Cybersecurity and Innovative Technology Journal, Vol.4, No.1, 2026, pp. 33-47
e-ISSN 3025-6682. DOI. 10.52889/citj.v4i1.856

Architecture-Driven Integration of Energy Harvesting in Resource-Constrained IoT Systems Using the Unified Architecture Framework (UAF)

Submitted 28 February 2026, Revised 7 April 2026, Accepted 7 April 2026

Christopher Green[1,2*]

[1]Department of System Engineering, Capitol Technology University, Laurel, MD., United States

[2]System Assurance Institute, Greentec EHS, Fredericksburg, VA., United States
Corresponding Email: *cgreen@captechu.edu

Abstract

As the use of resource constrained IoT becomes more prevalent, it relies more often on energy harvesting capabilities for sustaining autonomous operations in uncertain power environments. However, incorporating energy harvesting functionality poses challenges as a result of introducing strong interdependencies between energy generation, storage, operational behavior, security measures, and mission availability. Current methods for addressing the problem usually deal with these aspects on a component or subsystem level and therefore lack cross-domain interaction visibility and understanding, which results in an increased probability of integration errors. In this paper, we propose the architecture driven approach for energy harvesting integration by means of the Unified Architecture Framework (UAF). Instead of being considered separately, energy availability will be addressed as an architectural constraint at a system level in a meta-model driven environment. Through the instantiation of capabilities, operations, resources, security, and standards constructs within a semantic baseline, we show the ability to trace energy- security-mission dependencies across multiple domains. This paper describes how harvested energy variance affects system operations, communications, cybersecurity, capabilities, and system availability. The findings suggest that incorporating energy and cyber security principles in an integrated architectural framework can overcome the problem of fragmentation, enhance overall system reasoning, and facilitate energy-conscious joint design of functional and security-related features. The study provides a scalable architectural basis for the design and evaluation of secure IoT systems with energy constraints.

Keywords: Model-Based Systems Engineering (MBSE), Unified Architecture Framework (UAF), Internet of Things (IoT), Energy Harvesting

INTRODUCTION

These results show that integrating energy and cybersecurity concepts into one single architectural framework decreases integration fragmentation, enhances reasoning at the system level, and facilitates an energy-aware co-design of the operational and security components. Such research provides a scalable architectural approach to designing and analyzing the secure, energy-constrained Internet-of-Things (IoT) systems. The Internet of Things (IoT) technology has facilitated a greater scope of applications in terms of distributing sensors and automating processes in smart cities, industries, healthcare, and remote monitoring systems (Khan et al., 2019). Such systems are being implemented in environments that necessitate constant operation without the need for manual interventions (Stankovic, 2014; Lee, 2008). Consequently, power availability is becoming the main constraint in designing IoT devices rather than a secondary concern. Traditional approaches based on using batteries bring about certain constraints associated with limited power capacity, need for maintenance,

and ecological problems caused by battery disposal. Due to the large-scale deployment of IoT systems, the costs and difficulties of battery replacement grow rapidly..

Energy harvesting is another solution that makes it possible for systems to harvest energy from the environment. Nevertheless, incorporating energy harvesting leads to strong interdependencies between the processes of energy production, energy storage, system behavior, cybersecurity strategies, and mission accomplishment. Resource-limited IoT systems have a direct link between their behavior and the energy supply since any variations in energy affect their functioning and viability. Yet, many solutions focus on addressing the issues related to energy, communication, and security individually (Maier, 1998; Paradiso & Starner, 2005).

Energy Harvesting IoT systems share attributes of systems of systems wherein multiple interacting subsystems work together to achieve mission goals (Maier, 1998; Lee, 2008). In this case, constraints cascade through the various domains. For instance, choices made at the resource level impact the system's operational behavior, which will then impact the system's availability and mission execution. In addition, cybersecurity processes like encryption, authentication, and updating security parameters impose further energy costs, which can be highly coupled with the system's behavior (Shaikh, Adi, & Logrippo, 2009). Without a proper architectural integration framework, all these interdependencies remain implicit, posing potential integration problems (Paradiso & Starner, 2005). Energy harvesting IoT systems have the nature of systems of systems where constraints cascade through domains. Resource availability impacts the system's operation cycles and communication behavior. Additionally, cybersecurity techniques create extra energy requirements that impact system availability and mission execution (Maier, 1998; Lee, 2008; Shaikh, Adi, & Logrippo, 2009). Without an architectural description, these dependencies are implicitly defined and hard to quantify. Figure 1 illustrates the IoT Sensor Nodes, and Figure 2 illustrates the IoT Layered Architecture Example.

