Shah, Vikas (2021) The Integrity of Digital Technologies in the Evolving Characteristics of Real-time Enterprise Architecture. [Doctor of Philosophy by public works]

with author's formatting

The Integrity of Digital Technologies in the Evolving Characteristics of Real-time Enterprise Architecture

A thesis submitted to Middlesex University in the partial fulfillment of the requirements for the degree of the Doctor of Philosophy by public works

Vikas Suvratkumar Shah
M00783434

Director of Studies: Professor Balbir Barn
Supervisor: Dr. Hector Menendez Benito

School of Science and Technology
Department of Computer Science
Middlesex University

May 2022

ABSTRACT

Advancements in interactive and responsive enterprises involve real-time access to the information and capabilities of emerging technologies. Digital technologies (DTs) are emerging technologies that provide end-to-end business processes (BPs), engage a diversified set of real-time enterprise (RTE) participants, and institutes interactive DT services. This thesis offers a selection of the author's work over the last decade that addresses the real-time access to changing characteristics of information and integration of DTs. They are critical for RTEs to run a competitive business and respond to a dynamic marketplace. The primary contributions of this work are listed below.

- Performed an intense investigation to illustrate the challenges of the RTE during the advancement of DTs and corresponding business operations.
- Constituted a practical approach to continuously evolve the RTEs and measure the impact of DTs by developing, instrumenting, and inferring the standardized RTE architecture and DTs.
- Established the RTE operational governance framework and instituted it to provide structure, oversight responsibilities, features, and interdependencies of business operations.
- Formulated the incremental risk (IR) modeling framework to identify and correlate the evolving risks of the RTEs during the deployment of DT services.
- DT service classifications scheme is derived based on BPs, BP activities, DT's paradigms, RTE processes, and RTE policies.
- Identified and assessed the evaluation paradigms of the RTEs to measure the progress of the RTE architecture based on the DT service classifications.

The starting point was the author's experience with evolving aspects of DTs that are disrupting industries and consequently impacting the sustainability of the RTE. The initial publications emphasized innovative characteristics of DTs and lack of standardization, indicating the impact and adaptation of DTs are questionable for the RTEs. The publications are focused on developing different elements of RTE architecture. Each published work concerns the creation of an RTE architecture framework fit to the purpose of business operations in association with the DT services and associated capabilities. The RTE operational governance framework and incremental risk methodology presented in subsequent publications ensure the continuous evolution of RTE in advancements of DTs. Eventually, each publication presents the evaluation paradigms based on the identified scheme of DT service classification to measure the success of RTE architecture or corresponding elements of the RTE architecture.

DECLARATIONS

This work has not previously been accepted in substance for any degree and is not concurrently submitted in candidature for any degree.

Signed: V. S. Shah (Vikas Suvratkumar Shah)

Date: November 22nd, 2021.

STATEMENT ONE

This thesis is the result of my investigations, except where otherwise stated. Sources are acknowledged by in-text citations or footnotes giving explicit references. A complete bibliography is appended.

Signed: V. S. Shah (Vikas Suvratkumar Shah)

Date: November 22nd, 2021.

STATEMENT TWO

This copy has been supplied because it is Copyright material, and no quotation from this thesis may be published without proper acknowledgment. If approved, I hereby give my consent for this thesis to be available for photocopying by the British Library and for inter-library loan. I am authorizing open access of this thesis to the Electronic Theses Online Service (EthoS) linked to the British Library and the title and abstract available to outside organizations.

Signed: V. S. Shah (Vikas Suvratkumar Shah)

Date: November 22nd, 2021.

DEDICATION

This work is solely dedicated to my beloved parents, *Suvrat M Shah and Nayan S Shah*, who motivated, encouraged, and supported me to pursue higher education at every growing-up stage. Both enabled the pathways to study since childhood and instilled in me the passion and dedication to learn new concepts and innovate.

The unconditional inspiration and desired level of facilitation received from my wife *Titul Shah, bother Nilay Shah,* and twin sons, *Aarav V Shah and Aarush V Shah*, cannot be overlooked during the persuasion and completion of this research work. I wholeheartedly thank all the family members who have supported me during the progression of this thesis work.

ACKNOWLEDGEMENTS

My journey to pursue the research work was intriguing, complicated, and with initial failures. During this journey, many people have inspired me and collaborated with me. Since the first publications appeared in ACM Winter International Symposium on Information and Communication Technologies 2004, many organizations have provided intense resources and financial funding. The organizations supporting the research include *Samsung India Software Operation, Symphony Technology Group, Wipro Technologies, Ernst and Young US LLP, and Knights of Columbus*. Without endorsements and experimental setup provided by these organizations, I would not have built an immense network of research contacts and collaborators worldwide as the top global chief architect 2020. Many thanks to the team members and customers who provided their valuable inputs during the 22+ publications and multiple accepted patents.

