Predictions in Resilient Hybrid AC/DC Grids Leveraged by an Interoperable and Secure ICT Platform

Marzia Mammina
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
marzia.mammina@eng.it

Alessandro Rossi
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
alessandro.rossi@eng.it

Diego Arnone
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
diego.arnone@eng.it

Gaetano Zizzo
Università degli Studi di Palermo Engineering Department
Palermo, Italy
gaetano.zizzo@unipa.it

Salar Moradi
Università degli Studi di Palermo Engineering Department
Palermo, Italy
salar.moradi@community.unipa.it

Paul Smith
Austrian Institute of Technology
Vienna, Austria
paul.smith@ait.ac.at

***Abstract*—Power systems are undergoing a significant change and the main elements to address the new challenges is the new key-role played by the distribution grid and its transformation into a smart grid. While the distribution grid has traditionally operated with alternating current (AC), nowadays most devices operate with DC internally, and most distributed renewable resources generate power in DC. Furthermore, storage components, such as batteries and supercapacitors, have a DC character. DC seems to be the one of the most promising candidates to avoid stranded investments and to guarantee incredible saving for the community in Europe, making the transition to a fully decarbonised energy system an affordable reality. Anyway, hybrid AC/DC grids technologies make the control of these networks considerably complicated due to advent of the new power electronic devices with some critical controllable parameters. The protections of these parameters operate in a much short time in emergency states, leading to increase in cascade failures probability. In this framework, the HYPERRIDE project aims to enable a unique revolution in the electrical grid infrastructure creating the conditions to really unlock a wide application of DC technology in the distribution grid. Furthermore, HYPERRIDE provide a technology independent specification of a FIWARE-based interoperable and secure ICT platform. In this paper, the layered architecture of the platform will be described and a potential usage application of it for the predictions in resilient hybrid AC/DC grids will be presented.**

Keywords— hybrid grids, communication platform, cascading effect, root cause analysis, interoperability, resilience, FIWARE.

I. Introduction

Direct Current (DC) has several well-known advantages over Alternating Current (AC) [1]. The high efficiency resulting from recent developments in DC converters technology has allowed improvements in electricity delivery over long distances. Renewable energy sources such as solar and wind, although generate power intermittently, require a power conversion interface to the grid and this makes DC a naturally compatible interface. Most energy storage technologies are DC-based and, thus DC creates opportunities to enhance storages integration improving efficiency and reducing operating losses. DC and Hybrid AC/DC microgrids are being developed. Microgrids enhance efficient power distribution and cost effectiveness by the installation of power sources nearby the consumers' loads. Microgrids provide reliable power by incorporating local generation systems based on renewable and conventional power sources, energy storage systems, and energy consumption loads, being also able to disconnect from the main grid to operate autonomously. By "islanding" from the main grid in case of emergencies, a microgrid can both continue serving its included load when the grid is down and serve its surrounding community by supporting critical services [2]-[3]. Hybrid AC-DC microgrids reduce multiple power conversions in individual AC or DC microgrid and allows connection of variable AC and DC sources and their respective loads simultaneously. Electric vehicles use DC battery power and to charge their batteries is requested a shorter time than necessary in the case of charging using AC power.

The international goals for the decarbonisation are the main driver for the integration of DC in our energy supply system of renewable energy sources, decentralized energy resources, energy storage systems, electric vehicles and other new loads in homes and businesses, most of which internally operated in DC. Considering the advantages of DC for energy transmission (e.g., increased transmission capacity, reduced losses and voltage fluctuations, easier synchronisation, etc.), the introduction of DC in all grid voltage levels must be considered for secure and efficient electricity supply in the future. The potential DC grid technologies for the development of the electricity grid, thus, need to be demonstrated, the barriers to be overcome identified and the business models for further exploitation developed.

The HYPERRIDE project aims to enable a unique revolution in the electrical grid infrastructure creating the conditions to really unlock a wide application of DC technology in the distribution grid. HYPERRIDE (which is acronym of Hybrid Provision of Energy based on Reliability and Resiliency by Integration of Dc Equipment) is a European Union Horizon 2020 Research & Innovation project [4]. The HYPERRIDE consortium is composed of ten partners (which cover all system integration levels from planning and operation, via digitalization and automation, technology providers and system integrators from six countries: Sweden, Germany, Czech Republic, Switzerland, Italy, and Austria.

