Configurable Role Based Concrete Architecture Layers: Constituting Business Process Aware Internet-of-Things Services' Reference Architecture

Vikas S. Shah(✉)

Wipro Technologies, Connected Enterprise Services, East Brunswick, NJ, USA
vikas.shah@wipro.com

Abstract. Internet-of-Things (IoT) services offer a great potential in many different enterprise application areas for improving efficiency gains to completely new business processes (BPs). However, due to diversified nature of the devices involved and uncertainty of business objectives associated when structuring BP aware IoT services, significant concerns of standardizations still have to be overcome. In this paper, we identified and integrated contexts of BPs to IoT services by means of role-centric view in order to define BP aware IoT services' reference architecture. Configurable role based approach and model enables a systematic credentials and reuse of standardized IoT services in layers, while allowing participants of IoT services' reference architecture to understand and imply possible variations. It is proposing a configurable role based concrete architecture layers incorporating topographies for capturing resources, data, and physical objects involved to IoT services. The methodology is validated with a case study of commercial surveillance camera and security alarm systems.

Keywords: Business processes (BPs) · Configurable · Integration · Internet-of-Things (IoT) · Reference architecture · Role based

1 Introduction

The next wave in the era of IoT services will be outside the realm of the traditional automation paradigms, many of the objects that surround us will be in adherence to BPs in one form or another. BP modeling specializes on describing how activities interact and relate with services rendered for IoT while supporting the operation of the business. The representation of an enterprise and its BPs have been the focus of research in past years and significant work has been done on developing BP modeling concepts, methodologies and ontologies [1–3]. Recently, various attempts and analysis have been performed to synergies between BPs and the specification of IoT service modeling [4, 5].

In order to integrate IoT resources into BPs, it is therefore necessary to establish principles and reference architecture for service-enable IoT resources, example, utility device's monitoring services that are accurately structured, composited, and mapped to interact with the billing and payment BPs. Using a service-based approach offers the additional advantage of hiding the heterogeneity of IoT device and associated

B. Mandler et al. (Eds.): IoT 360° 2015, Part II, LNICST 170, pp. 10–19, 2016.
DOI: 10.1007/978-3-319-47075-7_2

information model from the BP orchestration. However, it results in the generation of enormous amounts of concrete relationship between IoT services and BPs. The relationship information have to be stored, processed, and presented in a seamless, efficient, and easily interpretable form. This model will consist of set of IoT services that are commodities and delivered in a standardized manner.

Inherently, it needs to be based on actual events that are either detected directly or by anticipated real-time behavioral analysis of the IoT services. Such events can occur at any time in the correlations of the BP activities [4]. Modelling such events into an IoT service is cumbersome, as they would have to be included into all possible BP activities. It leads to an additional complexity and making it more difficult to understand the modelled BP. Secondly, how to react on a single event can depend on the context of BP. A simple critical example is the smoke detecting device that recognizes a sharp rise in temperature then the nearest rescue team needs to be notified.

Modeling BP involves capturing the structure of enterprise's business objects and their relationships to correctly enumerate corresponding activities associated with the business object [2, 6]. A business object exhibits different role according to the relationships that it has at a given time. Currently, due to the uncertainty in the behavior of such business object, integrating IoT services into BPs requires a lot of engineering, deployment, configuration within middleware, and enablement of custom development. Every new IoT resource and installation requires significant effort. A major shortcoming of existing approaches to configurable BP modeling in the context of IoT services is the lack of mechanisms for standardizing and capturing categories of variability beyond the control flow perspective of business objects.

