SMART GRID / SMART METERING CONVERGENCE SOLUTIONS

SOLUȚII DE CONVERGENȚĂ ÎN DOMENIUL SMART GRID/SMART METERING

Gabriel GHEORGHE[1], Daniel CRĂCIUN[2]

Abstract: *The electricity distribution is facing fundamental changes at the network level as well as in the requirements of customers for increasingly high expectations in order to have a stable, secure and Cyber Security measures. Consideration must be given to the presence of the distributed energy sources as well as electro-mobility, each with their significant impact. There are several possible models of Smart Grid development that may represent the conceptual prototype of a future energy system. Creating the Smart Grid system is a complex task that involves a strategy with consistently pursued goals. The paper investigates the concepts that lead to the convergence of the specific solutions, such as SCADA/DMS, Smart Metering, ADMS, Cyber-Security, in order to optimize the integrated functioning of Smart Grids.*

Keywords: system, integration, standard, interoperability

Rezumat: *Sectorul distribuţiei de energie electrică se confruntă cu schimbări fundamentale sub aspectul reţelei precum şi cu modificări în privinţa cerinţelor clienţilor care au aşteptări din ce in ce mai ridicate pentru o funcţionare stabilă, sigură şi cu măsuri adecvate de Cyber Security. Trebuie să fie avută în vedere prezenţa surselor de energie distribuite ca şi a electro-mobilităţii care au, fiecare, un impact important. Există mai multe modele posibile de dezvoltare a reţelelor inteligente care pot reprezenta prototipul conceptual al viitorului sistem energetic. Realizarea unui sistem de tip Smart Grid este o sarcină complexă care presupune o strategie cu obiective urmărite cu consecvenţă. Articolul investighează conceptele ce conduc la convergenţa soluţiilor specifice, cum ar fi SCADA/DMS, smart-metering, ADMS, cyber-security, în scopul unei funcţionări integrate optime a reţelelor inteligente.*

Cuvinte cheie: sistem, integrare, standard, interoperabilitate

[1] Eng. PhD, Director of Engineering Department, SDEE Muntenia Nord, Romania, e-mail: gabriel.gheorghe@distributie-energie.ro
[2] Eng. PhD, SDEE Muntenia Nord, Romania, e-mail: daniel.craciun@distributie-energie.ro

1. Introduction. The need for convergence of solutions

The electricity distribution is facing fundamental changes at the network level as well as changes in the requirements of customers who have increasingly high expectations for a stable, secure and Cyber Security measures. Also, the presence in the grid of distributed energy sources, especially renewable, as well as the electro-mobility, which create an impact by changing power flows, from traditional unidirectional flows to bi-directional flows, must be taken into account. For this reason, the coordination of the protection systems of the medium and high voltage electrical network becomes a complex and difficult task. At the same time, there are important implications for ensuring the standardized of electricity quality parameters for all customers.

The benefits of Smart Grid are widely recognized today. The Smart Grid is capable of direct interaction and communication between consumers (households or businesses), other network users and distributors or energy providers. In combination with the differentiated tariffs per time zone, they offer for the first time the possibility of the consumers to directly control and manage their own structure of consumption, providing powerful incentives for the efficient use of energy. Better and more focused management of the networks increases their level of security and reduces maintenance costs [1].

Smart grids are considered to be the backbone of the future low carbon energy system. They will allow the integration of large quantities of energy from renewable sources, produced either on-shore or offshore, and the integration of electric vehicles, while maintaining the availability for the production of energy from conventional sources and the suitability for the distribution networks [2].

We can talk about specific challenges or requirements, such as:

- Increased consumer demand and regulatory requirements for ensuring the parameters of the performance standard, the quality of electricity, at all voltage levels;
- The need to reduce the technological own consumption, increase the energy efficiency and implement the policies to reduce the carbon footprint in the distribution networks;
- Increased electricity consumption especially for medium and low voltage levels;
- Aging of the existing infrastructure and the need for a comprehensive investment program;

- The need to integrate the renewable energy sources, the prosumers, in parallel with the energy supply required for electro-mobility and the development of Demand Response technologies;

- Creating the secure communication infrastructure and platform between the distribution operator and customers or other stakeholders;

Demand Response offers an opportunity to optimize the capacities and the generation regime, it can reduce the import of electricity at the peak, helping to stabilize the network and to significant revenues for the users participating in the energy market.

For these high complexity challenges, Smart Grid technologies are an important part of the solution. Of course, the aging of the existing infrastructure seems to be something different, but the new technology and development solutions must involve the vision for the future Smart Grid. This results in the first argument of the convergence of solutions, namely that complex or different needs should be dealt with a set of solutions that optimally and fully integrate the challenges and expectations of stakeholders. Different customers and the essential applications for the operation must be considered at this stage, to create the basic infrastructure. **The first stage of convergence (I)** of solutions is the conceptual one and must be designed.

In essence, it is necessary that the networks resulting from the implementation of the new solutions achieve three main objectives:

- High efficiency and loss reduction;
- Integration of a large share of renewable energy;
- Satisfying to the highest standards of very different consumers.

