Microgrid Systems

Subjects: Engineering, Electrical & Electronic

Contributor: Thorsten Reimann

A microgrid is an independent power system that can be connected to the grid or operated in an islanded mode. This single grid entity is widely used for furthering access to energy and ensuring reliable energy supply.

microgrid assessment performance metrics reliability distributed energy resources cybersecurity

1. Introduction

Wildly seen as a key to support large-scale integration of renewable energy sources and low carbon technologies connected to low and medium voltage networks, microgrids (MGs) are expected to play a substantial role in reaching the UN's goal of "sustainable energy for all". They could be a building block of the centralized grid and foster the coupling of different energy sectors, facilitate demand-side management (DSM), or provide ancillary services, such as increased resilience or flexibility. Especially in Europe, MG technologies will support the recent clean energy legislation that requires creating electricity markets with "active customers/consumers and citizens" and "energy communities" [1][2][3][4].

However, internationally harmonized testing protocols and performance assessment guidelines for MG systems have yet to be defined. Challenging obstacles for a comprehensive MG performance assessment are fast evolving MG technologies, changing requirements for grid-connected and islanded operation, and a lack of standardization. Moreover, their associated performance levels and indicators are not commonly available. Nevertheless, customers need to be able to compare MG controllers and functionalities on a neutral basis. The benchmarking of MGs functions would serve as a guideline for energy communities and industrial applications. Contributing to the effort of establishing standardized assessments of MGs, this paper describes the existing testing requirements and possible performance indicators for the following MG concerns: reliability, including the transition between operation modes, network protection, power quality and ancillary services, as well as energy dispatch and cybersecurity. However, the impact of outages by maintenance or faults on the system performance is not directly addressed in this paper. Those outages as also special flexibility aspects and self-healing capacities after faults are partly covered by the reliability aspects. Moreover, alternating current (AC) MGs are the main focus of this work as they can directly be integrated into existing power networks, making them a midterm growing market in developed economies and thus requiring a rapid standardization to ensure a coherent deployment.

2. Microgrid and Benchmarking

2.1. Microgrid Objectives and Functions

Different MG definitions have been set within the Institute of Electrical and Electronics Engineers (IEEE) 2030.7 standard [5], the US Department of Energy report [6], the International Electrotechnical Commission (IEC) 60050-617 standard [7] and the CIGRÉ MG evolution roadmap [2]. By aggregating them, an MG can be defined as a group of loads and generators that operates as a single entity in grid-connected or islanded mode concerning the utility grid, as illustrated by Figure 1.