My primary supervisor and advisor, *Dr. Hector Menendez Benito*, provided much-needed guidelines, reviews, and pointers through his remarkable research achievements. His continuous involvement and direction, despite the various obstacles, are remarkable. The Director of Studies at Middlesex University, *Professor Balbir Barn*, has given me valuable scientific advice and encouragement and reviews to improve the thesis. Without his support and understanding, I would not have been able to structure, complete, and submit this thesis work. Many thanks for his account, especially at difficult times. Special thanks go to the two Universities, *Mumbai University, Mumbai, India, and Worcester Polytechnic Institute, Worcester, MA, USA*, for their support during the Bachelor of Engineering (Computer Engineering) and Master of Science (Computer Science). It provided insight into understanding the fundamentals of computer science and their applicability to the industry and businesses.

LIST OF SUBMITTED PUBLICATIONS

PW1: Multi-agent cognitive architecture-enabled IoT applications of mobile edge computing*,* Annals of telecommunications, Vol. 73, No. 7*,* August 2018. DOI: https://doi.org/10.1007/s12243-018-0648-1. Electronic ISSN: 1958-9395. Print ISSN: 0003-4347.

PW2: Emerging Data Services Viscosity to Enrich Pivotal Capabilities of Interactive Enterprises: Towards a Lean Integration Architecture Approach, International Journal of Knowledge Engineering, Vol.1, No. 3, December 2015. ISSN: 2382-6185. DOI: 10.18178/ijke.2015.1.3.034.

PW3: Managing Inductivity of Digital Business Operations: Pervasive Scenario-based Incremental Risk Governance Framework, International Proceedings of Economics Development and Research, Vol. 85, December 2015. ISSN: 2010-4626.

PW4: Emerging Paradigms of Managing Digital Business: In Association with Factoring Incremental Risks, 2017, Journal of Advanced Management Science Vol. 5, No. 1, January 2017. ISSN 2168-0787. DOI: 10.18178/joams.5.1.1-8.

PW5: An Integrated Framework to Quantify Strategic Diversifications in Real-time Enterprise: Industrializing Alliances of Big Data Architecture Patterns in Business Process Lifecycle, International Journal of Knowledge Engineering, Vol. 3, No. 1, June 2017. ISSN: 2382-6185. DOI: 10.18178/ijke.2017.3.1.081.

PW6: An Empirical Method to Derive Principles, Categories, and Evaluation Criteria of Differentiated Services in an Enterprise, Advances in Computer Science: An International Journal, Vol. 4, No. 4, August 2015. ISSN (Online): 2322-5157.

PW7: Deterministic Consumer Applications Enabled Policy Architecture of Mobile Edge Computing Ecosystem, 7th IEEE Annual Computing and Communication Workshop and Conference, January 2017. Electronic ISBN: 978-1-5090-4228-9. DOI: 10.1109/CCWC.2017.7868441.

PW8: Ubiquitous Operational Governance Framework: Managing Consumer Mobile Commerce Active Index, The 7th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, October 2016. Electronic ISBN: 978-1-5090-1496-5. DOI: 10.1109/UEMCON.2016.7777893.

PW9: Pragmatic Modeling of Pervasive Cloud Enabled Trading Architecture for Smart City Ecosystem, International Conference in Smart Cities (ICSC 2016), September 2016. Electronic ISBN: 978-1-5090-5579-1. DOI: 10.1109/ICEMIS.2016.7745325.

PW10: Fragmented Architecture of IoT Services to Edge Relationship between Dimensions of Electronic Commerce, 2016 IEEE International Conference on Internet-of-Things and Pervasive Systems (IOT), September 2016. Electronic ISBN: 978-1-5090-5579-1. DOI: 10.1109/ICEMIS.2016.7745324.

PW11: An Integrative Methodology to Enable Compliance-aware Data Services: Accelerating Consumer Regulatory Governance Paradigms of an Enterprise, The 13th Annual IEEE Consumer Communication and Networking Conference, January 2016. Electronic ISSN: 2331-9860. DOI: 10.1109/CCNC.2016.7444842.

PW12: Configurable Role Based Concrete Architecture Layers: Constituting Business Process-Aware Internet-of-Things Services' Reference Architecture, 2nd International Conference on IoT as a Service 2015, October 2015. Online ISBN DOI: https://doi.org/10.1007/978-3-319-47075-7_2.

PW13: Blockchain-driven 3 Domain Secure Version 2.0 Service Architecture, SERVICES 2020 World Congress on Services, August 2020.

PW14: Evolving Dynamics of Heterogeneous SaaS Applications and Business Process Automation in Real-time Enterprises, 29th International Conference on Management of Technology, September 2020.

PW15: Incremental Risk Chain Mapping Manager and Linker (iRCM2L): Blockchain Driven Dynamic Risk Chain Framework, 28th International Conference on Management of Technology, April 2019, pp. 184-194. e-ISBN: 978-93-88237-54-3.

