICT systems of INTEGRAL by embedding the three Infrastructures mentioned above.

To support this embedding and enable system hardening we have developed two experimental environments in INTEGRAL [4] and [5, 6]. In fact, those two experimental environments supports our view of co-evolution in Figure 3.3_1.

Similar ideas of experiment-based co-evolution are expressed in planned EU supported efforts such as the Public Private Partnership (PPP) **European Future Internet Initiative (EFII)** (http://initiative.future-internet.eu/) and **EIT KIC InnoEnergy** (http://www.innoenergy-initiative.com/)

Another finding by the INTEGRAL project is that current examples of use cases or business cases from EU projects such as **FENIX** (http://www.fenix-project.org/) and **ADDRESS** (http://www.addressfp7.org/) describe high-level scenarios that are not usually mapped on any ICT infrastructure nor implemented. However, ADDRESS has a whole WP for ICT. ADDRESS maps use cases to CIM to ICT. in connection with CIM smart grids standards development. The ADDRESS use cases have: aggregators, other competitive electricity market actors (retailers etc.), regulated electricity market actors (TSO, DSO), electricity consumers. But, usually only a subset of stakeholders envisioned from future Smart grids are involved in the scenarios identified. In short, the identified scenarios have a limited value in addressing barriers and enablers of ICT systems supporting future Smart grids.

In fact, we propose in Section 9, a structured approach of mapping business models (use cases) onto ICT infrastructures.

7.1 Barriers indentified from the pilots and related projects

We have indentified the following sets of barriers from the pilots of the INTEGRAL project:

- Technical barriers
  - Related to SCADA systems (Section 7.1.1 and 7.1.2)
  - Related to IaaS of web services (Section 7.1.3)
  - Related to IaaS as OCP services (Section 7.1.4)
  - Related to VPN services (Section 7.1.5)
  - Related to integration of infrastructures in a system (Section 9,1)
  - Related to Customization of services
- Non-Technical barriers (Section 7)
  - Cost of investment
  - Cost of ownership
  - Customization of services
  - Acceptance by stakeholders
  - Compliance with regulatory frameworks
  - Methodological issues of system development

7.1.1 *Challenges of SCADA systems*

SCADA system is a vital component in today's utility/energy sector; it provides monitoring and controlling interfaces between the human and the machine. It helps the operator read sensors or to change state in actuators and other energy gadgets in order to provide a stream flow of energy to all its customer/consumers. There is a number of factors to support the need of new SCADA systems, for the use in Smart grids:

- The technology is getting older as it can only manage energy flow, while there is a huge demand on managing information flow, caused by the emergence of Smart Grid concepts.
- Future Smart Grid introduces new stakeholders that require information about the energy flow in real time that is arguably not being provided by the current SCADA systems.
- In Smart Grid the consumer is also an active participant (new stakeholder) that makes optimized decision based on his/her usage of energy.
- There are well known vulnerabilities, at different levels, in currently used SCADA technologies.

In SCADA systems, the monitoring concept is more related to telemetry, where you remotely measure the amount of some specific flow/state. These measurements are affixed to a static, typically hard coded, hierarchical representation of the grid or parts thereof. The energy flow process consists of thousands of devices from large scale transformers to small switches and sensors that relay measurements to a specific terminal for showing specific information.

Common SCADA system components:

- Human-Machine Interface
- A supervisory (computer) system
- Remote Terminal Units (RTUs)
- Programmable Logic Controller (PLCs)

- Communication infrastructure connecting the supervisory system with RTUs

Most control actions are performed automatically by (local loops) RTUs and PLCs. Host control functions mostly request *supervisory* level interventions.