By combining DC and AC technologies, HYPERRIDE will demonstrate potential solutions which are seen in AC-DC hybrid grids for LV and MV infrastructures, as most power electronics applications use internal DC power supplies. HYPERRIDE will:

- develop and demonstrate Microgrid MV DC circuit breakers along with related ICT systems and sensing;

- develop MVDC protection;
- develop converter control algorithms and architectures to be interface with higher-level control;
- develop the DC Measurement Unit (DMU), which extends the concept of synchro-phasors, whose advantages on grid observability are well known, to DC technology;
- define the control architectures for power converters that operate in the Hybrid AC/DC grids, which will be implemented in the demo-sites;
- develop and demonstrate LVDC Microgrid control method based on the virtual impedance method;
- design and implement a complete automation architecture for Hybrid AC/DC grids, which includes the monitoring of the grid and assessment of its state.

Moreover, specific energy services for the optimized and secure operation will be implemented leveraging on the HW and SW technologies developed in the context of the project itself. These deployments allow the technological integration of the DC sub-grids into the traditional AC distribution networks, in terms of system control, operational and protection strategies.

HYPERIDE intends to address the emerging new cases and utilises technologies and concepts of the rather very local or isolated state of the art DC applications, also providing clear recommendations for distribution grid applications. The new use cases are being implemented and will be validated via the three pilot sites:

- the Swiss pilot at the EPFL campus in Lausanne, which consists of the Distributed Electrical System Laboratory (DESL) and the Power Electronics Laboratory (PEL), which are interconnected. The rationale of this pilot is to test optimal control strategies for hybrid AC-DC grids as well as adaptive reconfiguration approaches. Another focus of the pilot is on protection coordination and stability investigations of AC-DC hybrid grids;
- the German demo-site at the RWTH-Aachen Campus Melaten, which is based on available infrastructure and converter technologies developed in previous projects. It provides a modular design, easily reconfigurable to test different network architectures. The goal in HYPERIDE is to demonstrate different hybrid AC-DC architectures to increase the technology readiness level of key enabling technologies and systems;
- the Italian pilot is located in Terni at local urban district, called ASM-CMCS. The rationale for the Italian pilot to demonstrate the potential offered by a more modular (cellular) smart hybrid AC-DC decentralized operation of MV/LV electricity grid, with a view to increase grid operation efficiency, reduce reverse power flow towards MV and reduce cyber-security risk.

Because of the deep penetration of unpredictable renewable energy sources, the power system is evolving toward the concept of smart grid. Smart grids and microgrids do strongly depend on information and communications technology (ICT), since monitoring, analysing, and managing of data are a key layer on top of which optimisation, re-configuration, fault detection, secure management ensure the reliable, stable, safe and efficient use of the grids. The HYPERRIDE project aims also to provide a technology independent specification of the Open interoperable ICT platform, as well as of the tools it includes, enabling:

- the seamless integration and management of devices, regardless of how smart they are;
- scalable and interoperable collection and management of data that support near real time observability and optimisation of the operation of modular and resilient hybrid AC/DC grids;
- the transmission of commands/setpoints to the actuators for the safe and reliable operation of the grid;
- detection, prediction, prevention of technical and cyber-contingencies.

This specification has to be considered as a reference for the development of the HYPERRIDE ICT platform for hybrid AC/DC grids secure monitoring, control, optimisation. As reference implementation of platform and tools, a FIWARE-compliant version will be developed, tested, and validated. The FIWARE Foundation is leading a joint collaboration program to support the adoption of a reference architecture and compatible common data models that underpin a digital market of interoperable and replicable smart solutions in multiple sectors, including smart energies. The FIWARE reference architecture, which is a curated framework of open-source components, called Generic Enabler (GE), that can be assembled together with other third-party components, and data models, use the ETSI NGSI API [5] and TM Forum Open APIs [6] to accelerate the development of interoperable and scalable smart solutions.

In this paper, the architecture of the FIWARE-compliant HYPERRIDE ICT platform for hybrid AC/DC grids [7] is described.

