



SEESGEN-ICT

4° GENERAL WORKSHOP

Paris - SAP Office, April 14th – 15th 2011

Kari Mäki, VTT:

***Technical Barriers – Non-Technical Barriers and
possible solutions in WP3***



PARIS 14/04/2011



Contents

- Introduction
- Infrastructure for Smart grids
- Identifying the barriers
- Barriers and possible solutions
- Conclusions



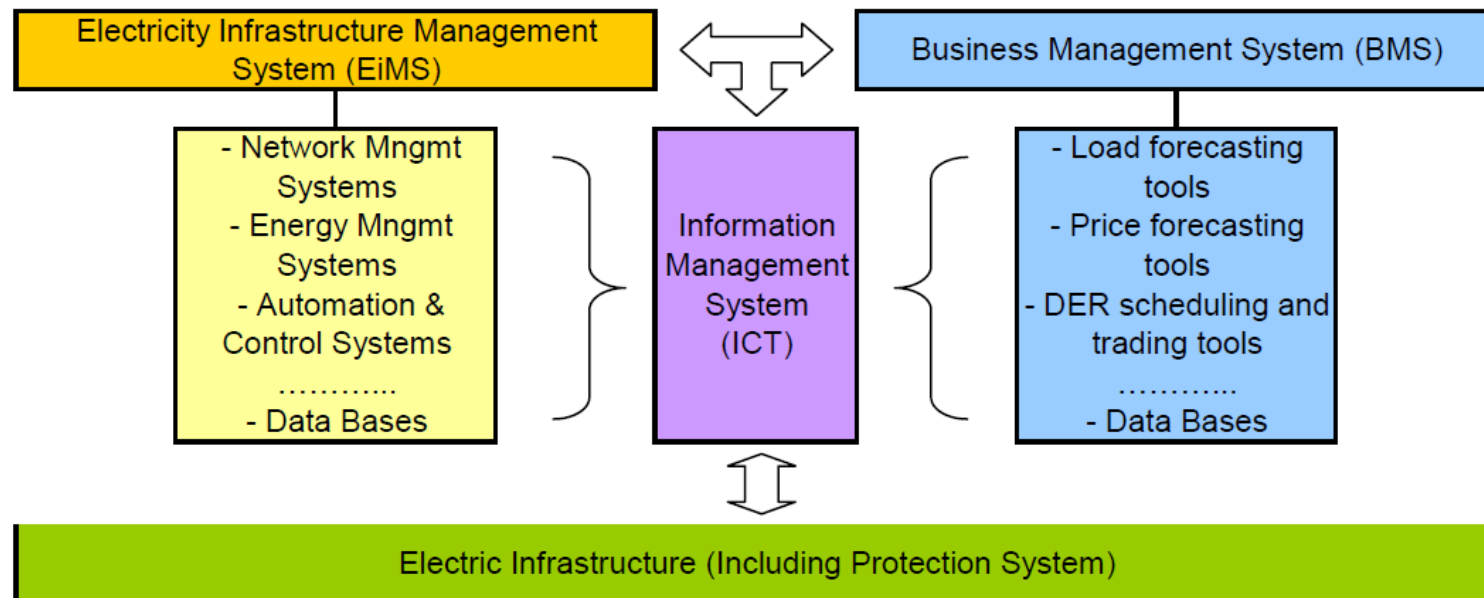
Introduction

- ❑ Various automation systems exist for energy production, transmission and distribution
- ❑ Present systems do not always meet the requirements of future Smart Grids
 - ❑ Integration of DER and RES
 - ❑ Customer involvement
 - ❑ Constraints of present SCADA systems
- ❑ Information management systems should support new energy based business processes
- ❑ Smart Grid means much more active stakeholders
- ❑ Interaction of SCADA and ICT is essential!



