EAI Endorsed Transactions
on Scalable Information Systems
Review Article EAI.EU

A Review of Reference Architectures for the Next-Generation Internet of Things Systems

Sorin-Daniel Gheorghe[1,*]

[1]Bucharest University of Economic Studies, Doctoral School of Economic Informatics, Bucharest, Romania

Abstract

The rapid evolution of the Internet of Things (IoT) demands robust architectural models capable of integrating emerging technologies and managing growing system complexity. This paper presents a structured review of IoT Reference Architectures (RAs), analysing their conceptual foundations, structural organization, and technological readiness in the context of Next-Generation IoT (NGIoT) technologies. The study examines RAs based on their support for disruptive technologies, including Edge/Fog/Cloud Computing, 5G, Artificial Intelligence, Digital Twins, Augmented Reality, Blockchain, and the Tactile Internet. Special emphasis is placed on the ASSIST-IoT RA, evaluated as a modular, cloud-native blueprint aligned with modern software design principles. Reflecting decentralization, scalability, interoperability, and resilience, ASSIST-IoT emerges as a production-ready framework for building intelligent and adaptive IoT systems. The findings synthesize current RAs trends and limitations, offering a forward-looking perspective that informs the development of NGIoT systems driven by data-driven and human-centric innovation.

Keywords: Internet of Things, Reference Architectures, Next-Generation IoT Systems, System Engineering, Industry 5.0.

Received on 05 August 2025, accepted on 29 January 2026, published on 03 February 2026

doi: 10.4108/eetsis.9877

1. Introduction

The Internet of Things (IoT), in its broader interpretation, is not a standalone technology but rather a convergence of multiple existing technologies that are integrated to meet the requirements of IoT applications [1]. IoT entails a comprehensive ecosystem composed of technologies, tools, methods, and services, all of which must be orchestrated to deliver end-to-end solutions.

According to [2], an IoT architecture can be defined as the fundamental organization of a system, articulated through its components, the interrelationships among them, and the operational environment, as well as the principles guiding its design and evolutionary trajectory.

However, IoT architectures are often highly specific, tailored to address the unique constraints or domain-specific characteristics of a particular use case or application [3].

In response to this limitation, the concept of a Reference Architecture (RA) has emerged. The interdependencies and conceptual relationships between specific IoT architectures and RAs are illustrated in Figure 1.

IoT RAs serve as high-level conceptual models of the IoT ecosystem, providing structured guidance for the implementation of specific IoT systems. These architectures aim to address the full spectrum of system requirements by defining a comprehensive set of functionalities, information structures, and operational mechanisms [4]. They function as foundational blueprints for the design of compliant, domain-specific IoT architectures.

The system requirements addressed by RAs encompass a wide range of concerns, including device management, data connectivity and communication, data collection, aggregation and analysis, as well as issues related to heterogeneity,

*Corresponding author. Email: gheorghesorin22@stud.ase.ro
This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

interoperability, dynamism, scalability, and data security. These elements are essential to ensure robust support for IoT services and applications.

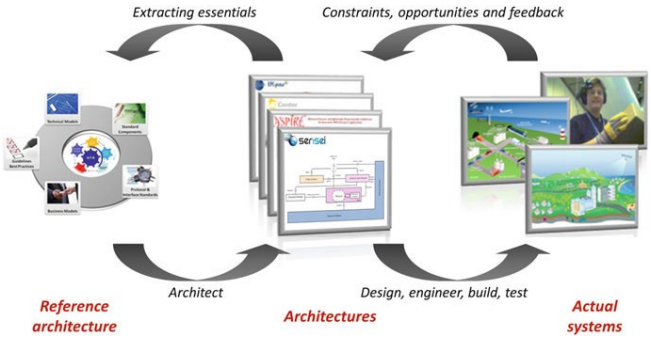

Figure 1. Relationship between the Reference Architecture, Domain Specific Architecture, and the Actual System [3]

Operating at a higher level of abstraction, a RA facilitates the identification of critical challenges and recurring design patterns across a broad spectrum of use cases [5]. However, to be truly effective, it must strike an appropriate balance in its level of abstraction – if the model is overly abstract, it may lack practical applicability; conversely, if it is too specific, it risks becoming inflexible or irrelevant in diverse contexts.

Accordingly, domain-specific IoT architectures are designed in alignment with the guidelines and principles established by a RA, while also incorporating domain-specific constraints, contextual opportunities, and other feedback essential for the tailored design of the target system (Figure 2).

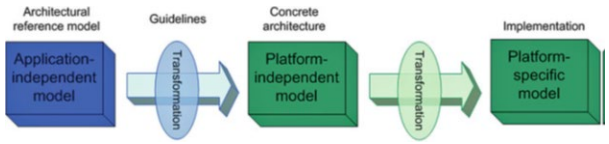

Figure 2. Implementation of a RA from an abstract model to a concrete model [3]

Since any concrete IoT architecture is inherently more specific and context-bound than a generic RA, not all components or aspects defined within a RA are necessarily addressed or implemented. Moreover, adherence to a RA becomes particularly relevant when the goal of an IoT system is broad in scope, involving multiple, interconnected use cases. On the other hand, in the context of small-scale or standalone IoT developments, the use of a RA may offer limited practical value and could introduce unnecessary complexity.

Defining a single, universal RA to serve as a design blueprint for all potential IoT system implementations is an inherently complex and impractical endeavour. Consequently, multiple RAs have emerged and coexist, each offering different levels of abstraction and emphasis.

The selection of a suitable RA for instantiating a specific IoT system is largely contingent upon the particular requirements of the targeted domain, the specific use case, and the functional scope of the intended application.

In recent years, the evolution toward Next-Generation Internet of Things (NGIoT) systems has introduced a set of requirements that significantly extend beyond the assumptions of early IoT architectures [1].

NGIoT systems are expected to support edge intelligence, ultra-low latency communication, decentralized orchestration, autonomous behaviour, and human-centric interaction, while integrating emerging technologies such as Artificial Intelligence, 5G, Digital Twins, Blockchain, and the Tactile Internet [1].

However, many existing IoT RAs were conceived before the maturation of these technologies and therefore only partially address NGIoT-specific concerns.

Despite the abundance of IoT architectural models proposed over the past decade, there is a lack of systematic studies that assess their suitability and limitations in the context of NGIoT. This gap motivates the present study, which aims to review and comparatively analyze prominent IoT RAs through the lens of NGIoT requirements, thereby identifying architectural trends, limitations, and opportunities for future-ready IoT system design.

2. Research Methodology

The research conducted in this study adheres to a qualitative, exploratory design aimed at investigating the evolution, structure, and practical relevance of IoT RAs, particularly in light of emerging NGIoT technologies and paradigms.

Given the multidisciplinary nature of the topic – encompassing IoT, architecture modeling, systems engineering, and digital transformation – the selected design emphasizes depth of analysis and systematic synthesis of knowledge from diverse scholarly and industrial sources.

The approach is intended to not only document the state of the art, but also uncover conceptual patterns, gaps, and future research trajectories in the domain of IoT RAs development and adoption.

This research adopts an exploratory literature review as its principal methodological framework. The exploratory literature review is a systematic approach which provides a structured, replicable, and transparent process for identifying, selecting, and analysing academic and technical literature relevant to the research in question.

As outlined by established methodological guidance, the research process facilitates comprehensive coverage of the topic space while minimizing bias in the selection and interpretation of sources.

The review process was carried out in several clearly defined phases:

- Definition of inclusion and exclusion criteria;
- Formulation of search queries and keyword strategies;

- Database selection and execution of the search;
- Screening and filtering of results based on relevance;
- Full-text review and thematic analysis.

The search queries employed included combinations of keywords such as "*Internet of Things*", "*IoT Reference Architecture*", "*Next-Generation IoT*", "*IoT Systems Engineering*" and "*Industry 5.0*". These were enhanced using Boolean operators (e.g. *AND*, *OR*, *NOT*) to refine and target the search results.

2.1. Data collection

A comprehensive search was conducted across multiple reputable and high-impact scholarly databases, including *IEEE Xplore*, *ScienceDirect*, *Scopus*, *Web of Science*, and *Google Scholar*.

Additionally, relevant *technical reports*, *white papers*, and *industry deliverables* (e.g. from EU-funded projects such as ASSIST-IoT, SerIoT, and CREATE-IoT) were considered to capture perspectives beyond academic publications.

The literature was limited to works published between 2000 and 2025, a period characterized by accelerated development and innovation in IoT technologies and architecture.

The inclusion criteria emphasized relevance to IoT architectural modeling, technical rigor, originality, and contribution to NGIoT discourse.

The exclusion criteria filtered out duplicates, non-peer-reviewed sources (unless of notable technical relevance), and articles lacking substantial architectural content.