II. Platform Architecture

A layered architectural pattern has been adopted to provide a high-level view of the HYPERRIDE Open ICT Platform. A layered architecture abstracts the view of the system as whole while providing enough details to understand the roles of individual layers and the relationships between them. Modules or components with similar functionalities are organized into multiple horizontal layers. Each layer plays a specific role in the whole system and contributes to the operation of the layer above it. Each layer depends on the layers beneath it and is completely independent of the layers on top of it. This leads to layers of isolation: changes made in one layer of the architecture generally do not impact or affect components in other layers. Separation of concerns among modules is the best feature of a layered architecture: modules within a specific layer deal only with the logic that pertains to that layer, making easier the subsequent phases of development.

The overarching view of the HYPERRIDE Open ICT Platform architecture and integrated tools, represented in Fig. 1, comprises three horizontal layers, namely:

- the Presentation Layer, which implement the functionalities required to allow users to interact with the system;
- the Knowledge Layer, which contains the knowledge base of the underlying domain;

- the Acquisition and Interoperability Layer, whose main role is to capture collect from different devices and, when requested, to convert those data in standardised context information.

An additional cross-cutting Security Layer is responsible for what concerns security, both cyber and physical. It supports situation awareness and provides insights about the root cause of the alerting events generated by the tools that provide for the continuous monitoring of the system behaviour. From the cyber point of view, it provides for authenticated and authorised access to the system resources.

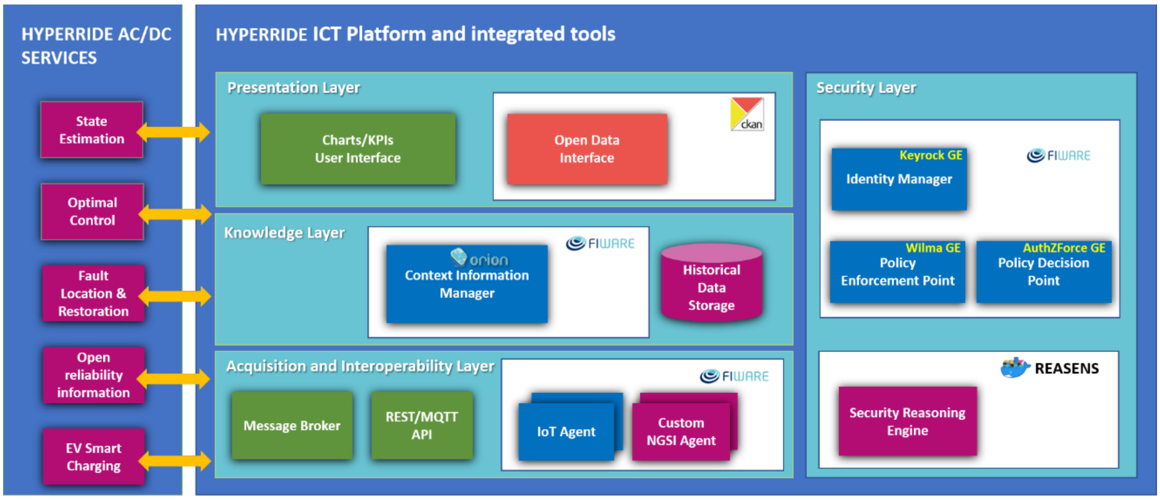

Fig. 1. Overarching HYPERRIDE Open ICT Platform Architecture and integrated tools [7].

Fig. 1 shows, on the the left side, the energy services that will be implemented in the context of HYPERRIDE and that will made use of data acquired through the Open ICT Platform [7].

The core component of the interoperability platform is the FIWARE Context Information Manager, or Context Broker, which allows to model, manage, and gather context information at large scale enabling context-aware applications. The Context Broker, which is a component of the Knowledge Layer, is able to manage the whole lifecycle of context information including updates, queries, and registrations. It allows for the creation of all necessary entities and does not require any database schema. Technically it is a publish-subscribe system; the changing of the context is notified to the subscribed applications. The FIWARE Context Broker comes with a reference implementation called Orion [8], which technically consists of a MongoDB database for short/medium term storage with an NGSI REST API on top of it using the Open Mobile Alliance Next Generation Service Interface (NGSI) protocol [9]. The FIWARE NGSI API defines:

- a data model for context information, based on a simple information model using the notion of context entities, which represents any physical or logical object (e.g., a sensor, a person, a room, an issue in a ticketing system, etc.), characterized by one or more context attributes, or properties;
- a context data interface for exchanging information by means of query, subscription, and update operations;
- a context availability (interface for exchanging information on how to obtain context information).