In order to achieve the stated objectives, convergent, standardized and interoperable solutions, regardless of the manufacturer / supplier, should preferably be addressed to the actual electrical infrastructure as well as to the communication and information infrastructure.

At the interface points with consumers or with the system operator, the electricity producers, Smart Grid operates with optimization applications, for example forecast for renewable energy and electric vehicles, Demand-Response or demand optimization, MDM (Metering Data Management), OMS (Outage Management Systems), GIS, Asset Management, etc. A new component added to the smart grid must have the possibility to integrate into the solutions and applications already created. We are talking about **the second stage of convergence (II)** of solutions, which refers to the interoperability and optimum efficiency after

commissioning and throughout the life of the equipment, respectively, of the intelligent solutions.

2. Development of the Smart Grid. The main functions and the strategy of implementation

Today's electricity distributors which are building on an existing network will have to follow the goal of an intelligent network (Smart Grid) by gradually integrating the necessary devices and functions, starting from a level of automation considered basic, pre-existing.

A description of the functions and applications resulting from the implementation of Smart Grids was presented in 2010 in the IEEE Power & Energy Magazine as a pyramid evolution by the well-known world expert PhD Hassan Farhangi [2]. Based on this Smart Grid general concept we configured an evolution presented in Figure 1. Maintaining the stability and availability of the electricity distribution service as well as the public safety of its own personnel is a fundamental responsibility of a public utility company. Existing networks, as well as the low degree of automation and visibility on some of these assets can create problems in exploiting them.

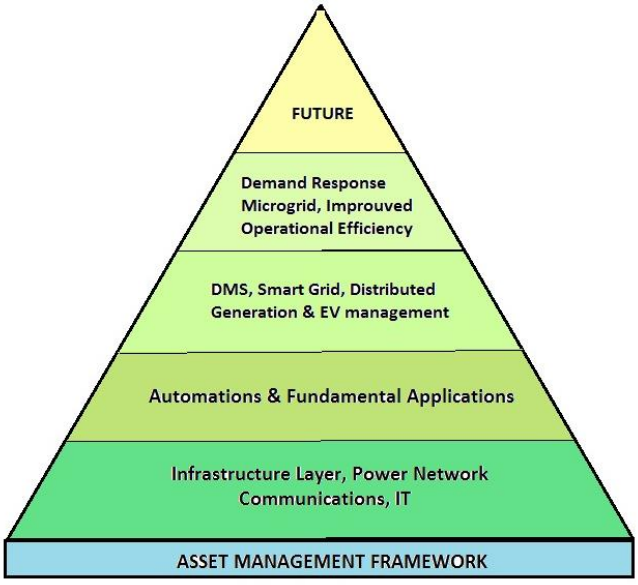

Figure 1. Smart Grid towards higher efficiency and integration of Distributed Generation

Customers are becoming increasingly demanding about the interruptions in electricity supply. In today's economy and the increasingly digital and interconnected lives, customers and the regulator are demanding compliance with a very severe standard regarding power outages. Switches in electricity supply, even small fluctuations, can create problems for a wide range of microprocessor controlled equipment, from personal computers connected to the internet to critical equipment such as assisted living in hospitals. More and more companies have computerized processes and a high degree of automation, even for short-term interruptions the control and automation systems can be blocked, considerable financial losses can occur at the level of those economic processes.

For all these reasons, it is necessary to adopt a holistic asset management strategy by using information from different systems and taking real-time information from the electricity network, using state-of-the-art technologies, coordinating the effort to reduce costs and disruptions. To ensure this integrated approach, the SDEE MN aims to develop existing SCADA / DMS systems and their automatic interconnection with all existing or future information systems. As the SCADA / DMS system monitors the basic activity of a distribution operator in real time, it is desired to consolidate this system with new information retrieval technologies and aggregate reporting capabilities together with financial systems, Metering (MDM), OMS, GIS.

By interconnecting Operation Technology systems (SCADA / DMS, OMS) with Information Technology systems (Financial, Reporting, etc.), the conditions for the realization of complex projects of Smart Grid, respectively, Demand Response, Peak Shifting, etc., are created... The complete automation of the transformation stations is a mandatory premise in order to ensure the visibility in the system and the control of the distribution network. The installed SCADA systems are in line with the international standards in the field: IEC 60870-5-104 for communications with the SCADA / DMS dispatcher and IEC 61850 for communications with the numerical protection relays. The architecture of the automation system at the SDEE MN level is shown in Figure 2, from [5].

The existence of 5 regional centers corresponding to the branches and a sixth center corresponding to the head office and the related branch (Ploiesti) are highlighted. There is also a backup server center and Disaster Recovery. The number of integrated online workstations is shown in the figure for each center. Through the routers using secure channels (VPN), both the branches and the stations integrated in SCADA and the intelligent equipment from the ADS (Automation Distribution Systems) application are made.