In this paper, we proposed configurable role based concrete architecture layers to streamline and classify IoT services and associated compositions. The key contribution is to place reference architecture for IoT services in the context of enterprise-grade BPs to support a range of variations in the way roles and business objects are associated to BP activities. It provides a framework and a platform to introduce and configure role models that can relate IoT services in association with the activities of BPs. Section 2 represents our analysis to indicate the significance of roles in BP aware IoT services. Section 3 describes the potential variability requirements of IoT services and desired configurability paradigms. Section 4 presents our approach to structure role based layered architecture to constitute BP aware IoT reference architecture, whereas, Sect. 5 provides a real case study performed and our observations. Section 6 concludes our findings and discusses future evolvement.

2 Implications of Roles in BP Aware IoT Services

Role-based modeling allows roles to focus on BP activities and their own parts of work. The role models are required to negotiate with each other in order to associate with the IoT services. Due to the collaborative nature of role-based modeling, negotiations among roles have a crucial impact on the overall BP. Typically, roles differs from each other based on the differences in their behavioral characteristics of responsibilities as well as method of negotiation. We have analyzed significance of roles and their categories in BP aware IoT services.

The concept of role is used in various different methodologies. As indicated in [3, 6], Kristiansen has proposed to set role properties, which are commonly regarded as a conceptual basis for defining roles. In BP modeling, there are also approaches based on role modeling such as Role Interaction Networks (RIN) and Role Activity Diagrams (RAD). Here, roles are considered as sets of ordered interactions. Role activities describe the interaction between pairs of roles, from a driving to a target role. However, these approaches do not fully depict context of IoT services and describe relationships or separate other concerns of IoT services.

IoT service delegation is often defined as a mechanism of all or a subset of roles to one or more other business objects including the physical devices that participate in BP activities [7–9]. No business object can delegate the defined role. However, in many cases, a business object may want to delegate some missions from specified role. In most cases, when IoT services are involved, IoT service to role delegation is needed. For example, if the satellite transmission of dedicated radio frequency is distressed due to signal to noise ratio, it must delegate to other radio frequency based on the defined role rather than based on business object (satellite). For instance, IoT services "evaluating the conditions of the quality of transmission" and "preparing the diversification to receive and/or transmit the information stream" can be delegated to the channels associated with the other radio frequencies pertaining to the role.

The analysis also indicates that the rules must be defined and configured [10], as there are constraints required to be imposed on the roles to IoT services delegation associated with the BP activity. In the presented scenario, not all dedicated radio frequencies can be utilized for the particular purpose in context or information stream that needs to be transmitted.

IoT service to role delegation allows precisely specifying and emulating anticipated physical behavior in the context of the BP activity. A role defines a set of extrinsic properties and behavior necessary to realize its participating IoT services. Roles can be

Table 1. Primary categories of role models for IoT services.

Type of role model	Example context of IoT service	Areas of implication
Representative	Specifying serial number and version of IoT device	IoT service binding and presentation
Observatory	Logical tracing of the physical IoT resource	IoT service's service level agreement (SLA) association and monitoring
Associative	Update states of multiple IoT devices to perform an activity	Multifaceted characterization of IoT services operations
Collaborative	Integrating platform or system feature capabilities to IoT service	Cross-functionality of IoT service operations
Operative	Defining actions and alternatives in the course of state change of IoT device	IoT service operations' action associated with BP activities
Executive	Decision to terminate or instantiate IoT service session	IoT service execution and transition
Enumerative	Listing states of IoT device to the IoT service variable	IoT service parameters and validation

constrained in the context of IoT services. A constraint asserts conditions between the roles and IoT services that can be expressed informally or formally. Binding the roles with the IoT services depicts the classification and association in the context of specific BP activity or set of BP activities. We have identified 7 different primary categories of role models that can be utilized for IoT services. Table 1 provides the type of role models identified, example context of IoT service, and their areas of implication.

A configurable IoT service to role model is needed to provide multiple forms of delegations and to enable flexible role model association with IoT service. We defined configurability paradigms as a mechanism that allows an IoT service to participate in various BP activities with different objectives.