The Context Broker alone does not allow to store time series data, since new sensor data replaces the existing one. In case historical data must be preserved, an additional component called Cygnus [10] is required. Cygnus is a connector in charge of persisting certain sources of data in proper storages. Indeed, it is allocated in the Knowledge Layer together with the Historical Data Storage module, which gives the opportunity to create a historical view of the context. According to the nature of the data to be stored, a particular kind of database is more appropriate than other ones. As an example, for monitoring data, the most suitable kind of database is timeseries-based. In this kind of databases timestamp plays a fundamental role: all measurements have at least a timestamp, which is indexed, and one or more fields to be stored, which are not indexed. Optionally also tags can be given, which are indexed as well. In this way, this kind of databases are particularly suitable to store and query data by means of time ranges and the optional tags. Another possible option for long-term storage are No-SQL databases, which have the possibility to store and query documents which are not related to particular tables; documents are instead stored in collections and are retrieved by a unique id. The Historical Data Storage is could be also conceived as DataStore for open datasets.

The Charts/Key Performance Indicators (KPIs) User Interface module in the Presentation Layer takes raw data from the Historical Data Storage, and displays this information, in addition to metrics or KPIs, in simple charts and graphs on dedicated dashboards. This module provides a simple tool for tracking and analysing performance towards prefixed goals, thus making data-driven decisions more efficiently.

The Open Data Interface module is in charge for the publication, management, and consumption of open data, both static and dynamic datasets: it allows to catalogue, upload, and manage open datasets and also supports searching, browsing, visualizing, or accessing open data as well as data from the Historical Data Storage.

In the Acquisition and Interoperability Layer, other essential tiles of the general FIWARE-compliant architecture reside, namely the IoT Agents and the Custom NGSI Agents. An IoT Agent is a component that lets a group of devices send their data to and be managed from a Context Broker using their own native protocols. IoT Agents allow to simplify the management and the integration of devices by collecting data from devices through heterogeneous protocols and translating them into the standard platform language that is in NGSI entities. IoT Agents also permit to send commands to devices. NGSI Agents may also facilitate the integration of vertical solutions (e.g., smart meters, smart industry, smart building, smart home, energy storages, e-vehicles, etc.) and of other sources of data (e.g., energy management systems, social networks, etc.) with the Open ICT Platform. IoT Agents already exist or are in development for many IoT communication protocols and data models. FIWARE provides libraries to enable IoT Agent developers to build Custom NGSI Agents for their devices that can easily connect to NGSI Context Broker.

For the sake of completeness, a Message Broker has been included in the Open ICT Platform architecture to enable potential communications that will not be managed via the Context Broker.

The Security Layer is responsible for all concerns related to security, both cyber and physical. The Identity Manager (IdM) module includes the functionalities needed to manage identities and automate identity-related business processes that improve security. It manages specific permissions and policies to authenticate users before having access to resources integrated into the Open ICT Platform. The IdM holds all user information and offer a single sign-on (SSO) service for the applications so that they do not need to maintain user information (e.g., no private credentials) and one user account can be used for all applications using the platform. The FIWARE IdM reference implementation KeyRock [11] will be integrated in the HYPERRIDE Open ICT Platform.

Used along with other two security modules, namely the Policy Enforcement Point (PEP), which protects a resource by enforcing access control, and the Policy Decision Point (PDP), which evaluates the policy and makes an access determination, the IdM enables business to business (B2B) authorization security to services and applications based on the OAuth2 open standard, which allows for access delegation to grant access rights. The HYPERRIDE Open ICT Platform will integrate the FIWARE PEP reference implementation Wilma [12], which acts a proxy that enforces access control to services and applications and only permitted users can access to applications or RESTful services, and the FIWARE PDP reference implementation AuthZForce [13], which provides REST API to get authorization decisions based on authorization policies, and authorization requests from the PEP.