PW16: System and Method of Performing Dynamic Orchestration of Rules in a Big Data Environment, US Patent 10,545,973, 2020, January 2020.

PW17: Method and System for Identifying Operating Modes of Communications in Mobile Edge Computing Environment, EU Patent ID: EP3282718A1, US Patent 10,104,672, 2018, October 2018.

PW18: Method and System for Regulating Request and Provision of Resources for Transactions in a Smart City, US Patent ID: US2018137591A1, 2018, May 2018.

PW19: Method and System for Classification of Heterogeneous Clouds, EU Patent ID: EP3361395A1, CN Patent ID: CN108536534A, US Patent ID: US2018234509A1, 2018, August 2018.

PW20: Methods for Provisioning an Industrial IoT Control Framework of Dynamic Multi-Cloud Events and Devices thereof, US Patent ID: 11169495, 2021, November 2021.

PW21: Method, System for Automatic Monitoring and Control of Compliance of Operations of Smart City Infrastructure in Real-Time, US Patent ID: US20170357563A1, 2017, December 2017.

GLOSSARY OF TERMS

Acronym	**Terminology**
API	Application Programming Interface
BC	Blockchain
BP	Business Process
CA	Consumer Applications
DS	Digital Technology Service
DBO	Digital Business Operation
DoC	Degree of Coverage
DoF	Degree of Fragmentation
DOPC	Degree of Process Classification
DT	Digital Technology
Ecommerce	Electronic Commerce
ePIG	Edge Policy Integrity Gradient
HC	Heterogeneous Cloud
IR	Incremental Risk
IRMF	Incremental Risk Management Framework
IoT	Internet of Things
KPI	Key Performance Indicator
Mcommerce	Mobile Commerce
MEC	Mobile Edge Computing
PEIR	Percentile of Incremental Risk
PPL	Policy provisioning lifecycle
RTE	Real-time Enterprise
ROGF	Real-time Enterprise Operational Governance Framework
SLA	Service Level Agreement
SOA	Service Oriented Architecture

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER 1.

INTRODUCTION

Today's enterprises require responding to the changing dynamics of the business and technology in real-time. The on-demand characteristics of an organization lead to the fundamental principle of constituting a real-time enterprise (RTE). Organizations are receptive to gaining numerous advantages by exposing operational capabilities, functionalities, real-time information, and computations capabilities through services, often in the RTE's application programming interfaces (APIs) [1]. Digital technologies (DTs) are electronic tools, platforms, systems, devices, and resources that generate, process, and store information and corresponding services. The advancements of DTs include Blockchain, internet-of-things (IoT), Big Data, heterogeneous clouds, electronic commerce, mobile edge computing (MEC), and cognitive computing. The advancements of the DTs and their employment in RTEs create more value for the brand in the marketplace [2] through automating the business processes (BPs) and proactively engaging customers. Each RTE differs in terms of DTs association with the diversified BPs of the different industry segments [3]. It necessitates an RTE to either derive or adapt a standardized architecture for continuously evolving BPs and associating functionalities at the pace of advancing DTs [4].

RTE capabilities are often affected by intangible and abstract goals of the customer, business operations, organizational processes, and employees. They are typically dependent on the actions of other parties. Application of the DTs in the presence of legacy systems and information services remains a daunting task and usually an erroneous process [5]. The evolution of RTEs due to the introduction of upcoming DTs is deficient in standardization. In some cases, they fail to provide generality in terms of implementation and diversification required for the participants of the RTE ecosystem.

Traditional approaches to standardizing RTE architecture typically focus on utilizing the core capabilities of a specific DT function [6] in the form of BPs. BPs are complex considering numerous dependencies, the unpredictability of the user scenarios, and necessary updates required due to changing dynamics of the businesses in real-time [7]. Another prime concern is the validity of the information in utilizing DT's capabilities by a specific RTE participant's roles in the BP and the diversity of temporal properties of DT capability within the RTE ecosystem [8]. For example, multipurpose health monitoring devices [9] delivered to different types of customers monitor health indicators based on the individual's current activity to generate the appropriate action for the health service providers. The monitoring criteria and actions differ for resting heart rate during the exercise over resting heart rate during the sleep.

Intense analysis and evaluation performed in [10], [11], [12], and [3] indicate that the essential RTE architecture elements provide a solid foundation for elaborated functionality built within the DTs as services. It enables a flexible RTE architecture and avoids large monolithic systems [13]. Monolithic systems typically have less synergy between and among various components of the overall enterprise. For instance, traditional finance applications are monolithic since users carry out a complete task end-to-end and are private data silos rather than parts of a more extensive system of applications that work together.

Diversified applications with different goals are also meshing [14"] as DTs get fabricated at the edge of RTE architecture and BPs. Pervasive paradigms of such applications increase the value offered by the information generated by the number of interconnections between users and the DTs [15]. The processed data gets transformed into insight knowledge [16]. It enables an extensive range of smart services and applications to cope with many of the challenges people and enterprises face in their everyday lives. Example of smart services includes smart grid [17], smart car [18], smart home [19], smart healthcare services [9], and smart manufacturing [20]. It is primarily due to advancements in DTs. DT extensively connects humans or things in any place and time [21] using the DT services [22].

