Open System for Energy Services (OS4ES)

An EU-funded research project to establish a non-discriminatory, multivendor-capability service delivery platform for smart grid services.

Dr.-Ing. Jörg Benze
Dr.-Ing. Andreas Lang
T-Systems Multimedia Solutions GmbH
(subsidiary of Deutsche Telekom)
Dresden, Germany
joerg.benze@t-systems.com
andreas.lang@t-systems.com

Antonis Papanikolaou, PhD
Hypertech SA
Athens, Greece
a.papanikolaou@hypertech.gr

Tim Dethlefs, M. Eng.
Prof. Dr. rer. nat. Wolfgang Renz
HAW Hamburg - MMLab
Hamburg, Germany
tim.dethlefs@haw-hamburg.de
wolfgang.renz@haw-hamburg.de

Dipl.-Ing. (FH) Andrea Schröder
Forschungsgemeinschaft für Elektrische Anlagen
und Stromwirtschaft e.V. (FGH).
Mannheim, Germany
andrea.schroeder@fgh-ma.de

Abstract—The Smart Grid is a paradigm shift towards a bi-directional energy and communication system relying on rich information exchange among all involved actors. Based on the experience of the participation in the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) report creation for the EU-Mandate 490 "European Smart Grid Standardization" [1], the EU-funded research project "Open System for Energy Services (OS4ES)" was initiated. It will develop and prototype a generic, non-discriminatory, multivendor-capability ICT-platform for easy cross-linking of smart grid entities. It perceives no active market role, but supports market role owners with an easy to use middleware for bi-directional energy communication. This paper gives an overview about the methodology, architecture and functionality of the OS4ES research project.

Keywords—Architecture, Distributed Energy Resources, Methodology, Registry, Service Delivery Platform, Smart Grid

I. INTRODUCTION

Today, mass presence of distributed energy resources (DERs) connected to the grid is often seen as having adverse effects on grid reliability and robustness. The apprehension is that it complicates or even compromises network management by distribution system operators (DSOs).

One of the central aims of the Open System for Energy Services (OS4ES) project is to provide a solution that closes the current information, communication and cooperation gap between DERs and DSOs. To this end, the OS4ES project delivers an innovative Open Service System that enables dynamic DER-Aggregator-DSO cooperation. A Distributed Registry for DERs offers to involved actors the opportunity to reserve the aggregated flexibility of DERs (even forming dynamic Virtual Power Plants) as a grid management service in order to improve Smart Grid robustness and reliability. OS4ES will be based on standardized and interoperable communication interfaces, as well as generic interfaces among components producing, consuming or storing electrical energy.

II. MOTIVATION

Large and still increasing numbers of DERs are built and connected to the energy distribution grids all around Europe. In the days that the numbers of DERs were still low, this connection to the grid typically followed a "fit-and-forget" policy that ignores the technical effects that DER devices may have on the grids. Moreover, what is also currently not exploited are the potential and capabilities that DERs have for smart grid management. A coordinated integration of DERs in the energy grid which can fully exploit their capabilities for mutual benefits – for grid balance/stability and for DER integration in energy markets - requires an automated "plug & play" approach.

For example, DER flexibilities could be exploited for important grid management functions such as demand/supply response, congestion management or load balancing. In recent years, some concepts have been developed for this, such as Virtual Power Plants (VPPs) and technical and/or commercial DER aggregation portfolios, managed by a single party (DSO or commercial aggregator).

1http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx, last visit 13.04.2015
2 http://www.os4es.eu
The smart distribution grid management of the future by DSOs and other BRPs however will require much more, namely services and capabilities to form VPPs and technical/commercial DER aggregation portfolios dynamically on-the-fly. The overall aim of the OS4ES project is to provide an IT system that will facilitate automated and effective interaction among grid actors so as to enable cost-efficient grid management.

III. OBJECTIVES OF THE OS4ES PROJECT

The detailed objectives of OS4ES are:

1. Deliver a Reference Architecture of an Open System for Energy Services (OS4ES), enabling DERs to be dynamically assigned and interconnected to Energy Management Applications of DSOs, Aggregators and BRPs.
2. Operationalize this Reference Architecture through the realization of a software reference implementation that contains all the necessary building blocks, is compliant with existing standards, and that demonstrably enables DSOs and DERs to dynamically work together in an integrated way (see Fig. 1).
3. Test this OS4ES system in lab and field tests for a number of mission-critical business use-case scenarios.
4. Make final results of the OS4ES service system available in Open Source format for wide take-up and disseminate key results via an OS4ES stakeholder Industrial User Group.
5. Prepare associated standardization efforts. Open Standards are crucial for the success of any System for Energy Management Applications. We will bring API for Energy Management Applications, DER Distributed System Registry Interface, and DER communication interface into existing standardization activities from the Standardization Bodies (e.g. TC57 WG17).