The selection process followed a two-tier approach:

- Initial screening of titles, abstracts, and keywords;
- In-depth full-text review to determine final eligibility for inclusion in the analysis.

Ultimately, a number of *30* high-quality and cited publications were retained and used as primary sources in this research.

2.2. Data analysis

The analytical phase employed a qualitative synthesis methodology, where various key architectural elements, design principles, and technology integrations were extracted, compared, and categorized.

Using a *thematic analysis* approach, the extracted data were organized into conceptual categories aligned with the structure of the review paper. Among these, we recognize the following: RA models and their evolution, IoT RAs and integration of emerging technologies, and NGIoT RAs.

Throughout the analysis, critical thinking approach was also applied to assess the completeness, flexibility, scalability, and future-readiness of each RA.

Recurrent themes and architectural patterns were synthesized to derive generalized insights, which inform the in-depth review sections of this paper.

3. NGIoT technologies

According to the Next Generation Internet of Things (NGIoT) initiative [1], several technologies have been identified as key enablers for the next generation of IoT systems.

These include Edge–Fog–Cloud computing architectures, 5G connectivity (including Network Function Virtualization), Artificial Intelligence (AI) and Big Data analytics, Augmented Reality (AR) and the Tactile Internet, Digital Twins (DT), as well as Distributed Ledger Technologies (DLTs) including Blockchain.

These technologies collectively underpin the transformation of IoT from isolated smart devices into intelligent, interconnected, and adaptive systems capable of operating across complex digital-physical ecosystems.

3.1. Edge–(Fog)–Cloud computing

The Edge–(Fog)–Cloud computing continuum introduces novel capabilities into IoT architectures by enabling data processing and analytics to occur with minimal or no reliance on centralized Cloud infrastructure.

This paradigm shift supports the development of new types of services and applications, particularly human-centric ones, and opens avenues for innovative business models [1]. As a key enabler, it significantly reduces the volume of data that must be transferred to Cloud data centers for processing.

When combined with complementary technologies such as AI, this architectural model enables the distribution of intelligence across Edge nodes – that is, peripheral computing devices located closer to data sources and end-users.

This localized decision-making capability not only reduces system latency and response times but also enhances the system's ability to make autonomous and intelligent decisions in real-time.

3.2. 5G networks

The ongoing evolution of cellular network technologies, particularly 5G, is pivotal in supporting large-scale IoT deployments [1]. It offers substantial improvements over existing wireless technologies such as Low-Power Wide-Area Networks (LPWANs) in terms of latency, reliability, and the density of connected devices.

Beyond enhancements to the access network, 5G introduces advanced capabilities for infrastructure virtualization and hardware abstraction through mechanisms such as Network Function Virtualization (NFV).

NFV provides flexible and agile means for deploying and orchestrating IoT infrastructures, thereby facilitating the dynamic instantiation and reconfiguration of other IoT-enabling technologies.

3.3. Artificial intelligence

The integration of AI into IoT ecosystems – particularly when combined with Edge Computing and 5G NFV – is fundamental to the performance and scalability of NGIoT platforms [1].

AI libraries, frameworks, and models can be deployed across various system layers, including smart devices, distributed Edge nodes, network elements, and Cloud data centers, depending on the computational capabilities of each layer [6].

AI empowers IoT systems with context-awareness, enabling decentralized and distributed intelligence, which in turn supports real-time, adaptive, and human-centric applications [6]. Furthermore, it unlocks the potential for new business models, based on advanced data interpretation, predictive analytics, and autonomous system behaviour.

3.4. Augmented reality and the tactile internet

AR offers users an intuitive interface for visualizing and interacting with IoT devices and their associated data. By providing a semi-tangible, direct user interface, AR can significantly enhance the comprehension and usability of complex IoT datasets. This makes it particularly valuable for everyday applications and for use in domain-specific operational contexts [6].

Conversely, the Tactile Internet (TI) is characterized by ultra-low latency, extremely short transmission times, high availability, high reliability, and strong security guarantees [1]. Its primary objective is to enable real-time interaction between humans and remote cyber-physical systems, often through haptic or tactile interfaces, thereby promoting a human-centric orientation in system design and control [8].

3.5. Digital twins

Rather than representing a standalone technology, DT constitute a convergence of multiple enabling technologies, including advanced software analytics, Edge/Cloud computing, and AI [1].

A DT is a virtual replica of a physical entity, designed to monitor, simulate, and control its real-world counterpart with a high degree of fidelity [8]. This capability is instrumental in enabling predictive maintenance, real-time optimization, and lifecycle management across industrial and operational domains.

3.6. Blockchain

Blockchain technology introduces novel mechanisms for data governance and trust management within distributed computing environments [7].

The inherently decentralized nature of Edge Computing presents significant security and privacy challenges, due to the heterogeneity of edge nodes and the dynamic migration of services across the IoT edge layer.

These challenges can be effectively addressed using Blockchain, which ensures trusted access control, data integrity, and computational verifiability.

Through blockchain-based architectures, data ownership is preserved, enabling data producers to retain control over who can access and use their data [7].

3.7. Hyperconnectivity

Similar enabling technologies are outlined in [8], which emphasize the importance of Hyperconnectivity as foundational pillar for NGIoT systems.

Hyperconnectivity encompasses not only 5G capabilities and network slicing, but also the application of concepts such as Software-Defined Networking (SDN) and NFV [8].

These paradigms collectively support dynamic, programmable, and scalable network infrastructures tailored to the complex demands of distributed IoT environments.

3.8. NGIoT capabilities

As a result of these Industry 5.0 technological advancements, modern IoT systems are expected to fulfil what has been conceptualized as the “6Cs” of IoT systems [1]:

- Collection – the acquisition of raw or processed data from heterogeneous devices;
- Connection – the reliable networking of distributed and diverse devices;
- Caching – the temporary or persistent storage of information across a distributed IoT ecosystem;
- Computation – the advanced processing and analysis of collected data;
- Cognition – the extraction of actionable insights through the application of AI;
- Creation – the generation of new interactions, services, and solutions, facilitating communication and functionality: (a) from anything, (b) to/from anyone, (c) at any location, (d) at any time, (e) through any pathway, (f) to deliver any service.

These 6Cs encapsulate the transformative potential of NGIoT ecosystems, promoting ubiquitous connectivity, real-time intelligence, and context-aware service delivery across sectors and domains [11].

4. RA concepts

There are various architectural styles and system models that can be adopted when designing an IoT architecture [9]. Among the most widely recognized styles are the following: layered architectures, cloud/fog/edge-based architectures, service-oriented architectures (SOA), microservice-based models, state-based models (e.g. Web/REST), and event-driven architectures (e.g. publish/subscribe).

One or more of these styles may be combined in a single IoT architecture, as they are not mutually exclusive.

Among them, the layered architectural style remains the most commonly applied design model [9]. In this approach, the functional responsibilities of each layer are clearly defined, with each layer addressing a specific subset of the overall IoT processes or functionalities [10].

A typical three-layer model reflects the core conceptual framework of IoT systems [3]:

- Perception layer – consists of sensors and devices that collect data;
- Network layer – handles transmission and interconnection between devices;
- Application layer – delivers user-facing services and interfaces.

Nevertheless, real-world IoT systems are often significantly more complex, necessitating the incorporation of additional layers beyond this foundational triad [11]. The number and naming of layers vary considerably across architectural proposals, with models comprising four, five, six, or seven layers [12], or even more – such as the LSP RA, which consists of eight layers [13].

In [10], the authors present a comprehensive analysis of the evolution of layered IoT architectures from 2008 to 2018. Their findings confirm a clear progression in the architectural maturity of IoT systems, particularly with regard to scalability, security, and interoperability. However, they also underscore a notable lack of data privacy protection mechanisms in most existing designs.

Cloud-based architectures are also prevalent and are frequently combined with layered models, further demonstrating the complementary nature of architectural styles in IoT design [11].

Conversely, distributed IoT models – which integrate both decentralized computing and peripheral AI capabilities – can be categorized into centralized, collaborative, interconnected intranets, and fully distributed paradigms [9].

As also highlighted in [9], the majority of current IoT architectures remain centralized, with only a limited number adopting truly distributed models, despite the growing emphasis on edge intelligence and autonomous operation.

Both RAs and domain-specific IoT architectures, regardless of the selected architectural style or distribution model, must address a common set of fundamental questions [14], including:

- What are the system's functional elements?
- How do these elements interact?
- How is information managed within the system?
- What are the system's operational characteristics?
- How is the system implemented?

To effectively respond to these questions, architects increasingly rely on the formal concepts of views, viewpoints, and perspectives, which have been recently consolidated and formalized in [15].