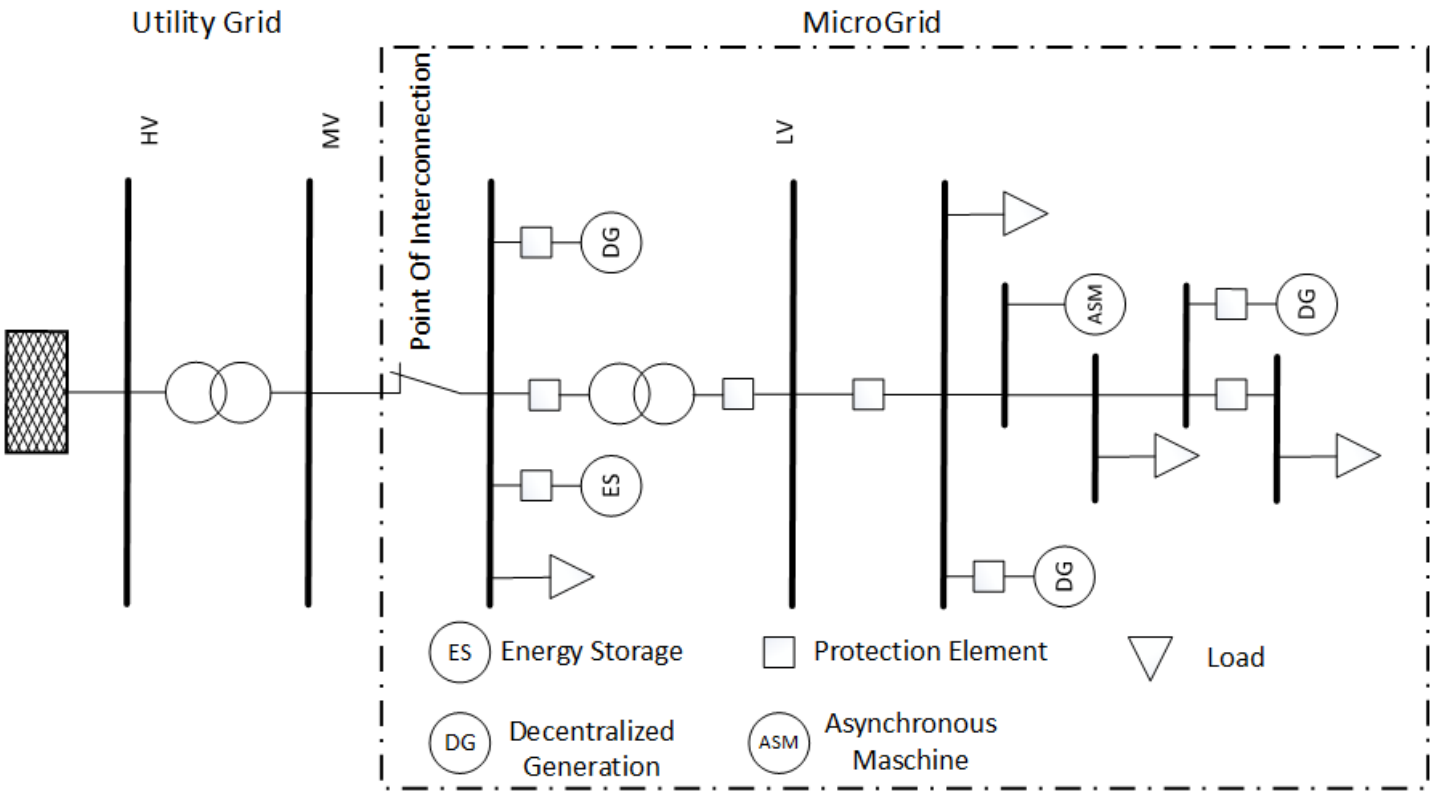

Figure 1. General microgrid schematic illustrating the interconnected (switch closed) and islanded (switch opened) operation modes. POI—point of interconnection; LV—low voltage; MV—medium voltage; HV—high voltage .

As detailed in [2], MGs have three main objectives: to provide an alternative to local energy service in terms of power quality and/or reliability, to enhance the usage of local energy assets and to interface the main grid with variable local sources and loads. These objectives can have different priorities or required quality levels depending on the use case. Critical infrastructures may prioritize reliability in terms of continuity of supply and cybersecurity, energy communities may prioritize usage of local generation and energy dispatch, and MGs with sensitive industrial or information communication technology (ICT) loads may prioritize power quality. However, while implementing those features, MGs are challenging in terms of operation and control, which requires appropriate standards and testing processes. Some of these challenges include stability issues, low inertia, bidirectional power flows and uncertainty [8][9].

2.2. Standards and Technical Specifications

Standards build a base of understanding the requirements of smart grids, including MG as a special kind of smart grid [10]. In particular, IEEE standards cover the interoperability and the interconnection of distributed resources with smart grids considering islanded microgrids (IMGs) and grid-connected microgrids (GMGs). Moreover, IEEE describes specific testing procedures for MG controllers and storage systems. Concerning IEC standard series 62898, it gives the requirements for the design and operation of MGs. Coming IEC publications will also tackle MG features, such as protecting MGs and its energy dispatch management. Those standards provide examples for MG structures, requirements and their control as well as protection in general that serve as recommendations, which are used and discussed later in this paper. Standards, grid codes and directives, as shown in Table 1, regulate the implementation and testing of MGs.

Table 1. Standards, grid codes and directives for delta-wye transformer (MG) systems.

Abbreviation	Title	Date of Issue
	Standard	
IEEE 1547.4	IEEE Guide for Design, Operation, and Integration of Distributed Resource Island Systems with Electric Power Systems	07-2011
IEEE 2030	IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads	09-2011
IEEE 2030.2	IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure	03-2015
IEEE 2030.3	IEEE Standard Test Procedures for Electric Energy Storage Equipment and Systems for Electric Power Systems Applications	06-2016
IEEE 2030.7	IEEE Standard for the Specification of Microgrid Controllers	12-2017
IEEE 2030.8	IEEE Standard for the Testing of Microgrid Controllers	06-2018
IEEE 2030.9	IEEE Recommended Practice for the Planning and Design of the	03-2019