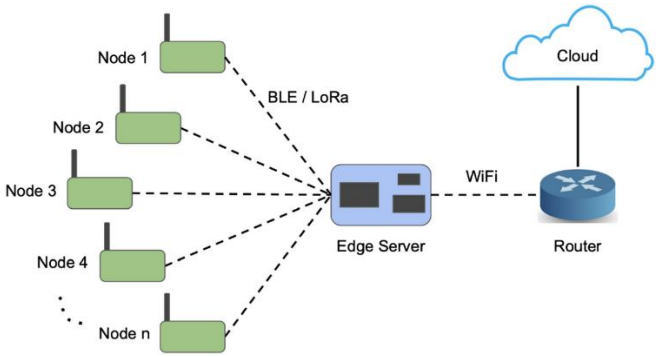

Figure 1. IoT Sensor Nodes

Cybersecurity and Innovative Technology Journal, Vol.4, No.1, 2026, pp. 33-47
e-ISSN 3025-6682. DOI. 10.52889/citj.v4i1.856

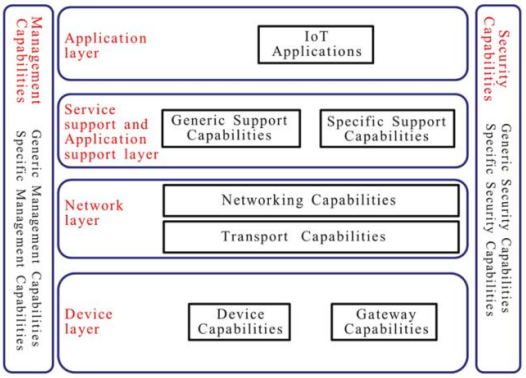

Figure 2. Example IoT Layered Architecture.

Digital Engineering focuses on leveraging trusted models to assist in lifecycle decisions and domain-based analyses (Department of Defense, 2018). The Unified Architecture Framework (UAF) offers a framework governed by a meta-model to structure elements within capability, operations, resource, security, and standards domains and maintain semantic relations among them (International Organization for Standardization, 2018; Object Management Group, 2021; Morkevicius et al., 2017). In this framework, UAF viewpoints facilitate the depiction of system behavior, constraints, parameters, and traceability relationships.

The current work considers the perspective viewpoints supporting traceability along with the parameters and constraints necessary for modeling energy-harvesting IoT systems. The technique assumes energy as an architectural constraint for the system architecture, and captures it through the viewpoints while associating it with behavior, cyber security, and missions at different levels. By using the Domain MetaModel in UAF, the presented approach offers cross-domain traceability as well as evaluates energy, security, and mission interactions in an organized way. The findings reveal that a viewpoint-based approach to architectural analysis is effective in integrating and reasoning about the system.

Resource-Constrained IoT Systems and Energy Harvesting

Resource-limited Internet of Things (IoT) devices function under stringent constraints of energy availability, computing power, and communication bandwidth. These devices depend on energy-efficient computations, sporadic communication, and duty cycling to continue functioning in environments where constant energy cannot be guaranteed (Stankovic, 2014; Zhou et al., 2018). While conventional embedded devices have steady energy supplies, IoT devices used in inaccessible or distant locations have to operate in an energy environment that is unstable and frequently unpredictable. Consequently, energy availability dictates the performance and feasibility of such systems.

However, energy harvesting provides another approach to battery-based operation by harnessing energy from the surrounding environment through the use of thermal differentials, vibrations, radio frequency (RF) sources, and sunlight. The aforementioned sources provide a relatively small amount of energy within the microwatt and milliwatt ranges that change depending on the surrounding environment. It is thus imperative for engineers to consider energy as a dynamic source of constraint when performing sensing operations, communications, and processing (Paradiso & Starner, 2005; Zhou et al., 2018; Adila et al., 2018; Sanislav et al., 2021).

An energy harvesting system usually comprises an energy source, transducer, power conditioning circuitry, energy storage units, and load applications. All the parts have constraints associated with the efficiency of the process, the ability to buffer energy, and energy losses during regulation (Erickson, 2020; Roundy, 2004; Beard, 2019). These constraints tend to interact, especially in multi-source energy harvesters, where multiple sources have to work together to stabilize the system (Shi et al., 2023; Safaei et al., 2025). The figure below illustrates the energy harvesting system and the other figure shows the energy sources in context.