The RTE ecosystem is always in continuous transition, and it encounters deployment and configuration challenges to incorporate and utilize DT services. RTE needs to keep pace with the advancements in DTs, changes to the BPs, and the performance requirements [23]. It prominently leads to several research questions, as indicated below.

- **Continuously evolving RTE architecture**: How are the DT services architected, deployed, and managed in continuously evolving DTs?
- **Define and derive the DT services**: What aspects should be considered during the definition and derivation of the DT services in the RTE architecture?
- **Real-time decisions capabilities**: How to represent the correlation with DTs, BPs, and decision capabilities in distributed intelligence within the RTE architecture?
- **DT service composition**: How to combine functionalities of RTE to generate coherent DT services?
- **Manual intervention to the BPs**: How to identify and operate the level of manual interventions necessary to perform the RTE functions associated with the BPs?

- **Deploying and changing DT services in real-time**: What characteristics of the DT services must be performance-sensitive and adaptable at the edge due to the unpredictable volume of the RTE participants' activities?
- **End-to-End DT service provisioning**: Whether the RTE architecture provides visibility for delivering end-to-end DT service provisioning to the BPs?

Since there were many questions and no clear direction and standardized architecture framework, RTEs adapted DTs either in silos or scattered approaches [24]. The standardization is either partially defined or undefined to adapt DTs. RTE is bound to introduce and streamline custom RTE architecture and corresponding BPs. Online mobile payment is an example of BP. It involves various activities, including receiving customer information, mobile device authentication, payment card verification, accepting payment, approving the transaction, and sending payment receipt. The RTE architecture and corresponding BPs were placed in the logical categories of layers, components, objects, services, or agents [25].

There are 21 publications included in this research that breakdowns the complexities and dynamics of RTE architecture to associate and utilize the capabilities of DTs. The primary emphasis is to address the above research questions and streamline the evolution of the RTEs in the advancements of DTs. The novelty is to streamline the RTE architecture to associate DT capabilities in configurable services across multiple BPs. These DT services differ in their association with the BPs of the RTE architecture framework. Figure 1 articulates the organization of the context statement. Chapter 2 provides an overarching approach to deriving the RTE architecture framework. It introduces the notion of digital business operation (DBO) to standardize the association of DT services with BPs. Chapter 3 presents the structural runtime elements of the DBOs.

Overlapping criteria of the RTE architecture were prominent during the research. The overarching RTE operational governance framework governs the DT services during either introduction or advancement of the DT services. Chapter 4 represents the RTE operational governance framework and the steps necessary to ensure the appropriate introduction, associations, and updates of DT services to the RTE architecture framework. The uncertainties of the BPs were recognized during the development and employment of the RTE operational governance framework due to the challenges in DT service adaptation or integration. These uncertainties turned into risks for the DBOs. The incremental risk (IR) identifies the number of uncertainties added to or degraded from a risk associated with managing RTE architecture by either incorporating new or updated DBOs. The Incremental risk modeling framework was developed and presented in Chapter 5 to correlate incremental risks to DBOs in the business scenarios.

