energies

MDPI

Article

Next Generation Real-Time Smart Meters for ICT Based Assessment of Grid Data Inconsistencies

Mihai Sanduleac [1,6,*], Gianluca Lipari [2], Antonello Monti [2], Artemis Voulkidis [3], Gianluca Zanetto [4], Antonello Corsi [5], Lucian Toma [6], Giampaolo Fiorentino [5] and Dumitru Federenciuc [7]

[1] Romanian Energy Center, 011838 Bucharest, Romania

[2] Rheinisch-Westfälische Technische Hochschule Aachen—RWTH, 52062 Aachen, Germany; glipari@eonerc.rwth-aachen.de (G.L.); amonti@eonerc.rwth-aachen.de (A.M.)

[3] Synelixis, GR-34100 Chalkida, Greece; voulkidis@synelixis.com

[4] R&D Department, Teamware, 20128 Milan, Italy; gianluca.zanetto@teamware.it

[5] Engineering Ingegneria Informatica S.p.A, Engineering, 00148 Rome, Italy; antonello.corsi@eng.it (A.C.); giampaolo.fiorentino@eng.it (G.F.)

[6] Department of Electrical Power Systems, University Politehnica of Bucharest, 060042 Bucharest, Romania; lucian.toma@upb.ro

[7] Department of Strategy, Electrica, 010621 Bucharest, Romania; dumitru.federenciuc@electrica.ro

* Correspondence: mihai.sanduleac@upb.ro or mihai.sanduleac@crenerg.org; Tel.: +40-722-315-123

Received: 25 May 2017; Accepted: 19 June 2017; Published: 27 June 2017

Abstract: The latest technological developments are challenging for finding new solutions to mitigate the massive integration of renewable-based electricity generation in the electrical networks and to support new and dynamic energy and ancillary services markets. Smart meters have become ubiquitous equipment in the low voltage grid, enabled by the decision made in many countries to support massive deployments. The smart meter is the only equipment mandatory to be mounted when supplying a grid connected user, as it primarily has the function to measure delivered and/or produced energy on its common coupling point with the network, as technical and legal support for billing. Active distribution networks need new functionalities, to cope with the bidirectional energy flow behaviour of the grid, and many smart grid requirements need to be implemented in the near future. However there is no real coupling between smart metering systems and smart grids, as there is not yet a synergy using the opportunity of the high deployment level in smart metering. The paper presents a new approach for managing the smart metering and smart grid orchestration by presenting a new general design based on an unbundled smart meter (USM) concept, labelled as next generation open real-time smart meters (NORM), for integrating the smart meter, phasor measurement unit (PMU) and cyber-security through an enhanced smart metering gateway (SMG). NORM is intended to be deployed everywhere at the prosumer's interface to the grid, as it is usually now done with the standard meter. Furthermore, rich data acquired from NORM is used to demonstrate the potential of assessing grid data inconsistencies at a higher level, as function to be deployed in distribution security monitoring centers, to address the higher level cyber-security threats, such as false data injections and to allow secure grid operations and complex market activities at the same time. The measures are considering only non-sensitive data from a privacy perspective, and is therefore able to be applied everywhere in the grid, down to the end-customer level, where a citizen's personal data protection is an important aspect.

Keywords: prosumer; smart meter; PMU; cyber-security; USM; smart grid; NORM

1. Introduction

Today electricity grids face multiple challenges due to high renewable penetration and to the dynamic evolution of the markets of energy and energy services. Some of the challenges related to renewables are: the stochastic behaviour of renewable energy production, the possible change of power flow direction in the distribution networks (initially designed to have only one-way power flow and a passive/loads only behaviour) or the production of energy in another period that is needed. These challenges are being widely considered in the scientific community and have been treated in many papers (e.g., [1–3]). Smart metering (SM) is the new technical solution for evolving markets and the smart grid is the new paradigm where the power network and its generic prosumers are highly linked by information and communication technologies (ICT) solutions, expecting to improve the overall network functionality. But at producer or consumer level, high levels of smart metering deployment do not highly support the emerging smart grid functionalities. It is a danger to have high deployments of SM and to simultaneously start introducing high numbers of equipment which helps the active distribution network, such as phasor measurement units (PMU) and grid automation.

Both smart metering and smart grids must also face cyber-security threats. Security aspects related to smart meters deployment have been analysed from different perspectives, e.g., by the authors of [4,5].

Today, state of the art smart meters are characterized by complex functionalities:

- Active and reactive energy measurement with metrology certification;
- Complex tariff implementations;
- Design based on communication with one important actor managing the billing data: DSO (distribution system operator)—as market facilitator in most EU countries, or the independent central hub—as third party market facilitator [6];
- The communication path is implemented in most cases through the PLC (power line carrier) and in some cases through GPRS (general packet radio service)/3G;
- Usual protocols for the data readout from smart meters are specialized for AMR/AMI (automatic meter reading/advanced metering infrastructure) data collection, e.g., DLMS/COSEM (device language message specification/companion specification for energy metering) protocol and its associated data model;
- Smart meters are able to provide, on request, instrumentation measurements at high reporting rates, between 1 and 10 s, as possible support for SCADA (supervisory control and data acquisition) functionalities. This instrumentation data (e.g., voltage u, current i, active power p, reactive power q) is not used at its full potential, for various reasons: the communication path is too slow, protocol is not appropriate for SCADA, etc.;
- load profiles (LP) of energy, instrumentation and of other data can be stored for medium to long periods, such as one month to several months, depending on the selected time period for LPs memorization;
- Some electrical energy smart meters have functionalities to collect data from other local meters: gas, water or heat meters; this architecture enables multi-utility/multi-service smart metering [7], allowing improvements in energy and market efficiency;
- Some electrical energy smart meters have a local interface to communicate with local devices and with end-users [8], thus enabling different services for final users.

An important step towards standardization has been made with the Open Meter project [9] which provided a comprehensive set of open and public standards for advanced metering infrastructure supporting multiple commodities (electricity, gas, water and heat).

For advancing towards a smart grid, and complex energy and energy services market, there are several aspects not implemented, or not well approached, in today's smart meters:

- Multi-user communication with the smart meter is usually not possible, because there is only one direct communication interface to remote users; thus, data availability is delayed through a trusted party (DSO or independent central hub) which collects meter data at regular intervals, such as each one day, or each six to one hour; the flexible data access point manager (DAM) approach is not applicable because the remote communication is used solely by the trusted party;
- Complex services using real-time (s) and/or near real-time (intra-hour) data cannot be used, due to low communication speed with the DSO, especially through the PLC technology;
- SCADA functionalities are not easily used by the DSO's dispatch centers because there is no real-time functional link between today's AMR/AMI systems and DSO SCADA systems. Moreover, the direct communication of the dispatch center's front-end cannot be made directly with the meter, due to protocol incompatibility (AMR protocols, such as DLMS, are different from SCADA protocols, such as IEC61850);
- There is no strong redundancy concept in the acquisition of data, in order to validate/invalidate acquired data at the meter level;
- Smart meter cyber-security strength is still not very high and smart meters are prone to direct cyber-threats;
- There is no holistic concept on the whole data chain in order to mitigate cyber-attacks, starting from the meter as the primary source of data;
- There is no functionality related to the integration of synchronous phase measurements (PMU), even if this becomes more and more important, especially in active distribution networks with high penetration of renewables. Different barriers regarding PMU large deployments are listed below;

  (a) Even by integrating the PMU similar to another "local meter", the PMU measurements are still difficult to introduce, due to difficulties in providing GPS synchronization, which need sky visibility;

  (b) PMU protocols are also different than SCADA protocols and there are difficulties with merging them, due to similar barriers as with meters: special acquisition and storing systems are specific to PMUs, which are different from the SCADA systems;

  (c) PMU data is much richer than meter data, allowing one to 50 measurements per second, thus having greater dynamics in comparison to the maximum energy meter reporting rate;

  (d) Regarding the collection of data from other local meters (gas, heat, water), there are still a limited number of meter types which can be accessed, for example, the "main" smart meter.