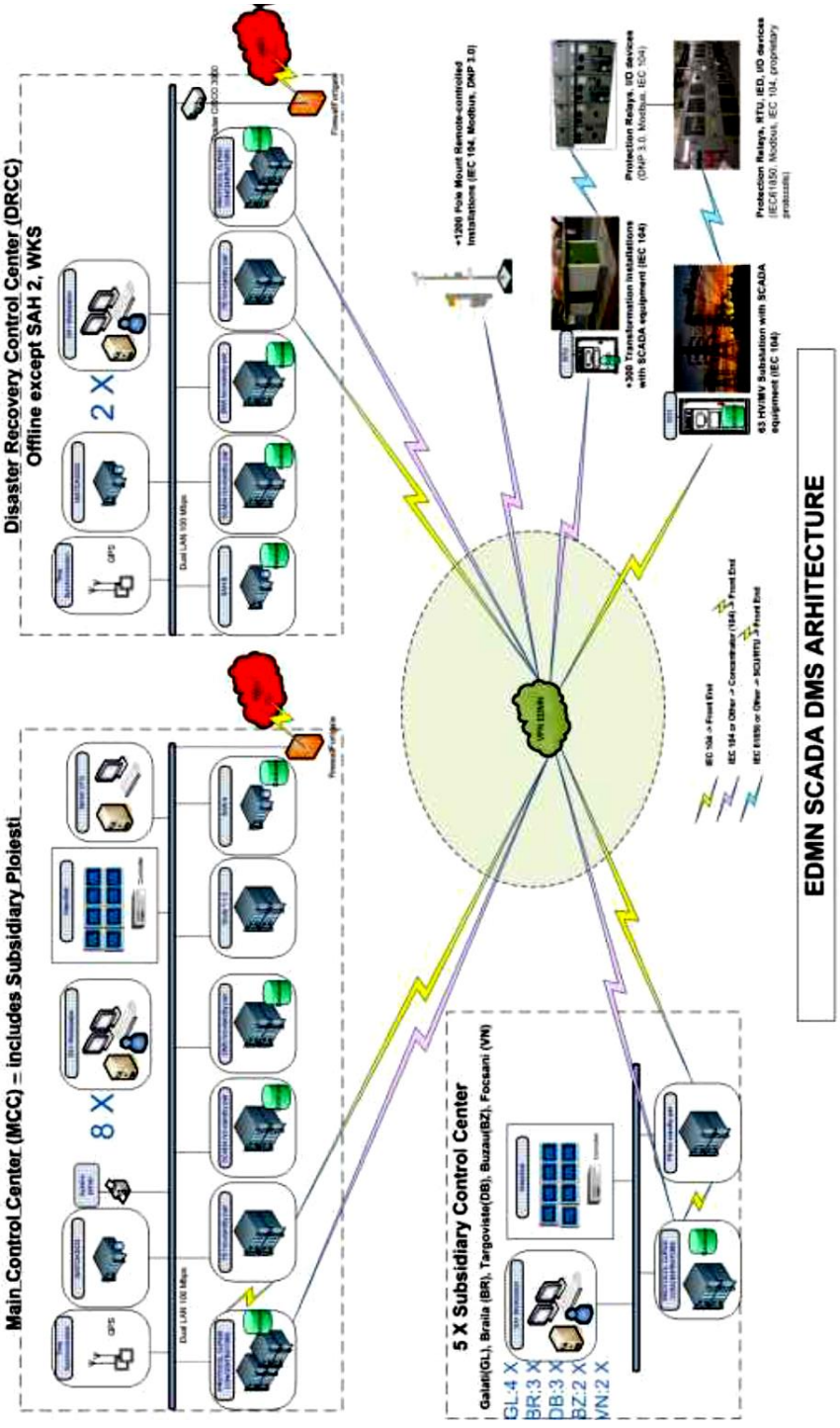

Figure 2. Configuration of SCADA/DMS, SDEE Muntenia Nord

The physical volume of integration into the electricity distribution network of SCADA and SAD systems is highlighted by the following representative figures:

- by 2020 the SCADA system is estimated to include 125 HV/MV stations and 1000 MV/LV substations and 2200 remote-controlled disconnectors, completely integrated;
- at present, the SCADA system includes approximatively 1500 switching equipments for HV/MV Stations, breakers and disconnectors, respectively, 1800 MV substations related equipment;
- The number of remote-controlled reclosers and disconnectors in the medium-voltage overhead network is 1900 at present.

In order to complete this process, must be considered SCADA systems which can offer the following functionalities:

• Distributed control and distributed data acquisition: As the evolution of SCADA systems over the past 12 years is considerable, SDMN aims to use SCADA systems based on distributed architectures (Substation Control Unit, Bay Control Unit, HMI, Disturbance Records Retrieval). Only state-of-the-art systems able for up-grading and reconfiguration over time will be considered.

• Performing distributed intelligent functions: Substation Control Unit type systems will be intelligent systems, capable of controlling regions within the transformation station area, being able to run distributed algorithms;

• Cyber security systems: the equipment provided must be in line with internationally defined cyber security standards, as well as the SCADA / DMS network specific standards.