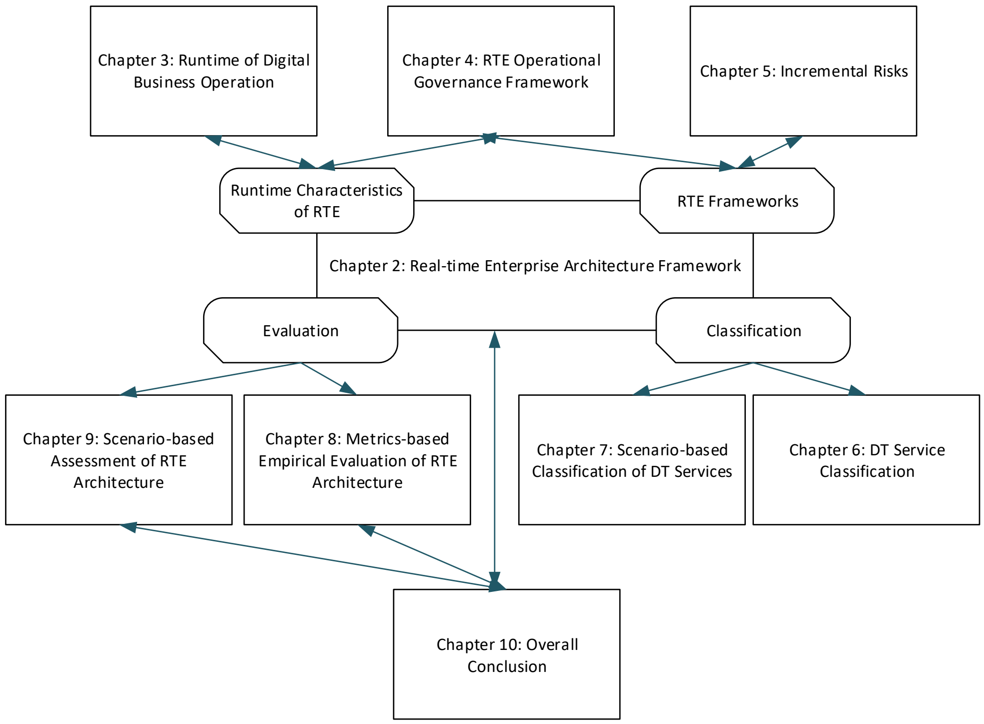


Figure 1: Organization of the context statement

Based on empirical analysis and investigation of various RTE initiatives across these publications, the architecture and governance frameworks were derived to address the diversity of DTs in the form of DT service classifications. Chapter 6 illustrates the steps and paradigms to perform DT service classifications. However, Chapter 7 presents business scenario-based DT service classifications.

Due to the industry benchmark data unavailability, the RTE architecture evaluation needed to be relative to the specific production deployment of the DTs for the specific industry sector. The metrics must compare in the production deployment iterations of the evolving capabilities of RTE architecture in association with the DTs. To the thrust behind the concepts in this research, the following are the industry sectors selected to derive the examples and evaluation criteria.

- Online purchasing experience of the consumers utilizing electronic commerce platform.
- Mobile eCommerce platform, online payment, and payment processing platform.

- Healthcare monitoring systems and accessories.
- Smart healthcare integration with other smart technologies, including smart cars and smart homes in the smart city.
- Smart city trading ecosystem and financial management platform in the cloud.
- Smart manufacturing system utilizing industrial IoT capabilities.
- Smart grid and metering system for the retail energy sector.
- Consumer packaged goods and food supply-chain ecosystem.
- A connected ecosystem of insurance technology.

Each evaluation method in Chapter 8 and Chapter 9 represents improvement areas and precision to structure (or restructure) the RTE architecture, RTE operational governance framework, incremental risks, and DT service classification in the inference of DBOs. Eventually, it formulates standardized and sustainable RTE in the presence of uncertainties of DTs, as concluded in Chapter 10.

During this research and deriving the evaluation of the RTE architecture, the primary concern for the RTEs was the fear of adapting to partially developed and complex DTs. The following represents the novelties and primary contributions to rationalizing the evolving RTEs in the volatility of adapting and introducing DTs.

1.1 Real-time enterprise architecture

The significant research contribution is to constitute the RTE architecture framework and its components. The RTE architecture includes a diversified set of DTs and its integrity with the already existing RTE ecosystem and BPs. The primary role of the RTE architecture framework is to standardize the introduction of the DTs in correlation with RTE's BPs. During this research and the standardized RTE architecture framework, it was evident that a unified RTE architecture framework may not fit all the types of industry segments in correlations to different DTs. Instead, generic RTE architecture framework components were introduced, tuned, or customized for a specific type of industry segment in the context of a particular DT. For instance, the published work PW10 derives the RTE architecture framework for IoT for the eCommerce industry. PW9 customizes the RTE architecture framework to introduce cloud-enabled trading for the smart city ecosystem.

RTE can dynamically associate specific functionalities and business operations for upcoming DTs. The example includes delivering and accepting mobile-enabled discount coupons or online reservations at restaurants. Each component of the RTE architecture framework is responsible for performing and ensuring automation or self-service aspect of the business. The following are the individual contribution and solely developed architecture frameworks over the past seven years.

- The published work PW1 uses the RTE architecture to deliver cognitive DT services in mobile edge computing with heterogeneous cloud technologies.
- The published work PW7 presents the policy architecture for mobile edge computing consumer applications to standardize the policies across RTEs through the consumer application's transport layer.
- The published work PW10 derives the fragmented architecture of IoT DT services from standardizing the relationship between DT and eCommerce applications.
- The published work PW12 enables role-based management and automation of IoT DT services in the RTE architecture.
- The published work PW13 establishes Blockchain-driven three domains secure 2.x service fabric architecture framework for online payment.
- The published work PW9 constitutes the mechanism for pragmatic modeling of pervasive cloud-enabled trading architecture for the RTEs of the smart city ecosystem.
- The ***published work PW16 illustrates the <u>patented</u> method*** to dynamically orchestrate business rules for the RTE architecture that leverages Big Data technology.
- The ***<u>patented</u> published work PW20*** provisions framework to dynamically capture runtime events and device-level activities of the multiple clouds associated with RTEs to identify necessary controls and policies for the industrial IoT in a manufacturing industry segment.

The following are the overarching outcomes of employing the standardized RTE architecture frameworks to streamline the introduction and updates of DTs in the context of BPs.