3 Variability of IoT Services and Configurability Paradigms

In principle, the variability of the IoT services can be depicted independently of the BPs by means of a set of IoT resource facts that form the space of IoT resource's logical states. IoT resource fact is a set of variables and their responsibilities representing a feature of the IoT service operations, example, performing a video recording of the installed surveillance camera to particular zone of construction site. The surveillance camera can be physically enabled or disabled. The Boolean variable to enable surveillance camera and zone are the IoT resource facts in above example.

IoT service operations can group IoT resource facts according to their content and required actions. All facts of the same IoT resource can be set at once by identifying the corresponding logical states and their transitioning. Interdependencies between these states can specify a partial order in which the IoT service operations should be posed in association with any of the role model identified in Sect. 2 Table 1.

The configuration expression of role model associated with the IoT service can then be conditionally dependent on such IoT resource facts. For example, the *operative role model* associated with the IoT service in which the video recording is performed must be set to allowed when the corresponding fact of installed surveillance camera is set to enabled, while it must be blocked or hidden when the fact is set to disabled. Such a configuration expression might also be dependent on a combination of multiple IoT resource facts. The facts can be combined in propositional logic within the configuration expression of role model that captures their interplay. It is then possible to ensure that a single instance of role model will never have two configuration values at the same time (example: blocked and hidden).

Additional constraints when associating instance of role model with IoT service can be specified in the configuration expression in the form of either through specifying maximum value, minimum value, or range of values to the facts. In the example of satellite radio frequency transmission in Sect. 2, type of information stream that is required to transmit can be constrained for specified range of satellite radio frequency.

During the modeling of roles for IoT services, we adapted and implied four distinct methods to identify configurability paradigms, each having its own application areas as detailed in [5]. Following is the list of methods and their overview.

- Design: The type of configurability paradigms is for handling anticipated changes in the IoT services, where supporting operations can be defined at design-time in considerations of the IoT resource facts.
- Deviation: It is for handling the occasional unforeseen behavior of IoT service operations, where differences with the expected behavior are minimal.
- Under-specification: It is for handling anticipated changes in the IoT service operations, where IoT resource facts cannot be defined at design-time due to the final state is not known in advance or is not generally applicable.
- Change: It is either for handling occasional unforeseen behavior, where differences require BP adaptations, or for handling permanent unforeseen behavior.

Each method provides insight of the correlations between the associated role model and IoT service. The role model specification and corresponding configuration expression participates to construct BP aware IoT services in the form of IoT services' metadata. They also ensure the anticipated completeness of IoT service for the BP activity in consideration. Based on the above methods, we distinguished 5 types of configuration expressions that can be leveraged to the role models identified in Sect. 2 Table 1 and corresponding IoT resource facts. Table 2 presents the types of configuration expressions of role models, the respective type of role models on which they can imply to, and example context of IoT resource facts.

Table 2. Types of configuration expression of role model associated with IoT service.

Configuration expression type	Role model type(s)	Example context of IoT resource facts
Reactive	Executive and operative	Setting lower and upper limits for voltage control
Proactive	Observatory, associative, collaborative, and enumerative	Configure specific system alert type for particular state of machine
Conjugative	All	Setting voltage control limit for particular state of the machine
Predictive	Observatory and enumerative	Setting valid states of machine for the specified timeframe
Conductive	Executive, operative, and associative	Allocate action type of "switch-off" for the particular state of machine

4 Deriving Role-Based Architecture Layers: BP Aware IoT Services

IoT services' reference architecture provides a generic solution that needs to be individualized to fit a specific set of BPs. An IoT service is anticipated to integrate multiple elements that are distributed across several enterprises and communicate with each other, at least partially, by using underline protocols and standards. Furthermore, the IoT services to be operated and maintained throughout the whole lifecycle of the enterprise and corresponding BPs. If BP activities are facilitated by an enterprise, the efforts expected from the IoT service providers can be streamlined and derived, thereby

enabling the entry of new requirements and new enterprise elements to the emerging ecosystem effectively through the established reference architecture.