Such applications require simultaneous information from different sources and require interoperability between all existing systems at the OD level. Starting from the level of automation achieved in recent years, SDEE MN has taken the necessary steps to implement a Smart Grid concept. By integrating the OMS and DMS modules, the advanced distribution management system, ADMS (Figure 3) will be created.

An Advanced Distribution Management System (ADMS) is the software platform which supports the complete suite of distribution management and optimization. ADMS includes functions that automate network restoration after outages and optimize distribution network performance. ADMS functions are developed specifically for utilities in the field of electricity and include fault localization, grid isolation and restoration; optimization (adjustment) of volt / volt-ampere reactive;

reducing losses by reducing voltage where possible; peak management; optimal treatment of micro-networks and energy demand in the field of electro-mobility.

The decision to implement ADMS is a strategic initiative that must be supported at the highest level within the organization and aligned with its long-term vision. We believe that the ADMS platform will fundamentally change the way the company operates, becoming necessary organizational changes and new skills of the employees. Of course, a cost-benefit analysis is needed, but there may be blessings that cannot be quantified at the initial moment, such as customer satisfaction [5].

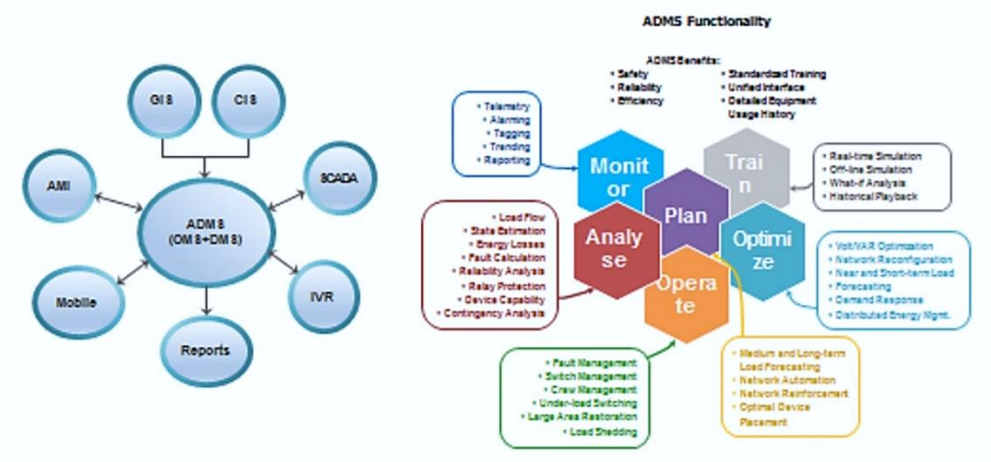

Figure 3. ADMS system and functionality

Developing ADMS solutions is a developing field that requires close collaboration between the IT solution provider and the company specialists, at a multi and multidisciplinary level. Integrating distinct activities, for decades, into a unitary platform will of course not be easy (Figure 4), from [5].

Figure 4. ADMS field

So we are talking about **another area of convergence in Smart Grid (the IIIrd)**, namely the software platform in which it will be necessary to integrate a whole series of activities and applications that may appear without a direct connection between them or have worked so far. Their unitary treatment is necessary in order to obtain the specific value of the unitary and complete processing of information.

3. Cyber Security of Smart Grid

The extended IT systems and solutions can also have a negative impact, namely that Cyber Security becomes a real problem that can be common to all companies in the energy industry. The companies in the field have realized that this must be a basic criterion to develop a stable system and able to handle the challenges of the future. Securing the SCADA network is a critical priority in the SDMN development strategy, so that existing systems will be upgraded to current security standards by adding a firewall, intrusion detection, access control, encryption, etc.. New installed applications and platforms will be provided since the installation with Cyber Security systems. As transformation substations represent critical nodes in the distribution system, the Cyber Security of the SCADA command and control system of the substation will be implemented as a core asset within SCADA. The development of the cyber security system will have to provide the following main functions, the list below being for the sake of clarification, within the specific documentation the necessary functions will be detailed:

• Encryption of data related to SCADA and other existing systems at the station level;

• Network segmentation to avoid generalization of a local security problem;

• Intrusion detection (IDS);

• SCADA traffic profiling and automatic alarm when the traffic exits from the predefined patterns;

• Firewall to properly block / restrict access.

Antivirus protection is required for SCADA related equipment (parameterization laptops, archiving systems, etc.). We consider that the approach of cyber security is a main criterion in the projects of automation and digitization of the energy network towards a Smart Grid type network. As cyber threats diversify, as the attack area grows by adding new smart devices to the network, utility companies must use the latest technologies

and methodologies to implement secure and robust architectures in Operational Technology type systems, OT, from SCADA / DMS. Without having a complete and unitary list of existing assets in SCADA/DMS systems and a permanent monitoring of them, it can be very difficult to establish the delimitation of the protected equipment, in order to apply the effective security policies in the SCADA integrated networks.

The inventory must contain:

• All SCADA components, including existing software;

• Network and telecommunication IT components (equipment, protocols);

• Dependencies between systems and applications participating in the automation processes and SCADA.