IV. OS4ES ARCHITECTURE

The high level architecture of the OS4ES-platform is shown in Fig. 2. The DER units at the supply and demand side are connected by a communication layer with the OS4ES platform, which natively supports a web-mapping of IEC 61850 based on XMPP. The communication layer will provide gateways from popular proprietary DER communication protocols to IEC 61850 and interfaces toward the web mapping to support integration to the platform.

The semantic middleware contains various services for the administration of the DER units. This includes for example a registration service and an authentication and rights management service, over which the access to the DER units are secured.

The registry contains the core functionality of the OS4ES system. It is the central information repository of the OS4ES system and offers capabilities towards the OS4ES users like...
registration of DER systems and functions, discovery functions and basic information retrieval services (location, power, etc.). This registry is not a monolithic system; it can exist in several distributed instances, which cooperate with each other. The main feature of the registry system is the publication of energy services, dynamic capability descriptions of DER systems which can be used by aggregators [2].

The registry system responds with a list of suitable energy services; the aggregator then selects the most appropriate ones for the target aggregated service offering. As described in [2], the DERs can dynamically update their energy services at runtime which allows aggregators to monitor the capabilities of the available DERs at all time and to choose dynamically suitable energy services for their operational requirements. In contrast to other established, more passive registry concepts e.g. [5][6], the novel energy service approach enables a market between aggregators and DER systems in the future in order to optimize the use of DERs. But apart from market platforms already in use, the OS4Es provides a semantic middleware to support the whole process of reservation and control.

To achieve this, the registry system needs to be capable of the following core functionalities: (1) users must be able to find suitable energy services provided by DER units through queries, (2) finding single devices and energy services by their unique identifier, (3) databases for technical and service data must be provided. The proposed registry system itself consists of two core components: white pages services and yellow pages service, similar to the UDDI concept [7].

The white pages service is an index of all available DER Systems participating containing nominal data (location, connection point, owner, type and specifications), while the yellow pages service contains the energy services (on-demand active/reactive power, autonomous frequency control) that can be provided by the DERs from the white pages service. Thus, one resource may provide multiple services which can be used by aggregators. In Fig. 4 an example configuration of such a registry system is shown. The distribution concept shown is based on the grid topology and the hierarchy of the system operators. Sections of the white and yellow pages cover so-called zones. These are logical segments of the grid topology, allowing the addressing of the DERs in such a zone and thus a more efficient search and also a sharing of responsibilities.

An index layer allows the addressing of the registry entities and routing of requests similar to the Domain Name Service (DNS) – System [9] of the Internet.

### V. DISTRIBUTED REGISTRY CONCEPT FOR ENERGY SERVICES

The OS4ES project focuses on the definition and development of the described registry system. As the registry system should be able to manage the data and energy services of thousands of DERs while infrastructural components like this must maintain a high degree of availability and reliability, the system could only be distributed [4].

The distributed registry system shall close the process and informational gap between DER inventory lists and large energy market platforms by enabling DERs to provide their capabilities for grid-related services. DER controllers can register their DER system in the registry system and set-up energy services according to the capabilities of the DER system. Aggregators can search the registry for energy services that match their demand by defining search criteria.

[Fig. 2. OS4ES-platform high level architecture]

The application layer is the "customer facing service creation point" for smart grid actors to integrate the OS4ES services in their business processes for their market roles.

The Smart Grid Actors are outside the OS4ES platform and can use inside the application layer on the one hand the build-in DER unit management services (under consideration of the authentication and rights management service). On the other hand they can implement their own control applications into each, the smart grid actor associated, runtime environment.
VI. SEMANTIC MIDDLEWARE

The semantic middleware of Fig. 2 allows for the run-time management of associations between Smart Grid control applications and DER systems for the implementation of targeted local control strategies for grid optimization and power loss minimization. The provision of balancing services using massive numbers of DER systems requires complex management processes to facilitate conflict-free reservation and operation in a free market environment. In the functional architecture of Fig. 5, the middleware has been broken down into a control layer (core functionality) and a conversion layer (interoperability layer). Furthermore, the middleware is responsible for the information exchange between the different components and entities (aggregators, DSOs, BRPs, etc.) by performing message control, transformation, mapping and routing, queuing and buffering. This Message Oriented Middleware (MOM) offers the required agility and flexibility with regards to the communications and interactions taking place during the operation of the system.