In can be observed that there is not yet ICT-enabled equipment to address, in a unified manner, the needs of smart metering, smart grids and advanced cyber-security. In general, it is missing a standardized way to link the customer in the system, and to unlock a two-way communication in order to be used for the large deployment of various services, in a flexible multi-user approach.

Our paper presents such solution, which is based on an unbundled architecture with three basic modules: (a) a metrology meter, (b) a low cost PMU and (c) a smart meter gateway, addressing the following three important aspects:

- Metering, in a multi-purpose approach;
- PMU measurements, for addressing smart grid aspects in active networks and;
- Cyber-security, as the "killing factor" for both the above aspects, if the system is not properly implemented.

Each of the basic measurement equipment (metrology meter and PMU) are not traditionally integrated. An important step has been made by the authors of [10], where the unbundled functionality had integrated a metrology meter labelled as "smart metrology meter" (SMM) in a multi-actor environment by using a "smart meter extension" (SMX). Authors involved in the project published papers showing different functional applications enabled by such a simple but versatile architecture [11,12].

In study [13] the unbundled smart meter (USM) concept was further extended and another important equipment was integrated, a low cost PMU, connected together with the SMM to an enhanced extension named "smart meter gateway" (SMG).

The data and its use for different functionalities specific to smart metering and to the smart grid is now collected and processed in the SMG, thus allowing synergies, complementarity and redundancy, for a robust acquisition and processing, at the level of the prosumer connection point to the active distributed grid.

The new architecture is labelled as "NORM" (next generation open real time smart meter). The NORM (Figure 1) goes beyond the tradition idea of a meter and proposes an open architecture where various services can be deployed. As a reference example, the implementation of a low cost PMU is proposed. This case is particularly significant because it shows that, thanks to this architecture, it is also possible for the final user to offer services and not only to buy them. This is a very important requisite to creating an open market of services, giving all the stakeholders the possibility to play any role, depending on the business model.

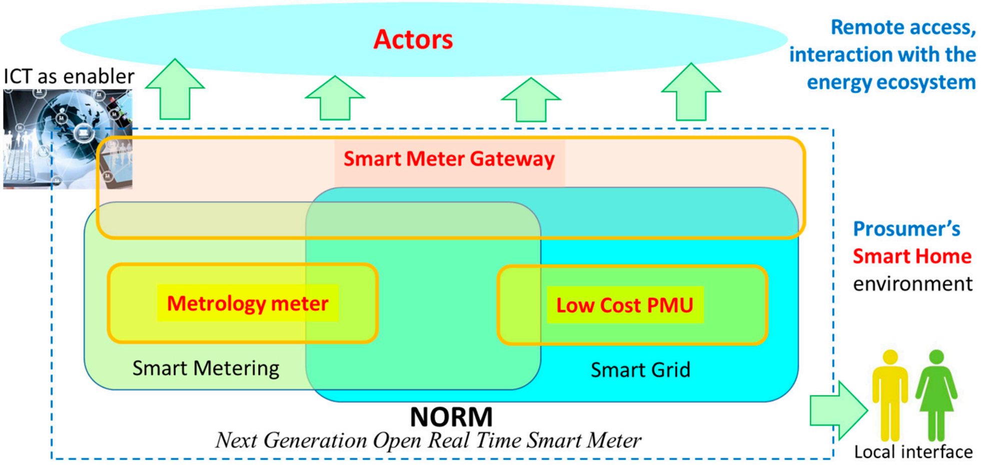
Actors
Remote access, interaction with the energy ecosystem
ICT as enabler
Smart Meter Gateway
Prosumer's Smart Home environment
Metrology meter
Low Cost PMU
Smart Metering
Smart Grid
NORM
Next Generation Open Real Time Smart Meter
Local interface

Figure 1. Architecture for serving both smart metering and smart grid functionalities.

Figure 1 shows also how overlapping functionalities between smart metering and smart grid paradigms are aggregated at the level of the smart meter gateway, with multiple benefits due to the potential interaction with all the stakeholders (DSO, supplier, producer, consumer, prosumer, aggregator, energy service company (ESCO), etc.) which are active in one or both domains (smart metering and smart grid), through a unified and secure multi-user/multi-protocol interaction.

2. NORM Architecture and Basic Functions

2.1. Basic Architecture for Integrating Meters, PMU and Advanced Security

As briefly presented before, NORM implements an advanced architecture of the unbundled smart meter (USM) concept, first presented in study [14] and developed in study [10], where SMM and SMX adequately split the overall Smart meter functionality in order to enable high flexibility by preserving legally relevant and secured data for billing purposes. The solution has been improved by adding a second module to cover a hard real-time zone, a low cost phase measurement unit (PMU) which adds important smart grid features, allowing the smart meter to provide frequency and voltage angles at accuracy rates higher than that of the traditional energy meter.

The NORM basic architecture is presented in Figure 2. The three unbundled parts are the SMM, the low cost PMU—which a new part compared with first USM architecture and the SMG, which is an evolution of the initial SMX.

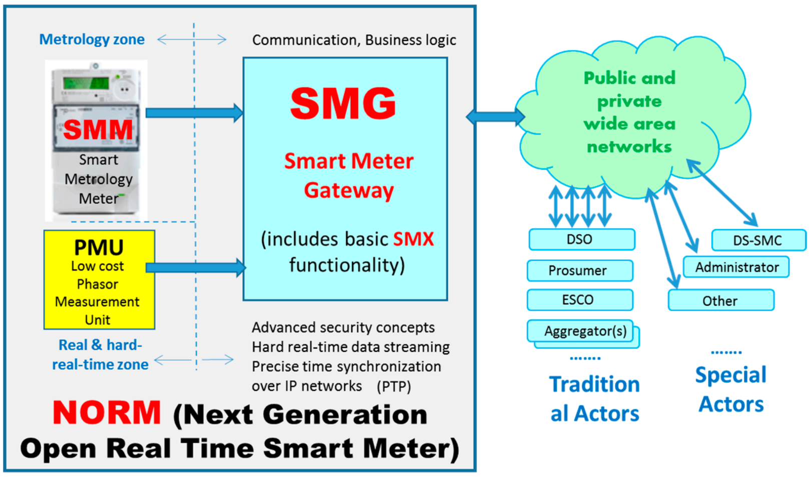
Metrology zone
Communication, Business logic
SMM
Smart Metrology Meter
SMG
Smart Meter Gateway
(includes basic SMX functionality)
PMU
Low cost Phasor Measurement Unit
Real & hard-real-time zone
Advanced security concepts
Hard real-time data streaming
Precise time synchronization over IP networks (PTP)
NORM (Next Generation Open Real Time Smart Meter)
Public and private wide area networks
DSO
Prosumer
ESCO
Aggregator(s)
....
Tradition al Actors
DS-SMC
Administrator
Other
....
Special Actors

Figure 2. Next generation open real-time smart meter (NORM) basic architecture.

