IAES Journal of Electrical and Electronics Engineering
Vol. 12, No. 1, June 2025, pp. 1~6
ISSN: 2338-7432, DOI: 10.11591/jeee.v12i1.pp1-6

Interoperable smart plug systems for building automation: a review of IoT platforms, standardization, and multi-device integration

Ahmad Raditya Cahya Baswara[1], Tole Sutikno[1], Anggit Pamungkas[2]
[1]Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

Article Info

Article history:

Received Dec 3, 2022
Revised Jun 26, 2023
Accepted Jan 11, 2024

Keywords:

Building automation
Internet of things
Interoperability
IoT platforms
Multi-device integration
Smart plugs
Standardization

ABSTRACT

Smart plugs are increasingly used to monitor and control electrical appliances, yet their value in building automation depends on their ability to communicate with devices and platforms from different manufacturers. Proprietary interfaces, incompatible communication protocols, inconsistent data models, and fragmented control applications frequently prevent smart plugs from operating as part of a unified building system. This review examines the development of interoperable smart plug systems through the perspectives of IoT communication technologies, integration platforms, standardization, and multi-device building automation. It discusses Wi-Fi, bluetooth low energy, Zigbee, Thread, message queuing telemetry transport (MQTT), constrained application protocol (CoAP), and web-based approaches, together with middleware and semantic models that support cross-platform communication. The literature indicates that protocol compatibility alone is insufficient because devices must also share consistent descriptions of functions, measurements, states, and control capabilities. Gateways, open application programming interfaces (APIs), and semantic frameworks such as Brick and smart applications reference ontology (SAREF) can help bridge these differences and connect smart plugs with building management systems. Nevertheless, security, lifecycle management, vendor dependence, and inconsistent implementation remain significant barriers. Future systems should combine open communication interfaces, standardized information models, secure device management, and scalable edge-cloud architectures to support reliable building-wide automation.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Tole Sutikno
Faculty of Industrial Technology, Universitas Ahmad Dahlan
Yogyakarta, Indonesia
Email: tole@te.uad.ac.id

1. INTRODUCTION

Building automation systems increasingly combine electrical appliances, lighting, heating, ventilation, air conditioning, sensors, meters, and supervisory controllers. Smart plugs extend this environment by providing outlet-level energy monitoring and remote switching without requiring extensive modifications to existing electrical installations. Their integration into building automation can support energy management, occupancy-responsive control, scheduled operation, and equipment monitoring. However, these benefits become limited when smart plugs operate independently through manufacturer-specific applications or cloud services [1], [2].

Interoperability is therefore a central requirement for transforming individual smart plugs into coordinated building resources. Devices from different manufacturers may use different wireless technologies, application programming interfaces, message formats, authentication procedures, and control conventions. A device may successfully connect to a wireless network but remain unable to exchange meaningful information with another platform. Consequently, interoperability must address communication, data representation, device discovery, security, and application-level coordination rather than connectivity alone [3], [4].

This review examines the technical foundations and integration strategies that can support interoperable smart plug systems in buildings. It considers communication technologies, IoT platforms, standardization frameworks, semantic information models, and multi-device automation. The central argument is that a scalable system requires both technical compatibility and a shared understanding of device functions and data. The discussion follows the research problem from protocol fragmentation to integration architecture, practical limitations, and future research directions.

2. INTEROPERABILITY REQUIREMENTS FOR SMART PLUG SYSTEMS

Interoperability can be understood through several complementary layers that determine whether heterogeneous devices can cooperate effectively. Transport interoperability enables devices to exchange information through compatible communication networks, while syntactic interoperability ensures that transmitted messages follow recognizable formats. Semantic interoperability allows different platforms to interpret measurements and commands consistently, even when their internal data models differ. Behavioral and security interoperability further ensure that devices respond predictably and exchange information under appropriate access-control policies [3], [5].

Smart plugs introduce specific requirements because they perform both measurement and control functions. A typical device may report active power, accumulated energy, voltage, current, switching state, and operational status. A building platform must understand whether a reported value represents instantaneous power, cumulative energy, or a device-specific status indicator. It must also distinguish a command to switch an outlet from a measurement describing its current operating state [6], [7].