The semantic middleware will be responsible for providing the following functionalities:

**Protocol/data model conversion:** Interoperability among actors/systems in the Smart Grid domain, including legacy IT systems, requires the capability to convert between a host of different protocols and data models. The middleware provides this functionality with initial emphasis on the main standards (IEC 61850, 61970, 61968) which will be extended in the future toward more proprietary communication protocols. A differentiation has been made in Fig. 2 between communication to DER systems (named “Communication Layer”) and other Smart Grid actors/systems. In the functional architecture of Fig. 5, the component named “conversion layer” will be in charge of all protocol/data model conversions, including IEC 61850 and, is modular to support extensions as mentioned above. The communication with Smart Grid applications will be also handled by the semantic middleware itself, with emphasis on the IEC 61970/61968 standards.

**Authorization/authentication capability:** A key requirement for any Smart Grid IT system to ensure the security and credibility of the OS4ES. Access of any Smart Grid actor or IT component of the OS4ES system to the DER systems will be granted by an authentication and authorization process provided by the middleware. Only certified/authenticated actors or IT components can request other actors’ or components’ services and APIs. The authentication flow will assess the access rights of the sender of the message and his permissions to the requested service or API of the recipient.

**Message validation capability:** Any incoming message to the OE4ES platform should pass the message validation process in order to avoid unnecessary message transferring. The validation process will perform data type checks that will ensure compatibility of the message payload, as well as, request validation checks concerning their compliance with the available capabilities of the recipient. Such validation is also crucial for avoidance of security risks that may be hidden in message payloads, hence the middleware will provide an added level of security.

**Message routing capability:** The middleware will act as a tunneling proxy to deliver messages to their recipients. All the fundamental communication services/types for message exchange between OS4ES components, external actors and DER systems are supported based on a proposed extension of the IEC 61850 communication protocol toward web mappings. The message routing process is realized through the TCP/IP network protocol through an end-to-end connectivity that will be provided by a standard telecommunication network.

**API management capability:** The middleware will also manage all the provided APIs (Application Programming Interfaces) of the OS4ES IT components. It provides functionalities like: (i) automating and controlling the
connections between the APIs and the components that use them, (ii) monitoring APIs performance and providing analytics concerning the APIs health and usage, and (iii) protecting the APIs from misuse by safeguarding it with authentication and authorization policies.

VII. OS4ES COMMON INFORMATION MODEL

The Open System for Energy Services is designed as an interoperability gateway among a multitude of actors in the Smart Grid domain. It will enable communications between diverse actors, like the in-the-field DER systems, system operators, balance responsible parties, aggregators, etc. Each of these actors potentially utilizes a different communication protocol and internal data model/representation. Main standardization efforts have already yielded standards with widespread use in the electricity grid domain: IEC 61850 (and its parts) for communication to/from substations and DER systems, IEC 61970/61968 for communication among Smart Grid actors. Bridging the gap between existing standards will require an internal OS4ES Common Information Model addressing different Smart Grid components and respective information elements of varying granularity that will ensure the semantic and syntactic interoperability between the various components.

This model will be developed based on the structure of the IEC 61850-7-420 standard [8] which governs the interfacing between control centers and distributed resources (DER clusters) commissioned and managed for different business purposes. On the other hand, new business models investigated in the project (e.g. decoupling value creation from aggregation to energy service monetization) as well as flexible relations and business collaborations between them (flexibility value chain definition) in the future deregulated markets (e.g. DER portfolio capacity trading), necessitate for the utilization of the IEC CIM standard and more specifically:

- IEC 61968 part 11 which addresses distribution management and data models for specialized applications such as demand side management and part 3 which specifies the core interfaces for specific Distribution Management Systems (DMS) processes like monitoring and control of equipment for power delivery,
- IEC 62325 standard (parts 301 and 450) for deregulated energy market communications, specifying the interfaces between different market actors and allowing for the efficient integration of information interchanges between them.

To this end, the middleware adopts existing models and will propose custom solutions (e.g. contextual CIM profiles, additional types of Logical Devices), on the conflicting/grey areas in the intersection of 61850-7-420 and CIM standards aiming at the future integration of the two standards under the reference architecture (IEC 62357). In this scope OS4ES defines:

1. The inter-aggregator and utility-aggregator communications, their semantics and the respective payloads and serializations, in line with the CIM standard along with the respective business cases,
2. Project specific and custom contextual profiles and models that extend the IEC 61970 CIM to match Smart Grid user and business requirements.

VIII. OS4ES SECURITY AND PRIVACY ASPECTS

Security and privacy are important parts of smart grid. The European Commission has established an Expert Group for privacy, data protection and cyber-security within the smart grid task force\(^3\). The most important information security and information privacy aspects are explained in the following sections.