In order to incorporate cyber security into SCADA systems, it is imperative that computer protection areas around SCADA perimeters be developed. This requires a thorough understanding of telecommunications networks and the interdependencies between existing systems and processes, based on the operational requirements of operational processes. Understanding the nature of the information flows between all the components involved in SCADA/OT processes, establishing entry/exit points, ranking and structuring the communication protocols lay the basis for the correct definition of the cyber perimeter.

Compliance with best practices in the IT field as well as harmonization with industry-specific standards for industrial automation such as IEC 62443 is critical to strong Cyber Security.

At the company level it is made aware that cyber security must be considered a permanent process that requires continuous improvement and constant monitoring because:

• Every day new vulnerabilities are discovered;

• The threats are increasing;

• Staff may be inattentive or find solutions to bypass existing security measures;

• The weaknesses of the system are constantly changing according to the evolution of the attack technologies.

Within existing or future cyber security projects, the evaluation of measures will be considered based on at least the following standards: IEC 62243, NISTIR 7628, IEC 15408, IEC 19790 similar and with NIST FIPS 140-2 , IEC 19791, IEC 21827, IEC 17799, ISA S99 Standards, COBIT. In future projects from the design stages will be considered the organization of the network according to the references of the standard IEC 62243, the

international standard for "Industrial Networks and Systems Security" (Figure 5).

Business analysis processes require data processing from different systems quickly and efficiently. This premise introduces the need to connect data from traditional IT systems (ERP, CALL CENTER, etc.) with data from traditional OT systems (SCADA, CAPEX / OPEX, etc.).

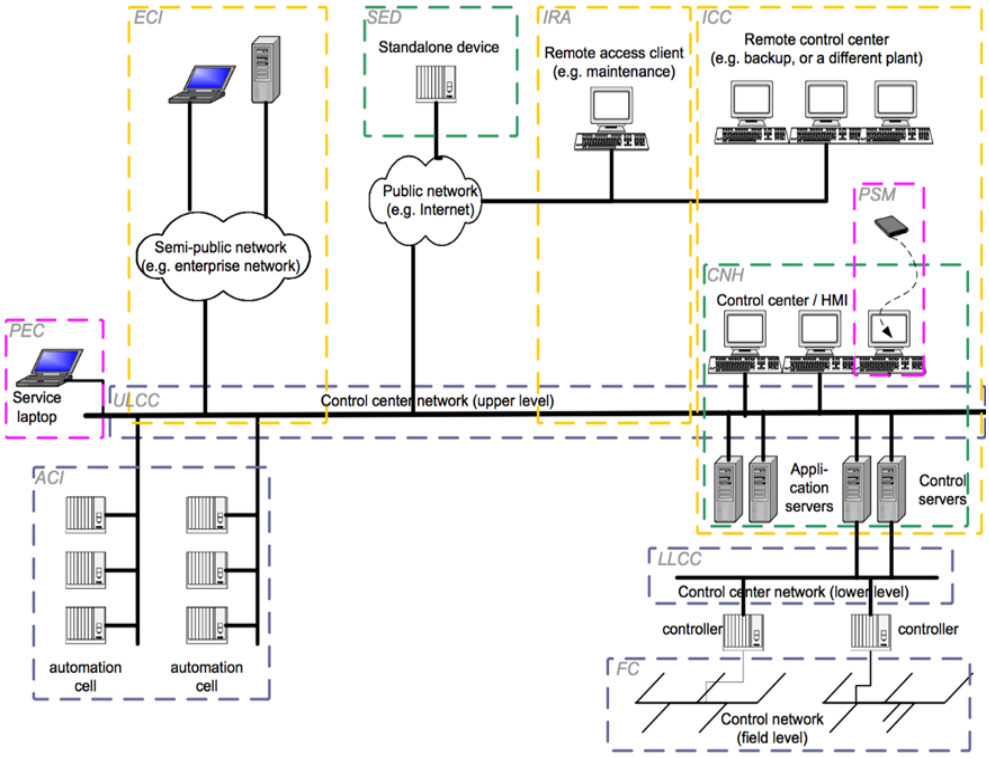

Figure 5. Standard reference model for Cyber Security implementation [16]

Where:
ECI - External network – Control Network Interconnection
IRA - Interactive Remote Access to a control network
ICC – inter-Control Center access to a shared control net
SED – Stand-alone Embedded Device
PEC – Portable Engineering Computer
PSM – Portable Storage medium
ACI – Inter-Area communication within a hierarchical multi-area control network
CCN –Control Center networks
FCN – Field Control Networks
CNH – Control Network Host
AFD - Automation Field Device

The logical reference model of the existing connections between the functional systems within the Smart Grid technologies, according to the American standard used intensively in the field, NISTIR 7628, is that of Figure 6.