Cross-brand integration becomes particularly difficult when manufacturers use proprietary device identifiers and application interfaces. Two smart plugs may provide similar electrical functions but expose different data structures and control endpoints. A middleware layer can translate these differences into a common representation without requiring every application to implement a separate interface for each manufacturer. Research on resource identifier interoperability demonstrates that mapping device identities and resource paths can enable services to operate across otherwise separate IoT platforms [8].

3. COMMUNICATION TECHNOLOGIES AND PROTOCOLS

Communication technologies determine how smart plugs connect to gateways, local controllers, and cloud platforms. Wi-Fi is widely used because it can connect directly to existing IP networks and supports relatively high data throughput. Bluetooth low energy is appropriate for short-range commissioning and low-power communication, while Zigbee provides mesh networking for devices that benefit from distributed connectivity. Thread offers another low-power mesh approach based on IPv6, whereas wired technologies such as Ethernet and established building automation networks remain relevant for reliable infrastructure integration [1], [9].

These technologies should not be treated as interchangeable because they have different network characteristics and integration requirements. Wi-Fi smart plugs may communicate directly with a local network, while Zigbee devices generally require a compatible coordinator or gateway. Bluetooth-based devices may require a bridge or local controller before their measurements can be shared with a building platform. The selection of a communication technology should therefore consider network coverage, power consumption, device density, latency, security, and the availability of suitable gateways [1], [10].

Application-layer protocols provide another level of interoperability between smart plugs and software platforms. Message queuing telemetry transport (MQTT) uses a publish-subscribe model that allows devices to publish measurements and receive control messages through a broker. Constrained application protocol (CoAP) provides a lightweight request-response approach for constrained devices, while HTTP-based application programming interfaces (APIs) support integration with web services and conventional software applications. These protocols can simplify data exchange, but they do not automatically guarantee semantic compatibility because different manufacturers may still use different topic structures, resource names, payload fields, and command definitions [7], [11].

4. IOT PLATFORMS AND INTEGRATION MIDDLEWARE

IoT platforms provide the software infrastructure required to register devices, collect telemetry, process events, and deliver automation services. Commercial platforms generally provide managed connectivity, device administration, cloud storage, analytics, and application development tools. Open-source platforms such as Home Assistant, openHAB, ThingsBoard, and FIWARE provide different combinations of local automation, device integration, dashboards, and data management. Their suitability depends on supported protocols, extensibility, deployment architecture, security capabilities, and the availability of integrations for the smart plugs being deployed [6], [12].

Middleware is particularly important when a building contains multiple device families and communication technologies. It can act as an intermediary between smart plugs, gateways, building controllers, and higher-level applications. Protocol adapters translate incoming messages, while device registries maintain information about connected equipment and available functions. A well-designed middleware architecture also separates device-specific communication from automation logic, allowing applications to be reused when individual devices or manufacturers change [13], [14].

Platform integration must also address device identity and resource discovery. A building application needs to identify each smart plug consistently, determine its location, and discover the measurements and commands it supports. Without a shared resource model, duplicate device records and incompatible identifiers can complicate automation across multiple platforms. Research on heterogeneous IoT platforms has demonstrated that resource mapping and identifier translation can support cross-platform service requests without requiring every device to be physically duplicated within a central system [8].

5. STANDARDIZATION AND SEMANTIC INTEROPERABILITY

Standardization provides a foundation for reducing fragmentation across smart building technologies. Established building automation technologies such as BACnet and KNX have long supported the integration of controllers and building equipment, while newer IoT approaches extend connectivity to wireless devices and cloud services. Standards such as ISO/IEC 21823 provide a framework for understanding interoperability in IoT systems, including transport, syntactic, semantic, behavioral, and policy aspects. The broader challenge is to connect these layers so that smart plugs can participate in building-wide applications rather than remain isolated consumer devices [1], [3], [10].