We have witnessed three generations of SCADA systems development:

- Mainframe (monolithic) systems
- Distributed systems. Mostly proprietary solutions!
- Networked systems. Open architectures and protocols

Moreover, due to the large installed base of SCADA systems, we have to deal with several legacy problems in the transition to future Smart grids:

SCADA systems, involves a large set of protocols and communication infrastructures and methods. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols built with them are SCADA-vendor specific, but widely adopted. In more modern systems these have been replaced by open standard protocols. These are DNP3 (Distributed Network Protocol), mainly applied in North America, and IEC sets of protocols developed under the IEC TC57 (IEC homepage: http://www.iec.ch/). All these sets are recognized and supported by all major SCADA vendors. The protocol sets can be divided into two generations as follows:

- Still widely used open standard protocols are IEC 60870-5-101 or 104, and DNP3. Many of these protocols now contain extensions to operate over TCP/IP. These protocols were designed for high performance with limited communication capacity which compromised possibilities for easy system networking, interoperability and upgrading. These protocols were not designed to be secure from cyber attacks and security features have been added afterwards.
- Globally accepted TCP/IP based and layered protocols. These are IEC 61850 in substations and SCADA, new IEC 61850 based protocols for communication with Distributed Energy Resources, and Common Information Model – CIM CIM includes IEC 61968 on system interfaces for distribution management and IEC 61970 on energy management system application interfaces for communication between control centres These standards are nowadays predominantly used, when either new systems or interfaces between systems are implemented. However, systems with the older protocols will still remain in widespread use and will be maintained,

IEC 62531 “Information Security for Power System Control Applications” is applied for information security with the above mentioned IEC protocol sets and also with the DNP3,

It is good security engineering practice to avoid connecting SCADA systems to the Internet in order for the attack surface to be reduced, albeit the communication infrastructure may already in part be overlaid on top of technology that in turn is connected to the Internet -- and assumptions towards the interconnectivity between such systems should be avoided and taken into account during risk management.

SCADA system complexity is due to that a large part of any complex SCADA system design is involved in matching the protocol and communication parameters between connecting devices. There are about 200 such real time user layer and application protocols. These include both proprietary and non- proprietary protocols.

The IEC 60870-5 provides a communication profile for sending basic telecontrol messages between two systems, which uses permanent directly connected data circuits between the systems. The IEC Technical Committee 57 (Working Group 03) has developed a protocol standard for Telecontrol, Teleprotection, and associated telecommunications for electric power systems. The result of this work is IEC 60870-5. Five documents specify the base IEC 60870-5:

- IEC 60870-5-1 Transmission Frame Formats
- IEC 60870-5-2 Data Link Transmission Service
- IEC 60870-5-3 General Structure of Applications
- IEC 60870-5-4 Definition and coding of Information Elements
- EC 60870-5-5 Basic Application Functions

The industry is now moving away from proprietary protocols and multitude of standards. In addition the IEC 60870-5 and DNP3 based protocols are gradually being replaced by more modern IEC standards that have proper layering (as described in the ISO/IEC 7468) and are based on TCP/IP whenever possible These new globally accepted IEC standards are IEC 61850 and Common Information Model (CIM, IEC 61968 and IEC 61970). Also new standards for communication with distributed energy resources are based on IEC 61850 and CIM principles. IEC 61850 is based on the latest version of the Manufacturing Message Specification MMS (ISO 9506). IEC 61850 and CIM are also being harmonized. Thus some barriers are being removed and at the same time new needs and opportunities emerge for service level monitoring.

7.1.2 *Cyber Security related to SCADA systems*

In the future power grid, similarly to an economy model, exist interdependent entities that need each other in order to survive and this requires the harmonized coexistence of them. One of the most important challenges of ICT infrastructure is the opening of until now closed and proprietary Control Systems (including SCADA) which will enable the interactions between the different stakeholders. These challenges are mostly related to Cyber Security. It is inevitable that we are going to migrate from the closed networks that are managed as 'plant assets' to Internet Protocol based systems. The risks of such a transition are high due to the present Internet status and configuration. The main reason for this is the fact that when the current network was being developed it was not foreseen that there would be also a transition to the power system such that would require the use of this infrastructure. Because of this, it is necessary to improve the security of present system.