Inside the Security Layer, the Security Reasoning Engine module is responsible for the root-cause analysis for identifying the root causes of faults or problems and the identification of countermeasures to prevent similar incidents. The REASENS Framework has been identified as starting point for the root-cause analysis. It is a hierarchical REAsoning system that enables the collection of events from distributed and heterogeneous SENSors. Its purpose is to support reasoning (analyses) about the potential root causes of events that are generated by sensors, e.g., to determine whether they pertain to a fault or a cyber-attack. REASENS framework will be extended to enable the ingestion of events from the systems that perform anomaly detection in hybrid AC/DC networks and suitable causal models will be developed that can be used to reason about their root causes, detection that leverages state estimation algorithms.

Among the energy services implemented in the context of the HYPERRIDE project, which make use of the HYPERRIDE Open ICT Platform to collect the necessary data, we can find the following.

The Optimal Control service that is being deployed in the HYPERRIDE ICT platform is based on the Optimal Power Flow (OPF) algorithm implemented within HYPERRIDE to determine the most optimal set of variables in an electrical network to achieve the fulfilment of pre-determined criteria related to power flow results. It focuses on the management of AC/DC distribution grids; hence it includes the accurate modelling of components and control systems for AC/DC power converters as well as loads and distributed generators in the DC sub-section of the network.

The State estimation is a technique used to acquire full knowledge of the power system in real-time conditions. Specifically, it consists of processing the available measurements, in order to provide an optimal estimate of the current operating state. Usually, the states are constituted by voltage phasors at each system bus for a given point in time. Consequently, all the other electrical quantities of the network are computed via the fundamental electro-technical functions. In case of hybrid AC/DC grids, main topics of HYPERRIDE, the main obstacle is constituted by the exchange of power flow values among the AC and DC sub-portions of the network (i.e., the modelling of losses and operating conditions and AC/DC converters); in this case, the deployed two-steps algorithm firstly solves the state estimations separately in AC and DC grid sub-portions and, then, it combines the outcomes to achieve an accurate estimation of the power network states.

The Service Restoration solution, developed and used within HYPERRIDE tasks, is a middleware software component particularly tailored to the fault management for AC/DC distribution grids at Medium Voltage level. The re-energization of disconnected nodes relies on the reconfiguration of grid topology (by closing normally open tie-switches) and the adjustment of AC/DC converter setpoints. The solution makes use of two additional HYPERRIDE grid services: the State Estimation and the Optimal Control solutions (described in the paragraphs above). Moreover, the Service Restoration solution considers as reconfiguration criteria the number of restored loads, their criticality, the power losses, and the priority of tele-controlled switches; the solution is computed by implementing a Multiple-Criteria Decision Analysis (MCDA) approach.

The goal of the Open Reliability Information system is to provide a common platform for storing and sharing component reliability information. The shared data will consist of system and subsystem reliability and maintenance statistics, information on system structure and operation conditions as well as estimations on data quality. The data will be used in quantitative reliability and availability assessments.

Electric vehicles (EV) smart charging service is provided to increase grid operation efficiency. Through a real-time monitoring system and a remote management system, the EV smart charging stations can be used to provide energy flexibility to the electricity grid, so as to avoid reverse power flow due to the distributed renewable energy plants.

III. Real-time Predictions

In this section a possible exploitation of the ICT platform for the prediction of possible failures inside the system is described.

To do that, a preliminary study is being conducted dealing with cascading effects, to determine how a failure can be propagated. This study, specifically conducted on hybrid grids, is letting emerge the significant differences with traditional AC grids and will allow to identify the parameters to take into account to predict and possibly prevent blackouts and failures.

Coupled with this, the ICT platform will include a powerful tool for the root cause analysis, based on machine-learning and evidential networks. This tool will be exploited in case of failures not covered or not identified before and predict the possible causes and take the appropriate countermeasures to avoid the insurgence of the same faults in the future.

A. Cascading Failures Dynamics and Resilience

According to the historical information, cascading failures have played the main role in blackouts in power systems around the world. Therefore, many studies have been conducted to find out the root causes of these failures, predicting and analysing them. Although we may not predict and address some unpredictable phenomena leading cascading failures like environmental disasters or intentional personal attacks, fortunately, the cascading failures are triggered by technical faults like three-phase short-circuits [14]. One of the main goals of cyber-physical systems (CPS) is to control the main operational parameters of the networks like bus voltage, and frequency to predict these failures and take countermeasures to prevent affecting other part of the grid through ICT platforms.

