ERAMIS: A Reference Architecture-based Methodology for IoT Systems

Paul Kearney and Rasool Asal
EBTIC, Khalifa University, Abu Dhabi, UAE
e-mail: paul.kearney@bcu.ac.uk. rasool.asal@bt.com

***Abstract*— Opportunities arising from IoT-enabled applications are significant, but market growth is inhibited by concerns over security and complexity. To address these issues, we propose the ERAMIS methodology, which is based on instantiation of a reference architecture that captures common design features, embodies best practice, incorporates good security properties by design, and makes explicit provision for operational security services and processes.**

Keywords- IoT; security; architecture, methodology

I. A Reference Architecture-Based Approach

IoT application concepts appear in many industry sectors with names such as Smart City, Smart Healthcare, Smart Building, Smart Home, Smart Grid, Intelligent Transportation System, Industrie 4.0, etc. – 'Smart X' for short. While these are diverse, they are all control systems in which smart devices couple the physical and cyber-worlds bidirectionally. The IoT market is already significant and is set to grow year on year for the foreseeable future. This is despite lack of progress on lowering barriers to adoption, which include concerns over complexity and security.

Clearly, then, the ability to deliver secure, robust and reliable Smart X solutions confers a major competitive advantage. This paper describes the on-going definition of a methodology called ERAMIS (EBTIC Reference Architecture-based Methodology for IoT Systems). It outlines ERAMIS' Reference Architecture (RA)-based approach, summarizes a survey of existing IoT RAs, describes how a 'best of breed' synthesis is used within ERAMIS, and points to on-going developments.

The term Reference Architecture (RA) is widely used, but poorly-defined. In simple terms, we consider an RA to be an abstract and/or incomplete architecture description embodying best practice knowledge derived from experience, that can be elaborated to generate a full system architecture for a specific application.

A more formal definition requires introduction of some terminology. According to International Standard ISO/IEC/IEEE 42010 [1] an architecture description consists of one or more views, each of which addresses the concerns of classes of stakeholder in the system. A view consists of one or more architecture models. Stakeholders and their concerns are grouped into viewpoints, which are said to frame the views. The viewpoints are the major elements in an architecture framework, to which views and their constituent models must be added to complete the architecture description.

In ERAMIS, an RA is seen as an architecture framework augmented by a set of architectural patterns, where a pattern is essentially a partially-instantiated model capturing a solution strategy abstracted from successful instances of architecture. Patterns, thus express best practice options within the relevant domain. The architecture design process involves successive selection, instantiation and elaboration of patterns until the required breadth and depth of description is achieved. Strategies that prove successful in practice are captured as new or improved patterns. Thus, the RA is a living knowledge repository that grows and improves over time. We envisage a specialization hierarchy with at least three levels: generic, industry/application-specific, and organization-specific.

Three main categories can be discerned among sources claiming to document IoT RAs: 'top-down' (comprehensive, technology-neutral coverage, often from the perspective of a particular Smart X application sector); 'model-based' (derived from a representation of IoT concepts); and 'bottom-up' (based on abstractions of specific IoT application platforms). The categories are largely complementary, with the top-down RAs being strong on overall structure and application insight, the model-based RAs providing the means to represent architecture models, and the bottom-up RAs facilitating implementation. A recent International Standard, ISO/IEC 30141 [2], builds upon top-down and model-based examples, notably IoT-A [3] (model-based) and the Industrial Internet Consortium's (IIC's) Industrial IoT Reference Architecture (IIRA, top-down) [4].

The top-down and model-based RAs treat security as a concern cutting across viewpoints, and a system property within views. The bottom-up RAs focus on security-related services provided by their underlying platforms.

II. ERAMIS

A. *Basic Structure*

ERAMIS adopts the viewpoints of the IIC's IIRA as the starting point for its architecture framework: Business, Usage, Functional and Implementation. The first two concern the relationship of the application with business stakeholders and users, respectively, while the latter two concern representation of the technical system at abstract and concrete levels.

In a methodology, the layers can be considered sequentially in a traditional, 'waterfall' lifecycle or iteratively in an agile one. In the Business Viewpoint, the application is seen as a socio-technical system enacting business processes in collaboration with its business environment, and thus addresses business requirements. In the Usage Viewpoint we see that the socio-technical system is made up of human users and operators interacting with a technical system (addressing user/operational requirements) that exhibits behavior (Functional viewpoint, functional requirements) distributed over a cyber-physical infrastructure (Implementation viewpoint, addressing implementation and deployment options and constraints).