The NORM connectivity to different actors is based on ubiquitous IP (internet protocol) based communication (public or private networks), which can embrace different technologies. This approach is in line with the efforts for digitalisation of activities and with the Internet of Things (IoT) concepts and E-society vision. This is an important aspect for unleashing the flexible participation of all interested actors through direct connection to NORM, for exchanging appropriate data for each type of service.

The SMM block acts as a black-block module embedding all the strictly related metrology functionalities involving hard real-time computations in order to provide both billing information and other interesting power grid quantities (voltage levels, frequency, vectors angle, power quality indicators) to the smart meter gateway over a dedicated and secured link.

Further processing of measured data as well as access rules to these data, which may involve privacy issues, are managed directly by the SMG, which implements (or may implement with future upgrades) most of the commonly used metering communication protocols (e.g., DLMS/COSEM, Modbus, etc.) or can act as client to access the APIs (application programming interface e.g., REST—representational state transfer) exposed by the SMM, granting a wide choice of meter devices, without requiring the adoption of specific models only.

The advantage of the unbundled design is that the basic metering functions, which are expected to be intrinsically stable as they refer to quite consolidated processing techniques and are subjected to third parts approvals and calibrations, does not limit the possibility to expand/evolve the business logic and the intelligence (e.g., role based access control) provided by the SMG, as smart grid actors increasingly require. Moreover, the NORM's additional PMU functionality adds value to the SMG functionality, allowing for additional features, which would enable smart grid functionalities for active distribution networks, as most of today's consumers will become prosumers.

2.2. Integration of Low Cost PMU in NORM

The PTP (precision time protocol) module is able to synchronize the CPU time base at much higher accuracy rates than the NTP does. It refers to IEEE 1588-2008 standard [15]. Even in its best condition, PTP can provide under-microsecond synchronization (expected to be in the order of 100 ns), whereas the real situation depends on both the network situation and on the local machines to be synchronized. In the NORM implementation a Raspberry Pi3 Linux machine is used, subject to being connected to various IP-networks. It is worth noting that NORM-SMG is a concept which is not solely Raspberry-based, but the same design and principles can be ported with the same software on other CPU/SOM (central processing unit/system on module) having more hardware resources (e.g., the Beagle Bone Black, or i.MX7 dual core A7) where hardware timestamping is available, taking full advantage of PTP. The fact that it has been adopted and tested already on the Raspberry Pi platform is for the sake of practice, due to the wide diffusion of that board and rich ecosystem of hardware and software related solutions, but it is not a mandatory requirement. Moreover, PTP has also been selected for the flexibility given by the concept of profiles, to specify combinations of options and attribute values to support a given application. A network infrastructure able to transfer the IEEE 1588 protocol will be also necessary for this new approach. Using PTP based synchronisation gives a big advantage for the NORM's PMU, because it avoids the necessity of a GPS device for each PMU, thus allowing for widespread and cost effective deployment of PMU functionality inside the proposed meter architecture, in the paradigm of active distribution networks, specific to high penetration of renewable energy resources, to support new smart grid requirements.

The basic principle of PTP is similar to NTP (network time protocol) protocol, where computers and other devices that have a clock are connected in a network and form a hierarchy of time sources in which time is distributed from top to bottom. The devices on top are normally synchronized to a reference time source (e.g., a timing signal from a GPS receiver). Devices "below" periodically exchange timestamps with their time sources in order to measure the offset of their clocks. The clocks are continuously adjusted to correct for random variations in their rate (due to effects like thermal changes) and to minimize the observed offset.

A realistic target is to have a synchronization between 10 to 100 μs, while our current tests show that this level of accuracy can be obtained in case of cabled ethernet and ptp4l driver, which allows for the execution of the PTP algorithm in the kernel space of the Linux machine. With this approach, such a synchronization can be made with a precise master time server connected in the same cabled local area network, the only one to be synchronized with classic GPS, while NORMs are synchronized with PTP. Future tests will be made for assessing the synchronization accuracy using less predictable networks, such as different wireless networks. This analysis is the subject of future work.

The PTP module in NORM features a single PTP port in the domain of the master clock and maintains the timescale used in the application. Furthermore, a built-in feature provided by the PTP module is a PPS (pulses per second) generation on a GPIO (general-purpose input/output), in order to provide a test point and a synchronization trigger source for the low cost PMU analogue-to-digital converters. Even in absence of hardware timestamping (as it is in the Raspberry Pi case), it is possible to mitigate the jitter of resulting instantaneous offset from the master clock by adopting a more "robust" digital filter (higher time constants and order filter), in the controller that mediates the tick rate adjustment. This increased stability will be obtained at the cost of a slower convergence, but in the context of PMU application it is acceptable. Under those conditions, the final target is to keep the overall uncertainty below 20–30 μs.

Other structures and algorithms are possible as well and are not excluded from the vision of NORM, which is enough flexible to allow for different upgrades on both synchronisation and PMU algorithms.

The phasor calculation algorithm uses both the PPS signal and the PTP time reference for synchronizing the data acquisition and timestamping the calculated phasors. The PPS is used to trigger the data acquisition board: when the pulse is received when the acquisition starts and samples are recorded at the desired sampling rate. The maximum sampling rate may vary, depending on the configuration and the number of signals acquired, between 100 kS/s and 12.5 kS/s, respectively for a single channel (e.g., single voltage acquired) and eight channels (e.g., four voltages and four currents).

The data acquisition and phasor calculation require one second to be performed. Data are collected for 880 ms from the data acquisition board, then they are transferred to a Raspberry PI, which performs the actual phasor, frequency and the rate of change of frequency (ROCOF) calculation in the remaining 120 ms of the one second window. The obtained results are then published following the IEC 61850 sampled values protocol (Figure 3).

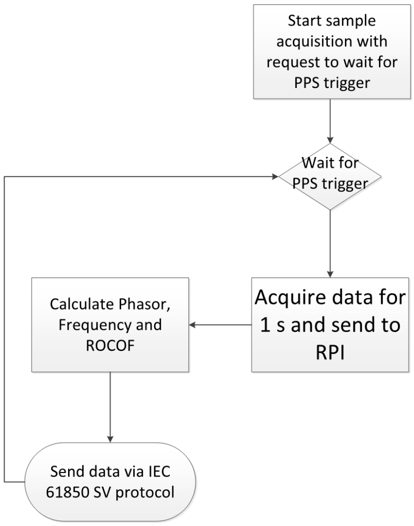
Start sample acquisition with request to wait for PPS trigger
Wait for PPS trigger
Acquire data for 1 s and send to RPI
Calculate Phasor, Frequency and ROCOF
Send data via IEC 61850 SV protocol

Figure 3. Low cost phasor measurement unit (PMU) data flow.