Despite all advantages of AC/DC hybrid grids in operation and cost point-of-view, they have increased challenges in cascading effects analysis. In traditional AC systems, for example, a fault in a line might cause other lines overloading near to it, so that, finally, a cascading failures and blackout is expected, while, in AC/DC systems, a tripped bus close to DC subsystem might affect the parameters of inverters, finally resulting in DC system blocking. In this way, DC generation is lost, and this in turn leads to AC lines overloading more and more. This means blocked DC subsystem might rises the probability of cascading failures. Consequently, there are more parameters which should be controlled in hybrid grids than in AC ones. The studies in [15] and [16] identified the most significant protections in converters such as 100Hz overcurrent protection, zero sequence overcurrent protection, commutation protection, which may response to AC subsystem failures and block DC system. They also suggested some controlling countermeasures to maintain stability. Another challenges for ICT platforms to control these parameters is that these protections response to faults much faster than parameters in AC systems.

In the HYPERRIDE project, we try to implement a state-transient Markov chain approach to estimate the situation of hybrid microgrids. In each emergency state like a short-circuit, topology of the grid is changed, and power flow is instantly dispatched. New topological and technical parameters are sent to the Acquisition and Interoperability Layer through IoT agent in open ICT platform. After analysing the steady-state probability using Markov transition matrix, and comparing to the root causes data in security layer, we can predict new state of the grid, values of parameters in both AC and DC subsystems, predict cascading failures, and finally take proper countermeasures to prevent DC subsystem blocking or whole system blackout.

B. Root Cause Analysis

There are several reasons why a system could fail, resulting in cascading effects. Example root causes might include the following list, to mention a few:

- a cyber-attack, the canonical examples being the Stuxnet virus [17] and the attacks to the Ukrainian power system in 2015 and 2016 [18];
- faults that result in failures, e.g., as devices reach end-of-life;
- misconfiguration by operators of software systems that are used to support control operations; and
- incorrect assumptions regarding the interfaces between systems, e.g., as new systems are added to those that already exist, as is often the case in the smart grid [19].

In many cases, it is important to be able to discriminate between these root causes of failure in an online manner. For example, an understanding of whether a system has failed due to a cyber-attack versus an isolated component failure could result in different consequences for a power system and any cascading effects that must be addressed.

To address this issue in the HYPPERIDE ICT platform, it is proposed to use the REASENS Framework [20]. The framework integrates loosely coupled sensors that generate events that potentially describe the cause of a failure. Sensors might include those used to detect adversarial behaviour, such as intrusion detection systems, or anomalous power system behaviour. In addition, contextual information can be used to support the determination of the root cause of events from sensors – this context might describe the services that are executing on associated IT systems or expected demand profiles, which might explain anomalies.

At the core of the REASENS Framework is an engine that generates alerts that describe the probabilities of distinct root causes of observed events (e.g., an attack or fault). In the current implementation, a formalism called evidential networks (ENs) [21] is used to generate these root cause hypotheses. In short, an EN is a graph structure that is constructed using expert knowledge. Nodes in the graph represent variables that have a so-called frame of discernment – mutually exclusive states that a node could be in. Mass functions describe the relationship between nodes and states.

In the HYPERRIDE project, we will explore the use of components in the ICT Platform to determine potential root causes of failures, specifically those located in the Knowledge

Layer (see Fig. 1) and sensors that are tailored to detecting both cyber-attacks and anomalous power systems behaviour for AC/DC networks. Building on these sensors, in close cooperation with experts from the pilot site partners, ENs will be developed that can be used to determine the root causes of events that support the secure and resilient operation of hybrid AC/DC networks.

In this work, we will explore the nature of the failures that can be identified in a timely manner using REASENS, such that effective mitigation strategies can be deployed. For example, failures that require hard real-time mitigations are not well-suited to this approach, but we will examine other cases in which the framework could provide benefits to operators, including those from the project's pilot sites.

Acknowledgments

The research leading to these results has received funding from the European UnionH2020 Framework Programme (H2020 / 2014-2020) under Grant Agreement No 957788.