The IIRA Functional viewpoint is divided into five domains organized in three tiers. The lowest tier consists of the Control domain, which couples the IoT application to the physical world via sensing and actuation functionality. It also encompasses fine-grained, reactive control functionality responding to sensory input by triggering actions. Of the three domains in the middle tier, Information and Application support functional requirements (i.e. what the system should do), while the Operations concerns how the system is managed. Operations encompasses management aspects of both. The final domain (Business) deals with high level application functionality. It obtains analyzed intelligence from the Information domain, makes business decisions based on it, and implements the decisions through the Application domain. Functionality concerning the relevant Smart-X application is concentrated in the top tier, and that characteristic of IoT (i.e. making use of smart, connected devices) is concentrated in the bottom tier. Middle-tier functionality is relatively generic, though how it is used is conditioned by requirements from Business and Control domains. The corresponding functional domain structure in the ISO/IEC 30141 is mostly similar, although the Business Domain is replaced by a User Domain that interacts directly with the Control Domain directly as well as with the middle tier. In our view this is more than a superficial difference as the concepts of User and Owner should be kept distinct.

The visual similarity between the three-tier models often used at the Functional and Implementation levels is dangerously seductive. It is important to maintain a clear distinction between the two views. The former is concerned with the logical decomposition, organization and co-ordination of the abstract functional elements required for the IoT application to fulfill its role, while the latter concerns the architecture of ICT an OT infrastructure and its relationship with real-world domain entities. Clearly, there must be a mapping between the two for the functionality to be realized, but there are often many ways to achieve this.

B. Modelling and Architecture Description

The Functional level is the central focus of ERAMIS. Business and operational concerns collected at the higher levels are mapped onto an abstract solution organized according to the five functional domains. This abstract solution can in turn be mapped onto platforms, networks and physical infrastructure at the Implementation level.

We follow the model-based RAs in taking a service-oriented approach, i.e. the architecture is expressed in terms of entities that provide and consume services to and from each other. The entity types are based on a conceptual model that captures the key IoT domain abstractions. Constructing the functional architecture then becomes a process of populating the domains with instances of these concepts.

Developing the conceptual model into the basis for an IoT architecture description language (ADL) is the subject of on-going research. The ADL needs to be able to model dynamic properties as well as the static structural aspects. As IoT applications are control systems, it is important to be able to model the application's interaction with its environment, which includes not only inanimate objects but also legitimate users and malicious threat agents.

C. Security

ERAMIS must ensure that security concerns are captured and addressed at an appropriate level of abstraction within each view and are reconciled and traceable across views. The IIRA Business Viewpoint can be extended to include e.g. Risk Optimization and Compliance as specializations of Key Objective. Similarly, in the Usage Viewpoint, security-specific roles, activities and tasks can be defined. In ERAMIS, the Functional architecture is amended to include operational IoT security functionality explicitly by introducing IoT Security sub-domains of the Control and Operations domains. The IoT Security Operations sub-domain is responsible for interpreting security requirements, establishing and maintaining policies, monitoring their effectiveness, etc. The IoT Security Control sub-domain is responsible for enforcing security policies, monitoring the security state of things, devices, etc., local reactive response to events, reporting incidents, anomalies, indicators of compromise, etc. to IoT Security Operations. The model-based ADL being developed will include means of describing the architecture of the IoT Security Operations and Control sub-domains.

ACKNOWLEDGMENT

PK is also Professor of Cybersecurity at Birmingham City University, UK.

REFERENCES

[1] International Standard ISO/IEC/IEEE 42010:2011(E) "Systems and software engineering — Architecture description", First edition, 2011-12-01

[2] International Standard ISO/IEC 30141, "Internet of Things (IoT) – Reference architecture", Edition 1.0 2018-08, ISBN 978-2-8322-5972-6

[3] M. Bauer, M. Boussard, N. Bui, F. Carrez, C. Jardak, J. De Loof, C. Magerkurth, S. Meissner, A. Nettsträter, A. Olivereau, M. Thoma (SAP, Matthias & J. Walewski, J. Stefa, and A. Salinas,. "Internet of Things – Architecture IoT-A Deliverable D1.5 – Final architectural reference model for the IoT", Version 3.0, 2013.

[4] S-W. Lin, M. Crawford and S. Mellor (eds.), "The Industrial Internet of Things Volume G1: Reference architecture", Industrial Internet Consortium publication IIC:PUB:G1:V1.80:20170131, Version 1.8, 2017.