Abbreviation	Title	Date of Issue
	Standard	
	Microgrid	
IEC 62898-1	Microgrids—Part 1: Guidelines for microgrid projects planning and specification	05-2017
IEC 62898-2	Microgrids—Part 2: Guidelines for operation	09-2018
IEC 62898-3-1	Microgrids—Part 3-1: Technical requirements—Protection and dynamic control	09-2020
IEC 62898-3-2	Microgrids—Part 3-2: Technical requirements—Energy management systems	Expected in 12-2022
IEC 62898-3-3	Microgrids—Part 3-3: Technical requirements—Self-regulation of dispatchable loads	Expected in 12-2021
DIN EN 50160	Voltage characteristics of electricity supplied by public electricity networks	11-2020
	Grid codes for interoperability with the electrical power system/grid	
Commission Regulation (EU) 2016/631	Establishing a network code on requirements for grid connection of generators	04-2016
	Directives	

Abbreviation	Title	Date of Issue
	Standard	
Directive 2009/72/EC	Common rules for the internal market in electricity and repealing Directive 2003/54/EC	07-2019
FERC Order 888	The Federal Energy Regulatory Commission's Open Access Rule	1996
IT-SiG 2.0	Draft of a second law to promote the security of information technology systems (title translated from German)	05-2020
BSI-KritisV	Decree on the regulation of critical infrastructures according to the BSI-Act (title translated from German) [11][12][13]	04-2016
NISRIR 7628 [2]	Guidelines for Smart Grid Cybersecurity	07-2014

nalities to id market numerous ed view is alities are parison of or Electric ions. The ity of MG From the marizes a literature review on microgrid test-beds according to their application, power level and described tests. We notice that direct current (DC) MG systems are underrepresented compare to AC ones. Moreover, information about systems presenting recent activities and, thus, potential availability for further testing is given when available.

Table 2. MG systems and test-beds for MG with points of interconnection (POI) [11][12][13]. The information from the column "Specific Test" is extracted from the previous references. Acronyms: Centre for Renewable Energy Sources and Saving (CRES), Fraunhofer Institute for Energy Economics and Energy System Technology (IEE), Central Research Institute of Electric Power Industry (CRIEPI), and New Energy and Industrial Technology Development Organization (NEDO). Note that the sign "−" indicates that the information is not available for the considered site.

Application (Location)	Name (Organization)	Voltage Level	Rated Power (kW)	Specific Test	Site Available
Mixed, AC	Boralex planned islanding (Hydro Quebec)	25 kV	8750	Transient response, outage solution	−

Application (Location)	Name (Organization)	Voltage Level	Rated Power (kW)	Specific Test	Site Available
(Canada, Senneterre)					
Test system, AC (US, Wisconsin—Madison)	UW microgrid (University of Wisconsin—Madison)	<1 kV	–	Investigation controls diesel generators	yes
Residential, AC (The Netherland, Bronsbergen)	Bronsbergen Holiday Park (CONTINUON)	<1 kV	315	Central control	–
Residential, AC (US, Columbus, OH)	CERTS testbed (CERTS)	<1 kV	173	Power quality optimization and energy management	yes
Test microgrid, DC (Italy, -)	CESI RICERCA DER test microgrid (CESI)	<1 kV	251	Local and supervisory control with fast transients	yes
Residential, AC (Greece, Kythnos Island)	Kythnos island microgrid (CRES)	<1 kV	102	Islanded	yes
Residential and small business, AC	SysTec LV smart grid and MV hybrid system test bench (IEE)	<1 kV/20 kV	120/500	Islanding switches Local und supervisory control	–

Application (Location)	Name (Organization)	Voltage Level	Rated Power (kW)	Specific Test	Site Available
(Germany, Kassel)					
Test system, AC (UK, Manchester)	Microgrid/flywheel energy storage laboratory prototype (University of Manchester)	<1 kV	42	Intelligent control	–
Test system, AC (Japan, Gunma)	Test network at Akagi (CRIEPI)	6.6 kV	1775	Algorithms for day-ahead planning	yes
Rural grid, AC (Japan, Kyotango)	Kyoto eco-energy project (NEDO)	MV	450	Internet-based communication for DER	–
Residential, AC (-)	CIGRE low voltage distribution benchmark system (CIGRE)	<1 kV	99	Control options for DER	–
Mixed loads, AC (-)	IEC microgrid benchmark (IEC)	25 kV	16,200	Setting of optimal protection systems	–

and that
he risk of
n-specific
der three

trol

ity, safety
use partly
overlapping functionalities.