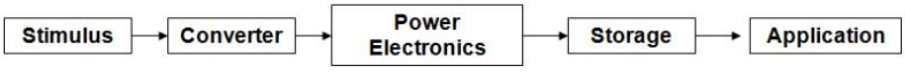

Figure 3. Energy Harvesting System

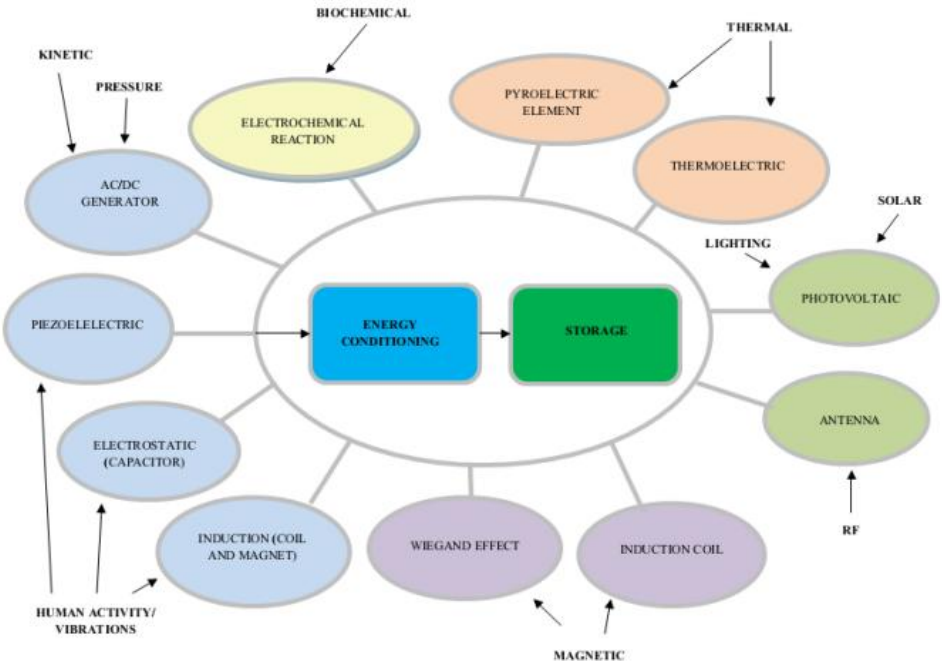

Figure 4. Energy Sources in Relation to The System

Unified Architecture Framework (UAF)

The Unified Architecture Framework (UAF) provides a meta-model-governed structure for integrating multiple domains within a unified architectural baseline (International Organization for Standardization, 2018; Object Management Group, 2021; Morkevicius et al., 2017). UAF organizes architectural elements across capability, operational, resource, security, and standards domains and enforces semantic relationships among them. Tables 1 and 2 present the column and row headings, and Figure 3 depicts the UAF Grid as defined in the OMG specification (OMG, 2021).

Table 1. Column Headings

Viewpoint	Abbreviation	Description
Strategic	St	Capability management process. Describes the capability taxonomy, composition, dependencies, and evolution.
Operational	Op	Describes the requirements, operational behavior, structure, and exchanges required to support (exhibit) capabilities.
Services	Sv	The Service-Oriented View (SOV) is a description of services needed to directly support the operational domain as described in the Operational View.
Personnel	Ps	Shows the taxonomy of types of organizational resources as well as connections, interaction, and growth over time.
Resources	Rs	Captures a solution architecture consisting of resources, e.g., organizational, software, artifacts, capability configurations, and natural resources that implement the operational requirements.
Security	Sc	Defines the hierarchy of security assets and asset owners, security constraints (policies, laws, and guidance), and the locations of these assets (security enclaves).
Projects	Pj	Describes projects and project milestones, how those projects deliver capabilities, the organizations contributing to the projects, and dependencies between projects.
Standards	Sd	A set of rules governing the arrangement, interaction, and interdependence of solution parts or elements.
Actual Resources	Ar	The analysis, e.g., evaluation of different alternatives, what-if analyses, trade-offs, and V&V of the actual resource configurations.