The risks from Cyber Attacks to control systems of power plants or other power infrastructures may vary according to factors like motivation of the attacking parties (e.g. terrorism attack, human mistake) and could even cause destruction of equipment or long-term outages. From the perspective of WP3, such risks could include the impact to QoS, and non-compliance with the terms and conditions of SLAs between stakeholders, something that could lead to possible conflicts. A very characteristic example of how critical is a cyber attack to control system, was recorded in March 2007, during an experiment carried out in the U.S. (Idaho Falls, Idaho) [11]. The test revealed that it was possible due to a specific vulnerability of the control system for someone outside the plant to gain control of a generator turbine, forcing it to shut down and moreover causing it to overheat by changing the operation cycle.

The above experiment revealed how critical are vulnerabilities to threats and how much crucial impact could have to the system security. Another more recent example related to SCADA and specifically PLCs is the appearance of a Windows worm called Stuxnet, which by writing code to PLCs, can potentially control or alter how the system operates [12]. The previous are only few of the examples including also other sectors apart from power systems which stress the importance of shielding and securing systems against such kind of threats. To this context, it is important that a coordinated effort should be made, which would be based in data exchange not only internally but also between different entities of the power system. Such a strategy could reveal risks even in real-time frame. Many regional system operators are already sharing data with transmission utilities, distribution utilities, and generators using the Inter-Control Center Communications Protocol (ICCP)—usually over TCP/IP networks—so they can proactively respond to any problems affecting the grid. This is very important especially in the frame of WP3 which regards interactions between different entities through SLAs. However, there are some inherent difficulties into this due to possible unwillingness of entities to share data due to intellectual property, access or even competition affairs.

The assessment of vulnerabilities in SCADA systems as well as the mitigation of related risks is not an easy task. Extensive experience with much interesting results in the field are presented by INL (Idaho National Laboratory) in the U.S. through [13] and [8]. It should be pointed out that it is a settled policy that discovered vulnerabilities are not publicly disclosed before efforts for mitigating or even eliminating the risks are made. Due to this, a vulnerability database existing in the U.S. (National Vulnerability Database-NVD) [14] receives around 15 new and not publicly disclosed vulnerabilities every day. According to [13] it is estimated that at least 12% of the reported vulnerabilities in NVD apply to control systems. Moreover, by introducing the concept of '0Day' vulnerability, a method for estimating and how many vulnerabilities of that kind exist on any given day, is presented. It is worth mentioning that as 0Day vulnerability is described any vulnerability, in deployed software, which has been discovered by at least one person but has not yet been publicly announced or patched. In order to identify the publicly disclosed vulnerabilities applicable to control systems the authors used two different approaches:

- Review of vendor marketing information
- Components known to be deployed in control system environments

In the project report [8], results concerning the INL NSTB project are presented. During this, 16 control system assessments were performed under from 2003 through 2007. Basic aim of the project was on the one hand information collection from individual stakeholder reports but mainly assessment in the INL SCADA TestBed and in operational installation. The discovered vulnerabilities are analyzed and organized in specific categories based on a control system and security metrics approach. For each category, mitigation strategies are given. The primary goal of the INL cyber assessment tasks is to improve the security of the energy infrastructure by delivering to each industry partner a report of all security problems found during the assessment along with associated recommendations for improving the security of their product or infrastructure (as appropriate).

The assessment procedure is divided into two steps. The first one includes the laboratory assessments which are designed to evaluate vendor-specific products and services, in two separate phases: a baseline system assessment that identifies vulnerabilities in the vendor's default configuration, and (2) an evaluation of the system following implementation of mitigation

strategies based on baseline assessment results. After the end of the initial step an assessment performed on an asset-owner installed version of the system followed which provided the opportunity work with owners and operators and help validate the impact and possible mitigation strategies for vulnerabilities identified in the laboratory assessment.
The assessments yielded a number of vulnerabilities, grouped in four security dimensions, namely:

- Security group knowledge
- Attack group knowledge
- Access
- Vulnerability

Each of these includes different vulnerability categories, resulting into totally eleven (11) categories (from Change management deficiencies to unpatched systems) and twenty eight (28) concrete vulnerabilities. In the document for each vulnerability category a mitigation recommendation is given.