These architectural concepts can be defined as follows:

- An architectural view is a representation of one or more structural aspects of a system's architecture. It illustrates how the architecture addresses one or more stakeholder concerns – such as those of IoT system users – by visually depicting relevant components and relationships [16].
- An architectural viewpoint is a collection of models, patterns, and conventions used to construct a particular type of view. It defines the stakeholders whose concerns are reflected in the view, along with the guidelines, principles, and template models that govern the construction of the view [17]. In practice, the terms view and viewpoint are often used interchangeably, although they represent distinct concepts.
- An architectural perspective is a collection of activities, checklists, tactics, and design guidelines intended to ensure that the system exhibits a cohesive set of quality attributes. These attributes often cut across multiple architectural views and require system-wide consideration [16]. Within many RAs, such perspectives are also referred to as cross-cutting concerns or system-wide functions.

These formalizations serve to structure architectural reasoning and enable the systematic evaluation of architectural integrity, especially in the design of complex, large-scale IoT ecosystems.

In addition, according to 17], the aforementioned definitions must be extended to include the following key concepts:

- Stakeholders: Individuals, groups, or organizations that possess a specific architectural interest in the design and development of a system.
- Concerns (or functions): Topics or issues of interest to one or more stakeholders, specifically related to the architectural aspects of the IoT system.

5. IoT RAs

5.1. IoT RAs Review

The first European conference dedicated to the Internet of Things took place in 2008, a year also recognized by Cisco as a pivotal moment in IoT history – when the number of connected devices surpassed the global human population, symbolically marking the birth of IoT.

It is within this historical context that the first IoT architectures began to emerge [10]. However, the first major initiative to provide a comprehensive RA for IoT was the European project IoT-A (Internet of Things – Architecture) [18].

One of the project's principal goals was to define a broad and extensible reference framework to guide the design of compliant, domain-specific IoT architectures tailored to a variety of application scenarios and stakeholder needs.

Unlike traditional architectures that are structured in layered formats, the IoT-A RA adopts a modular organization based on Functional Groups (FGs), each comprising a set of clearly defined architectural components.

According to its latest version, the IoT-A RA organizes its components into the following FGs:

- IoT Process Management FG – This group provides the interfaces necessary to augment traditional business processes with IoT capabilities, such as the integration of external business management systems.
- Service Organisation FG – Acts as a communication hub between other FGs and is responsible for composing and orchestrating services across different levels of abstraction.
- Virtual Entity FG – Functions as a virtualization mechanism that introduces a layer of abstraction for IoT data and services, enabling uniform manipulation and representation of managed data.
- IoT Service FG – Encompasses the core IoT service components, including functionalities for service discovery, lookup, and name resolution.
- Communication FG – Provides an abstraction layer for the IoT Service FG, serving as a gateway to connected devices by modeling the diverse interaction schemes of IoT protocols and networks.
- Security FG – Addresses cross-cutting security functionalities, including authorization, authentication, identity management, trust establishment, and other related mechanisms.
- Management FG – Also a cross-cutting group, this FG is responsible for several FCAPS functionalities: Fault, Configuration, Accounting (monitoring and reporting), Performance, and Security management.

These FGs and their interrelations are depicted in Figure 3.

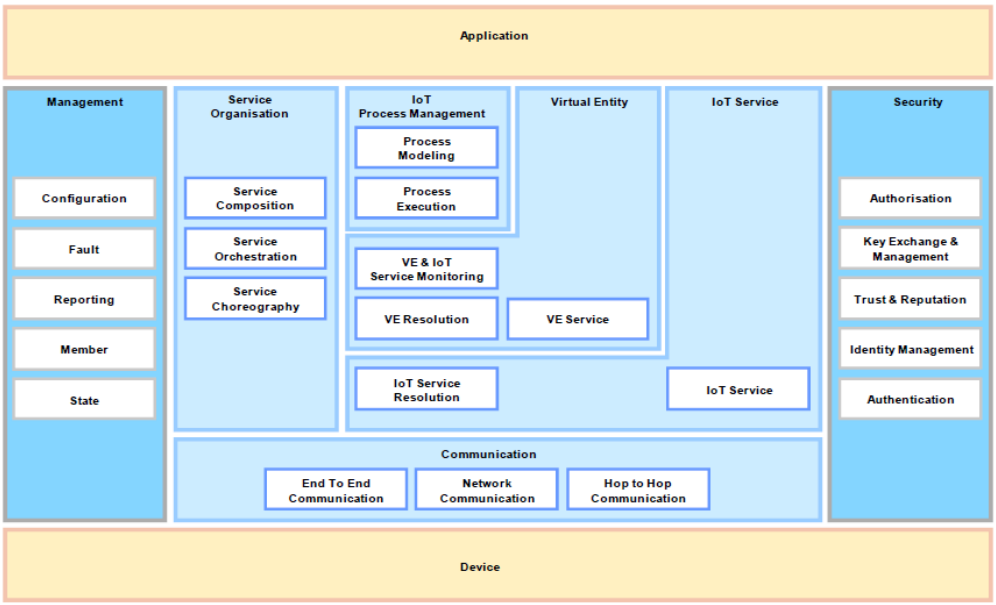

Figure 3. IoT-A Reference Architecture (Functional Decomposition Viewpoint) [18]

It is important to note that device-specific and application-specific layers lie outside the scope of the IoT-A RA, which focuses primarily on platform-level and systemic abstractions.

Many subsequent RAs have adopted and extended this model, aligning their structure with the ISO/IEC/IEEE 42010:2011 standard [15]. This international standard not only harmonizes key architectural terminology such as architecture, architectural framework, views, viewpoints, and perspectives, but also defines architectural requirements across system, software, and enterprise levels, thus offering a unified foundation for IoT architectural modeling.

One of the earliest architectures to apply the ISO/IEC/IEEE 42010:2011 standard was the Smart Grid Architecture Model (SGAM) [19], a RA developed by the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI). SGAM was specifically designed to address interoperability challenges across heterogeneous systems involved in Smart Grid environments, particularly at multiple architectural levels.

The SGAM architecture draws heavily on prior documentation and frameworks, including the NIST Conceptual Model [20], the GridWise Architecture Council's interoperability categories, and well-established enterprise architecture standards such as TOGAF and ArchiMate.

By synthesizing these sources, SGAM presents a multi-dimensional reference model structured around three key axes:

- Five interoperability layers: component, communication, information, function, and business process/activity.
- Five domains, reflecting the physical view of the energy value chain: generation, transmission, distribution, distributed energy resources, and customer premises.
- Six zones, corresponding to the hierarchical control levels of energy system management: process, field, station, operation, enterprise, and market.

These dimensions are integrated into a three-dimensional architectural framework (Figure 4), enabling a comprehensive mapping of smart grid functions, actors, and technologies across interoperability concerns, functional roles, and physical system domains.

In 2015, the Industrial Internet Consortium (IIC) introduced a RA specifically focused on the Industrial Internet of Things (IIoT). The resulting model, known as the Industrial Internet Reference Architecture (IIRA), also adheres to the ISO/IEC/IEEE 42010:2011 standard.

The IIRA is intended to serve as a set of best practices and guidelines for the design, documentation, communication, and implementation of IIoT systems [5], with the overarching goal of defining the necessary components and interfaces required to develop end-to-end architectures within the industrial IoT ecosystem.

According to its most recent version (v1.10) published in 2022 [5], and focusing on its functional viewpoint, the IIRA decomposes a typical IIoT system into five core functional domains, each supported by a set of system characteristics and cross-cutting functions that must span the entirety of the system architecture.