Table 2. Row Headings

Aspect	Abbreviation	Description
Architecture Management	Am	Identifies the metadata required to develop a suitable architecture that is fit for its purpose.
Traceability	T*r*	Describes the mapping between elements in the architecture.
Taxonomy	T*x*	Presents all the elements as a standalone structure.
Structure	Sr	Describes the breakdown of structural elements, e.g., logical performers, systems, projects, etc., into their smaller parts.
States	St	Captures state-based behavior of an element.
Sequences	Sq	Expresses a time-ordered examination of the exchanges as a result of a particular scenario.
Roadmap	Rm	Addresses how architectural elements change over time.
Processes	Pr	Captures activity-based behavior and flows.
Parameters	Pm	Shows the measurable properties of something in the physical world and elements and relationships that are involved in defining the environments applicable to capability, operational concept, or set of systems.
Motivation	Mv	Captures motivational elements that pertain to enterprise transformation efforts, as well as different types of requirements.
Information	If	Address the information perspective on operational, service, and resource architectures.
Constraints	Ct	Details the measurements that set performance requirements constraining capabilities.
Connectivity	Cn	Describes the connections, relationships, and interactions between the different elements.

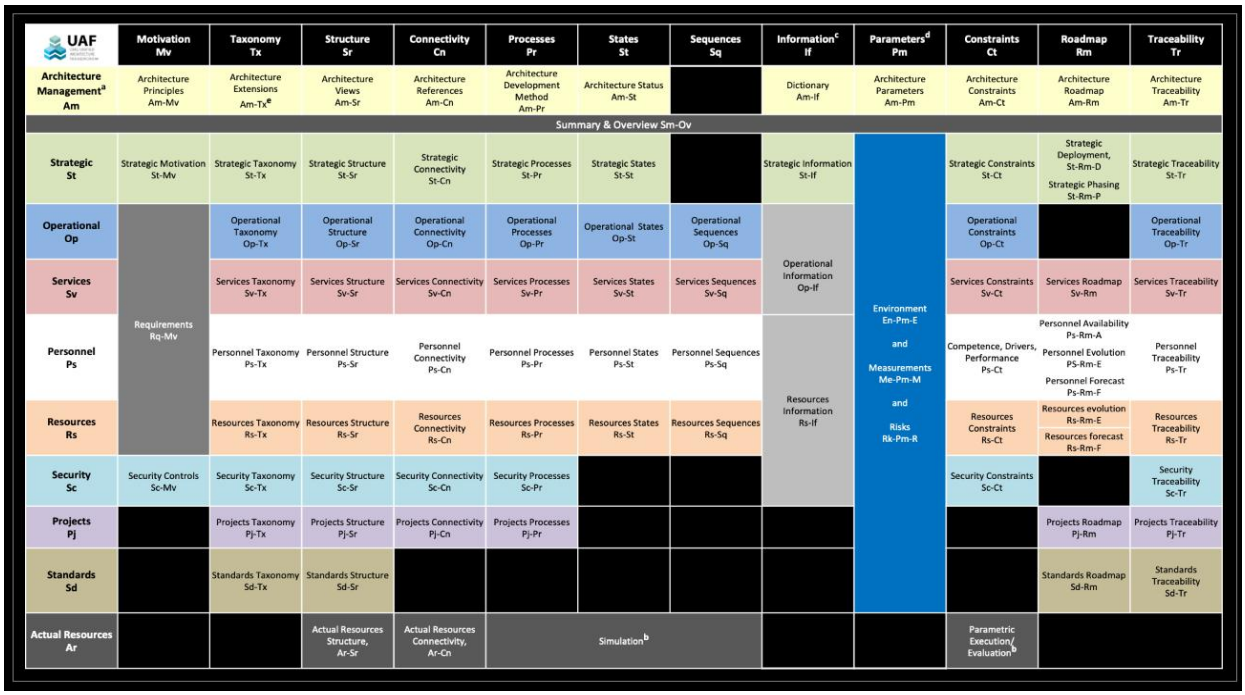

Figure 5. UAF Grid

Two features of UAF in Figure 5 are particularly relevant to energy-harvested IoT systems. First, cross-domain traceability enables explicit linkage between mission capabilities, operational behavior, and physical resources within a shared semantic structure. Second, the separation between logical intent and physical implementation allows engineers to evaluate alternative configurations without redefining mission objectives. By providing a unified representation of system elements and their interactions, UAF supports structured reasoning

about how constraints propagate across domains. This capability is essential for energy-harvested systems, where energy availability interacts directly with operational behavior and cybersecurity requirements (Hause & Kihlström, 2024; Hause, 2019).