The first step of the phasor calculation algorithm is the application of a flat top window to the acquired data, in order to filter data and reduce errors induced by spectral leakage. Then a discrete Fourier transform (DFT) is performed on the filtered data, thus obtaining amplitude and phase values of the desired signal. For frequency calculation, a zero-crossing algorithm is applied to the acquired data and frequency is calculated for each period. The mean value of all calculated frequencies is the value published as representative of the whole acquisition window, while the ROCOF is the difference between the frequency obtained for the first period and that obtained for the last period of the acquired data.

The presented implementation of the low cost PMU could be modified or further developed, both from a hardware and software point of view in order to improve performances or reduce total costs. For example different acquisition hardware could be used, like DSP (digital signal processing) based acquisition boards, or the processing unit could be implemented on different low cost boards, e.g., the Beagle Bone Black board [16]. On the other hand different algorithms could be used for windowing or phasor calculation and in general software, implementation could be different.

However, this well fits in the NORM vision and unbundled design, since it is not closely tied to a specific implementation or hardware product.

2.3. Higher Security through Advanced PUF (Physical Unclonable Functions) and Critical Data Monitoring

Although NORM can operate in a standalone way, able to provide multi-dimensional, localized information related to the prosumer energy consumption/production and smart grid status to various designated actors, its utility from a security standpoint is maximized when cooperating with relevant cloud-based services that combine information from multiple NORM devices and perform various stream and batch data-oriented analytics to identify any threats at NORM or aggregate smart grid level.

To communicate with these cloud-based services, hosted under the premises of a DSO and summarized as Distribution Service Operator Security Monitoring Center (DSO-SMC), an active communication link should be opened between a NORM and the latter. To this end, guaranteeing the security of the relevant communication link is extremely important in order to ensure that data manipulation or overhearing is not possible.

As depicted in Figure 4, NORM incorporates two distinct security layers to assure secure communication with the DSO-SMC, the first one being based on standard channel encryption techniques and the second one being based on hardware cryptographic operations. Such a higher security level is needed for the DSO-SMC and the administrator, as they have access to the trusted zone of SMG (core part, access to system resources), where actions need the most trust. Other actors (e.g., actor 1 and 2 in the Figure 4) connect to sandboxed zones (Docker containers [17]) of the SMG and not to the core part, allowing for a standard security level for communication.

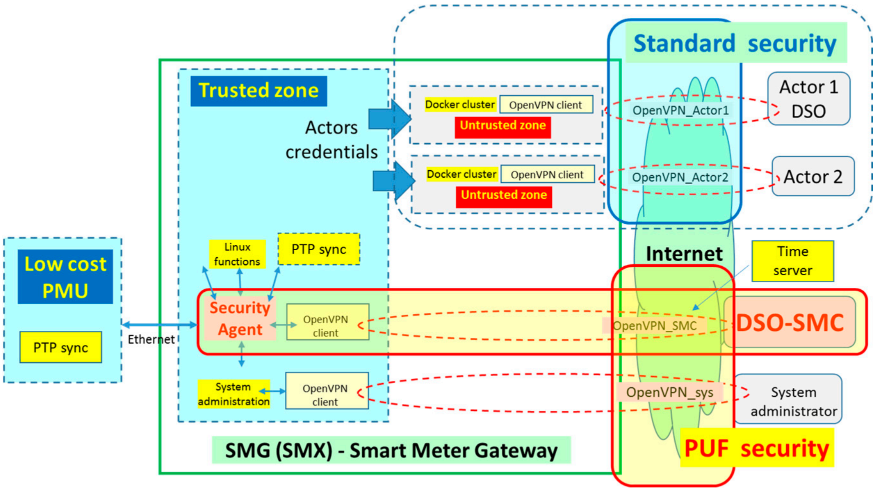

Figure 4. Security concept in an information and communication technology (ICT)-based smart metering/smart grid domain.

Regarding channel encryption, a VPN (virtual private network) connection [18] will be considered, following the current industrial trends as set by leading companies ([19,20]).

The next security layer considered in the context of NORM, is a hardware-based one, based on physical unclonable functions (PUFs) [21] implemented on an FPGA (field-programmable gate array) board. Hardware-based security is employed, used for purposes of authentication and encryption at data messages level. Formally, a PUF may be considered as a black box which provides a seemingly random output r (called "response") to any given input c (called "challenge"), $r = f(c)$, where f represents the hardware function implemented by the PUF, namely the input/output relation. Since function f is, by definition, related to the hardware construction micro-characteristics and is not controllable during the manufacturing procedure [22], it is theoretically impossible to clone it, hence the hardware function is considered unclonable. In the same framework, the response of the same PUF to the same challenge should be always the same. Moreover, to avoid the possibility of extracting a challenge–response pair and limit the chances of modelling the PUF (hence implicitly extracting the behaviour of f e.g., through machine learning [23]), a strong PUF [24] implementation has been considered.

NORM exploits the unclonable character of PUFs, basing the NORM authentication on continuous challenge–response exchanges between the NORM and the DSO-SMC, the latter ensuring consistency between a reported challenge–response pair and an expected one. Lastly, hardware-based encryption at the level of the data chunk is achieved by means of implementing AES (advanced encryption standard) on top of the FPGA architecture and using the response of the PUF to the currently active challenge as an encryption key. The encrypted data chunks are then sent to the DSO-SMC through the VPN-encrypted channel, implementing the aforementioned two-level security approach.

2.4. NORM's SMG Compared with the German Smart Meter Gateway

As already presented, NORM has a smart meter gateway (NORM-SMG) which has similarities with the German model of smart meter gateway (SMGW).

The most important similarity is related to the data management model regarding smart grid data [6]. The DSO as market facilitator and the independent central data hub as third party market facilitator, have been already presented as de facto implementations in most of the European countries. There is a third model, which is the data access point manager (DAM), supported by both NORM and German SMG. DAM is the most complex but also the most promising model in terms of flexibility.

In study [6] it is staged as motivation that: "smart grids and smart grid consumer oriented programs in particular, require the cooperation and coordination of the entire energy value chain. Any regulatory initiative looking to actualize the smart grid in a manner serving consumers will be required to take this fact into consideration. This entails creating a holistic view of the smart grid's regulatory principles with the particular focus on developing a framework to manage the generation-, storage- and consumption-resources which in most cases will be owned or operated by private sector third parties (citizens or legal entities)"... "Another area, in which predicting the actors and service requirements is even more difficult, are all types of solutions supporting demand response."

NORM is flexible and able to implement SMGW functionality. Below are highlighted some important aspects related to SMGW and NORM-SMG:

- SMGW is an independent device which implements a special network only for metering devices—all of them being similar in importance and having metrology enforcement, including the electricity smart meter, and an another one for the home area network; NORM-SMG is a Linux machine versatile to implement similar networks, with strong logical separation through ICT means; however, it has a specific and direct connection with the metrology electricity meter, because this meter has also the most demanding/smart grid related functionalities, thus being able to access real-time data with high efficiency;
- SMGW allows for multi-user access to the user's data, which is similar to NORM-SMG. The flexibility of NORM goes beyond this by implementing a variety of communication protocols, to allow for direct connection of actors based on their usual protocols, such as IEC61850 for smart grid/SCADA.
- SMGW allows a data manager (named gateway administrator) to adjust a so-called protection profile (PP). NORM-SMG is using a similar privacy profile, allowing different data exchange with each actor, based on two components, country-specific and user-specific PP, to combine mandatory regulations with user options. There is more flexibility in administrating data through this double PP. It is not the intention of this paper to enter more in these aspects in detail;
- SMGW has a security module to implement cyber-security credentials; NORM-SMG is advancing with its PUF approach, thus bringing additional flexibility and enhanced cyber-security.
- NORM integrates an essential additional device: the low cost PMU, which is also directly connected to the SMG, allowing high speed data access and precise time synchronisation. Even if SMGW can access through the local metrology network to access new devices, the real-time requirements may be difficult if not impossible to be implemented in this framework.