References

[1] G. Reed, "9 Reasons Why DC May Replace AC", available at: https://www.electricalindustry.ca/latest-news/1018-9-reasons-why-dc-may-replace-ac (accessed on 21st March 2022).

[2] A. Bonì, S. Favuzza, M. G. Ippolito, F. Massaro, S. Moradi, R. Musca, V. Porgi, G. Zizzo, "A Simulation Analysis for Assessing the Reliability of AC/DC Hybrid Microgrids – Part I: Underground Station and Car Parking", 2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 7-10 September 2021, Bari (Italy).

[3] A. Bonì, S. Favuzza, M. G. Ippolito, F. Massaro, S. Moradi, R. Musca, V. Porgi, G. Zizzo, "A Simulation Analysis for Assessing the Reliability of AC/DC Hybrid Microgrids – Part II: Port Area and Residential Area", 2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 7-10 September 2021, Bari (Italy).

[4] HYPERRIDE Project webiste, available at: https://hyperride.eu/ (accessed on 21st March 2022).

[5] "Context Information Management (CIM) NGSI-LD AP"I, https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.02.02_60/gs_CIM009v010202p.pdf (accessed on 4th April 2022).

[6] TM Forum Open APIs https://www.tmforum.org/open-apis/ (accessed on 4th April 2022).

[7] M. Mammina, A. Rossi, H. Humer, P. Smith, F. Bellesini, E. Mancinelli, A. Dognini, C. Joglekar, Z. Pan, "HYPERRIDE ICT platform specification (1.4)", 2021, Zenodo, available at: https://doi.org/10.5281/zenodo.5537587 (accessed on 21st March 2022).

[8] FIWARE Orion https://github.com/telefonicaid/fiware-orion/ (accessed on 4th April 2022).

[9] "NGSI Context Management - Approved Version 1.0," 2012. http://www.openmobilealliance.org/release/NGSI/V1_0-20120529-A/OMA-TS-NGSI_Context_Management-V1_0-20120529-A.pdf (accessed on 4th April 2022).

[10] FIWARE Cygnus Team, 2017, Cygnus, http://fiwarecygnus.readthedocs.io/en/1.2.2/index.html (accessed on 4th April 2022).

[11] FIWARE, "IDENTITY MANAGER - KEYROCK," https://fiware-idm.readthedocs.io/en/latest/index.html (accessed on 4th April 2022).

[12] FIWARE, "PEP PROXY - WILMA," https://fiware-pep-proxy.readthedocs.io/en/latest/ (accessed on 4th April 2022).

[13] FIWARE, "WELCOME TO AUTHZFORCE'S OFFICIAL DOCUMENTATION," https://authzforce-ce-fiware.readthedocs.io/en/latest/ (accessed on 4th April 2022).

[14] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, ''A critical review of cascading failure analysis and modeling of power system,'' Renew. Sustain. Energy Rev., vol. 80, pp. 9–22, Apr. 2017.

[15] Y. Zhong, X. Zhang, S. Huang, X. Yu, Z. Zhang, and Q. Zhu, "Cascading failure model of AC-DC system and blackout mechanism analysis," in Proc. IEEE PES General Meeting, 2014, pp. 1–5.

[16] Taoxi Zhu, Chao Wang and Jing Zhang, "Influence of the AC system faults on HVDC system and recommendations for improvement," in Proc. IEEE Power & Energy Society General Meeting (PES 2009), pp. 1-6, 26-30 July 2009.

[17] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Secur. Priv. Mag., vol. 9, no. 3, pp. 49–51, May 2011, doi: 10.1109/MSP.2011.67.

[18] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," IEEE Trans. Power Syst., vol. 32, no. 4, pp. 3317–3318, 2017.

[19] N. G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press, 2012.

[20] E. Piatkowska, C. Gavriluta, P. Smith, and F. P. Andrén, "Online Reasoning about the Root Causes of Software Rollout Failures in the Smart Grid," in 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2020, pp. 1–7. doi: 10.1109/SmartGridComm47815.2020.9303005.

[21] P. P. Shenoy, "A valuation-based language for expert systems," Int. J. Approx. Reason., vol. 3, no. 5, pp. 383–411, 1989, doi: https://doi.org/10.1016/0888-613X(89)90009-1.