Research Gap: The Need for a Holistic Architectural Framework

Despite advances in energy-harvesting technologies and optimization methods, there remains a lack of formal approaches that integrate energy availability, operational behavior, cybersecurity mechanisms, and mission-level objectives into a unified architectural representation. Existing methods emphasize component-level optimization or isolated analytical models, limiting their ability to capture cross-domain dependencies and to propagate constraints across system elements.

Model-Based Systems Engineering (MBSE) provides a foundation for addressing system complexity through lifecycle models (INCOSE, 2007; Friedenthal et al., 2015). Within this context, the Unified Architecture Framework (UAF) enables cross-domain traceability and dependency analysis through its meta-model-governed structure (International Organization for Standardization, 2018; Object Management Group, 2021). Although prior studies demonstrate how engineers can use UAF to model complex systems and Industrial IoT architectures, researchers give limited attention to the specific UAF viewpoints required to represent energy-constrained behavior in IoT systems.

In energy-harvested systems, energy availability varies with environmental conditions and couples tightly with operational and security behavior. However, existing approaches do not explicitly leverage UAF viewpoints, particularly those associated with traceability, parameters, and constraints, to represent these interactions. A viewpoint-driven architectural approach is therefore needed to enable explicit representation of energy–security–mission dependencies and to support structured reasoning about trade-offs across domains (Morkevicius et al., 2017).

METHOD

This study applies an architecture-driven conceptual analysis to evaluate how UAF viewpoints enable the integration of energy harvesting in resource-constrained Internet of Things (IoT) systems. The approach treats architecture as an authoritative analytical artifact and emphasizes explicit representation of cross-domain dependencies among energy availability, operational behavior, cybersecurity mechanisms, and mission-level capabilities. Consistent with digital engineering principles, the method focuses on cross-domain reasoning, structured trade-space evaluation, and lifecycle resilience.

Research Approach

In this paper, an architecture-based perspective was used to analyze how the meta-model-based architecture helps support energy harvesting in IoT systems. The methodology does not consider optimization at the component level or any other numerical calculation; rather, it considers how the use of UAF perspectives such as traceability, parameters, and constraints allows for modeling energy-constrained behavior.

The Unified Architecture Framework (UAF) offers the modeling framework via its Domain MetaModel, which is responsible for describing semantic relations between the capability, operational, resource, security, and standard domains. In this case, the model describes the availability of energy at the system level by leveraging parameters and constraints. Simultaneously, traceability relations exist that bind such constraints to operational activities, cybersecurity approaches, and mission capabilities. The approach to modeling takes into consideration energy-security-mission relationships from the point of view of a consistent modeling approach within a unified architectural basis. Such an approach to analysis leverages the viewpoint-based analysis framework.

RESULTS AND DISCUSSION

Uaf-Based Integration of Energy Harvesting In Iot Architectures

Energy harvesting can be incorporated into resource-constrained IoT systems using the Unified Architecture Framework (UAF), which offers an architecture framework that operates through a meta-model-driven architecture framework based on domains and aspects. Some of the domains specified by the UAF include capability domain, operational domain, resource domain, security domain, and standard domain, among others, while the aspects used include traceability (Tr), parameter (Pm), and constraint (Ct) aspects, among others, to create architectural views (International Organization for Standardization, 2018; Object Management Group, 2021; Morkevicius et al., 2017).

In such an approach, the engineers consider energy harvesting as a cross-domain architectural constraint and not as a subsystem. Engineers describe energy availability in terms of parameter (Pm) and constraint (Ct), while associating these parameters and constraints with each other across domains using traceability (Tr) associations. Variability in energy harvest affects operational behavior, resource usage, and cybersecurity measures, which ultimately impacts mission capability realization (Paradiso & Starner, 2005). Through this representation, the architecture allows for assessment of how energy availability affects the capabilities of the system (International Organization for Standardization, 2018; Object Management Group, 2021).

Capability Domain (Cp)

Views of capability domains represent mission objectives, performance levels, and constraints by means of the constructs Capability and its corresponding Constraints elements. In the case of energy harvesting IoT devices, views of capability domains represent availability needs, reliability levels, and service continuity constraints in changing energy environments. With the help of traceability (Tr) associations, the engineers relate capability constraints to operational behaviors and resource allocation. Engineers may be able to trace a needed level of availability to operational duty cycles and energy resource capacity, thus establishing coherence between the mission objectives and system feasibility.