As a conclusion, SMGW functionalities can be implemented with NORM-SMG, while adding additional functions to support smart grid evolution.

3. Assessing Grid Data Inconsistencies through ICT by Using NORM Data in Real Environment

The demonstration of NORM functionalities is already in progress and particular test cases are already analysed. In order to analyse grid data inconsistencies, this paper presents some of the results, showing the correlation of data acquired from different places of the same neighbourhood grid. The examples below show generic applications for targeting grid data inconsistencies which are enabled by NORM, a complete solution being more complex and not the subject of this paper. The tests have already been done in specific places from Italy and Romania.

The main threats are related to cyber-penetration at the level of the smart meter (in our case NORM) which may bring manipulation of the grid data through false data injection at the lowest acquisition level. Wrong data acquired from the meters can affect several functionalities at the grid control level, which can threaten major functionalities such as grid stability, power quality, e.g., voltage levels as well as microgrid functionalities, thus needing detection in order to apply countermeasures.

The presented cases deals with grid data inconsistency (data sets which are not consistent with the normal grid behaviour) by acquiring, as real-time data, the frequency and voltage level over different points of the network. Using real-time data of smart meters has also been reported in other works [8]. A framework for identifying multiple power line outages based on the PMUs' measurements in the presence of bad data is presented in study [25]. Observing consumers' energy usage pattern and exploiting this information to assist the grid in improving energy supply stability is analysed in study [26]. In study [27] the authors analysed the detection of tolerable false data injection in smart grids based on knowledge of the grid by decomposing it in several subsystems. A vulnerability analysis of cyber-physical power systems based on power flow and grid topology is also analysed in study [28].

In our approach, in order to avoid barriers due to increasingly high privacy requirements in EU legislation, we are intentionally focusing the assessment on data which has no private aspects, meaning data related to grid, such as voltage level and voltage phases obtained from PMUs and grid frequency are part of a privacy by design approach.

While voltage may differ between metering points, frequency in the same area should have a very good similarity, forming a dataset which needs to be consistent. NORM acquires from the meter part the most important real-time data, which is available on the communication interface. An example of data acquired from a metering point in Italy is given in Figure 5, based on a market available SMM implementation [29]. Records can be made every 1 to 10 s. In Figure 5 the acquisition had a period of 5 s, which has also been used in the next examples.

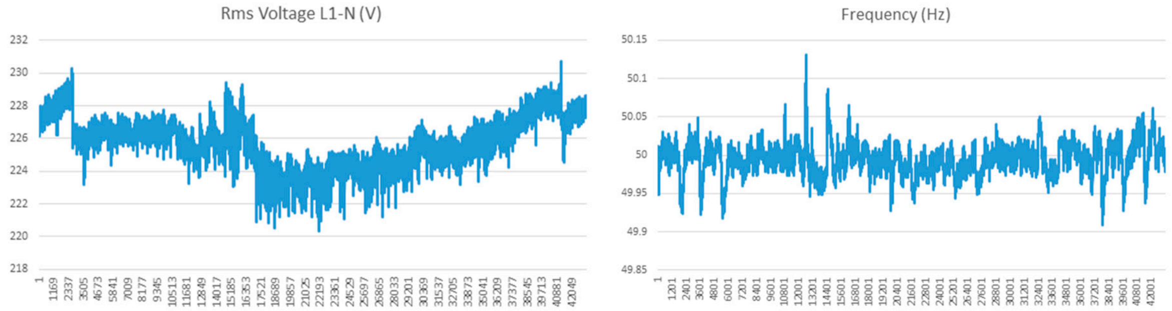

Figure 5. Voltage and frequency records in NORM's smart metering gateway (SMG), based on metering data from Italy.

As NORMs are synchronized in time, consistency of the same type of data can be checked at higher levels, thus allowing a consistency in the monitoring level, which is useful for a DSO-based functionality to detect cyber-security threats.

3.1. Grid Data Inconsistencies through Frequency Analysis

The first studied case is the correlation of frequencies measured by NORM in different network places. Frequency has practically the same value in a synchronous connected network, thus being a good "sentinel" for validating data coming from different NORMs, by analysing its small dispersal over the grid. A certain number of grouped frequency values may also show the case of a microgrid working in off-grid mode (different frequency evolution in the microgrid compared with the one in the main grid), which may be also correlated with the microgrid supply point breaker position for the same reason, as a way to detect inconsistency due to data manipulation somewhere in the ICT system.

Figure 6 shows experimental measurements of frequency acquired by the meters of two NORM devices, placed nearby in the same grid. In a widespread deployment, the acquired frequency dataset contains frequency values all from deployed NORMs. The figure shows that checking the consistency of data over different measurements has to deal also with the difference between the two SMM (in this case the NORMs used metering data acquired from two different types of integrated meters [30,31], accuracy class 0.5. The meters are considered as "metrology smart meters", as their smartness allows bidirectional communication and provide real-time data which can be obtained through NORM-SMG periodical real-time requests.

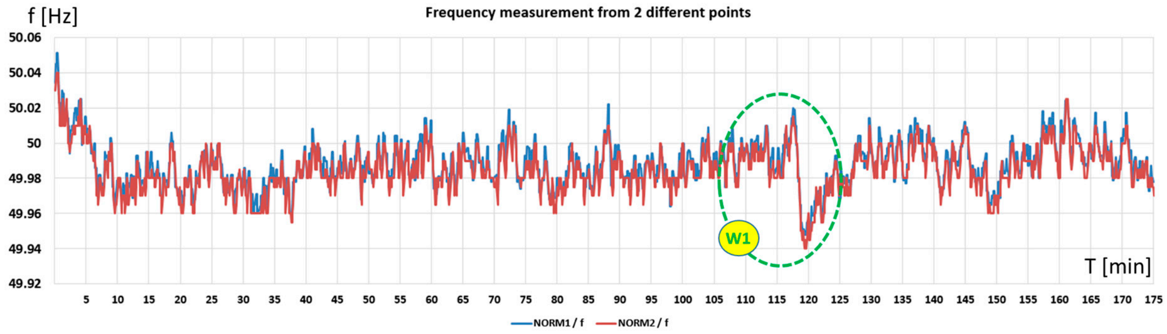

Figure 6. Grid frequency received from 2 × NORM placed nearby in the same grid.

Figure 7 presents a smaller part of the time window, around the region W1 shown in the Figure 6, providing a more clear view of the evolution of data from each source and of the difference between them. It can be seen that the frequency evolution in time is similar for the two NORMs, with very small differences caused by the intrinsic error of each device and by the fact that the meter types are different, which is a usual situation in practice, as there is no guarantee to have the same equipment deployed in the whole network.