Infrastructure for Smart grids

Electricity infrastructure Management (EiMS)
interacting with Business Management (BMS)
coordinated by Information Management (ICT)





Identifying the barriers

- ❑ Structured approach for managing emerging barriers
 - ❑ Technical barriers
 - ❑ Traditional, technology dependant
 - ❑ New, Smart Grid related
 - ❑ Non-technical barriers

- ❑ Progress of work
 - ❑ First step: Barriers to wide deployment of ICT approaches (WP2)
 - ❑ Second step: System engineering approach for identifying emergent barriers (WP3)



Identifying the barriers

□ Barriers to wide deployment of ICT approaches (WP2)

A. Voltage Control
 B. Adaptive Protection
 C. Reconfiguration

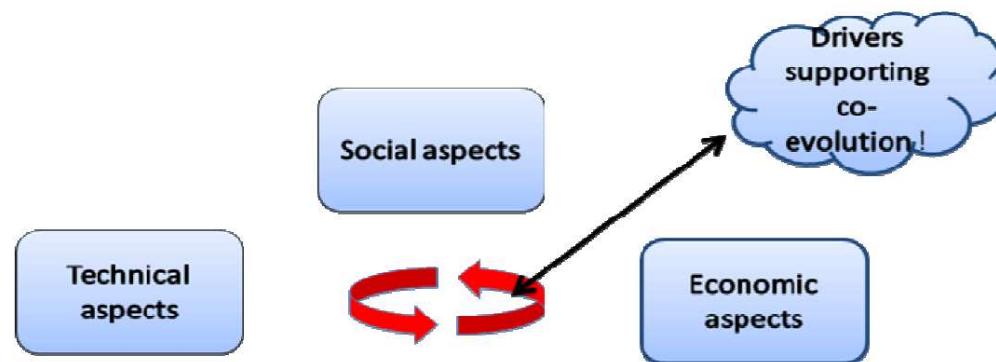
#	Description	Ranking		
		A	B	C
1	Bandwidth of the communication channel	3	3	3
2	Latency supported by the communication channel	3	5	3
3	Dependability of the communication channel	5	5	5
4	Flexibility of the communication technology deployed	2	2	2
5	Security of the communication channel	5	5	5
6	Scalability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





Identifying the barriers

- ❑ **System engineering approach** is used for identifying emergent barriers within WP3
- ❑ Smart Grid is a **socio-technical-economic system**
 - ❑ Social aspects (e.g. user requirements)
 - ❑ Technical aspects (e.g. energy system related)
 - ❑ Economic aspects (e.g. business models)
- ❑ Interactions between these aspects must be evaluated





Challenges of transition

Barriers related to the transition to smart grids:

- ❑ Lack of clear frameworks and regulations supporting business and technical processes in Smart Grids
- ❑ Totally new stakeholders and their different views and needs in monitoring and controlling the processes of Smart Grids
- ❑ Dependencies between information on different layers
 - ❑ Higher layers for business applications, customer support etc.
 - ❑ Lower layers for technical infrastructure
 - ❑ Time dependencies of information
 - Coordination between the layers as service exchange between SLA services



Monitoring states of Smart grids

- ❑ Future Smart grids can be modelled as an integration of EiMS and BMS supported by ICT
- ❑ Modelled system states are needed for monitoring and controlling critical processes
- ❑ System states are used for describing the interactions of system and SLAs
 - ❑ Normal / critical / emergency / loss of service / black start
 - ❑ Modelling the transitions can be challenging
 - ❑ States can also be applied within the subsystems
- ❑ Overall system state is a combination of states of EiMS, BMS and ICT



Cyber security of Smart grids

- ❑ Cyber security is likely the most critical issue for future Smart grids
 - ❑ Lacking security can become the main barrier
- ❑ Processes for Energy management, Business management and Information management need to be monitored and protected
 - ❑ Detecting vulnerabilities
 - ❑ Detecting exploits and attacks
- ❑ SLAs could support in the form of:
 - ❑ Intrusion detection
 - ❑ Access Control
 - ❑ Monitoring



Challenges of SCADA systems

- ❑ Technology built for energy flow management; huge demand on managing also information flows
- ❑ New stakeholders require energy information in real time
- ❑ Legacy problems due to different protocols and communication infrastructures
- ❑ Scalability, especially towards small active customers
- ❑ Control systems need to be opened for enabling new kind of interactions
 - ❑ Security related challenges will follow
 - ❑ Varying degrees of risk (human mistake to direct attack)