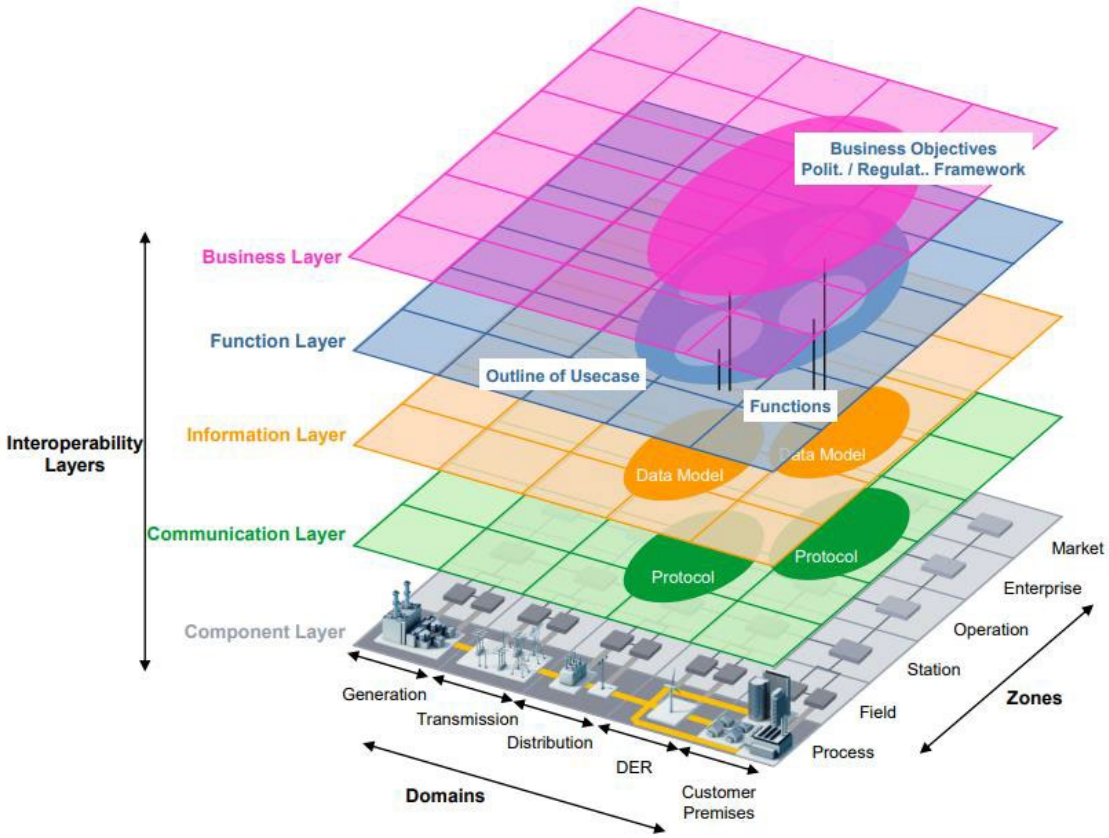

Figure 4. SGAM Reference Architecture [19]

These are illustrated in Figure 5 and described below:

- Control Domain – Encompasses functionalities executed by industrial assets or control systems that perform fine-grained closed-loop operations. This includes sensor data acquisition, rule-based processing, and physical actuation via control mechanisms.
- Operations Domain – Responsible for the maintenance and management of the Control Domain to ensure its continuous functioning. This includes health monitoring, configuration, updates, and diagnostics.

- Information Domain – Manages and processes data across the system. This includes data storage, modeling, and analytics, aimed at generating high-level system intelligence.
- Application Domain – Implements use case-specific logic, including rules and models at a macro level to support global optimization. It also incorporates application programming interfaces (APIs) and user-facing interfaces.
- Business Domain – Supports business processes and procedural functions, such as CRM, ERP, and MES, which are essential for end-to-end system integration within IIoT deployments. This domain is conceptually similar to the IoT Process Management Functional Group in the IoT-A RA.

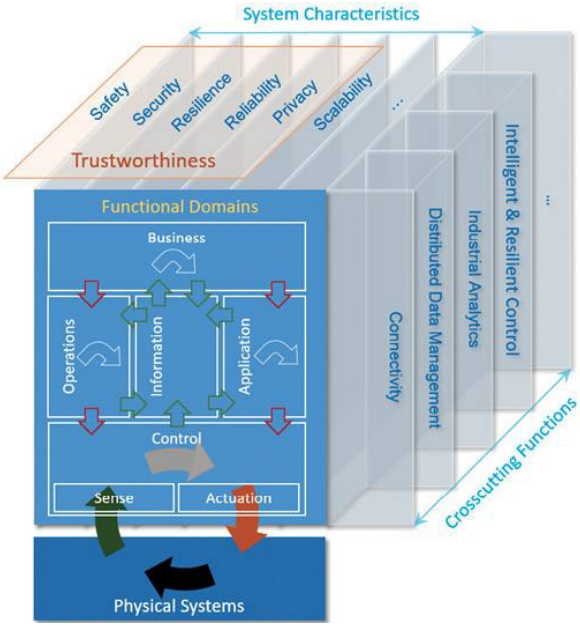

Figure 5. IIRA Reference Architecture [5]

The IIRA also defines a set of system characteristics, which may include Safety, Security, Resilience, Reliability, Privacy, and Scalability. In parallel, it identifies cross-cutting functions such as Connectivity, Distributed Data Management, Analytics, and Intelligent Control – all of which are essential for ensuring robust and interoperable IIoT systems. These two architectural axes may be further extended with additional system properties and functions, depending on the specific requirements of the deployment context.

In 2015, the German Industrie 4.0 initiative introduced the first version of the Reference Architecture Model for Industry 4.0 (RAMI 4.0). Unlike previous reference models, RAMI 4.0 achieved formal recognition as an international pre-standard under IEC PAS 63088.

The RAMI 4.0 architecture defines a service-oriented architecture (SOA) tailored to Industry 4.0 use cases and is visually represented as a three-dimensional model that maps the structure and dynamics of the Industry 4.0 ecosystem, as illustrated in Figure 6 [21].

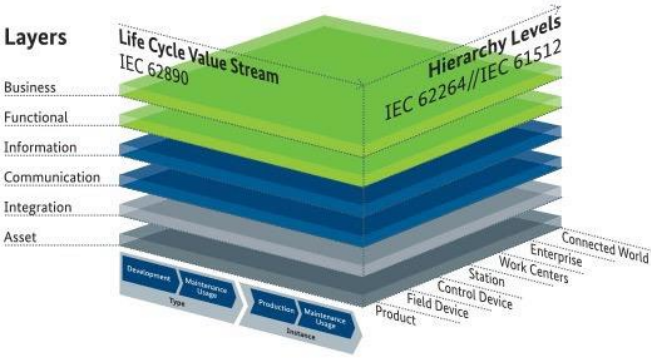

Figure 6. Reference Architecture for Industry 4.0 (RAMI 4.0) [21]

- The model's first dimension comprises the following six architectural layers: Asset, Integration, Communication, Information, Functional, and Business. These layers describe the system's structure, its properties, and the associated functions and data, reflecting both vertical and horizontal integration across system elements. Most of these layers can be directly mapped to the functional domains and cross-cutting concerns of the IIRA, with the exception of the Asset layer, which corresponds to IIRA's physical systems – though these are not formally defined in the IIRA framework.
- The second dimension, referred to as the Life Cycle and Value Stream, captures the entire lifespan of a product – from its conceptual design through development, production, and operation, to its maintenance and eventual decommissioning. It includes essential metadata such as product identifiers, certificates, and instance-level information.
- The third dimension, the Hierarchy Levels, corresponds to the decomposition of industrial systems according to traditional automation pyramids. It spans from individual components and machines up to connected world scenarios, thereby addressing integration across device, control, station, enterprise, and cloud levels. This enables the architectural representation of modular and scalable manufacturing systems.

While RAMI 4.0 is focused primarily on manufacturing processes (i.e. the production of goods), the IIRA adopts a broader scope, emphasizing cross-industry interoperability and the operation of products across various industrial contexts. In this way, RAMI 4.0 complements IIRA by offering a more domain-specific implementation aligned with the goals of smart manufacturing.

In fact, the IIRA and RAMI 4.0 are among the most widely referenced models for the development of IoT architectures, they are predominantly focused on industrial domains, with RAMI 4.0 being particularly aligned with manufacturing processes.

To address the need for a domain-independent reference model, the CREATE-IoT project – part of the European Large-Scale Pilots (LSP) programme – proposed in 2018 a three-dimensional IoT RA, known as the LSP IoT 3D Architecture [22].

While sharing several conceptual elements with IIRA and RAMI 4.0, this architecture presents a more generalized model, based on layers, cross-cutting functions, and non-functional properties, thus reflecting a structural alignment with the IIRA.

In this model, presented in Figure 7, there are the following layers:

- The Physical Layer consists of devices responsible for data acquisition and actuation, including the required hardware and embedded software.
- The Network Communication Layer defines the technologies and protocols for data transport, incorporating network gateways and communication infrastructures.
- The Processing Layer includes Edge Computing capabilities for near-real-time data stream analytics. Importantly, this is separated from the Storage Layer, which can be centralized or decentralized, and is responsible for long-term analytics and data persistence.
- The Abstraction Layer covers the semantic representation of data, enabling the construction of high-level models of the physical world.

The top three layers are concerned with IoT service and application orchestration, and provide capabilities such as advanced visualization, analytics, reporting, and integration with business-level solutions and third-party systems. These functions closely resemble the upper modules of other RAs previously discussed.

A notable feature of this architecture is the explicit inclusion of Edge Computing as a dedicated architectural layer, highlighting the increasing strategic importance of this paradigm in modern IoT system design. Indeed, similar layers will appear in subsequent RAs, although Edge capabilities may also be embedded within other layers in earlier models.