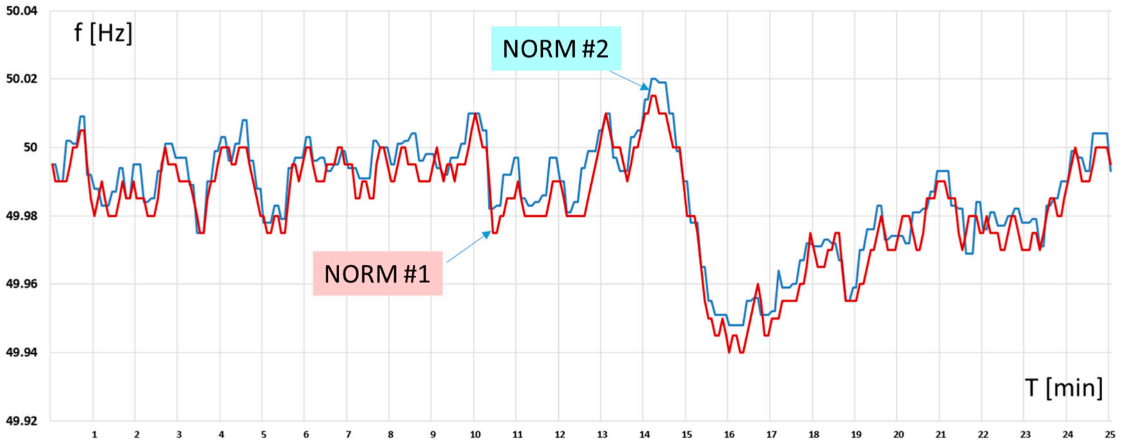

Figure 7. Grid frequency received from 2 × NORM (detail).

In order to check consistency and to detect possible malfunctioning, the two streams of data need to be assessed based on statistical means. We already used sliding windows of average errors between the two metering points, based on formula:

$$\varepsilon_{Med}(Tk) = \frac{1}{n}\sum_{j=Tk-n}^{Tk} \Delta f_j \tag{1}$$

where the sliding error calculated each time window between $[Tk - n, Tk]$ gives the mediation (averaged error) of real inconsistency between the different NORM measurements. In Formula (1), Δf_j is the difference between frequencies in two different network points at each moment j, based on synchronized measurements over the whole network.

The averaging through a sliding window reduces noise and allows a more stable analysis of the inconsistency. The calculation on the sliding windows take advantage of the PMU synchronous time stamp. In Figure 8 it has been used a sliding window of four consecutive values (n = 4).

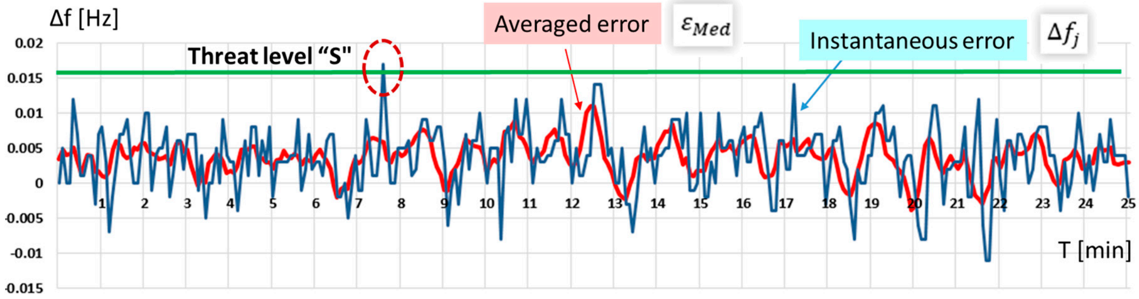

Figure 8. Instantaneous and average deviation of frequency measurements from two different NORMs.

Based on the proper time window, a signalisation and an alarm level of the allowed inconsistency can be decided:

$$Status = \begin{cases} if\ \varepsilon_{Med}(Tk) > S\ \rightarrow\ Status = \text{“Signalisation”} \\ if\ \varepsilon_{Med}(Tk) > A\ \rightarrow Status = \text{“Alarm”} \end{cases} \quad (2)$$

where S and A are threat levels for detecting inconsistency of acquired data in a particular grid. In Figure 8 above, the threat level S (Signalisation) is set at 0.016 Hz = 16 mHz, while A (Alarm), not shown in the figure, starting from a double value, e.g., A = 30 mHz, or set at higher levels, e.g., A = 50 mHz, which is a clear deviation to show abnormal situations.

In normal operation there is no credible situation for attending threat level A, because the grid or a smaller grid portion to be considered as microgrid does not allow such mediated differences on time windows as considered above (e.g., 30 s).

A higher deviation can be interpreted in different ways, for instance:

- Part of the measurements are coming from an islanded grid zone,
- Wrong measurements due to meter or PMU decalibration or defective measurement channel,
- Cyber-attack due to compromised ICT equipment and/or channels,

but more details and developments on methods are not the subject of this paper, which shows only generic situations which can be further detailed, e.g., by correlating with grid information which can show an island situation.

3.2. Grid Data Inconsistencies through Voltage Analysis

The second studied case is the correlation of voltage levels measured by NORM in different network places. This task is more complicated because the voltage is not the same in different parts of the network, but its evolution depends also on active and reactive power flow. However, as being a measurement which does not unveil privacy aspects, it is a valuable type of information to be assessed against suspicious evolution.

We analyse the voltage evolution in three different points in the network, with NORMs making records from their metering part. NORM1 and NORM2 are connected at small distance, while NORM3 is at a higher electrical distance and more near to the MV/LV (medium voltage/low voltage) transformer supplying the whole network.

Different types of meters have been used in each location [30–32]. Figure 9 shows the approximate place of the metering points, analysed for testing purposes, including point 4 which will add more diversity (not integrated in this work).

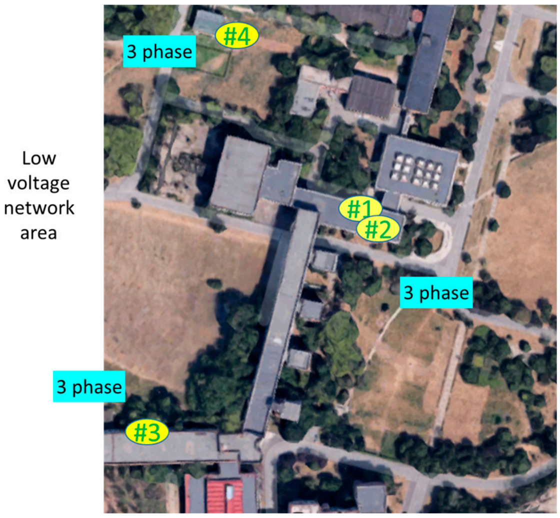

Figure 9. Metering points read by NORM's SMG, placed in a low voltage network with university buildings, at the University Politehnica of Bucharest, Romania.