Operational Domain (Op): Behavioral Energy Demand

Behavioral models in operational domain modeling capture behavior through entities that indicate sensing interval, communication, and process behavior, and this defines the energy consumption needs of the system (Zhou et al., 2018). Using the association between behavioral requirements and Pm and Ct attributes, energy consumption is modeled by considering the behavior of the system. Relationships of traceability between behavioral elements and capability constraints and resource parameters allow for the assessment of feasibility of behavioral needs depending on variations in the energy consumed (International Organization for Standardization, 2018; Object Management Group, 2021).

Resource Domain (Rs): Energy Generation, Storage, and Processing

In the Resource category, the architecture implements energy harvesters, storage components, microcontrollers, and communication units as resource components specified in the DMM framework. They have attributes that can be quantified like the rate of energy generation, storage capabilities, and energy consumption, hence allowing the modeling of energy as a source of power as well as a consumable commodity (Paradiso & Starner, 2005; Zhou et al., 2018).

Aspects of Pm include properties that define energy in terms of generation and consumption as an environmental variable. Aspects of Ct include factors like storage, maximum power, and environmental aspects. The link between parameters and constraints can be established through traceability (Tr), thereby providing a means of evaluating the supply-demand ratio of energy and assessing the feasibility of a given system dynamically (International Organization for Standardization, 2018; Object Management Group, 2021; Morkevicius et al., 2017).

Security Domain (Sc): Energy-Aware Cybersecurity Integration

The Security domain implements cybersecurity functionality through constructs that model encryption, authentication, secure boot, and over-the-air updating and incur overhead both computationally and communicatively (International Organization for Standardization, 2018; Object Management Group, 2021; Morkevicius et al., 2017).

In constrained IoT systems, such mechanisms will have direct implications on energy usage and practicality. By integrating security features within the same architecture framework as operational and resource components, UAF facilitates energy accounting for these components. Higher encryption implies higher duty cycles for processors; authentication requires longer communication periods, and secure update procedures cause temporary energy bursts (Shaikh, Adi, & Logrippo, 2009).

Through logical partitioning of domains and semantic integration, engineers can compare different security architectures without restating the mission objective. Energy-aware cybersecurity co-design is thus supported and allows for a balanced evaluation among confidentiality, integrity, availability, and power limitations. The Security domain will consequently ensure that the design incorporates cybersecurity elements in the energy-limited system (Hause & Kihlström, 2024; Hause, 2019).

Standards Domain (Sd): Compliance as an Energy Driver

However, IoT systems are likely to be governed by standards on regulatory and cybersecurity compliance, such as ISO/IEC 27001 and NIST SP 800-53. Under UAF, such standards manifest themselves through the Standard, Rule, and Constraint classes within the Standards Ontology domain and are associated with capabilities and security constructs (International Organization for Standardization, 2018; Object Management Group, 2021). Such association makes sure that compliance-based requirements undergo energy feasibility checks.

As opposed to tacking the mechanisms for compliance onto the design process at a later stage, the architecture makes them a key part of its definition as the drivers behind the behavior of the system. Compliance-related factors frequently add extra overhead in terms of computation and communications, and this, in turn, has an effect on the amount of energy used. As the compliance-related factors are represented in the architecture, it becomes possible to evaluate their effects in terms of the power requirements of the system.

Cross-Domain Dependency Propagation

In terms of architectural benefits of UAF, cross-domain dependency propagation through the Domain MetaModel is considered the main benefit (International Organization for

Standardization, 2018; Object Management Group, 2021). Since the architecture integrates capabilities, operations, resources, security, and standards, modifications made in one domain affect other domains. Energy variability is an excellent illustration of this feature. If energy variability at the resource domain decreases, it impacts operation behavior and may lead to problems with services provision, which results in capability degradation at the mission level. This chain can be traced in DMM relationships by engineers. Thanks to embedding such dependencies into the architecture, UAF allows for identifying risky scenarios early on and conducting trade-space exploration in a structured way. It allows evaluating different scenarios and assessing their consequences without having to modify the model. Instead of using fragmented approaches to trade-space assessment, UAF allows integrating energy and security impacts into the architectural solution itself.

Architectural Implications

UAF energy harvesting is an example that illustrates how architectural views, defined in terms of aspects and domains, affect analysis capabilities. In fact, the use of traceability (Tr), parameter (Pm), and constraint (Ct) aspects within the UAF architecture makes it possible to represent explicitly the cross-domain interdependence and conduct logical reasoning about the system. System engineering becomes focused on reasoning rather than optimizing components, and therefore, interaction between energy availability, behavior, security measures, and constraints can be analyzed in a comprehensive manner.