Two additional initiatives have made substantial contributions to the advancement of Edge Computing paradigms in IoT:

- The OpenFog Consortium – a public-private partnership founded by ARM, Cisco, Dell, Intel, Microsoft, and Princeton University's Edge Computing Laboratory, comprising over 750 members, including system integrators, industrial technology vendors, and academic institutions. OpenFog has since been merged into the Industrial Internet Consortium (IIC).
- The European Edge Computing Consortium (EECC) – an industry-led initiative involving major stakeholders such as ARM, Huawei, Intel, and National Instruments, aimed at accelerating the adoption of Edge Computing through the publication and promotion of dedicated RAs tailored to IoT contexts.

These efforts reflect a broader shift toward distributed intelligence, low-latency computation, and context-aware services, which are now central to the evolution of scalable and resilient IoT architectures.

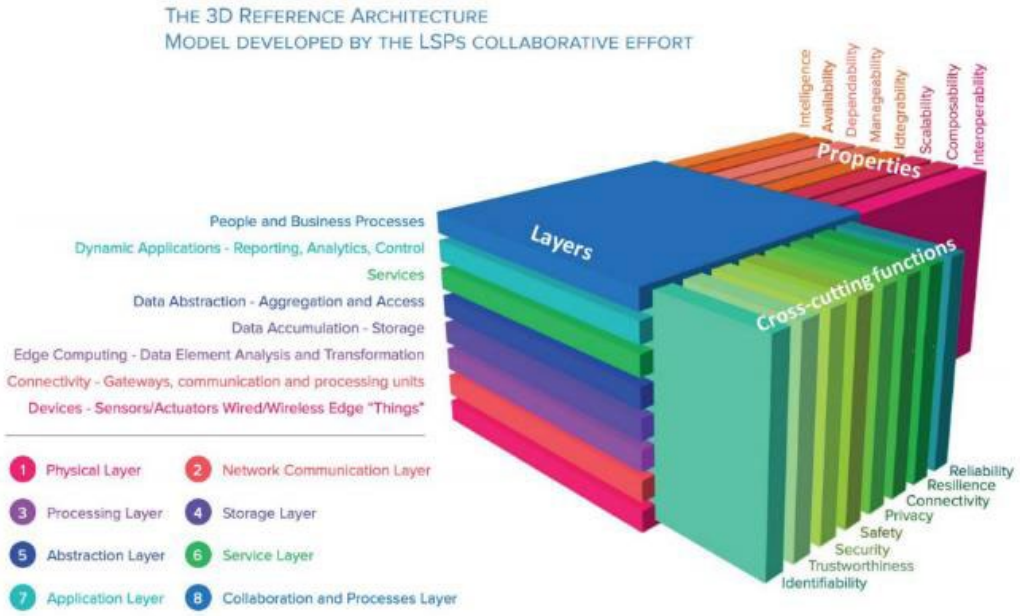

Figure 7. LSP 3D IoT Reference Architecture [22]

In 2017, the OpenFog Consortium introduced the OpenFog RA [23], developed in alignment with the ISO/IEC/IEEE 42010:2011 standard. This architecture promotes the adoption of Fog Computing – a distributed computing paradigm positioned between the Edge layer and the Cloud layer – with the aim of enhancing key communication attributes such as bandwidth optimization, latency reduction, and real-time responsiveness in IoT, AI, and robotic systems.

The OpenFog RA, illustrated in Figure 8, presents a unified framework that integrates both:

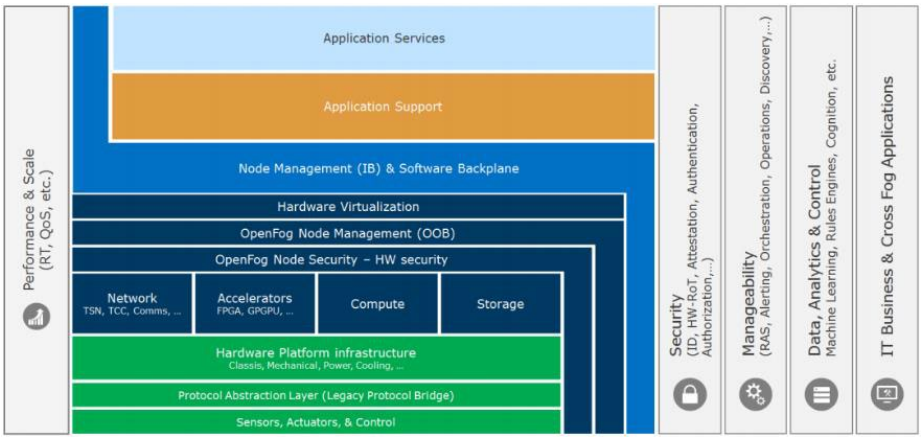

Figure 8. OpenFog Reference Architecture [23]

(i) Perspectives (analogous to cross-cutting concerns), represented as vertical grey bars, which include dimensions such as performance (e.g. latency), security, manageability, data analytics and control, and interoperability with broader IT business processes and cross-domain Fog applications.

(ii) Views and their corresponding layers, including:

- Node View: encompassing sensors, actuators, and the protocol abstraction layer;
- System View: covering intermediary layers such as platform hardware, networking, security, and virtualization;
- Software View: composed of three upper layers – Application Services, Application Support, and Node Management.

In 2019, the OpenFog Consortium was integrated into the Industrial Internet Consortium (IIC), paving the way for the convergence of architectural frameworks, particularly the potential synthesis between the OpenFog RA and the IIRA.

Concurrently, in the same year, the European Edge Computing Consortium (EECC) introduced the Reference Architecture Model for Edge Computing (RAMEC) [24], with the goal of accelerating the adoption of industrial ICT infrastructures that are software-defined, interoperable, programmable, secure, and user-friendly.

RAMEC is structured as a three-dimensional matrix, composed of the following dimensions, as depicted in Figure 9 and described below.

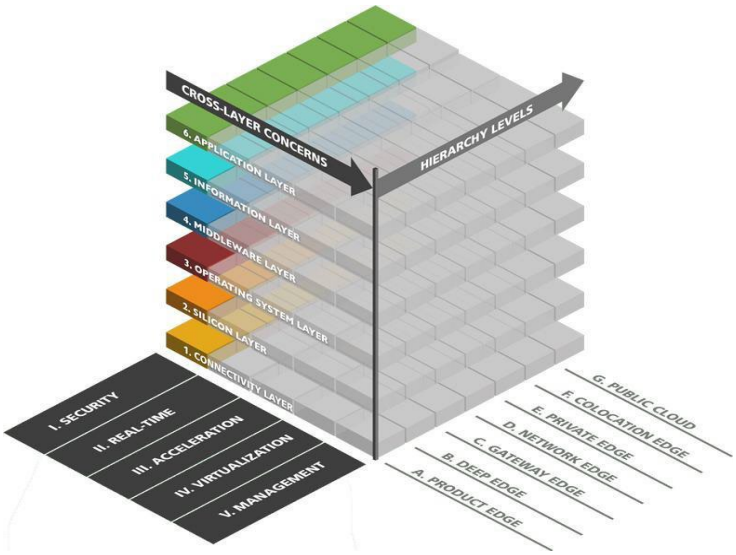

Figure 9. RAMEC Reference Architecture [24]

- Concerns – representing system-wide requirements such as security, latency constraints, AI acceleration technologies (e.g. TPU, GPU, FPGA), virtualization, and management functions;
- Layers – encompassing the technology stack, from connectivity (e.g. Ethernet/IP, TSN, 5G), to middleware (including data transport protocols), information layers (e.g. data models and semantics), and application layers;
- Hierarchy Levels – capturing the localization of Edge Computing functionalities across the continuum of industrial deployment, from embedded components (within products or actuators), to gateways, network nodes, and private cloud infrastructures, depending on application-specific requirements.

Importantly, RAMEC is not intended to be a technical architecture in the traditional sense, but rather a guidance framework for navigating a multidimensional problem space, conceptually analogous to SGAM and RAMI 4.0.

It serves as a strategic model for contextualizing and aligning technological, functional, and operational choices within the evolving Edge Computing paradigm.

5.2. Comparative overview of IoT RAs in the NGIoT context

Building upon the NGIoT-enabling technologies introduced in Section 3, this subsection provides a comparative assessment of the IoT RAs reviewed in this study.

The analysis focuses on the extent to which each architecture explicitly or implicitly supports key NGIoT technologies, including Edge–Fog–Cloud computing, 5G and Network Virtualization, Artificial Intelligence, Digital Twins, Augmented Reality and the Tactile Internet, Distributed Ledger Technologies (Blockchain), and Hyperconnectivity (Software Defined Networks).

Early architectures such as IoT-A and SGAM primarily emphasize interoperability, abstraction, and system modeling, but do not explicitly address emerging NGIoT technologies. Their designs predate large-scale Edge Computing adoption and therefore rely mainly on centralized or hierarchical system assumptions.