By superposing the voltages acquired from the three NORM devices and by considering the same network phase, we obtain the voltage evolution of Figure 10, where the three voltages evolve similarly until a higher possible load appears at the end of the period (time window designated as W1), where voltages acquired in NORM1 and NORM2 remain grouped, while NORM3 voltages show a "near-to-source" behaviour (smaller drop of voltage level due to lower impedance to the medium to low voltage MV/LV supply point), even if the wave evolution is similar.

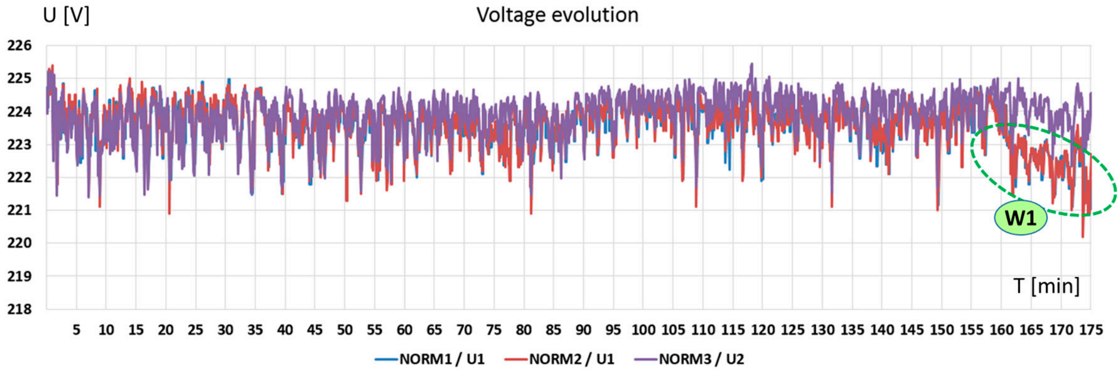

Figure 10. Voltage evolution recorded in 3 different metering points read by NORM's SMG.

By applying a similar approach with the frequency, through the calculation of average deviations between voltages measured in different places of the same distribution network, we can obtain the evolution in Figure 11, using voltage data from three NORM measurement points. In our example, the instantaneous deviation is calculated as a sum of absolute deviations of each voltage compared with the mean (average) voltage level in the local grid, according with the formula below:

$$\varepsilon_U(t) = \sum abs\big(U_k(t) - U_{avrg}(t)\big) \tag{3}$$

It can be seen that the 1 min (60 s) averaging through sliding windows gives an acceptable noise cancellation for making data comparisons until the W1 and W2 zones are reached. Averaging is performed by using previously presented Formula (1). Threat levels *S* and *A* (based on Formula (2)) can be applied until 160 min have been reached. However, in the W1–W2 zone level *S* is reached and additional non-private data need to be considered, e.g., by combining the deviation with the MV/LV transformer load (active power), which is not considered as being private data (the measurement is a superposition of powers from many users and is therefore well anonymized) and can be used as well by a DSO Security Monitoring Centre. The example for processing the data is generic, and additional levels of computations may be needed, including learning algorithms, which allow for a performance even with unknown grid topology.

Such analysis does not breach any privacy but ensures a higher level of assessment of data consistency, thus allowing for ICT, through its chain based on NORMs, real-time communication chains using public or private IP-based communication and through the Security Monitoring Centre, to become a precious instrument for assessing grid health and for detecting malfunctioning aspects in the smart grid system in time, thus being able to apply countermeasures.

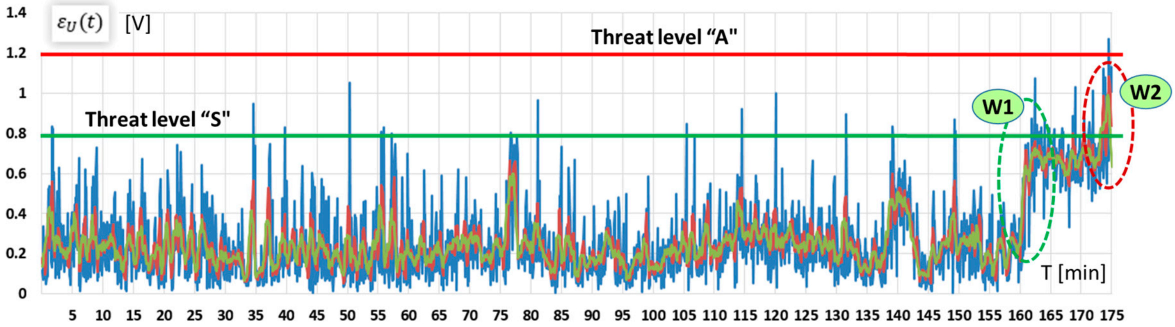

Figure 11. Instantaneous (each 5 s, in blue) and average deviation of voltage measurements (on 30 and 60 s, in red and green) from three different NORMs.

4. Conclusions

The paper is introducing the NORM architecture. NORM is a new HW/SW (hardware/software) solution designed to enable a real involvement of the customer in the grid. While so far, smart meters have been designed to support a very limited number of use cases and they are limited by the fact that they operate in a regulated market, the NORM explores and unlocks the possibility to address more functionalities based on the integration of energy metering and PMU functionality in a unified concept based on an unbundled architecture. A new meter architecture has an important impact in the energy field, because the smart meter is the only equipment requested in any network node which supplies a grid connected user, thus becoming a ubiquitous equipment in the low voltage grid, to support a wide range of actors in the energy ecosystem.

With the PUF-based high cyber-security added inside the smart meter gateway of NORM, it becomes more secure, allowing the same time secure grid operation for the grid operator, as well as end-customers involvement in a free market of services, to be purchased or offered in various forms, by using the same NORM as new and complex meter device placed at any prosumer level. It is worth noting that NORM allows multi-user connectivity through public or private IP-based networks, thus allowing complex and simultaneous interactions between NORM and different actors.

To stress the essential cyber-security aspect, this paper reports a generic use case of data provision, in which the local advanced measurement information of NORM is provided to a specialised DSO Security Monitoring Centre (DSO-SMC), which can be used to monitor consistency of grid data across the network in order to address false data injection threats, without jeopardising the end-customer privacy during its regular services activity. Non privacy intrusive methods of consistency assessment are possible in parallel with other activities performed by NORM. This case is particularly interesting because it gives solutions for relying on both secure grid operation as well as enabled free market of services, while determining significant savings in investment costs, thanks to a dual or multiple use of available information, which is assessed for inconsistency in parallel with normal communication of NORM with various actors. As cyber-security concerns are killing factors for all these activities, the NORM security-by-design approach intends to reduce risks and allows for more secure actor activity, in an ICT enabled environment.

The main contributions of the presented work rely on the new concept of NORM—integrating both metering and PMU functionality, in its improved cyber-security level and in the potential of implementing security monitoring concepts at a higher level, thus being able to apply countermeasures triggered by data inconsistency detection, as has been exemplified above. The motivation of this architecture relies on presenting a coherent solution for enabling a secure and flexible control of the grid based on new meters placed everywhere in the smart grid, while unleashing also a multitude of secure energy related services, with great impact on future energy ecosystems.

Acknowledgments: The work has been done in the frame of the European Union's Horizon 2020 research and innovation programme under the SUCCESS project grant agreement No 700416.