Semantic interoperability is especially important because identical measurements may be described differently by different manufacturers. One platform may report power using a field named power, while another may use a different property name, unit convention, or measurement description. Semantic models provide machine-readable definitions of devices, properties, relationships, and functions so that applications can interpret information consistently. Research on IoT semantic interoperability highlights ontologies and middleware as important approaches for integrating heterogeneous systems [5], [15]. Table 1 is technologies and frameworks supporting smart plug interoperability

Table 1. Technologies and frameworks supporting smart plug interoperability

Technology or framework	Primary role	Relevance to smart plug integration	Main consideration
Wi-Fi	IP-based wireless connectivity	Direct network connection for many smart plugs	Network congestion and device security
Bluetooth Low Energy	Short-range wireless communication	Commissioning and local device access	Gateway or bridge may be required
Zigbee	Low-power mesh networking	Integrating multiple low-power devices	Coordinator and device-profile compatibility
Thread	IPv6-based mesh networking	IP connectivity for low-power devices	Ecosystem and controller compatibility
MQTT	Publish-subscribe messaging	Telemetry and command exchange	Common topic and payload definitions
CoAP	Lightweight resource communication	Constrained-device integration	Application and security configuration
BACnet / KNX	Building automation communication	Connection to established building systems	Gateway and object-model mapping
Brick / SAREF	Semantic information modeling	Consistent description of devices and data	Ontology alignment and maintenance
IoT middleware	Protocol and platform integration	Device discovery, translation, and orchestration	Scalability and lifecycle management

Building-oriented information models provide a practical foundation for this integration. Brick offers a structured vocabulary for describing building equipment, points, relationships, and telemetry, while

SAREF provides a reference ontology for smart applications and connected devices. Project Haystack and RealEstateCore provide additional approaches for representing building assets and operational information. Comparative studies of building ontologies show that these models have different scopes and strengths, and that harmonization remains necessary when multiple schemas are used together [11], [13].

Table 1 summarizes the main technologies and standardization approaches relevant to interoperable smart plug systems. It distinguishes the function of each approach from the integration challenge that must be addressed during implementation.

6. MULTI-DEVICE INTEGRATION AND BUILDING AUTOMATION

Interoperable smart plugs become more valuable when their measurements and switching capabilities are coordinated with other building systems. For example, a building controller can combine plug-level energy data with occupancy sensors, lighting controls, and heating, ventilation, and air conditioning (HVAC) schedules to implement coordinated energy-management strategies. A smart plug may switch a non-critical appliance according to an occupancy schedule or respond to a demand-response signal from the building platform. Such coordination requires reliable device status information, consistent command handling, and appropriate control priorities [16], [17].

Integration with building information modeling and building management systems can further improve the contextual use of smart plug data. A plug should ideally be associated with a specific room, circuit, equipment category, and operational purpose rather than represented only by a network address. This context allows building applications to group loads by location or function and evaluate energy consumption at different levels. Research on smart-building digital twins and ontology-based data integration indicates that connecting building information with operational IoT data can support more consistent monitoring and management [18], [19].

Multi-device automation must also account for reliability and safety. A network failure should not leave essential building functions dependent on an unavailable cloud service, and control commands should be checked against device status and operational constraints. Critical loads should have appropriate local protection and should not be switched solely according to generic energy-saving rules. A robust architecture therefore combines local control, centralized supervision, event logging, and clearly defined fallback behavior [14], [20].

7. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Despite progress in IoT platforms and communication standards, full interoperability remains difficult to achieve in practical building environments. Devices may support the same protocol but implement different subsets of its functions or use manufacturer-specific extensions. Gateways can translate messages, but they may introduce additional latency, configuration effort, and maintenance requirements. Future research should therefore evaluate interoperability through practical multi-vendor testing rather than relying only on protocol support statements or nominal compliance [4], [8], [10].

Security and privacy are equally important because smart plugs can expose information about appliance use, occupancy patterns, and building operations. Insecure credentials, weak authentication, outdated firmware, and excessive cloud permissions can create risks across connected systems. Interoperable platforms should provide secure onboarding, encrypted communication, role-based authorization, software-update mechanisms, and auditable device management. These controls must be applied consistently across gateways, local controllers, cloud services, and third-party applications [3], [14].