Similarly, while IIRA and RAMI 4.0 introduce strong support for industrial integration, lifecycle management, and functional decomposition with notable examples with RAMI 4.0 explicitly formalizing Digital Twins through the Asset Administration Shell, their treatment of AI, Blockchain, and ultra-low-latency human–machine interaction remains largely implicit or domain-specific,

More recent architectures, such as the LSP 3D IoT RA, OpenFog RA, and RAMEC, reflect a clear shift toward NGIoT requirements. These models explicitly incorporate Edge and Fog Computing as first-class architectural elements, recognize the role of advanced networking technologies, and address non-functional properties such as latency, scalability, and real-time processing. However, their support for higher-level NGIoT capabilities, such as Digital Twins, AI-driven autonomy, or trust mechanisms based on Blockchain, remains fragmented or conceptual.

In contrast, the ASSIST-IoT RA, presented in detail in Sector 6, has been designed explicitly to support NGIoT requirements. It integrates Edge–Fog–Cloud computing, 5G/NFV, AI, DT, DLT, and human-centric interaction mechanisms as first-class architectural concerns. This holistic integration reflects a shift toward cloud-native, decentralized, and production-ready architectural models, positioning ASSIST-IoT as a comprehensive framework for next-generation, intelligent, and human-centric IoT systems.

The comparative overview presented in Table 1 evaluates the reviewed RAs with respect to their support for key NGIoT technologies. The assessment is intentionally conservative and is based on the explicit architectural scope and design intent of each RA, rather than on specific implementations, later extensions, or domain-specific use cases.

In this context, “Y” (Yes) indicates that a given technology is explicitly modeled, named, or structurally integrated within the architecture; “P” (Partial) denotes implicit, indirect, or domain-dependent support, where the technology is enabled conceptually but not treated as a first-class architectural concern; and “N” (No) indicates that the technology is outside the scope of the RA.

Table 1. Comparative overview of IoT RAs in the NGIoT context

Reference Architecture	NGIoT technologies						
	Edge-Fog-Cloud	5G	AI	DT	DLT	SDN / NFV	AR / TI
IoT-A	P	N	N	P	N	N	N
SGAM	P	N	N	P	N	N	N
IIRA	P	P	P	P	P	P	P
RAMI 4.0	P	P	P	Y	P	P	P
LSP IoT 3D	Y	P	P	P	P	P	P
OpenFog	Y	N	P	N	N	P	N
RAMEC	Y	Y	P	N	N	Y	P
ASSIST-IoT	Y	Y	Y	Y	Y	Y	Y

This comparative analysis highlights a progressive architectural evolution from centralized, connectivity-focused models toward decentralized, intelligence-driven, and human-centric NGIoT frameworks.

6. NGIoT RAs

6.1. NGIoT RAs Review

The RAs discussed in the previous section represent some of the most relevant and influential models currently available and collectively illustrate the evolving trends in IoT system design. However, to date, most existing IoT RAs do not

explicitly address many of the technologies required for NGIoT systems.

Notably, Edge Computing has gained significant traction – as evidenced in the LSP RA, OpenFog RA, and particularly in RAMEC – where it is addressed through the inclusion of dedicated architectural layers. Moreover, RAMEC extends its scope to incorporate emerging technologies such as 5G, along with the promising Time-Sensitive Networking (TSN) standard in its connectivity layer. It also includes critical concerns such as virtualization, real-time processing, and even elements that align conceptually with AR and the Tactile Internet.

In parallel, ongoing research efforts are exploring how to incorporate NGIoT technologies into innovative architectural proposals. Notable examples include:

The SerIoT project, a European initiative, introduced a security-centric RA that leverages both traditional mechanisms (e.g. honeypots) and advanced technologies, such as cognitive routing for SDN and Blockchain-based trust infrastructures [25].

BlockIoTIntelligence [26] focuses on the integration of Blockchain and AI for decentralized IoT systems, spanning across Cloud, Fog, Edge, and device layers. The authors provide an in-depth analysis of current trends in these enabling technologies and their convergence within the IoT landscape.

In [27], the AI4SAFE-IoT architecture is presented – a three-layered model (edge/network/application) that enhances security features at the edge computing level through the application of AI-based detection and prevention techniques.

Furthermore, [28] introduces a NGIoT architecture for Industrial Edge Computing built on 5G and emerging technologies, comprising eight distinct layers: Physical Devices, Connectivity and Device-to-Device (D2D) Communication (both powered by 5G), Edge/Fog Computing, Data Storage, Management Services (including data analytics, cloud computing, and network management), Application Layer, Collaboration and Business Processes, and a Cross-Cutting Security Layer. Although this architecture offers a generalized and extensible framework, it does not address DLTs such as Blockchain, nor does it explicitly incorporate Tactile Internet capabilities.

These emerging proposals reflect the direction of architectural innovation in IoT, emphasizing the growing need for security, decentralization, AI integration, and real-time responsiveness, as next-generation systems move toward greater autonomy, scalability, and interoperability across domains.

The European ASSIST-IoT project extends the capabilities of existing RA models by introducing a novel RA for NGIoT [29].

This RA depicted in Figure 10 reinterprets the Cloud-native distributed computing paradigm in the context of a seamless Edge–Fog–Cloud continuum, serving as a foundational framework for building the next generation of intelligent, adaptive, and decentralized IoT systems.

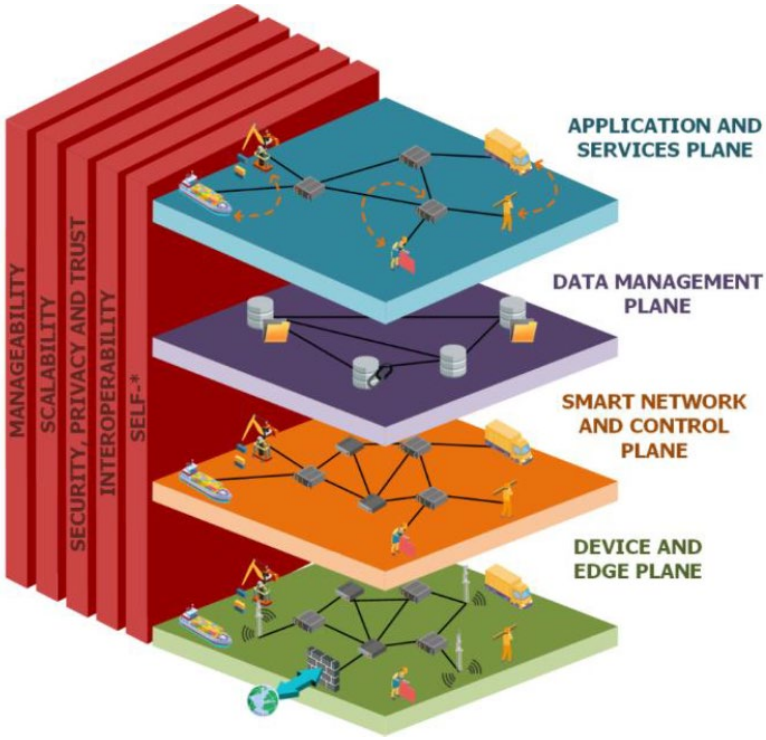

Figure 10. ASSIST-IoT Reference Architecture (Conceptual Viewpoint) [29]

6.2. ASSIST-IoT

At its core, the ASSIST-IoT RA integrates a suite of key enabling technologies, including: 5G networking with support for NFV, AI and Big Data Analytics, AR and the Tactile Internet, DT and Blockchain.

These technologies are not treated in isolation but are systematically incorporated to support the design, development, and deployment of NGIoT systems capable of addressing complex and ambitious use cases – notably those involving integration with the processes and business models associated with the new economic models such as the circular economy.

The ASSIST-IoT RA is conceptual, multidimensional, and inherently decentralized, structured around both horizontal and vertical planes [30].

The horizontal planes represent logically grouped functionalities, reflecting specific domains of activity or service layers within the system.

The vertical planes correspond to cross-cutting concerns, system-wide functions, and non-functional properties – such as security, resilience, context-awareness, or data privacy – that require coordination across multiple functional domains or that may operate independently across different planes.

This architectural approach promotes modularity, interoperability, and scalability, while also enabling the inclusion of domain-specific adaptations needed for emerging socio-technical challenges, as seen in Figure 11.

ASSIST-IoT thus represents a forward-looking architectural framework, designed to bridge the gap between advanced technological enablers and real-world deployment requirements in next-generation, distributed IoT ecosystems.