7.1.3 *Challenges of Web Services as IaaS*

Web services is a key technology in implementing Internet based business models on top of the Internet http protocol. Web services: www.webservices.org/

Implementing web services as an IaaS.

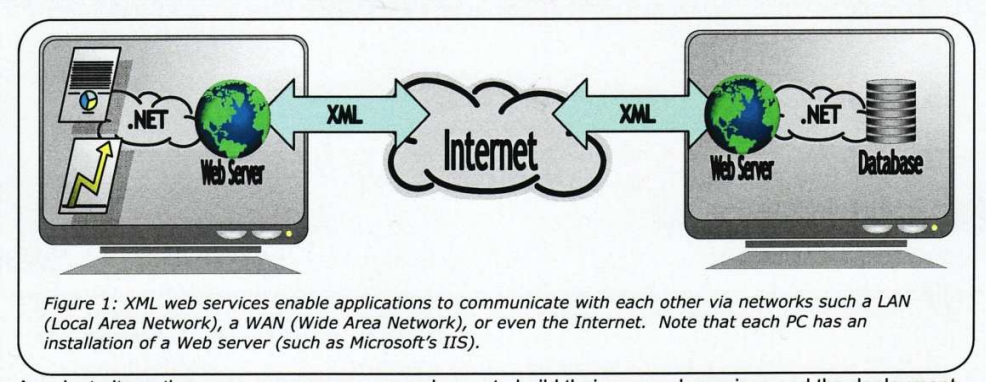

Figure 1: XML web services enable applications to communicate with each other via networks such a LAN (Local Area Network), a WAN (Wide Area Network), or even the Internet. Note that each PC has an installation of a Web server (such as Microsoft's IIS).

Figure 3.3_4

XML structure:

- The XML web services architecture leverages several standards to enable data transfer between applications on remote computers. Programmers have several choices to consider for their design.
- These technologies and tools (web servers, libraries, APIs, etc) leverage the evolving security standards, user authentication, data transfers, data states and a lot more. Applications programmers can rapidly build and deploy XML web services using existing tools and frameworks. It is important to stress that a web server (like Microsoft's IIS)

provides the necessary infrastructure to deploy XML web services. This is a common acceptable practice in the business world!

- XML web services provide that all-important independence from any hardware or software platform.

XML characteristics.

The poll-report-by-exception mechanism of XML web services works well for business applications. However, in the real-time world, this approach works very poorly for applications such as:

- HMI (Human-Machine Interface) applications that require a quick updates of the screen. Operators require quick updates (usually every second) to enable them to monitor system response effectively. This is especially required during abnormal situations and hazardous operations such as startups or shutdowns.
- Real-time monitoring applications that operators would be use to set alarms or trigger various other applications to take action.
- MPC (Multivariate Predictive Controllers) applications that require fast process updates. These applications typically require process data every second or faster. They also change set points quickly.

Consequently, XML web services are a poor choice for applications that require fast real-time updates. A few applications that use XML web services to transfer OPC data have surfaced recently. The vendor's hope is to transfer OPC data seamlessly from one computer to another using a "standard" interface. However, their implementation quickly shows the limitation of such a transfer, as they either suffer from extremely high bandwidth usage (since they have to constantly poll for changes), or they suffer a slow update rate. This update rate is unacceptable by the applications listed above.

XML messages are very large in comparison to similar DCOM messages that carry the same information, and their sheer size makes them difficult to transport en masse. One solution is to compress these messages in a binary format, but the compression process effectively renders the message to be of a proprietary format. This cancels the benefit of using XML in the first place. Thus, if one can't compress the message, its large size would have an impact in any network that is subject to any of the following:

- Limited network bandwidth such as a WAN (Wide Area Network) as well as radio, satellite or modem based networks.
- "Pay-per-byte" transmission such as that due to satellite communication.
- Noisy or unreliable communication has a lower chance of properly transmitting larger messages. Slow data transfer as in serial communication.
- Networks that must keep bandwidth usage under normal conditions to a minimum to allow for connectivity during abnormal situations.