Future systems should combine open communication interfaces with standardized semantic models and modular integration middleware. Edge computing can support local automation and reduce dependence on remote services, while cloud platforms can provide building-wide analytics and centralized device management. Digital twins can connect smart plug measurements with building spaces, assets, and operational relationships, supporting more context-aware automation. Research should also establish repeatable interoperability benchmarks that measure device discovery, data consistency, command reliability, latency, security, and recovery after network disruptions [11], [22], [23].

8. CONCLUSION

Interoperable smart plug systems can extend building automation by connecting outlet-level monitoring and control with broader IoT and building management infrastructures. However, reliable integration requires more than wireless connectivity because devices must also share compatible interfaces, resource identifiers, data structures, semantics, and security mechanisms. Communication technologies such

as Wi-Fi, Zigbee, bluetooth low energy, and Thread provide different connectivity options, while MQTT, CoAP, gateways, and middleware support the exchange of information across platforms. Semantic models such as Brick and SAREF can provide the shared context required to integrate smart plugs with building assets and automation applications. The remaining challenges include vendor-specific implementations, ontology alignment, cybersecurity, lifecycle management, and dependable multi-device control. Future development should prioritize open interfaces, harmonized information models, local resilience, and measurable cross-vendor conformance. These developments can enable smart plugs to function as interoperable components of scalable, secure, and energy-aware building automation systems.

REFERENCES

[1] V. A. Orfanos, S. D. Kaminaris, P. Papageorgas, D. Piromalis, and D. Kandris, "A comprehensive review of IoT networking technologies for smart home automation applications," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, 2023, doi: 10.3390/jsan12020030.

[2] S. Verbeke, K. Laffont, and D. Rua, "Interoperability as a driver or barrier of smart building technologies?," in *CLIMA 2022 conference*, 2022, pp. 1–7, [Online]. Available: https://proceedings.open.tudelft.nl/clima2022/article/view/327.

[3] S. S. Albouq, A. A. A. Sen, N. Almashf, M. Yamin, A. Alshanqiti, and N. M. Bahbouh, "A survey of interoperability challenges and solutions for dealing with them in IoT environment," *IEEE Access*, vol. 10, pp. 36416–36428, 2022, doi: 10.1109/ACCESS.2022.3162219.

[4] A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, "A Comprehensive Survey on Interoperability for IIoT: taxonomy, standards, and future directions," *ACM Computing Surveys*, vol. 55, no. 1, 2022, doi: 10.1145/3485130.

[5] H. Rahman and M. I. Hussain, "A comprehensive survey on semantic interoperability for internet of things: state-of-the-art and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, 2020, doi: 10.1002/ett.3902.

[6] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, "An overview of IoT architectures, technologies, and existing open-source projects," *Internet of Things (Netherlands)*, vol. 20, 2022, doi: 10.1016/j.iot.2022.100626.

[7] A. Yudidharma, N. Nathaniel, T. N. Gimli, S. Achmad, and A. Kurniawan, "A systematic literature review: Messaging protocols and electronic platforms used in the internet of things for the purpose of building smart homes," *Procedia Computer Science*, vol. 216, pp. 194–203, 2023, doi: 10.1016/j.procs.2022.12.127.

[8] J. Koo and Y. G. Kim, "Resource identifier interoperability among heterogeneous IoT platforms," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4191–4208, 2022, doi: 10.1016/j.jksuci.2022.05.003.

[9] P. Antonios, K. Konstantinos, and G. Christos, "A systematic review on semantic interoperability in the IoE-enabled smart cities," *Internet of Things (Netherlands)*, vol. 22, 2023, doi: 10.1016/j.iot.2023.100754.

[10] M. Pritoni *et al.*, "Metadata schemas and ontologies for building energy applications: A critical review and use case analysis," *Energies*, vol. 14, no. 7, 2021, doi: 10.3390/en14072024.

[11] F. de A. Pereira *et al.*, "Towards semantic interoperability for demand-side management: a review of bim and bas ontologies," *Proceedings of the European Conference on Computing in Construction*, pp. 162–169, 2022, doi: 10.35490/EC3.2022.154.