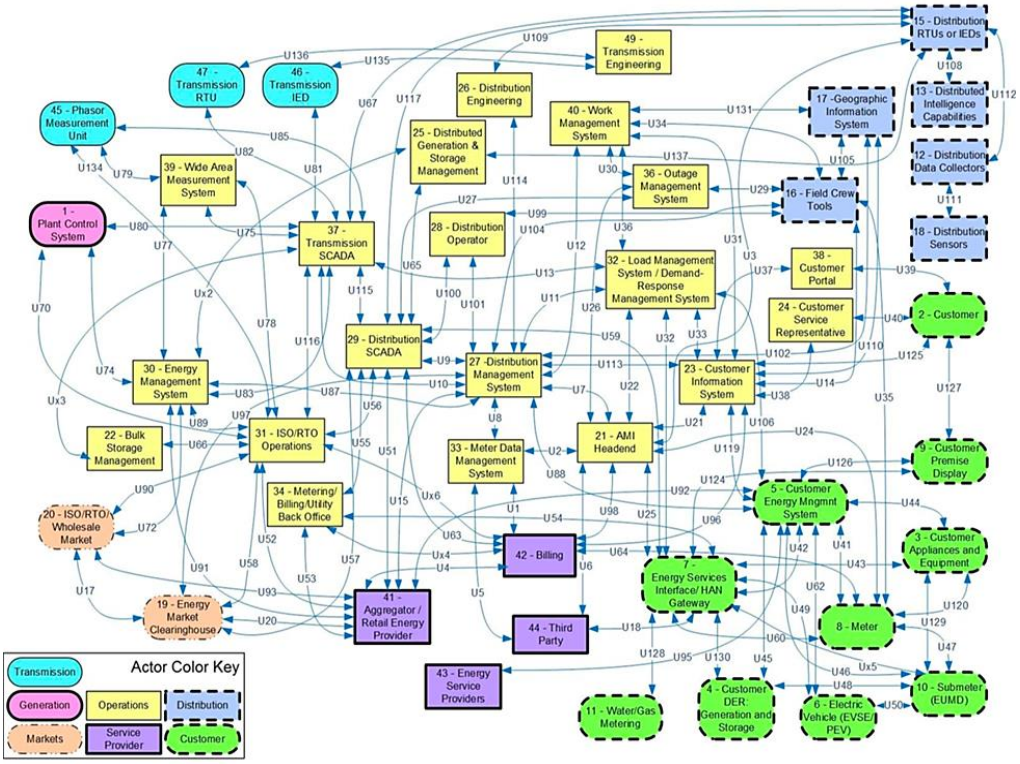

Figure 6. Interconnections map in the integrated informatic system standard NISTIR 7628 [16]

The map of interconnections and processes indicates that the field of operations has, of course, the most numerous and complex connections with the other processes. This results in the possibility of intrusion, respectively, of Cyber Security problems with consequence of the most serious. Any process, even a "marginal" one, can be a gateway for computer viruses, Cyber Security attacks. As you can see no system is no longer an "island", all represent a controlled information flow in order to be able to provide the information bases needed to build an intelligent network capable of managing the challenges of the future.

Due to the interconnected nature of Smart Grid networks, it is essential that Cyber Security measures implemented protect critical systems

from being infected by less critical systems. Physical access control is a necessary measure to reduce risks.

Cyber Security services, mechanisms and objects must be implemented in layers, with one or more security methods for each layer. The main objective of this approach is to reduce the impact when one of the protective layers or one of the methods did not work. This methodology is commonly known as "defense-in-depth". One conclusion of this paragraph is that standardized solutions and best practices must always be used at international level, to constantly evaluate the concrete risks and to design multilayered or in-depth defense systems, using established computer technologies (firewall, antivirus, access limitation, intrusion detection, password and codes). These measures should be taken at all stages of conception, realization, development (up-degrees).

4. Smart Metering systems

It is well known that by ANRE Regulation no. 177/2018 were approved the framework conditions for the realization of intelligent measurement systems at national level. According to this document, a strategy has been developed, aiming at the implementation of smart meters and, finally, the development of an advanced metering infrastructure (AMI). The development requirements of the Smar Metering systems are included in Order 177/2018 harmonized with the EU standards in the field. This development involves:

- Smart meters for consumers with the possibility of communication, bidirectional exchange of information, switching tariffs;
- Servers with data acquisition systems and concentrators;
- A fully automated process "from the meter to the billing", including the management of the data from the meters (MDMS) and the integration of the measurement systems in the solution of the metering and energy management at the branch level.

The duplex information flow provides consumers and utilities with data on the price of electricity and the achieved consumption, including the volume of energy consumed and the time it was consumed. This information as well as other possible applications ("smart" applications) will be part of the offer package addressed to a consumer integrated in the Smart Metering system.