For this reason, the reference architecture shall provide support throughout all the lifecycle phases of the IoT services. These phases can be derived in the perception of delegations of role models and IoT services. It must enable IoT services to support associating the configuration expression of role model necessary to meet the completeness of IoT services in the context of BP activities. In the reference architecture, the difference is made between the processes dealing with the design, development, and deployment of the IoT services (that is, strategy, system, information, infrastructure, and product related events associated with the IoT resources and their facts) and their core operations, which include the anticipated groups of fulfillment and assurance of BP activities. Following principles of service oriented architecture [11–13], we defined discrete IoT services' reference architecture layers by means of specifying delegations of role model and IoT service.

Figure 1 provides the layers of reference architecture and corresponding responsibilities. Each layer reveals and factorizes correlations between role model and IoT service to depict the concrete architecture for a specific set of BP activities.

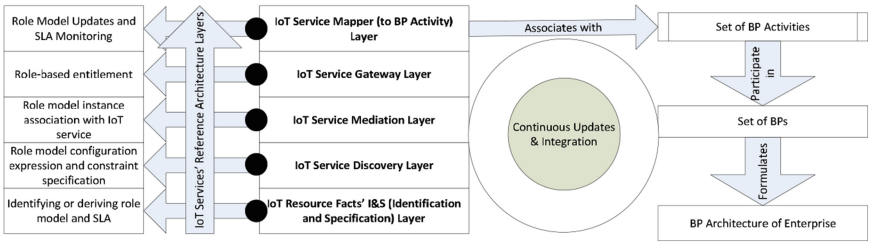

Fig. 1. Layers of BP aware IoT services' reference architecture

IoT Resource Facts' I&S (Identification and Specification) Layer: It is the foremost and initial layer to recognize IoT resource facts including paradigms of physical objects involved. The example facts that can be captured are installation zone, version, and status of security alarm device. The layer is also responsible to either identifying or deriving (if already exists) role model and SLA (service level agreement) specification in association with the IoT resources' facts. In the specific example, observatory role model can be recognized with the zone to monitor any deviation in status of security alarm device.

IoT Service Discovery Layer: Discovery layer is to define and model granularity of the IoT service. It includes modeling service output, service type, service level metadata, and the geographic area for which the service is provided. The representation of the service specification will also be linked to the service description during the modeling. Role model configuration expression and constraint specification in adherence to identified facts are the responsibilities of this layer. For instance, IoT service model to manage security alarm device requires to express and designate security alarm observatory role derived from observatory role model with the firmly defined status values (example: it can either be away, stay, bypass, not ready, ready, alarm, and check, however, can't be anything else than the specified values).

IoT Service Mediation Layer: Actual composition of the IoT services and definition of the corresponding operation are the primary responsibilities of the layer. IoT services can be invoked either in a synchronous way by responding to service requests or in an asynchronous way by sending notifications according to subscriptions previously made through the service. Service registry is being utilized to register resource history and metadata associated with IoT service operations. Role model instance association with IoT service model and specification are also integral part of service mediation layer. It actually provides reusability across multiple BP activities by differentiating IoT services in presence of type of role model associated with it. The IoT service to manage security alarm device can be associated with observatory role model as well as operative role model, however, the purpose of the IoT service changes and respective model, instance, and utilization differs (as indicated in the case study of Sect. 5).

IoT Service Gateway Layer: IoT service gateway responsible, at the very minimum, for enabling the secure connectivity between the short range IoT resources, sensing and actuating devices, and other services of the enterprise and/or BPs. It may also implement security-related functions as well as perform run-time discovery and validity of the devices and their services. Role-based entitlement and enforcing security policies are also the accountabilities of this layer. The policies for security alarm observatory role can be defined and checked to ensure that the right level of access to the manage security alarm device IoT service is available including any security protocol (such as token based authentication) needs to be utilized.