This work reveals that the integration of energy harvesting within a viewpoint-based approach that is constrained by meta-models will lead to a fundamental shift in the design and analysis of resource-limited IoT systems. In other words, the energy availability is no longer considered as an auxiliary factor but rather as a parameter and a constraint in itself, which is related through traceability within the domains of the Unified Abstract Framework (UAF).

In UAF, Domain MetaModel is the source of the semantics used to relate capabilities, operations, resources, security, and standards domains (International Organization for Standardization, 2018; Object Management Group, 2021). Traceability (Tr), Parameter (Pm), and Constraint (Ct) aspects are the focus of the architecture framework when propagating the energy constraints throughout the domain. Differences in available energy, which manifest as parameters in the resource domain, pass through the operations, affecting communication and processing and the possibility of implementing certain cybersecurity measures. In turn, these aspects determine mission-level capabilities, which the model captures through capability domain perspectives.

Conclusions drawn from the study reveal the deficiencies of an isolated method that separates the generation, storage, communication, and security processes in relation to the energy harvesting system. Although the method can assist in local optimization of the processes in question, it fails to consider the dependency factors that dictate performance at a system level (Maier, 1998; Lee, 2008). On the other hand, using the viewpoint methodology, engineers are able to analyze the impacts of local designs via traceability relationships in order to avoid negative impacts on a system level.

The application of the cybersecurity integration is another example that emphasizes the importance of viewpoint-oriented modeling. The implementation of security measures results in computational and communications overheads that influence energy consumption. With the presentation of those measures as constraints in security domain views along with the linking to the energy parameters by means of traceability associations, the architecture model makes it possible to make an assessment of energy-aware cybersecurity trade-offs. It also provides for co-designing both security and energy measures while making trade-off assessments between confidentiality, integrity, availability, and energy parameters (Shaikh et al., 2009; Hause, 2019; Hause & Kihlström, 2024).

The parameter and constraint aspects enable structured trade-space analysis. Because of the use of an architectural framework that defines energy availability, system behavior, and security methods, engineers are able to analyze competing designs without needing to redefine system context. The ability is especially useful for energy-harvesting IoTs because of the influence environment changes may have on system behavior. Through the use of the architecture, engineers can examine how various behaviors or security systems impact energy utilization and mission success.

In conclusion, this research shows that the perspective-based architecture approach increases integration, minimizes fragmentation, and boosts the capacity to assess system performance in conditions of limited energy. The explicit representation of energy, security, and mission interactions using traceability, parameters, and constraints allows for developing the basis for creating energy-aware IoT systems.

CONCLUSION

In this paper, an architectural based method to incorporate energy harvesting in resource constrained IoT applications was described through the use of the Unified Architectural Framework (UAF). In the case study conducted here, energy availability was considered at the architectural level rather than as a design element of a particular component

of the IoT system. Energy, behavior, cybersecurity elements, and capabilities were all incorporated in the architecture through a meta-model driven framework.

The findings showed that variation in energy harvesting would eventually impact system availability and the achievement of mission capabilities via operation duty cycles, communications, and cybersecurity techniques. From the perspective of the UAF Domain MetaModel, these dependencies could be evaluated from the perspective of the capability, operational, resource, security, and standard domains, allowing the same criteria to be used to consistently assess the impact of decisions made at the local level on the overall system outcome (International Organization for Standardization, 2018; Object Management Group, 2021).

By keeping a consistent semantic baseline, the architecture allows for a rigorous evaluation of trade-offs between energy usage, security, and mission success. Different architectures can be compared using the same model, which will enable engineers to assess the effect of different operating modes and cybersecurity measures on energy usage and system performance (INCOSE, 2007; Lee, 2008).

On a wider scale, the paper emphasizes the use of architecture as an analysis tool in designing complex systems. With a meta-model-driven architecture, one can model relationships between various components in the system, support lifecycle reasoning, and create an extensible basis to incorporate new technologies, such as energy harvesting, in IoT architectures. Moreover, by promoting energy from being a subsystem consideration to an architectural one, the design becomes more viable and resilient in constrained environments.

REFERENCES

Adila, A. S., Husam, A., & Husi, G. (2018). Towards The Self-Powered Internet Of Things (IoT) By Energy Harvesting: Trends And Technologies For Green IoT. In *2018, IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (pp. 183–188). IEEE.