A consumer who benefits from the smart metering system will first of all have a counter with the possibility of two-way communication, which

will allow tariff switching. He will be really involved and informed about the financial benefits he can have by actively participating in selecting the optimal tariff and establishing the level of electricity consumption of his home (Consumer Engagement). It will benefit from an advantageous package, "Time-of-use", TOU Pricing Programs, whose purpose is obviously to flatten the load curve. Internet payment tools, from the smartphone, are inherent, including information for the payments to which he is entitled, considering the quality of a prosumer. A whole series of controllers and sensors will adjust the home appliances in the home network (HAN Devices), power the car, etc.. A range of functionalities is required, involving the ability to collect, store, process and report energy consumption at hourly intervals, practically, in real time, detailed task profiles, time of use of pricing information, location identification, interruptions, disconnection and reconnection to distance, loss and theft detection, better collection of the price due for the consumed energy and invoicing of the actual electricity consumption. In this sense, the intelligent measuring devices, the digital meter, will be an equipment with functions and utilities that contribute to the optimal and complete monitoring of the requirements of the performance standard. Wireless or PLC systems can complement each other within the required level and volume of communications. The use of Cloud for data and application exchange is envisaged as an alternative to physical networks.

The interoperability aspects between systems and between providers are very important, this being one of the convergence levels pursued. An adequate dimensioning of HES for the number of consumers and the optimal data processing time, being other aspects of the chosen technology. It is necessary that the equipment integrated in the system comply with the measurement code [9] and the provisions of the IEC standards in the field, respectively: IEC 60050-300, IEC 61968-1 ÷ 11, IEC 61970-301, IEC 62051: 1999, IEC 62051-1 , IEC 62055-31, IEC 62056, current editions.

The data collected from the meters integrated in the SMI requires a software platform for data storage and processing (MDMS) designed to fulfill the following functionalities:

- Processing and storing validated and complete data for the billing interval ("Data Warehouse");
- Identification of events and transmission of information to the enterprise systems;
- Aggregation and / or transformation of measurement data into information for company systems, respectively, Network Planning, Task Forecasting, Customer Management, etc .;

- Unique interface for present and future AMI systems (planning, updating, number setting);
- Support for customer metering infrastructure;
- Analyzes meter reading data and identifies problems, supports AMI operations.

An important criterion is to ensure the interoperability of system devices, counters, data and device concentrators, auxiliary devices and equipment. Clear convergence criteria must be followed, one of them being interoperability by observing the open and harmonized standards valid at the present time. Considering that there are systems that come into direct contact with the client, also needs to be taken into account demanding requirements, at the level of current standards, cyber-security.

The Smart Metering system is, including through the related MDMS platform, a pillar of the smart grid, Smart Grid. From the outset, as we have already shown, a complex network with distributed generation (prosumers), electro-mobility, residential and tertiary area consumption is envisaged, as a typical case. The intelligent electricity measurement and metering system will benefit from the integration with the Demand Response type application at the company and network areas. The activities of measuring, monitoring the quality of electricity, forecasting, flattening the load curve, will be completed in order to optimize the decision levels, in order to reach the objectives and indicators. Intelligence metering with all the applications that can be integrated through this facility is also a way to increase energy efficiency, reduce the capacity and comply with the environmental objectives set by European directives. One of the most important developments expected from Smart Metering and Smart Grid systems is to empower "Empowering consumers". The center of gravity of the future network is moving to the consumer, who will benefit from such a series of advantages:

- The consumers will be able to have sufficient and timely information on energy consumption, to learn how to act for their own benefit for efficient consumption and lowering the electricity bill;
- Enabling consumers as active participants in the energy market through the use of new technologies will contribute to a paradigm shift in the functioning of the energy system as a whole;
- Smart Grid can be a useful tool for consumers to act more efficiently on energy demand, which can be part of a broader strategy to reduce carbon emissions related to electricity production;

- In order to be successful, it is necessary to develop Smart Grid communication infrastructure to enable consumers to exploit electricity prices in real time and to become more active players within the internal energy market;

- "Smart" tariffs must be introduced in such a way as to ensure that all consumers can benefit from reduced energy bills if their consumption pattern changes, and vulnerable people and low-income consumers are not adversely affected or disadvantaged;

- Smart Grid create benefits for energy companies in the form of reduced management costs through less meter readings and lower debt handling costs. Also it is estimated a more efficient functioning of the network and improvements on the line of management, the reduction of commercial losses;

- Consumer engagement and education is a key task in this process, as there will be fundamental changes in the retail energy market;

- In order to achieve the broader energy objectives, the efficiency and security of supply will require a significant change in the nature of the energy consumption of consumers (prosumers, electromobility);

- A central task will be the confidentiality and ownership of the data collected, related to consumers, through Smart Meters and Smart Grid. Consumers must feel and ensure that their identification and consumption data remain confidential;

- The consumer must have free access to his historical consumption data, in order to be able to maximize his commitment on the market and to make behavior change decisions. The lack of confidence or choice of consumers about the new systems will lead to the failure to realize all the potential benefits of Smart Metering and Smart Grid.