Furthermore, the origins of XML as a document format with little to no boundaries in terms of element size or depth that are accessible outside a post-processing / parsing context make it less than optimal for the use as a data exchange format and protocol due in large part to the inability to reliably stream-process, filter and monitor its contents in real-time.

In summary: XML web services based architectures are an attractive alternative in the business world that requires only a few messages, and delivery time is not important. However, web services are not well suited for process control or monitoring.

7.1.4 *Challenges of OPC as IaaS*

Industrial Control System (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, **Distributed Control Systems** (**DCS**) and other smaller control system configurations such as skid-mounted **Programmable Logic Controllers (PLC),** often found in the industrial sectors and critical infrastructures.

OPC Foundation (http://www.opcfoundation.org/) promotes open standards enabling connectivity of ICSOPC environments for process monitoring and control include several extensions and interfaces; for example, extensions increasing security (through, for instance, data tunnelling, see Section 7.1.5).

Initially, OPC stood for OLE (Object Link-Embedding) for Process Control and is a standard for real-time data-coordination and exchange between devices. It was originally built upon-, and heavily integrated with-, Microsoft COM/DCOM technology. Although the technologies involved are to be considered dated and current efforts strive towards a transition to the newer, more portable OPC-UA (Unified Architecture), which is designated as the next generation of OPC standards. Given the range of available OPC product, their widespread use and the long development cycles involved. ,the complete transition to OPC-UA compliant solutions is likely to be a decade long iterative process. Such a transition however, should be planned - and prepared for - early on.

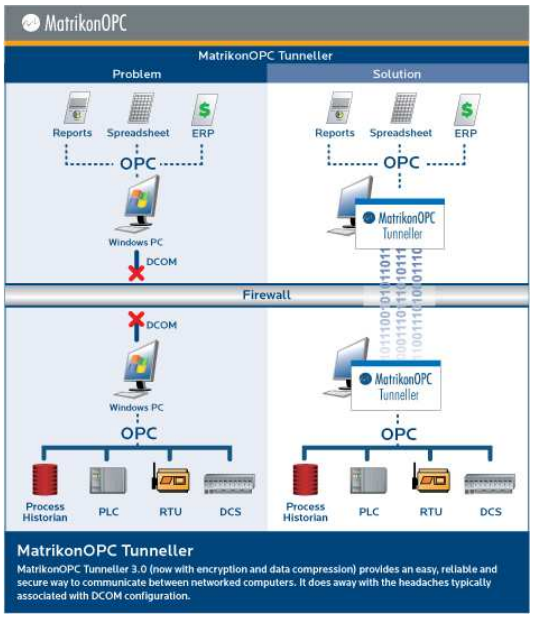

Figure 3.3_5

As illustrated by the figure above, OPC solutions typically have the additional responsibility of data-exchange between the demilitarized SCADA and business enabling processes and services. It is therefore a sensitive and critical interaction point for which additional measures ought to be taken as to not expose the considerably more brittle SCADA with undesired influences that might be present in the often more exposed corporate network.

The challenges involved with the OPC solution very much mimics and inherits the challenges of working with any SCADA system, as described in Section 7.1, because OPC is typically used for building whole - or parts of- SCADA-type systems. As such, they are also susceptible to the generic challenges of creating, using and maintaining any large-scale software intensive endeavour. While the immediate concerns and challenges of integrating a solution and making it both stable and secure, the long-term challenges of maintenance and upgrades, along with procedures for implementing security hot-fixes with minimal response time are no less important.