A. Confidentiality

Confidentiality is the protection against unauthorized disclosure of information and access to systems and services. Confidential data and services shall be accessible only for persons or parties who are authorized [10]. It is important to understand that threats against confidentiality (e.g. unauthorized access to confidential data or resources) will have a direct impact to organizations like the DSO (Distribution System Operator).

B. Integrity

Integrity ensures the correctness (integrity) of data and the correct functioning of systems and services. When the concept of integrity is applied to data in information technology (IT), it means that data must be complete, unaltered and current in delivery associations. When the concept of integrity is applied to systems, it means that system operation is steady and thorough. Integrity is an important protection requirement for the DSO and all stakeholders. Solutions to detect integrity failures include Hashes or a message authentication codes (MAC). After a fault detection of a data request, this data must be requested again to ensure correctness of the data transfer including integrity check.

C. Availability

Availability comes with a multiplicity of other requirements. One of them is reliability. Depending on the service, only a few minutes of downtime per year are acceptable. Other availability requirements are the availability of consumption and production measurements and the availability of control mechanisms. A typical technical measure to enhance availability is to provide redundancy. Among others, availability is important to guarantee an uninterruptable communication. Furthermore, the integration of mechanisms for restarting after a power failure (black-start) should be considered. Because there are many objects in OS4ES which work together, availability leads to a main focus in the risk disclosure statement.

D. Authenticity

Authenticity ensures that a communication partner is actually the person, system or process it claims to be (evidence of the sender and/or receiver). The term is not only used when the identity of persons will be approved/tested, but also in IT components like card readers or smartcards (specifically: the certificate) should also be authenticated (Online Certificate Status Protocol). Each role must be authenticated correctly at all times when needed. Typical implementations can be digital signatures, passwords, challenge responses or an OTP (One Time Password).

E. Non-Repudiation

Non-Repudiation is the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party of a communication (e.g. a contract) cannot deny the authenticity of their signature on a document or the sending of a message that they originated. In practice, someone must initially certify this person. Non-repudiation implies one's intention to fulfill their obligations to a contract and has to be seen in the context with authentication and integrity. Sender and/or receiver authenticity and information integrity must be proven. This is typically done using digital certificates, a form of public key infrastructure.

F. Privacy

In ubiquitous, distributed and highly complex systems such as OS4ES, information security plays a key role in ensuring an adequate level of information protection. Encased in this field is also privacy, which is encircled with personal reference to somebody. Ensuring a fully compliant environment which meets all applicable requirements is associated with high costs. Taking this into account the best strategy is to choose a reasonable foundation, because requirements are versatile.

Rigorous application of good information security practices minimizes costs while adhering to requirements. Such practices are documented for example by the German Federal Office for Information Security (BSI). The core concept in connection with privacy relation is called “BSI IT-Grundschutz Data Protection, module 1.5” [11]

In the context of privacy by design, it is important to build in technical, organizational and process-related mechanisms in the system architecture early enough. It is also important to implement mechanisms so that only necessary personal data will be considered and collected.

IX. FURTHER WORK

Future work in the OS4ES project will focus on defining the information that DER systems need to have at their power system connection point and for the registry in order enable a Smart Grid Actor to decide if a DER system matches its request. This information will then be mapped to IEC 61850 data which will be fed to the respective national and international IEC 61850 standardization committees and their task forces.

Furthermore registry algorithms for finding DER systems and their offered services will be developed. A registry prototype will be set up and tested, including the matchmaking algorithm and the OS4ES aspects for privacy and security presented in this paper. Besides, web based communication protocols such as OPC-UA, XMPP and REST will be evaluated in terms of their applicability for the OS4ES platform. The most appropriate communication protocol will be identified and implemented in the OS4ES platform prototype. Based on the use cases defined at the start of the project Smart Grid applications will be developed and tested. In lab and field tests the whole OS4ES System and the Smart Grid applications will be assessed in a final test phase. Non-complying components will be improved.

Further information to the OS4ES project is provided on the project website www.os4es.eu. OS4ES maintains a User Group with access to all project developments, which can be freely joined by any interested party.

Acknowledgment

The authors would like to thank the European Commission for the funding this project receives from the European Union’s Seventh Framework Program for research, technological development and demonstration under grant agreement no. 619302. Furthermore we would kindly like to thank all other OS4ES project members.

References

[7] OASIS, “Universal Description, Discovery and Integration (UDDI) 3.0.2”, Organization of the Advancement of Structural Information Standards, 2004