The ASSIST-IoT RA is composed of four horizontal planes, each representing a logically grouped set of functionalities critical to the development and operation of NGIoT systems:

- IoT Devices and Edge Computing Nodes: This plane encompasses the physical components that form the foundation of the architecture, ranging from Edge servers and computing nodes to IoT devices, sensors, and networking hardware. It also includes the functional capabilities required for executing local intelligent analytics or actions, as well as pre-processing and forwarding data to higher-level services.
- Smart Network and Control: This plane integrates technologies that enable virtualized and SDN, including Software-Defined Wide Area Networks (SD-WAN), NFV, and Management and Orchestration (MANO) frameworks. It supports key features such as dynamic network configuration, tunneling, routing, and load balancing, enabling adaptive and efficient communication across the system.
- Data Management: This plane groups together all functionalities related to data handling, encompassing the full pipeline from data acquisition, routing, fusion, and aggregation, to transformation and storage. It ensures that data is processed, contextualized, and made available for higher-level decision-making.
- Applications and Services: Dedicated to end-user functionality, this plane supports the development and deployment of applications for users, system administrators, and/or external systems. It relies on the services provided by the lower planes (as well as on the vertical concerns) to deliver value-added applications tailored to the needs of various stakeholders.

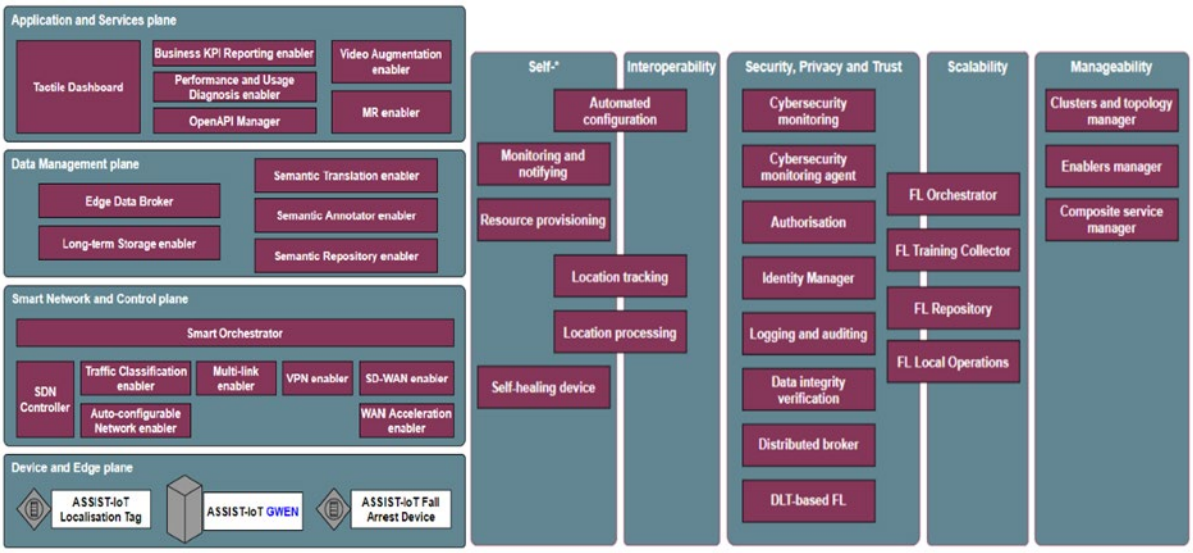

Figure 11. ASSIST-IoT Reference Architecture (Functional Viewpoint) [29]

Together, these horizontal planes provide a comprehensive and modular foundation for architecting scalable, secure, and interoperable NGIoT systems. Their interaction with the vertical planes ensures that system-

wide concerns such as security, context-awareness, and performance are consistently addressed across all layers of the architecture.

The vertical planes in the ASSIST-IoT RA play a supporting role for the functionalities defined in the horizontal planes. They reflect both inherent system properties and emerging technological capabilities, ensuring that essential cross-cutting concerns are integrated consistently across the architecture. These vertical planes include:

- Auto- (Self-) Capabilities: This category encompasses system properties related to autonomy or semi-autonomy, referring to operations that do not require human intervention. It includes features such as self-healing, self-configuration, self-awareness, and self-organization, all of which are critical to enabling resilient and adaptive behaviours in NGIoT systems.
- Interoperability: A core architectural property that ensures cross-vendor compatibility at the hardware level enabling devices from different manufacturers to communicate within a unified implementation and data sharing at the software level through the use of common formats, standardized protocols, or dedicated translation tools. This capability is essential for achieving seamless integration in heterogeneous IoT environments.
- Security, Privacy, and Trust: A set of system-level properties aimed at preserving data integrity, access control, and protection against malicious threats. This vertical plane ensures that the architecture adheres to security-by-design principles, safeguarding sensitive operations and fostering trust among users, devices, and services.
- Scalability: Refers to the system's ability to maintain performance and resource allocation under changing operational conditions or evolving business requirements. This property encompasses not only software scalability, but also hardware and network scalability, thereby supporting the dynamic expansion of system capabilities.
- Manageability: Encompasses the management of the full lifecycle of functionalities across both horizontal and vertical planes. This includes instantiation, configuration, monitoring, and termination of services and components. Additionally, it involves device management and the coordination of workflows, which are essential for maintaining operational efficiency and control in large-scale IoT deployments.

Together, these vertical concerns form the system-wide foundation upon which the horizontal functional layers operate. Their integration ensures that the architecture remains robust, secure, and adaptable to evolving technological and operational demands.

The design principles underpinning the ASSIST-IoT RA are founded on five key pillars: decentralization, scalability, software modularity and simplicity, adoption potential, and production-readiness.

Accordingly, the design of IoT systems based on the ASSIST-IoT architecture must account for the fundamental differences between Edge Computing and Cloud Computing. In contrast to Cloud infrastructures, computational resources at the edge are typically more limited, less stationary, and may be dynamically scaled, reduced, or reallocated. Furthermore, these resources are often geographically distributed, leading to increased complexity in orchestration and management.

Therefore, the selected design principles must explicitly support the heterogeneity and dynamism of system topologies, ensuring the architecture is flexible enough to accommodate changes in both hardware availability and resource utilization patterns. This flexibility is essential for enabling resilient, adaptive, and context-aware IoT deployments, particularly in environments where computational capacity, connectivity, and system composition may vary significantly over time or space.

Building upon the principles outlined above, the ASSIST-IoT architecture is governed by a set of core design principles and strategic architectural decisions, which reflect both technological flexibility and operational robustness:

- Microservices-based Software Architecture: Given the diversity of technologies and functionalities involved in NGIoT systems, the architecture adopts a modular design approach grounded in microservices. By maintaining software as independent, loosely coupled modules that can be selectively interconnected, the architecture promotes ease of maintenance, reusability, and on-demand deployment of specific functionalities.
- Service Containerization: The instantiation of microservices is realized through containerization, enabling lightweight, portable, and scalable deployments across heterogeneous environments. This approach enhances system flexibility and resource efficiency, while supporting rapid deployment and rollback operations.
- Abstract Concept of Facilitator: A novel architectural abstraction termed the facilitator is introduced. A facilitator is a logical grouping of software components deployed on computational nodes, which collaborate to deliver a specific functionality within the IoT system. This abstraction supports encapsulation, coordination, and dynamic composition of services.
- Use of Kubernetes for Orchestration: Kubernetes is proposed as the recommended orchestration platform for managing facilitators. It offers a mature and production-ready solution for automated deployment, scaling, load balancing, resilience, and lifecycle management of containerized microservices, thus supporting robust and scalable system operation in real-world IoT scenarios.

These decisions collectively contribute to an architecture that is modular, scalable, and aligned with

modern DevOps and cloud-native practices, while remaining suitable for deployment in resource-constrained, distributed edge environments.

6.2. Alignment of ASSIST-IoT RA with NGIoT technologies

The ASSIST-IoT RA has been explicitly designed to address the technological and systemic requirements of NGIoT systems. Unlike earlier RAs, ASSIST-IoT embeds NGIoT-enabling technologies as integral architectural components rather than treating them as optional extensions.

Edge–Fog–Cloud computing is realized through the distributed deployment of microservices across IoT devices, Edge nodes, and Cloud infrastructures, enabling localized intelligence, reduced latency, and scalable processing.

5G connectivity and Network Function Virtualization are incorporated within the Smart Network and Control plane, supporting dynamic network configuration, slicing, and service orchestration.

Artificial Intelligence is integrated across multiple planes, enabling data-driven cognition, autonomous decision-making, and self- capabilities, while Digital Twins are supported through the Data Management and Application planes by enabling synchronized digital representations of physical assets.

Augmented Reality and Tactile Internet applications are facilitated by the Hyperconnectivity with the low-latency, edge-centric design of the architecture, enabling real-time human–machine interaction.

Furthermore, Blockchain technologies are incorporated to enhance trust, data integrity, and decentralized governance, particularly in distributed and multi-stakeholder environments.

Through this tight coupling between architectural structure and NGIoT technologies, ASSIST-IoT represents a production-ready and future-oriented RA tailored to the demands of next-generation, intelligent, and human-centric IoT ecosystems.