7.1.5 *Challenges of VPN as IaaS*

Virtual Private Network (VPN) is first and foremost a tunneling approach for bridging several networks together across an otherwise untrustworthy communications link, and is implemented through virtualization at a selected layer of the OSI stack, enabling the bridging of communication protocols from not only the selected layer but for all layers above the selected one. This is commonly done on layers 1 (physical), 2 (link) or 3 (network) but can in some cases be even higher, such as layer 5 (session) for SSL-VPN. For reference of a highly configurable and flexible VPN solution, please refer to OpenVPN (http://www.openvpn.net).

In addition to the choice of level at which to implement the VPN, something that ultimately affects the set of protocols that are likely to be compatible across the networks at respective end-points (illustrated in the figure below), there is also a large assortment of technologies to select from which influences the end-results in different ways. Major categories in this regard are level of encryption and associated topics of key-management and key-exchange, but also network management on each side of the nodes, both in terms of bandwidth allocation for the tunnel but also address allocation and routing. Furthermore, the selection of mode of transport (TCP or UDP) between the client and the server is of additional interest, as they can exert different behaviors based on the protocols that are being tunneled. TCP used in local network communication tunneled over a TCP-VPN based tunnel, for instance, suffer a notable performance loss when the transmission control algorithms for dealing with packet- loss interact recursively. There is a lot of work involved in properly tuning protocol implementation at this level, and for time-critical situations such tuning have to be validated against the possible influence of VPN links and other forms of tunneling.

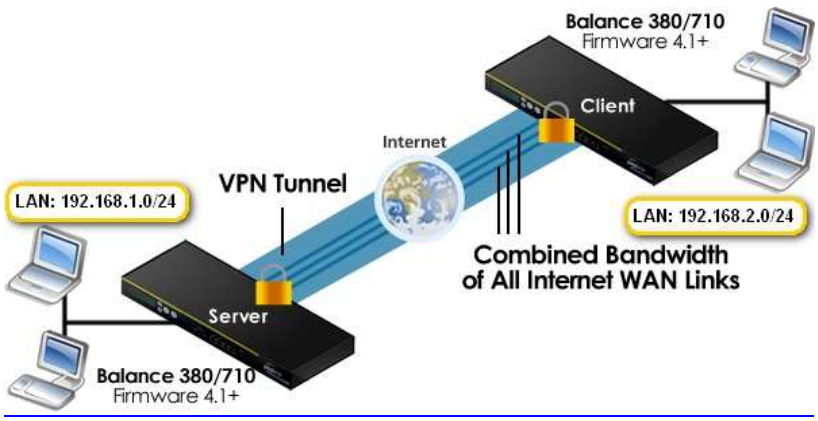

Figure 3.3_6

Challenges in terms of the security and integrity of the information exchanged across a VPN tunnel will also need to be dealt with. First and foremost in the terms of the security and integrity of both end-points, if either one of the nodes are compromised the VPN itself brings little to no benefits. Noteworthy in this regard is the web browser, both in terms of VPN solutions that are implemented on such a level (running the risk of Cross-Site Scripting class of attacks, XSS) but also in terms of the clients involuntarily exporting access through malicious web browsers through Cross-Site Request Forgery kind of attacks. Lastly, even though the tunnel encrypts the data properly and even though end-point security is managed, there's still the underlying challenge of managing side-channel attacks, i.e. exposing information about what is being communicated using metadata such as packet size and latency between packets.

7.1.6 *A possible solution*

The ICT systems in Figure 3.3_3 can be viewed as consisting of a **low-level ICT** system supporting the SCADA and EiMS systems and a **high-level ICT** system supporting the BMS. From the analysis above we deduce that the ***IaaS of web services*** is a high-level ICT system. In fact it is not suitable at all as a low-level ICT to support the EiMS! On the other hand the ***IaaS of OPC*** is intended to be a low-level ICT but not easy to complement to support a BMS in an appropriate way. As we need to sometimes integrate a low-level IaaS with a high-level Iaas into a system we propose a bridge between those two kinds of IaaS utilizing bundles of SLAs [4] and [6].