5. Conclusions

The realization of the Smart Grid system at the electricity distribution operator level is a complex task that involves a strategy with objectives pursued consistently. In a broad sense, such an objective changes the way of working in depth and the company culture. Among the overall objectives, the following can be stated:

• Accuracy, the rapid location of the affected network areas and the correct establishment of the nature of a defect;

• Mobility, adaptability and restoration of problems before they become serious;

• Optimal integration of electricity producers, prosumers, electro-mobility;

• Energy efficiency and cpt reduction;

• Real-time communication with customers and other market operators or stakeholders;

• Process optimization to use resources efficiently;

• Predictive treatment by adapting and correct monitoring of equipment status, rather than reactive, so that damage can be prevented and optimization of maintenance / investment ratio;

• Assets distributed and tracked in real time, regardless of geographical area or type of assets;

• Integration of information into centralized applications for efficient management, efficient use within the ADMS platform;

• Effective policies and practices in cybersecurity and against vandalism or other anti-social phenomena.

The criterion of interoperability and convergence must be clearly stated and followed during the design of the realization of the systems that will be subsequently integrated into unitary solutions of Smart Grid. Smart Grid will be crucial in moving to a low carbon economy. By implementing them and developing a market response in relation to the clients' requirement, it involves three fundamental actions:

I. The DO must be stimulated to invest in smart grids and to manage the grids smarter using modern optimization systems for all operations. The regulatory framework must provide economic incentives to invest in innovative solutions, such as smart meters, surveillance and control devices, network automation;

II. Developing a network model provided with a two-way communication interface with the customer, which will facilitate customer awareness and active participation in the retail electricity markets. Increasing customer power can be achieved through education, but also by significant incentives in case of adopting a new type of behavior, more active, in relation to the energy market;

III. Data security and computer networks, data protection of customers and all stakeholders is a point of convergence of the concerns in the field of Smart grid and Smart metering, as well as of the specialists in the IT and communications fields involved.

In this paper we focused on the principle of convergence, identifying three distinct and complementary stages:

1. **The first stage of convergence** is the design of the systems and applications part of SCADA / DMS, Smart Metering OMS, with their complete development towards ADMS;

2. **Here comes the second stage of convergence** of solutions, which refers to the interoperability and optimum efficiency after commissioning and throughout the life of the equipment, respectively, of the intelligent solutions;

3. **The third area of convergence in Smart Grid** will consist in the software platform in which it will be necessary to integrate a whole series of activities and applications that may appear without a direct connection between them or have worked so far. Their unitary treatment is necessary in order to obtain the specific value of the unitary and complete processing of information.

R E F E R E N C E S

[1] *D. J. Leeds*, „The Smart Grid In 2010: Market Segments, Applications And Industry Players", Greentech Media Inc., 2010;

[2] *H. Farhangi*, "The Path of the Smart Grid", IEEE Power & Energy Magazine, january/february 2010, pages 2-11;

[3] *Unnikrishnan Raveendran Nair*, "An evolution towards smart grids: the role of storage systems",http://www.incite-itn.eu/blog/an-evolution-towards-smart-grids-the-role-of-storage-systems/, bloog, November 2018.

[4] **** *EU - SC* „Task Force Smart Grids – vision and work programme", approved by the SC on 1st March 2010;

[5] *V. Brănescu, G. Gheorghe*, „Stage of Automation in DSO – Muntenia Nord & Perspectives 2019-2023", Conference CNR-CME, 15 martie 2019;

[6] *CEN-CENELEC-ETSI*, Smart Grid Reference Arhitecture, November 2012;

[7] *ABB white paper*, „Toward a Smarter Grid ABB's Vision for the Power System of the Future", Nov. 2009;

[8] *A.Wright, P.Kalv, R.Sibery*, „Interoperability and Security for Converged Smart Grid Networks", Grid-Interop Forum, 2010;

[9] *T. Phinney*, „IEC 32443: Industrial Network and System Security", Honeywell Integrated Security Technology Lab, 2019;

[10] *Siemens AG IC*, "MDM Presentation – COC MCS Europe" April 2012;

[11] *ANRE, Ordin 177/2018*, "Condiţiile-cadru pentru realizarea calendarului de implementare a sistemelor de măsurare inteligentă a energiei electrice la nivel naţional", Bucureşti 2018;

[12] *EPRI Technical Report*, „Program on Technology Innovation: Seamless Energy Management System Part I: Assessment of Energy Management Systems and Key Technological Requirements", EPRI Palo Alto, 2014, USA;

[13] *M. Castro, M. Sprawson, E. Meskhi, R. Burns*, "Modelling the DSO transition using the Smart Grid Architecture Model" EA Technology Limited, 19.07.2018, England;
[14] *CEN-CENELEC-ETSI*, "Smart Grid Coordination Group - Smart Grid Reference Architecture", Working Group M/490 mandate EU November 2012;
[15] *US Department of Energy*, "Insights into Advanced Distribution Management Systems", DOE/GO-OT-6A42-63689 February 2015;
[16] *NIST – National Institute of Standards and Technology*, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, http://dx.doi.org/10.6028/NIST.SP.1108r3, September 2014;
[17] *N. Silva*, "Smart Grid Solutions and current projects deployment: InovGrid Project", EFACEC Engenharia e Sistemas S.A., Bran, Romenia, 2 - 3 November 2010;
[18] *Siemens AG IC*, MDM General Presentation - COC MCS Europe, April 2012;