3.2. Use of Distributed Local Resources

Energy dispatch or energy management system (EMS) refers to the slowest MG control where operations are carried out at the minute scale or more. Furthermore, called tertiary control, this level consists of the operating and controlling features acting on the energy resources and loads to manage the power flow exchanges within the MG and with the main grid to ensure optimal operations [14]. This optimality is usually defined in terms of economic as well as ecological criteria. In charge of the energy dispatch optimization, EMS can be divided into different modules dealing with the demand and the production side as well as the forecasting of both [15]. Those modules are defined as:

- Demand-side management (DSM);
- Dispatch optimization (DO);
- Forecasting module (FM).

DSM includes methods used to adapt demand to available generation, for example, to promote self-consumption and reduce the aggregated energy consumption during peak demand [16]. These processes are encouraged by financial incentives, such as off-peak rates that lower the electricity cost during specific times as well as through consumer education. The aim of those preventive methods is not only to reduce the overall consumption but also to spread it temporally so as to match generation and infrastructure capacities with energy demand. By ensuring this energy balance, DSM reduces the need for investments in power system capacity. On the generation side, DO refers to the methods used to optimally generate energy and allocate it according to the loads, storage systems and sources [17].

The sources can be all kinds, including diesel generators, solar panels, or wind turbines. DO can aim for different optimization objectives, such as economical ones by reducing the energy costs or environmental by reducing the CO2 emissions or by increasing the share of renewable energy used. Another optimization objective can be the power stability in the MG to ensure a high-power quality. Finally, FM refers to the forecasting techniques applied to predict power generation [18] as well as energy load [19] and electricity prices [20] based on external and internal factors. Forecasting techniques are numerous and can range from linear to nonlinear methods as well as machine learning ones. The techniques are selected according to the forecast requirements, the data available and the time resolution. Common forecasts for power generation are mainly related to renewable energy, such as solar and wind power.

Comparing EMS control features is challenging as various strategies, having distinct characteristics and objectives, have been developed to carry out those functionalities. To interpret the performance difference, it is necessary to identify the characteristics of the compared control modules. For example, the comparison of two energy load FMs having different time resolutions, prediction methods and data inputs will not allow concluding, which characteristics influence the variations of performance on the MG fuel consumption. Additionally, comparing DSM modules presenting distinct control architectures and prediction horizons will also lead to a weak interpretation of their performance differences as their source is uncertain. Moreover, to evaluate tertiary control modules, it is recommended to identify and limit their characteristics differences.

3.3. Cybersecurity

Cybersecurity is an important factor in the life cycle and operation of an MG. This section gives an overview of cybersecurity aspects as well as current approaches for improving security on different levels. Subsequently, a summary of quality benchmarks for a cyber-secure MG is presented, along with recommended actions, which can reduce security risks in such systems.

The MG is a cyber-physical system, which comprises information, control, communication and field levels [21]. The information level refers to the processing, storing, and provisioning of information in data centers and cloud applications. The aggregated information is also used at the control level, which coordinates the secure, reliable and stable operation of the grid. Control-level applications (e.g., SCADA and DCS) are concerned with monitoring and managing grid operations. The communication level comprises information and ICT, which allows the timely and secure transmission of information between different actors (e.g., measurements or control commands). Lastly, the field level includes the electrical equipment and smart devices involved in energy generation, transmission, distribution, consumption, and measurement.

Attacks targeting an MG can be initially classified as passive and active. Passive attacks extract valuable information, such as consumer data, credentials, and configurations. Information leakage is generally a high-risk problem if privacy is a concern, but it appears at first inconsequential for the grid's safe operation. However, the leaked information could allow passive actors to corrupt a system actively in the future [22]. Active attacks include injection of meter readings, forging or replaying commands, and elevating the privilege of users to corrupt a system temporarily (e.g., to disrupt or destroy it) or permanently (i.e., as a strategic access point in the future). Adversaries can exploit several attack vectors, which introduce significant risks in the electrical infrastructure. In a worst-case scenario, attacks can lead to blackouts, physical damage, and loss of life. Exploitable attack vectors must be addressed on a device, software, communication, and orchestration level [23].