→ *"Transition of SCADA technologies towards open protocols may take time"*



Challenges of SCADA systems

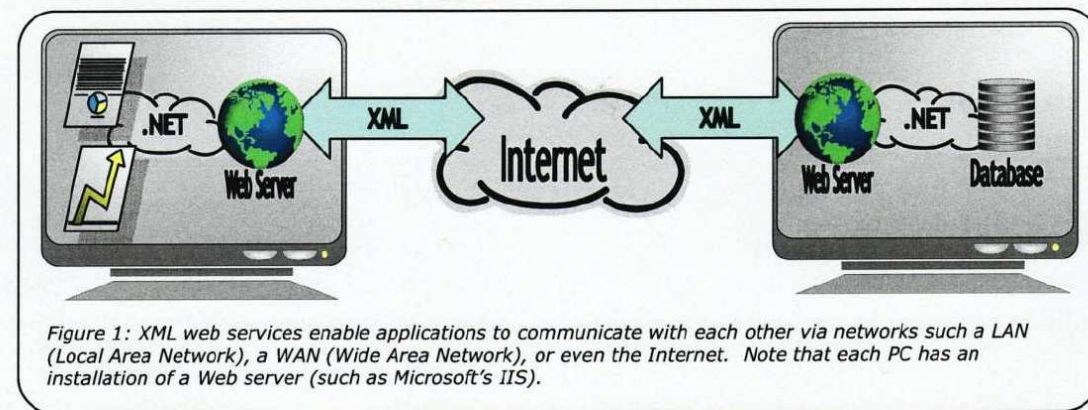
- ❑ The amount of data available from the network is increasing rapidly
 - ❑ More metering on all levels; especially end user level
 - ❑ More information from relays and other equipment
- ❑ Not just collecting and storing the data
 - ❑ Finding the essential information
 - ❑ Using the data efficiently
 - ❑ Interfacing to other information systems
- ❑ Real-time management of network topology and switching state is crucial with high share of DG

→ *"More information from the network will be available; efficient use is the key"*



Challenges of XML Web Services

- ❑ HMI applications requiring quick updates
- ❑ Real-time monitoring applications
- ❑ Controller applications requiring fast process data
- ❑ Large size of XML messages
- ❑ Security challenges



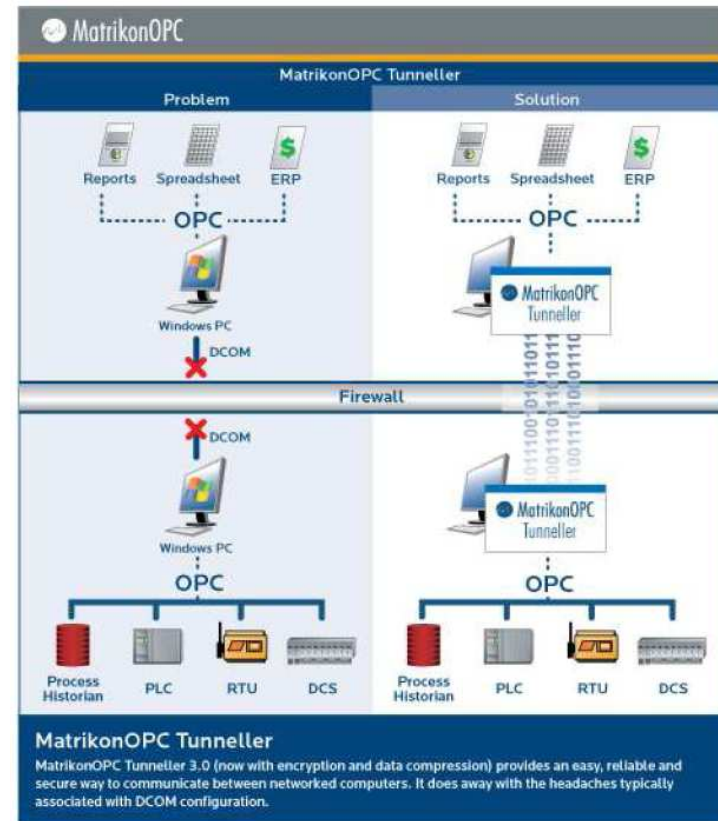
→ "Web services are attractive for smart grids, however not very suitable for time-critical use"



Challenges of OPC

- ❑ SCADA-related challenges
- ❑ Large-scale software maintenance
- ❑ Stability and security
- ❑ Integration to other systems