Author Contributions: Mihai Sanduleac and Antonello Monti have the main contributions to NORM concept, to the paper content and main coordination of the paper content; Gianluca Lipari contributed with aspects related to the low cost PMU; Artemis Voulkidis contributed on PUF technology; Gianluca Zanetto contributed on Italian meters integration in real environment and with PTP synchronization; Antonello Corsi and Giampaolo Fiorentino focused on NORM integration in a DSO security monitoring center and data inconsistency analysis; Lucian Toma contributed with aspects of the NORM functionality compared with state of the art of smart meters and gaps towards the new design, as well as on data inconsistency analysis at the level of the DSO security monitoring center; Dumitru Federeneciuc contributed on Romanian meters integration in real environment and NORM integration in a DSO security monitoring center and data inconsistency analysis.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chu, T.; Qin, J.; Wei, J. Distributed storage operation in distribution network with stochastic renewable generation. In Proceedings of the IEEE PES General Meeting Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014.
2. Wu, K.; Jiang, Y.; Marinakis, D. A stochastic calculus for network systems with renewable energy sources. In Proceedings of the IEEE Conference on Computer Communications Workshops, Orlando, FL, USA, 25–30 March 2012.
3. Zoeller, H.; Reischboeck, M.; Henselmeyer, S. Managing volatility in distribution networks with active network management. In Proceedings of the CIRED Workshop 2016, Helsinki, Finland, 14–15 June 2016.
4. Parvez, I.; Sarwat, A.I.; Wei, L.; Sundararajan, A. Securing metering infrastructure of smart grid: A machine learning and localization based key management approach. *Energies* **2016**, *9*, 691. [CrossRef]
5. Saxena, N.; Choi, B.J. State of the art authentication, access control, and secure integration in smart grid. *Energies* **2015**, *8*, 11883–11915. [CrossRef]
6. EG3 First Year Report: Options on Handling Smart Grids Data. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group3_first_year_report.pdf (access on 24 June 2017).
7. Patti, E.; Pons, E.; Martellacci, D.; Castagnetti, F.B.; Acquaviva, A.; Macii, E. MultiFLEX: Flexible multi-utility, multi-service smart metering architecture for energy vectors with active prosumers. In Proceedings of the 2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), Lisbon, Portugal, 20–22 May 2015.
8. Pitì, A.; Verticale, G.; Rottondi, C.; Capone, A.; Schiavo, L.L. The role of smart meters in enabling real-time energy services for households: The Italian case. *Energies* **2017**, *10*, 199. [CrossRef]
9. Final Report—OPEN METER (Open Public Extended Network Metering). Available online: http://cordis.europa.eu/publication/rcn/14381_en.html (accessed 20 April 2017).
10. H2020 Nobel Grid Project. Available online: www.nobelgrid.eu (accessed on 24 April 2017).
11. Sanduleac, M.; Stanescu, C.; Alacreu, L.; Pons, L.; Solar, A.; Alemany, R. Medium/low voltage smart grid observability and PQ assessment with unbundled smart meters. In Proceedings of the IEEE International Energy Conference ENERGYCON, Leuven, Belgium, 4–8 April 2016.
12. Sanduleac, M.; Pons, L.; Fiorentino, G.; Pop, R.; Albu, M. The unbundled Smart Meter concept in a synchro-SCADA framework. In Proceedings of the IEEE I2MTC—2016 International Instrumentation and Measurement Technology Conference, Taipei, Taiwan, 23–26 May 2016.

13. H2020 SUCCESS Project. Available online: success-energy.eu (accessed on 24 April 2017).
14. Sanduleac, M.; Eremia, M.; Toma, L.; Borza, P. Integrating the electrical vehicles in the smart grid through unbundled smart metering and multi-objective virtual power plants. In Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (IEEE PES ISGT Europe 2011), Manchester, UK, 5–7 December 2011.
15. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. Available online: https://www.nist.gov/sites/default/files/documents/el/isd/ieee/tutorial-basic.pdf (accessed on 24 June 2017).
16. BeagleBone Black Official Site. Available online: https://beagleboard.org/black (accessed on 22 April 2017).
17. Docker Official Site. Available online: https://www.docker.com/ (accessed on 14 May 2017).
18. OpenVPN Official Site. Available online: https://openvpn.net/ (accessed on 22 April 2017).
19. Cisco Smart Grid Security Solutions Brief, Meeting the Challenge of Smart Grid Security. Available online: http://www.cisco.com/c/dam/assets/docs/ciscosmartgridsecurity-ssolutions-brief-c22-556936.pdf (accessed on 25 April 2017).
20. Grid Security for Intelligent Power Supply Networks, Background Information, Erlangen. February 2016. Available online: https://www.siemens.com/press/pool/de/events/2016/energymanagement/2016-02-e-world/background-grid-security-e.pdf (accessed on 25 April 2017).
21. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
22. Guajardo, J.; Kumar, S.; Schrijen, G.-J.; Tuyls, P. FPGA Intrinsic PUFs and Their Use for IP Protection. Available online: https://pdfs.semanticscholar.org/4512/4ebcde598bbdbb3abe4db93005eae40c7269.pdf (accessed on 24 June 2017).
23. Majzoobi, M.; Koushanfar, F.; Potkonjak, M. Techniques for design and implementation of secure reconfigurable PUFs. *ACM Trans. Reconfig. Technol. Syst.* **2009**, *2*, 5. [CrossRef]
24. Pappu, R.S.; Ravikanth, P.S.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030. [CrossRef] [PubMed]
25. Li, W.-T.; Wen, C.-K.; Chen, J.-C.; Wong, K.-K.; Teng, J.-H.; Yuen, C. Location identification of power line outages using PMU measurements with bad data. *IEEE Trans. Power Syst.* **2016**, *31*, 3624–3635. [CrossRef]
26. Tushar, W.; Yuen, C.; Chai, B.; Huang, S.; Wood, K.L.; Kerk, S.G.; Yang, Z. Smart Grid Testbed for Demand Focused Energy Management in End User Environments. Available online: https://pdfs.semanticscholar.org/b672/16cc25771a377c61f4c2041d539f21157703.pdf (accessed on 24 June 2017).
27. Wang, D.; Guan, X.; Liu, T.; Gu, Y.; Shen, C.; Xu, Z. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. *Energies* **2014**, *7*, 1517–1538. [CrossRef]
28. Guo, J.; Han, Y.; Guo, C.; Lou, F.; Wang, Y. Modelling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties. *Energies* **2017**, *10*, 87. [CrossRef]
29. TW-TeamWare WallyA3. Available online: http://www.teamware.it/en/product/wally-a3/ (accessed 20 April 2017).
30. Brochure Elster A1800 ALPHA Meter 2010. Available online: https://www.elstersolutions.com/assets/products/products_elster_files/DS42-1003F.pdf (accessed 25 April 2017).
31. Technical data—Electricity Meters Landis+Gyr E650 Series 3 (ZMD400AT/CT, ZFD400AT/CT) Meter. Available online: https://www.prodemel.es/manuales/LANDIS_GYR_ZMD_INTERNACIONAL-datos_tecnicos.pdf (accessed on 25 April 2017).
32. Brochure Itron SL7000 Meter. Available online: https://www.itron.com/eu/-/media/itron/integration/brochure/acesl7000el00191fr0615.pdf (accessed on 24 April 2017).