A critical mechanism of cloud computing is ***Elasticity***. Elasticity in cloud computing stands for, according to NIST. (http://csrc.nist.gov/groups/SNS/cloud-computing/):

"Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the customer, the capabilities available for provisioning often appear as unlimited and can be purchased in any quantity at any time".

However, there are several open R&D questions to address to ensure intended elasticity. An experimental approach is here very promising.

The following Figure 3.3_7 illustrates an architecture provided by **Amazon Elastic Compute Cloud (EC2)** (http://aws.amazon.com/ec2/)

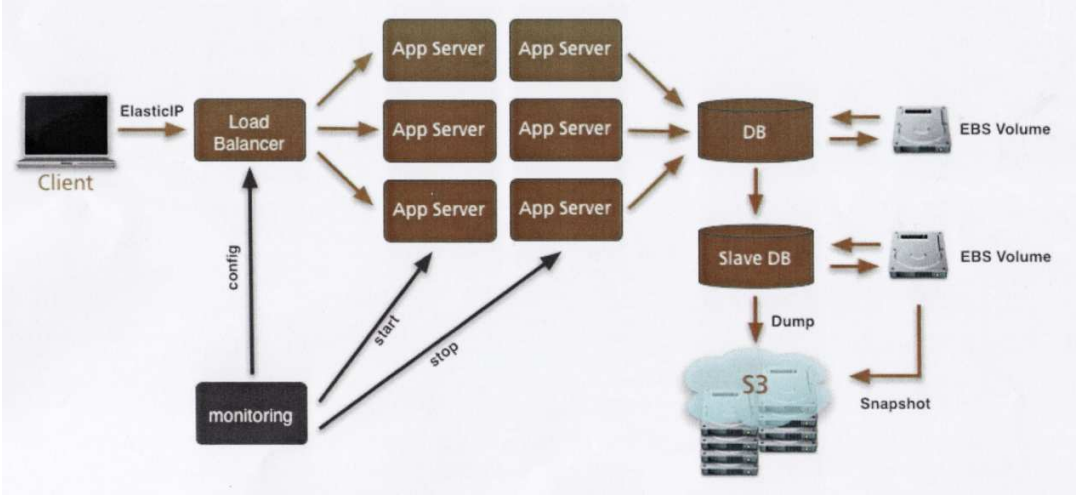

Figure 3.3_7 Architecture of digital service applications supported by EC2 environment

The EC2 support is accessed via the ElasticIP. Primary EC2 components are: *Amazon S3* a storage for the Internet. It is designed to make web-scale computing easier for developer (http://aws.amazon.com/s3/), and the Load *Balancer* and the *Monitoring* modules. Those are essential to ensure expected behaviour and performance.

7.2 Challenges of integrating IaaS

We have implemented three IaaS as subparts of ICT solutions in INTEGRAL (Section 7). In each case the IaaS is integrated into the ICT system via a server. The integration of the server environment is complex due to choices of supporting protocols and data structures.

- The server may itself introduce a vulnerability in the overall system (e.g., indirect access to unprotected network components)
- In practice, we might need to integrate several IaaS to meet the full requirement of the supporting ICT for future Smart grids

Conclusion: We need supporting environments in order to integrate the selected IaaSs in a proper and secure way [4] and [6].

7.3 Addressing costs of investments and costs of ownership

We argue that cost of investments and ownership can be reduced and estimated by using models of Cloud Computing such as IaaS, as exemplified above. The different shared Infrastructures could be developed/owned by different groups of stakeholders.

8 Conclusions

The suggested coordinating mechanisms of SLAs have to be further developed to be suitable in the Smart grid settings. Not the least, to enable suitable and traceable monitoring of related processes.