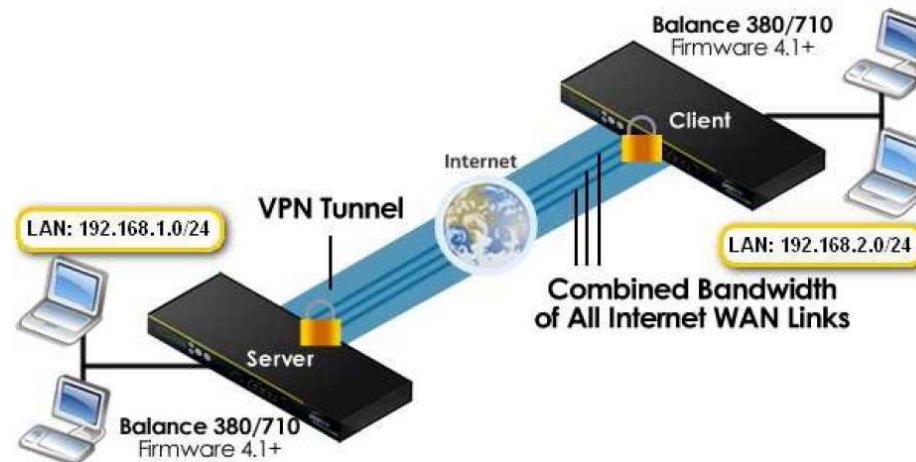
→ *”Stability, security and maintenance together with real-time performance”*





Challenges of VPN

- ❑ Security risks
- ❑ Tuning for time-critical situations
- ❑ Performance loss of the link

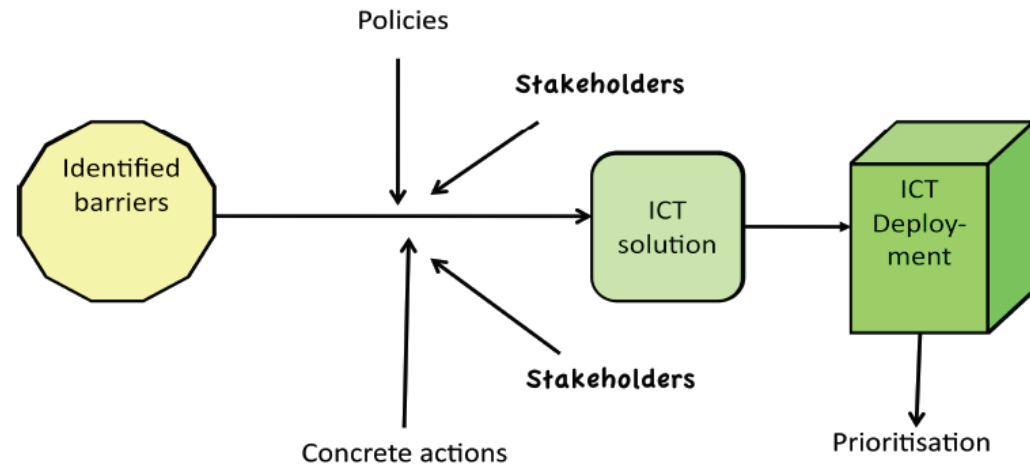


→ *“Proper use of VPN allows security and integrity”*



Possible solutions

- ❑ Relations between Barriers and Solutions
 - ❑ Policies – regulatory frameworks and policies
 - ❑ Concrete actions – actions initiated by stakeholders
 - ❑ ICT solutions
 - ❑ Category 1. Selected ICT Platforms based on smart grid pilots
 - ❑ Category 2. ICT platforms built from a suitable architecture
 - ❑ ICT Deployment





Possible solutions

- ❑ About the proposed ICT solutions
 - ❑ Purpose is to manage the information flows
 - ❑ Stakeholders are divided to two types:
 - ❑ High-level stakeholders – focus on business processes
 - ❑ Low-level stakeholders – focus on technical infrastructure
- ❑ ICT solutions can be classified:
 - ❑ For supporting business processes
 - ❑ For supporting technical processes
 - ❑ For supporting a mixture of business and technical processes