[12] Z. Qiang *et al.*, "A systematic comparison and evaluation of building ontologies for deploying data-driven analytics in smart buildings," *Energy and Buildings*, vol. 292, 2023, doi: 10.1016/j.enbuild.2023.113054.

[13] J. Zhang, M. Ma, P. Wang, and X. dong Sun, "Middleware for the internet of things: a survey on requirements, enabling technologies, and solutions," *Journal of Systems Architecture*, vol. 117, 2021, doi: 10.1016/j.sysarc.2021.102098.

[14] A. Martikkala, A. Lobov, M. Lanz, and I. F. Ituarte, "Towards the interoperability of IoT platforms: a case study for data collection and data storage," *IFAC-PapersOnLine*, vol. 54, no. 1, pp. 1138–1143, 2021, doi: 10.1016/j.ifacol.2021.08.134.

[15] B. Balaji *et al.*, "Brick: metadata schema for portable smart building applications," *Applied Energy*, vol. 226, pp. 1273–1292, 2018, doi: 10.1016/j.apenergy.2018.02.091.

[16] P. Delgoshaei, M. Heidarinejad, and M. A. Austin, "A semantic approach for building system operations: knowledge representation and reasoning," *Sustainability (Switzerland)*, vol. 14, no. 10, 2022, doi: 10.3390/su14105810.

[17] A. Laadhar *et al.*, "Web of things semantic interoperability in smart buildings," *Procedia Computer Science*, vol. 207, pp. 997–1006, 2022, doi: 10.1016/j.procs.2022.09.155.

[18] D. D. Eneyew, M. A. M. Capretz, and G. T. Bitsuamlak, "Toward smart-building digital twins: BIM and IoT data integration," *IEEE Access*, vol. 10, pp. 130487–130506, 2022, doi: 10.1109/ACCESS.2022.3229370.

[19] R. A. Abdelouahid, O. Debauche, and A. Marzak, "Internet of things: a new interoperable IoT platform. Application to a smart building," *Procedia Computer Science*, vol. 191, pp. 511–517, 2021, doi: 10.1016/j.procs.2021.07.066.

BIOGRAPHIES OF AUTHORS



Ahmad Raditya Cahya Baswara is a lecturer and researcher at Universitas Ahmad Dahlan (UAD), Yogyakarta, Indonesia. His primary research interests include renewable energy, power electronics, wireless power, energy conversion. He has authored and co-authored several scientific papers published in peer-reviewed journals and international conference proceedings. Alongside his research activities, he is actively involved in teaching and academic development within his department. He can be contacted at email: ahmadradityac@ee.uad.ac.id.



Tole Sutikno is a lecturer and the head of the Master Program of Electrical Engineering at the Faculty of Industrial Technology, Universitas Ahmad Dahlan (UAD) in Yogyakarta, Indonesia. He received his Bachelor of Engineering from Universitas Diponegoro in 1999, Master of Engineering from Universitas Gadjah Mada in 2004, and Doctor of Philosophy in Electrical Engineering from Universiti Teknologi Malaysia in 2016. All three degrees are in the Electrical Engineering area. He has been a Professor at UAD in Yogyakarta, Indonesia, since July 2023, following his tenure as an associate professor in June 2008. He is the Editor-in-Chief of TELKOMNIKA and Head of the Embedded Systems and Power Electronics Research Group (ESPERG). He is listed as one of the top 2% of researchers worldwide, according to Stanford University and Elsevier BV's list of the most influential scientists from 2021 to the present. His research interests cover digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded systems, artificial intelligence, intelligent control, digital libraries, and information technology. He can be contacted at email: tole@te.uad.ac.id, or tole@ee.uad.ac.id.



Anggit Pamungkas received his B.Eng. degree in Electrical Engineering from Universitas Ahmad Dahlan, Yogyakarta, Indonesia in 2018. After receiving his degree, he became a member of the Embedded Systems and Power Electronics Research Group (ESPERG). His research interests include power electronics, renewable energy technology, robotics, and the Internet of Things. He can be contacted at email: anggitpamungkas17@gmail.com.