At present, the following identified barriers and partial solutions have been addressed:

- Transformation, replacement, upgrading and transitions of technologies used for SCADA systems towards standard open protocols such as EIC 61850 might take time to be globally adapted.
- Cyber security of Smart grids, specifically SCADA systems and Smart metering infrastructures need to be more investigated.
- The adaption of web services is an attractive alternative of ICT solutions of business processes of Smart grids. However, those ICT solutions are not well suited for time critical process control and monitoring.
- Implementing OPC solutions that are stable, secure and allowing maintenance and upgrading, while guaranteeing specified real-time performance, is feasible.
- Security, integrity and information protection related to network and information management can be implemented by proper use and embedding of VPN solutions.
- Supporting environments are needed to integrate the selected IaaS in a proper, cost efficient and secure way . The proper form and use of SLAs in this context has to be further investigated.

Solutions to some of these challenges were suggested in D3-3, but developing new solutions is left to future work, because it is beyond the resources and scope of SEESGEN-ICT.

References

1. Goertzel, B. (2006): *The Hidden Pattern*. *A Patternist Philosophy of Mind*. BrownWalker Press, Boca Raton, 2006. ISBN 1- 58112- 989 – 0.
2. Gros, C. (2008): *Complex and Adaptive Dynamical Systems. A Primer*. Springer Verlag. ISBN 978 – 3 – 540 - 718 73 - 4.
3. Gustavsson, R. and Ståhl, B. (2010): The empowered user – The critical interface to critical infrastructures. In Proceedings of *The Fifth international CRIS conference on Critical Infrastructures – Interacting Critical Infrastructures for the 21st Century*. Beijing 20-22, September 2010.
4. Hussain, S. and Gustavsson, R. (2010): Coordinating Energy Business Models and Customer Empowerment in Future Smart Grids. In Proceedings of *First International ICST Conference on E-Energy. E-Energy, 2010*. October 14 15, 2010, Athens, Greece.
5. Mellstrand, P. (2007): *Informed System Protection*. Doctoral Dissertation Series No. 2007:10, Blekinge Institute of Engineering. ISBN 978-01-7295-106-8.
6. Ståhl, B., Caire, R., Le Thanh, L. and Gustavsson, R (2010): Experimenting with Infra-structures. In Proceedings of The Fifth international CRIS conference on Critical Infrastructures – Interacting Critical Infrastructures for the 21st Century. Beijing 20□22 September 2010.
7. Wirsing, M., Banatre, J-P., Hölzl, M. and Rauchmayer, A. (eds) (2008): *Software-Intensive Systems and New Computing Paradigms. Challenges and Visions*. State-of the-Art Survey, LNCS No 5380, Springer Verlag. ISBN-10 3 – 540 – 89436 – 5.
8. National SCADA Test Bed (NSTP) (2008): *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*. U.S. Department of Energy - Office of Electricity Delivery and Energy Reliability.
9. INL Critical Infrastructure Protection/resilience Center (2009): *Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues*. U.S. Department of Energy - Office of Electricity Delivery and Energy Reliability.
10. Lisovich, M.A,, Mulligan, D.K. and Wicker, S.B. (2010): Inferring personal information from demand-response systems. IEEE *Security and Privacy*, vol. 8, pp.11-20.
11. Transition of Power-Staying current requires improved communications and control, CIO-DIGEST: Strategies and Analysis from Symantec, pp. 24-28, April 2009
12. http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices
13. McQueen, Miles, Wayne Boyer, Trevor McQueen, Sean McBride, “Empirical Estimates of 0Day Vulnerabilities in Control Systems,” Proceedings of the SCADA Security Scientific Symposium 2009 (S4), pp. 6-1–6-26, January 21–23, 2009.
14. http://nvd.nist.gov/
15. http://www.smartgrids.eu/documents/SmartGrids_SDD_FINAL_APRIL2010.pdf

Paper 4 describes an agent-based platform for investigations on monitoring SLAs. SLAs related to the trade-off between customer empowerment and voltage control related to incorporation of vast amounts of DER is indicated.

Paper 6 describes an experimental environment implemented by G2Elab and BTH for the INTEGRAL C Field test. The paper also describes some further experiments that could be performed to build and integrate context dependant ICT infrastructures