IoT Service Mapper (to BP Activity) Layer: IoT service mapping to BP activities that complements the capabilities of BP aware IoT service. It establishes common understanding between the IoT services utilization with respective to the identified and placed BPs. Continuous update to the role model and their desired variations based on BP activity and SLA monitoring are the critical aspect of the functionalities of this layer. The manage security alarm device IoT service with associated security alarm observatory role can be utilized within the BP activity of inventory check pertaining to billing and payment BP.

5 Case Study and Observations: Security Alarm System and Surveillance Camera

For the initial proof-of-concept, we considered first level primary BPs for the enterprise offering commercial security alarm system and surveillance camera to their customers. Following are the four initial BPs modeled for various desired activities to manage integrated security products along with accessible commercial monitoring services option. For each of the four selected BPs, we then identified all the differences among the associated requirements and activities variants. Based on this information, we created a single multifaceted BP model for each BP that incorporates all the BP activities and respective ordinary runtime choices using IBM WebSphere Process Server's process modeling capabilities [2]. Following are the four BPs.

- **Prospect and Quote to Order**: It is a BP to approach the prospect and generate the quotation based on the required integrated security products by the customers. It also validates the legitimacy of customer, product, and location.
- **Installation and Activation**: This BP is to procure material, establish physical equipment and agent support, initial system level updates and setup, customer approval, and closing of an order.
- **Provisioning and Monitoring**: It is the subsequent BP to installation and activation to offer monitoring and surveillance of activities based on installed products. However, it is independent of installation and activation process as customer has option to subscribe or degrade levels of provisioning.
- **Billing and Payment**: The BP is to introduce automation to trigger invoicing and online payment based on the utilization of the installed and activated products as well as subscribed provisioning levels. It also addressed non-payment through termination of provisioning and initiating collections.

The IoT solution architecture is derived from the presented reference architecture and the role model variants for acknowledging the utilization of IoT services in daily practice. We modeled IoT resources facts of all versions of the surveillance camera and security alarm products that are either deployed or under deployment to the customers. Each layer of the reference architecture is disseminated, for example, IoT Resource Facts' I&S layer considers the properties of security alarms such as zone that observatory role has to monitor for billing and payment BP.

We have logically categorized and build the information model that carries 146 IoT resources facts. Eventually, the analysis to model IoT services has been performed and 17 IoT services are being deployed in the production environment using IBM integration bus features [12]. As part of a BP definition, a process designer defines BP activities that describe the high-level interfaces and business objects to an IoT service in association with configured role model.

The total number of mapped (to the identified BP activities) differentiated IoT services with the variant role model association is 64. It indicates the factor of reuse is significantly higher (1:4 and 276 %) than legacy methodologies and existing approaches. Table 3 provides an example of differentiated IoT service for managing security alarm device in the context of diversified BP activities of different BPs.

Table 3. Differentiated IoT services example for *managing security alarm device* and its utilization.

Reference architecture paradigms	Provisioning and monitoring BP	Billing and Payment BP
Associated BP activity	Create alert	Create invoice
Number of IoT resource facts participated	7	4
Role model type	Operative	Observatory
Configuration expression type	Conductive	Predictive
IoT service operation responsibility	Identify provisioning level subscribed and compute the severity of alert	Identify provisioning level subscribed and compute the associated pricing

During the modeling as well as deployment of the IoT services, we have observed certain subjective advantages and challenges. Following list describes the primary findings when constituting BP aware IoT services utilizing configurable role-based architecture layers that BP architect can take into consideration.