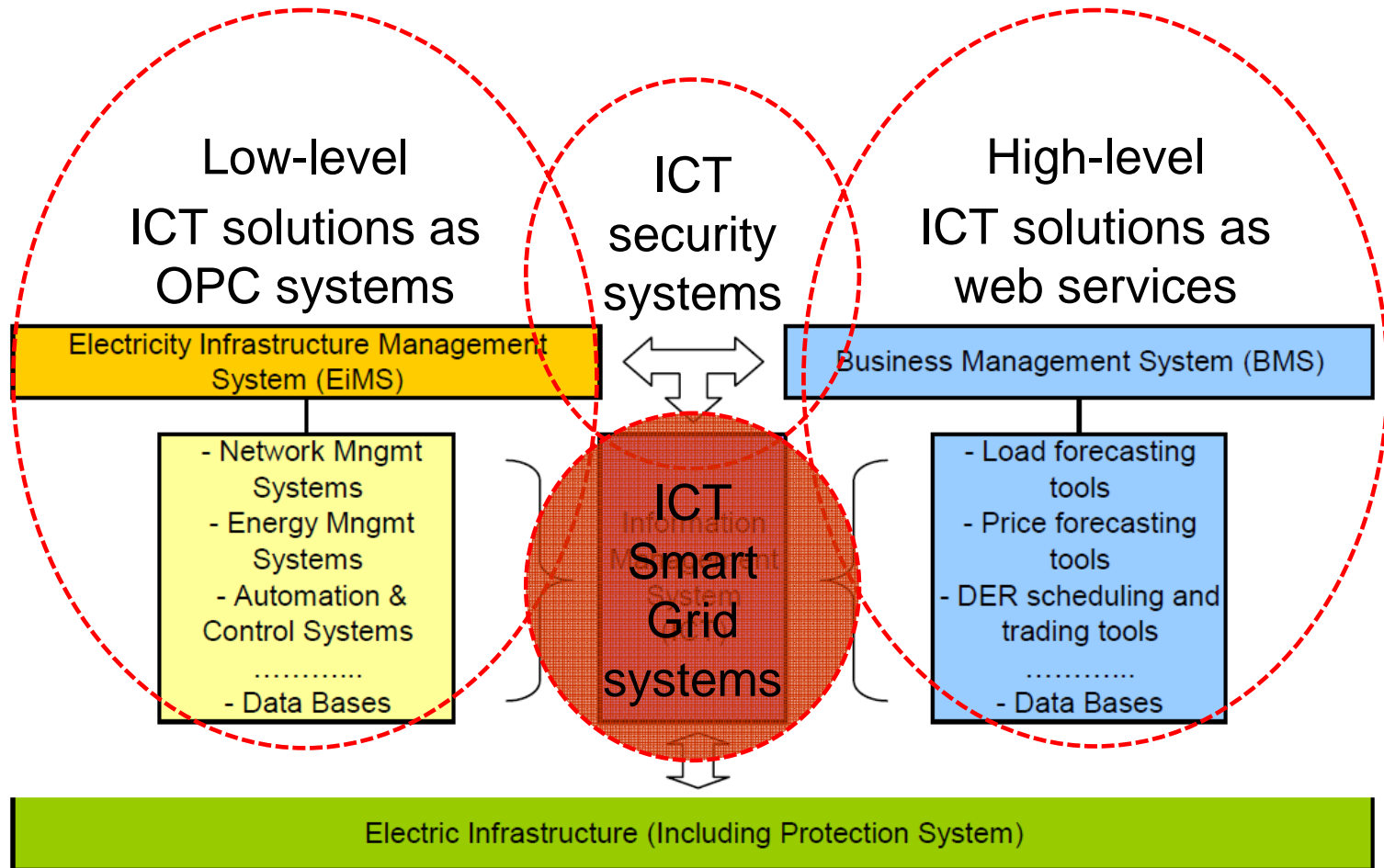


Possible solutions

- ICT solutions as web services
 - For high-level stakeholders
- ICT solutions as OPC systems
 - For low-level stakeholders
- ICT security systems
 - For instance VPN
- ICT smart grid systems
 - Considering both business cases and physical constraints
 - Forming bundles combining high-level stakeholders and low-level stakeholders
 - Aggregators are common stakeholders for the bundles



Possible solutions





Conclusions

□ Conclusions stated in report D3-3:

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 IEC 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.



Conclusions

- ❑ Main barrier is the lack of clear frameworks and regulations supporting business and technical processes
- ❑ Missing collection of experiences (for instance from pilots) is an important barrier
- ❑ A significant technical barrier is formed by different stakeholder's views on monitoring and controlling the smart grid processes
 - ❑ Service Level Agreements (SLAs) form a promising technology for this
- ❑ High expectations – but also challenges – towards smart grid implementations