The main cyber-security challenge on a field or device level can be summarized as the reliance on inputs and actions of devices that may be in the hands of an adversary. Indeed, the issue is compounded by the fast deployment of smart devices without adequate security and protection. Trust in the MG control and operation can be defined as some degree of confidence that, during some specific interval, the appropriate actor is accessing accurate and unmodified data, which is created by the intended device in the expected location at the proper time and communicated using the expected protocols [24]. Traditionally, the grid's control system is viewed as an environment with implicit security and trust (e.g., because the infrastructure is owned, operated, and protected by the operator). However, MG devices do not necessarily have physical protection and are owned and operated by multiple parties, including potential adversaries. Devices must be designed to be tamper-resistant to prevent physical manipulation. Additionally, the push towards cloud services for grid management has significantly increased the number and variety of devices and parties involved such that often, access control-based policies will not be applicable or scale well [25]. The use of trusted computing hardware for MG devices can effectively address the need for adequate authentication, authorization, and credential protection as they offer a secure foundation (a root of trust) for important security guarantees, such as integrity, authenticity, confidentiality, provenance, and resilience [26][27][28].

The complexity of software systems, which enable the function, control, and processing in a smart MG, is increasing and rivals that of today's commodity systems (e.g., IoT devices, mobile and desktop computers) [29]. MG layers commonly share software from other domains and computing systems and with it their bugs and vulnerabilities. However, threats related to software engineering are well known and can be addressed in several ways [30]. The software systems in an MG will have to be designed and tested to the same principles as software,

which is expected to be secure. Safety-critical systems often must undergo much more rigorous testing and certification procedure. One approach to improve software quality is referred to as formal specification and verification. However, large pieces of software (e.g., legacy code, updates, or patches) are notoriously laborious to specify, verify, or certify [31]. Fuzzing technologies provide an efficient way for testing such software systems for bugs and errors [32]. The MG is an essential infrastructure where non-critical software (e.g., user interfaces) should not interfere with critical software components. Applications from different security domains and with different levels of criticality must be isolated from another.

References

1. Sophie Marchand; Cristian Monsalve; Thorsten Reimann; Wolfram Heckmann; Jakob Ungerland; Hagen Lauer; Stephan Ruhe; Christoph Krauß; Microgrid Systems: Towards a Technical Performance Assessment Frame. Energies 2021, 14, 2161, 10.3390/en14082161.
2. Marnay, C.; Chatzivasileiadis, S.; Abbey, C.; Iravani, R.; Joos, G.; Lombardi, P.; Mancarella, P.; von Appen, J. Microgrid Evolution Roadmap. In Proceedings of the Smart Electric Distribution Systems and Technologies (EDST), 2015 International Symposium on IEEE, Vienna, Austria, 8–11 September 2015; pp. 139–144.
3. Oleinikova, I.; Hillberg, E. Micro vs MEGA: Trends Influencing the Development of the Power System. May 2020. Available online: (accessed on 1 March 2021).
4. Ackeby, S.; Tjäder, J.; Bastholm, C. The role and interaction of microgrids and centralized grids in developing modern power systems. Cigrée Electricity Supply to Africa and Developing Economies: Challenges and Opportunities. In Proceedings of the 8th Southern Africa Regional Conference, Cape Town, South Africa, 14–17 November 2017.
5. IEEE 2030.7-2017. IEEE Standard for the Specification of Microgrid Controllers; IEEE Std: Piscataway, NJ, USA, 2018.
6. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability Smart Grid R&D Program. DOE Microgrid Workshop Report; U.S. Department of Energy: Washington, DC, USA, 2011; pp. 1–32.
7. 60050-617. Amendment 2—International Electrotechnical Vocabulary (IEV)—Part 617: Organization/Market of Electricity. 2017. Volume 01.040.29. Available online: (accessed on 1 March 2021).
8. Olivares, D.E.; Mehrizi-Sani, A.; Etemadi, A.H.; Cañizares, C.A.; Iravani, R.; Kazerani, M.; Hajimiragha, A.H.; Gomis-Bellmunt, O.; Saeedifard, M.; Palma-Behnke, R.; et al. Trends in microgrid control. IEEE Trans. Smart Grid 2014, 5, 1905–1919.
9. Soshinskaya, M.; Crijns-Graus, W.H.J.; Guerrero, J.M.; Vasquez, J.C. Microgrids: Experiences, barriers and success factors. Renew. Sustain. Energy Rev. 2014, 40, 659–672.