- When modeling IoT service and their variants in terms of role association, we have to decide which information flow or control flow alternatives are subject to configuration and which ones shall be common across BP activities.
- When defining relevant constraints for a set of IoT resource facts within the configuration expression of role model, the architecture usually does not only refer to one type of constraint, however, to increase the correctness of the operations, different constraint types must be considered.
- To combine several options to configure a specific role model variant, the IoT services' solution architecture derived from reference architecture must decide how to group IoT resource facts to the operations. Thereby aspects such as maintainability as well as extendibility have to be considered. The resolution and judgement between coarse-grained versus fine-grained also must have to be implied when deriving as well as delegating IoT services with role models.
- If different facts pertaining to different IoT resources shall be applied conjointly to the IoT service due to semantical dependencies then architecture may explicitly define an implication constraint between them. Implication constraints are always directed to the configuration expression of the dedicated role model for the specific IoT service.

6 Conclusion and Future Work

This paper has presented the fundamental concepts towards generating BP aware IoT services' reference architecture framework by means of configurable role-based architecture layers. It relies on specifying role models and corresponding configuration expression in association with IoT services to consistently utilize them into the identified BP activities. Furthermore, the IoT services' reference architecture provides the principles to guide the definition of the IoT services. Essentially, it is an effort to streamline and standardize building and deploying IoT services with variations in the dilemma of enterprise-grade BPs.

The case study of integrated security products indicates the advantages and potential challenges that needs to be overcome during the deployment of the IoT services. The results are encouraging considering the consistency, reusability, maintainability, and variability being accomplished across the enterprise. The present effort is to formalize and imply constraint specification with the configuration expression pertaining to the identified categories of role model across enterprise. Subsequent research interest is to extend the dynamicity as well as many-to-many relationship between the role models and IoT services.

References

1. La Rosa, M., et al.: Configurable multi-perspective business process models. Inf. Syst. **36**(2), 313–340 (2011)
2. Pillai, U., et al.: Business Process Management Deployment Guide Using IBM Business Process Manager V8.5. IBM Redbooks, January 2014. ISBN 0738438944
3. Ertugrul, A.M., Demirors, O.: An exploratory study on role-based collaborative business process modeling approaches. In: Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, S-BPM ONE 2015, NY, USA, p. 14 (2015)
4. Haller, S., Magerkurth, C.: The real-time enterprise: IoT-enabled business processes. In: IETF IAB Workshop on Interconnecting Smart Objects, March 2011
5. Ferreira, P., Martinho, R., Domingos, D.: IoT-aware business processes for logistics: limitations of current approaches. In: INForum 2010 – II, pp. 611–622 (2010)
6. Caetano, A., et al.: A role-based framework for business process modeling. In: IEEE Proceedings of the 38th Hawaii International Conference on System Sciences, January 2005
7. Bauer, M., et al.: IoT reference architecture. In: Bassi, A., et al. (eds.) Enabling Things to Talk, pp. 165–210. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40403-0_8
8. Thoma, M., Meyer, S., Sperner, K., Meissner, S., Braun, T.: On IoT-services: survey, classification and enterprise integration. In: 2012 IEEE International Conference on Green Computing and Communications (GreenCom), pp. 257–260, November 2012
9. Guo, B., et al.: Opportunistic IoT: exploring the harmonious interaction between human and the Internet of Things. J. Netw. Comput. Appl. **36**(6), 1531–1539 (2013). doi:10.1016/j.jnca.2012.12.028
10. Elkhodr, M., Shahrestani, S., Cheung, H.: The Internet of Things: vision & challenges. In: IEEE 2013 TENCON Spring Conference, pp. 218–222, April 2013
11. Zhou, Z., et al.: CPS track report: 2nd track on cyber physical society with SOA, BPM and sensor networks. In: 2012 IEEE 21st International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 25–27, June 2012
12. Howes, A.J., Wong, G.: Integrating IBM Business Process Manager Standard with synchronous and asynchronous applications using IBM Integration Bus V9. IBM DeveloperWorks, July 2013
13. Espinha, T., Zaidman, A., Gross, H.-G.: Understanding the runtime topology of SOA systems. In: IEEE 19th Working Conference on Reverse Engineering (WCRE), pp. 87–196, October 2012