- The RTE participants, including employees, vendors, suppliers, and partners, can utilize DTs to improve how they serve their customers, collaborate, and operate.
- The level of visibility to perform a trade-off between cost, quality, and operational agility to attend to changing characteristics of DBOs and the corresponding composition of DT services or feature capabilities.

- Incremental risk association and evaluation metrics of digital forces [26] include globalization, consumer melaninization, prosumerization, business virtualization, and digital platform.
- Effectively manage RTEs in the presence of DTs advancements or disruptive technologies in the marketplace to benefit the consumerization and remain competitive by continuously evaluating the effectiveness and utilization of DTs.
- Precisely identify and place policies, controls, and rules in adherence to the evolving nature of the regulatory requirements and compliance with the DTs.

1.2 The runtime of digital business operations

The digital business operations (DBOs) [27] introduce structuring of the business operations using the capabilities of DTs to the RTE architecture framework. The runtime model of DBO is responsible for ensuring the strength of the binding between the DT functional and operational capabilities in the form of DT services to the BPs or BP activities. The following are the practical level contribution to introducing the structure of the DBOs across RTEs.

- The published work PW3 provides contexts to the DBOs for the enterprise data entities in correlation to the BP activities, ensuring the objectives of the RTEs to provision end-to-end BPs.
- The published work PW14 describes the implementation of the business operations manager to construct the responsive RTE architecture for the runtime digital activities associated with the BPs.
- The published work PW15 institutes a digital risk model to correlate the DT services and BPs in the form of incremental risks.

Essentially, the published work PW3 provides an approach to derive DBOs associated with the incremental risks associated with the DTs. The overlapping structural constitution of business operations prescribed in PW3 and the digital risk model described in PW15 provide the implementation of the DBOs. The implementation of DBOs focuses on placing the structural integrity to evaluate the runtime characteristics of DTs.

1.3 Real-time enterprise operational governance framework

RTE operational governance framework systematizes the properties of RTE architecture. The RTE operational governance framework vindicates the delivery and management of DBOs. It establishes the activity map of DBOs to evolve, dimensionalize, control, monitor, and dynamically deliver with the desired level of alternations necessary for the RTEs. The RTE governance framework was developed and applied to the existing or updated DBOs.

- The published work PW4 derives an approach for factoring incremental risks to identify the right level of controls that constrain DBOs.
- The published work PW8 establishes the ubiquitous operational governance framework to manage mobile commerce-based RTE architecture.
- The published work PW6 introduces an empirical method to derive principles, categories, and continuous evaluation criteria for the RTE architecture to govern the differentiated DT services.
- The published work PW18 standardizes regulating the request and provisioning of resources for the transactions performed across multiple participant RTEs in the smart city ecosystem.

1.4 Incremental risks

The procedural approach to determine the incremental risk for the DT services ascertains the early detection of and continuously evaluation of the risks of utilizing the capabilities of DTs. The factors in assessing the incremental risks can differ depending on the DT type, business objectives, corporate priorities, and RTE participants involved in many transactions. The primary contribution is to develop methods to model and govern the incremental risks associated with DBOs.

- The published work PW4 formulates an incremental risk modeling framework to model incremental risks accurately and continuously monitor and update them based on the advancements of DBOs.
- The published work PW3 fabricates the incremental risk governance framework to continuously assess and mitigate risks of DBOs in diversified business scenarios of the various industry sectors.
- The published work PW15 endows an incremental risk chain mapping manager and linker for the DBOs of the RTE architecture through the conceptual use of Blockchain. The framework formulates the mechanisms to associate risks to the DBOs dynamically. The published work PW15 conducts the preliminary functional implementation [28] using the supply-chain operations aspect of the consumer-packaged goods industry to validate the concept.
- The published work PW13 presents risk factor association manager to the RTE architecture developed using Blockchain for three-domain secure 2.x in digital payment services.

1.5 The digital technology service classifications

Since each RTE has a different approach or paradigm to viewing and evolving DT services, it was essential to identify the classification mechanism for DT services. These classification paradigms iteratively update existing or add new DT services.