10. Basso, T.; Hambrick, J.; DeBlasio, D. Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards. In Proceedings of the Innovative Smart Grid Technologies (ISGT), Washigton, DC, USA, 16–20 January 2012; pp. 1–7.
11. Papathanassiou, S.; Hatziargyriou, N.; Strunz, K. A benchmark low voltage microgrid network; Technol. impacts Dev. Oper. Performances. In Proceedings of the CIGRE Symposium: Power Systems with Dispersed Generation, Athens, Greece, 13–16 April 2005; pp. 1–8.
12. Lidula, N.W.A.; Rajapakse, A.D. Microgrids research: A review of experimental microgrids and test systems. Renew. Sustain. Energy Rev. 2011, 15, 186–202.
13. Naily, N.E.; Saad, S.M.; El Misslati, M.M.; Mohamed, F.A. Optimal Protection Coordination for IEC Microgrid Benchmark Using Water Cycle Algorithm. In Proceedings of the 10th International Renewable Energy Congress (IREC), Sousse, Tunisia, 26–28 March 2019; pp. 1–6.
14. Bidram, A.; Davoudi, A. Hierarchical structure of microgrids control system. IEEE Trans. Smart Grid 2012, 3, 1963–1976.
15. Shayeghi, H.; Shahryari, E.; Moradzadeh, M.; Siano, P. A survey on microgrid energy management considering flexible energy sources. Energies 2019, 12, 2156.
16. Meyabadi, A.F.; Deihimi, M.H. A review of demand-side management: Reconsidering theoretical framework. Renew. Sustain. Energy Rev. 2017, 80, 367–379.
17. Gandhi, O.; Rodriguez-Gallegos, C.D.; Srinivasan, D. Review of optimization of power dispatch in renewable energy system. In Proceedings of the IEEE PES Innovative Smart Grid Technolologies, Melbourne, VIC, Austalia, 28 November–1 December 2016; pp. 250–257.
18. Sobri, S.; Koohi-Kamali, S.; Rahim, N.A. Solar photovoltaic generation forecasting methods: A review. Energy Convers. Manag. 2018, 156, 459–497.
19. Fallah, S.N.; Deo, R.C.; Shojafar, M.; Conti, M.; Shamshirband, S. Computational intelligence approaches for energy load forecasting in smart energy management grids: State of the art, future challenges, and research directions. Energies 2018, 11, 596.
20. Jiang, L.; Hu, G. A Review on Short-Term Electricity Price Forecasting Techniques for Energy Markets. In Proceedings of the 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 18–21 November 2018; pp. 937–944.
21. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. Proc. IEEE 2017, 105, 1367–1388.
22. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity 2019, 2, 384.
23. Kummerow, A.; Rösch, D.; Monsalve, C.; Nicolai, S.; Bretschneider, P. Challenges and opportunities for phasor data based event detection in transmission control centers under cyber

security constraints. In Proceedings of the IEEE Milan PowerTech, Milano, Italy, 23–27 June 2019; pp. 3–8.

24. Khurana, H.; Hadley, M.; Lu, N.; Frincke, D.A. Smart-grid security issues. IEEE Secur. Priv. 2010, 8, 81–85.
25. Ryan, M.D. Cloud computing security: The scientific challenge, and a survey of solutions. J. Syst. Softw. 2013, 86, 2263–2268.
26. Metke, A.R.; Ekl, R.L. Security Technology for Smart Grid Networks. IEEE Trans. Smart Grid 2010, 1, 99–107.
27. Kuntze, N.; Rudolph, C.; Bente, I.; Vieweg, J.; von Helden, J. Interoperable device identification in smart-grid environments. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–7.
28. Lauer, H.; Salehi, A.; Rudolph, C.; Nepal, S. User-centered attestation for layered and decentralized systems. In Proceedings of the Workshop on Decentralized IoT Security and Standards (DISS), San Diego, CA, USA, 18 February 2018.
29. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey. IEEE Commun. Surv. Tutor. 2019, 21, 2637–2670.
30. McGraw, G. Software security. IEEE Secur. Priv. 2004, 2, 80–83.
31. Klein, G.; Elphinstone, K.; Heiser, G.; Andronick, J.; Cock, D.; Derrin, P.; Elkaduwe, D.; Engelhardt, K.; Kolanski, R.; Norrish, M.; et al. seL4: Formal verification of an OS kernel. In Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles; Big Sky, MT, USA, 11–14 October 2009, pp. 207–220.
32. Godefroid, P.; Levin, M.Y.; Molnar, D. SAGE: Whitebox Fuzzing for Security Testing; ACM: New York, NY, USA, 2012; Volume 55.