6.3. Deployment considerations

Several practical considerations and challenges should be considered when transitioning from RA conceptual models to real-world deployments, such as:

- performance trade-offs across the Edge–Fog–Cloud continuum, where latency reduction and localized intelligence must be balanced against resource constraints, orchestration overhead, and data consistency requirements
- operational complexity represents another significant challenge, particularly in cloud-native and microservices-based architectures. While containerization and orchestration platforms enable scalability and flexibility, they also introduce additional management overhead, requiring advanced monitoring, lifecycle management, and DevOps practices to ensure reliable system operation.
- migration from legacy IoT systems to NGIoT architectures remains a non-trivial task. Existing deployments are often based on monolithic, centralized designs and proprietary interfaces, making gradual integration with decentralized, service-oriented RAs necessary. In this context, interoperability mechanisms, backward compatibility, and phased migration strategies play a critical role in enabling adoption without disrupting operational continuity.

Addressing these challenges is essential for translating NGIoT RAs into sustainable, large-scale deployments and represents an important direction for future research and industrial experimentation.

7. Conclusion

The IoT represents a convergence of integrated technologies designed to address increasingly diverse and evolving application requirements. In this context, RAs play a critical role by providing structured frameworks of functionalities, components, and design principles that guide the development of interoperable, scalable, and secure IoT systems.

This study has shown that while established RAs such as IoT-A, SGAM, IIRA, and RAMI 4.0 have laid important foundations for sector-specific deployments, many of them lack the architectural flexibility required to fully accommodate the complexity introduced by NGIoT.

In this evolving landscape, the European ASSIST-IoT RA emerges as a forward-looking and comprehensive framework explicitly designed for NGIoT systems. By integrating Edge–Fog–Cloud computing, 5G, Artificial Intelligence, Digital Twins, Distributed Ledger Technologies, and human-centric interaction paradigms via Augmented Reality and Tactile Internet within a cloud-native, microservices-based architecture, ASSIST-IoT provides a modular, scalable, and production-ready blueprint for complex and distributed IoT deployments.

Future research on IoT RAs should focus on enhancing trust and explainability in AI-enabled IoT systems, advancing security models suitable for highly distributed edge and fog environments, incorporating regulatory compliance mechanisms for privacy, data sovereignty, and cross-border data flows, and designing adaptive architectures capable of autonomous reconfiguration in response to contextual changes. In addition, the role of NGIoT architectures in supporting sustainable development and emerging Circular Economy models warrants further investigation through real-world validation and large-scale deployment scenarios.

This review contributes to a clearer understanding of the evolution of IoT RAs and their alignment with NGIoT

requirements, offering guidance for researchers and practitioners involved in the design and implementation of future intelligent, decentralized, and human-centric IoT ecosystems.

Acknowledgements.

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

References

[1] NGIoT Project. D3.1. IoT research, innovation and deployment priorities in the EU [Internet]. 2020 [cited 2025 Aug 5]. Available from: https://ngiot.eu/wp-content/uploads/2020/09/D3.1.pdf

[2] Maier MW, Emery D, Hilliard R. Software architecture: Introducing IEEE standard 1471. Computer (Long Beach Calif). 2001;34(4):107–9.

[3] Bassi A, Bauer M, Fiedler M, Kramp T, Van Kranenburg R, Lange S, et al. Enabling Things to Talk: Designing IoT Solutions with The IoT Architectural Reference Model. Berlin: Springer Nature; 2013. p. 379.

[4] Weyrich M, Ebert C. Reference architectures for the internet of things. IEEE Softw. 2016;33(1):112–6.

[5] Industrial Internet Consortium. The Industrial Internet of Things Volume G1: Reference Architecture v1.10 [Internet]. 2022 [cited 2025 Aug 5]. Available from: https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf

[6] Jo D, Kim GJ. IoT + AR: pervasive and augmented environments for 'Digi-log' shopping experience. Hum Centric Comput Inf Sci. 2019;9(1):1.

[7] Yang R, Yu FR, Si P, Yang Z, Zhang Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. IEEE Commun Surv Tutorials. 2019;21(2):1508–32.

[8] Vermesan O, et al. The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge. River Publishers Series in Communications; 2018. p. 19–102.

[9] Muccini H, Moghaddam MT. IoT architectural styles: A systematic mapping study. In: Lecture Notes in Computer Science. 2018;11048:68–85.

[10] Alshohoumi F, Sarrab M, AlHamadani A, Al-Abri D. Systematic review of existing IoT architectures security and privacy issues and concerns. Int J Adv Comput Sci Appl. 2019;10(7):232–51.

[11] Sethi P, Sarangi SR. Internet of Things: Architectures, Protocols, and Applications. J Electr Comput Eng. 2017;2017:1–25.

[12] Singh SP, Kumar V, Singh AK, Singh S. A Survey on Internet of Things (IoT): Layer Specific vs. Domain Specific Architecture. In: Lecture Notes on Data Engineering and Communications Technologies. Springer; 2020. Vol. 44, p. 333–41.

[13] CREATE-IoT Project. D6.2. Recommendations for commonalities and interoperability profiles of IoT platforms [Internet]. 2018 [cited 2025 Aug 5]. Available from: https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf

[14] Bauer M, Walewski JW. The IoT architectural reference model as enabler. In: Bassi A, et al., editors. Enabling Things to Talk. Berlin: Springer; 2013. p. 17–25.

[15] ISO/IEC/IEEE 42010. Systems and software engineering – Architecture description [Internet]. 2022 [cited 2025 Aug 5]. Available from: https://www.iso.org/standard/74393.html

[16] Rozanski N, Woods E. Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives. Boston: Addison Wesley; 2011.

[17] IEEE. IEEE 1471-2000 - IEEE Recommended Practice for Architectural Description for Software-Intensive Systems [Internet]. 2000 [cited 2025 Aug 5]. Available from: https://standards.ieee.org/standard/1471-2000.html

[18] IoT-A Project. D1.5. Final architectural reference model for the IoT [Internet]. 2013 [cited 2025 Aug 5]. Available from: https://www.researchgate.net/publication/272814818_Internet_of_Things_-_Architecture_IoT-A_Deliverable_D15_-_Final_architectural_reference_model_for_the_IoT_v30

[19] CEN-CENELEC-ETSI Smart Grid Coordination Group. CEN-CENELEC-ETSI Smart Grid Reference Architecture [Internet]. 2012 [cited 2025 Aug 5]. Available from: https://energy.ec.europa.eu/system/files/2014-11/xpert_group1_reference_architecture_0.pdf

[20] NIST. NISTIR 7628 - Guidelines for smart grid cyber security [Internet]. Gaithersburg, MD: NIST; 2014 [cited 2025 Aug 5]. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[21] VDI/VDE Society Measurement and Automatic Control (GMA). Status Report Reference Architecture Model Industrie 4.0 (RAMI4.0) [Internet]. 2015 [cited 2025 Aug 5]. Available from: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report__Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf

[22] CREATE-IoT Project. D1.12. EU IoT value chain integration framework [Internet]. 2020 [cited 2025 Aug 5]. Available from: https://european-iot-pilots.eu/wp-content/uploads/2020/06/D01_12_WP01_H2020_CREATE-IoT_Final.pdf

[23] OpenFog Consortium. OpenFog Reference Architecture for Fog Computing [Internet]. 2017 [cited 2025 Aug 5]. Available from: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf

[24] Willner A, Gowtham V. Towards a Reference Architecture Model for Industrial Edge Computing. Comput Sci. 2020.

[25] SerIoT Project. D2.1. SerIoT Architecture & Specifications [Internet]. 2018 [cited 2025 Aug 5]. Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c052e1b7&appId=PPGMS

[26] Singh SK, Rathore S, Park JH. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Future Gener Comput Syst. 2020;110:721–43.

[27] HaddadPajouh H, Khayami R, Dehghantanha A, Choo KKR, Parizi RM. AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things. Neural Comput Appl. 2020;32(20):16119–33.

[28] Rahimi H, Zibaeenejad A, Safavi AA. A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies. In: 2018 IEEE 9th Annual Information

Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE; 2019. p. 81–8.

[29] ASSIST-IoT Project. D3.7 – ASSIST-IoT Architecture Definition – Final [Internet]. 2022 [cited 2025 Aug 5]. Available from: https://assist-iot.eu/wp-content/uploads/2022/09/ASSIST-IoT_D3.7_Architecture_Definition_Final_v1.0.pdf

[30] Szmeja P, Fornés-Leal A, Lacalle I, Palau CE, Ganzha M, Pawłowski W, et al. ASSIST-IoT: A Modular Implementation of a Reference Architecture for the Next Generation Internet of Things. Electronics. 2023;12(4):854. Available from: https://doi.org/10.3390/electronics12040854