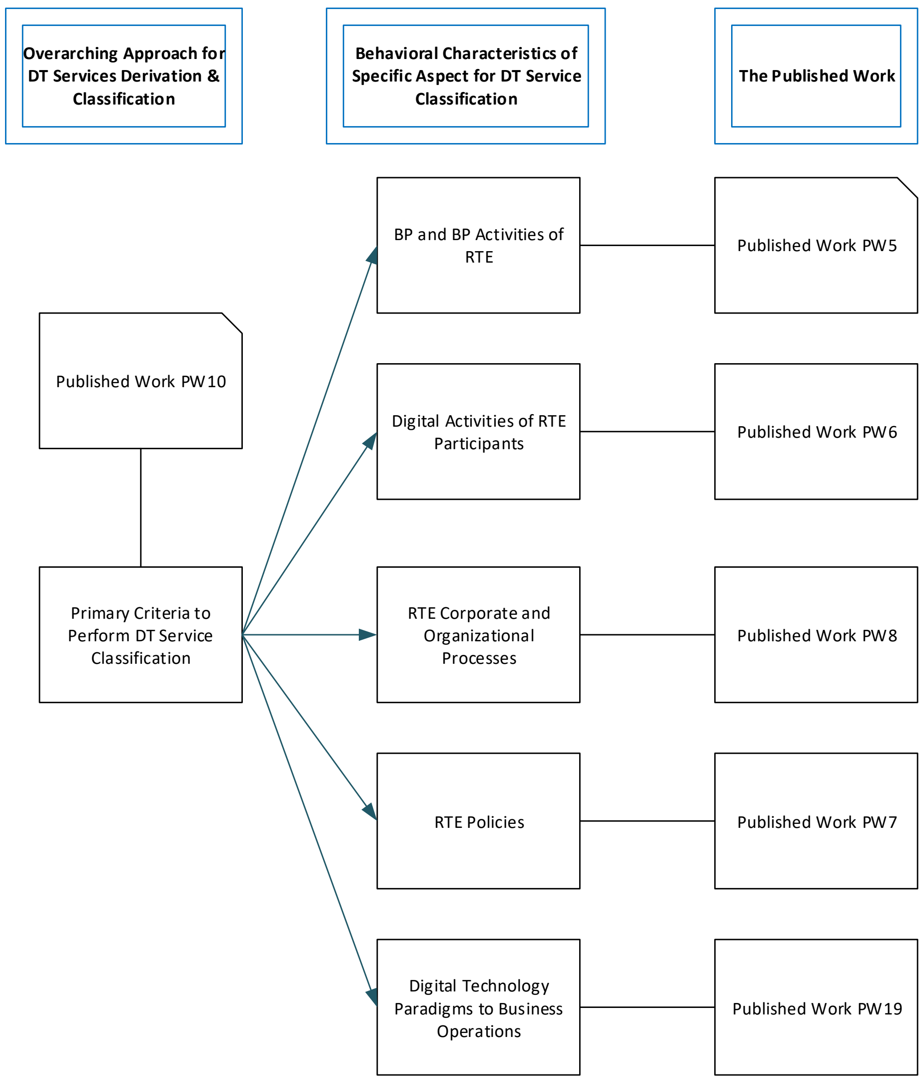


Figure 2: The published works for the classification of DT services

The step-by-step process of deriving a DT service classification scheme stipulates the DT capabilities for the distinct purpose of the RTE's DBOs. The DT service classification localizes the foundation for learning the impact of introducing or advancing the variety of DTs and their integrity with RTE architecture framework components and participants. As illustrated in Figure 2, distinguishing behavioral characteristics of BPs of RTE, digital activities by the different participants of the RTE, DTs paradigms, RTE processes, and RTE policies utilized to perform the DT service classifications.

The primary contribution is to recognize the most influential paradigms to categorize the DT services classification and derive the most accurate DT service classification in the RTE architecture framework and RTE operational governance framework.

- The published work PW10 emphasizes that diversification and customization necessary for the DT services stems from the advancements in DTs and their impact on the business operations to derive the DT service classification. It formalizes the steps to identify the paradigms and process of classification for DT services.
- The published work PW5 derives the scheme of DT service classification depending on the implications of associated BPs that utilize the DT services. It introduces the category based on the operational characteristics of the BPs in the attainment of DT services.
- The published work PW6 devises DT service classification to characterize the response to an event associated with the digital activities performed by the RTE participants.
- The published work PW8 enacts the DT service classification from the diversified RTE processes of either management of groups, departments, lines of businesses, internal or external RTE entities, customers, and RTE's qualitative or quantitively measures of services and products.
- The published work PW7 determines the DT service classification placed to attend to the policies and business rules. Typically, regulatory requirements, compliance, corporate strategy, and prioritization schemes elicit the policies.
- The published work PW19 prescribes a method to classify a heterogeneous cloud based on the DT services utilization by the RTEs over the enveloping of applications under the specific cloud environment.

1.6 Scenario-based classification of digital technology services

Scenario-based classification of DT services enables RTEs to recognize the variety of business scenarios that can receive the practical value of transforming the business operations with DTs. The scenarios connect the DTs' capabilities to arbitrate the incremental risks with the business operation in the context of the business situation and the upcoming regulatory requirements. The following are the key elements contributing to introducing scenario-based classification of DT services.

- The published work PW3 constitutes scenario classification for the incremental risks of the DBOs that participate in the specific business scenario.
- The published work PW1 classifies functional scenarios representing the characteristics of the DT service capability utilized under the scenarios.
- The published work PW11 focuses on compliance-aware DT services instantiating a set of rules associated with RTE's DBOs' scenarios. The rule characteristics associated with DT services determine the classification of the scenarios.