Beard, K. W. (2019). *Linden's Handbook of Batteries*. (Fifth edition). McGraw-Hill.

Department of Defense. (2018). *DoD Digital Engineering Strategy*. U.S. Department of Defense. https://www.acq.osd.mil/asda/dse/docs/DoD-Digital-Engineering-Strategy.pdf

Erickson, R. W. (2020). *Fundamentals of Power Electronics* (3rd ed. 2020). Springer Nature. https://doi.org/10.1007/978-3-030-43881-4

Friedenthal, S., Moore, A., & Steiner, R. (2015). *A Practical Guide to SysML: The Systems Modeling Language* (3rd ed.). Morgan Kaufmann.

Hause, M. (2019). *Model-Based Systems Engineering (MBSE) with UAF*. INCOSE International Workshop

Hause, M. (2025). What is UAF, and why do I care? Object Management Group.

Hause, M., & Kihlström, J. (2024). Logical Architectures In MBSE and UAF. *INCOSE International Symposium Proceedings, 34*(1).

INCOSE. (2007). *Systems Engineering Vision 2020*. International Council on Systems Engineering.

International Organization for Standardization. (2018). *ISO/IEC 19540:2018 – Information technology — Object Management Group Unified Architecture Framework (UAF)*. ISO.

Khan, M. A., & Salah, K. (2019). Internet of Things: Applications, challenges, and future directions. *Future Generation Computer Systems*, 99, 581–602. https://doi.org/10.1016/j.future.2019.04.020

Lee, E. A. (2008). Cyber-Physical Systems: Design challenges. In *Proceedings of the 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing* (pp. 363–369). IEEE. https://doi.org/10.1109/ISORC.2008.25

Ma, X., Zhang, Y., & Liu, Y. (2020). Environmental impact of battery usage in IoT systems and sustainable energy alternatives. *Journal of Cleaner Production, 258*, 120675. https://doi.org/10.1016/j.jclepro.2020.120675

Maier, M. W. (1998). Architecting Principles For Systems-Of-Systems. *Systems Engineering, 1*(4), 267–284. https://doi.org/10.1002/(SICI)1520-6858(1998)1:4

Morkevicius, A., Bisikirskiene, L., & Bleakley, G. (2017). Using a Systems-of-Systems Modeling Approach For Developing Industrial Internet Of Things Applications. *2017 Annual IEEE International Systems Conference (SysCon)* (pp. 1–6). IEEE.

Object Management Group. (2017). *OMG Systems Modeling Language (SysML), version 1.5*. https://www.omg.org/spec/SysML/

Object Management Group. (2021). *Unified Architecture Framework (UAF), version 1.2 specification*. https://www.omg.org/spec/UAF/

Paradiso, J. A., & Starner, T. (2005). Energy Scavenging For Mobile And Wireless Electronics. *IEEE Pervasive Computing, 4*(1), 18–27. https://doi.org/10.1109/MPRV.2005.9

Roundy, S., Wright, P. K., & Rabaey, J. M. (2004). *Energy Scavenging for Wireless Sensor Networks: With Special Focus on Vibrations*. Kluwer Academic Publishers.

Safaei, B., Peiravian, M., & Siamaki, M. (2025). Eco-friendly IoT: Leveraging Energy Harvesting for a Sustainable Future. *IEEE Sensors Reviews, 2*, 32–75.

Sanislav, T., Mois, G. D., Zeadally, S., & Folea, S. C. (2021). Energy-harvesting Techniques For The Internet of Things (IoT). *IEEE Access, 9*, 39530–39549.

Selematsela, N., Takawira, F., & Chabalala, C. (2025). Battery Lifetime Analysis of Energy-Harvesting IoT Network Nodes. *2025 IEEE 3rd Wireless Africa Conference (WAC)*.

Shaikh, R. A., Adi, K., & Logrippo, L. (2009). Dynamic Risk Analysis of Internet of Things Systems. *International Journal of Communication Networks and Information Security, 1*(1), 1–9.

Stankovic, J. A. (2014). Research Directions for the Internet of Things. *IEEE Internet of Things Journal, 1*(1), 3–9. https://doi.org/10.1109/JIOT.2014.2312291

Zhou, L., Zhang, Y., & Liu, Y. (2018). Energy-Efficient IoT Systems: A Survey. *IEEE Communications Surveys & Tutorials, 20*(3), 2349–2375. https://doi.org/10.1109/COMST.2018.2834470