1.7 Empirical evaluation of the real-time enterprise architecture

Empirical evaluation of the RTE architecture recognizes the effectiveness of the DTs to the DBOs to continuously evolve along the side of RTE paradigms utilized to classify the digital business services. The BP, BP activities, RTE participant's digital activities, DT paradigms, RTE processes, incremental risks, DT capabilities utilization, and compliance are the predominant RTE paradigms diagnosed and exploited.

The evaluation mechanisms are created solely by the primary researcher of this context statement as an individual contributor. However, the development, testing, and business analysts were involved to either deploy or update the DT services under the supervision and guideline of the primary researcher of this context statement as a Chief Architect. During the production deployment, iterations for the evaluation, agile development methodologies [29], qualitative assessments, and retrospective sessions were the primary responsibilities of the primary researcher of this context statement or Chief Architect.

- The published work PW4 defines the percentiles of incremental risks of DBOs. It assesses the increase or decrease in incremental risks of DBOs during the advancements of RTE using or implying DTs.
- The published work PW5 derives the degree of coverage by the DT services for the BPs.
- The published work PW2 introduces the viscosity of DT services by assessing the compactness of DT services for a set of BPs and BP activities.
- The published work PW10 computes the degree of fragmentation for the classification of the DT services under the fragmentation of RTE architecture components and their operational behavior during the introduction or updates of DTs.
- The published work PW6 measures the maintainability index of the DT services in the diversification of digital activities performed by the various RTE participants.

- PW8 grades the degree of process classification to assess the RTE operational governance framework corresponding to the correlation between the classification of RTE processes and advancements in DBOs.
- The published work PW7 equates the edge policy integrity gradient assessing the ability of DT services (or APIs) under the specific type to attend to the policies during the introduction or update of DTs.
- The published work PW3 introduces the inductivity of the scenarios to measure the changes performed to mitigate the incremental risks while introducing and updating the DT services. The inductivity measures changes performed to the RTEs for mitigating the incremental risks during the introduction or update of the DT services.
- The published work PW1 evaluates average standard deviations in throughput based on the utilization of DT services' capabilities at runtime.
- The published work PW11 degree of divergence in DT services and compliance-aware DT services governance index to attend to the regulatory requirements and compliances in the diversified business scenarios.

As DT providers are growing, it is vital to overcome this situation by either standardizing the RTE architecture to associate DTs with the existing BPs or additional BPs. RTE should have the means to manage the evolving characteristics between DT functionalities or capabilities in the form of DT services and actual business operations. The RTE architecture framework provides the vehicle to streamline, manage, and advance these associations in Chapter 3.

CHAPTER 2.

REAL-TIME ENTERPRISE ARCHITECTURE

Memoona Javeria Anwar et al. [30] addressed the complexities of real-time enterprise architecture in evolving characteristics of DTs. The architecture of the RTE needs to be adaptable to advancements in DT in association with the BPs in pace with RTE's business operations. This review indicates that every modeling methodology is different in scope and coverage and demands the integration and specific modeling approach to support digital ecosystems.

Several generic standards and model frameworks are available and widely utilized by the RTEs to articulate the different aspects of RTE architecture and BPs. The enterprise architecture standards and modeling frameworks include ArchiMate [31], Zachman [32], federal enterprise architecture (FEA) [33], and the open group architecture framework (TOGAF) [34]. However, these frameworks are abstract and unable to provide the granular aspects of architecture modeling required for the RTE to evolve in the integrity of DTs. For example, the Zachman framework [35] views enterprise architecture as a logical framework for classifying and organizing descriptive representations to develop the specific RTE capability. It conceptualizes the representation of information over recognizing the effect of DTs on the RTEs' BPs.

A precise, lightweight framework for enterprise architecture (LEAP) [36] defines enterprise architecture with standard notations. The LEAP focuses on delivering accurate inter-layer relationships for the RTEs over dynamic changeability necessary to integrate actual functionalities of DTs. It allows precisely defining architecture aspects using standard modeling notations and a wide range of EA analysis techniques, including simulation, compliance, and consistency checking [37]. The RTE participants' activities performed utilizing the capabilities of DTs are not disclosed under the ontological approaches presented in the generic architecture standards and frameworks, starting from the top level, where a compiled list of activities does not have the reference to time in the RTEs.

According to Mikhael Johannes et al. [38], architectural practices have evolved significantly by composing layers of DTs' knowledge into the architecture frameworks, methods, and approaches. The architectural practice incorporates DT to meet the current demand and pursue the vast possibilities ahead. The theoretical exploration of the architecture methods of DTs indicates that the existing architecture approaches and practices are either deficient or incomplete in consideration to accommodate evolving characteristics of DTs for the diversified nature of the RTE's BPs. Alfred Zimmermann et al. [39] investigate mechanisms for flexible adaptation and evolution of digital enterprise architectures in integrating DTs, including cloud computing and big data technology. The primary objective is to support flexibility and agile transformations for BPs and related RTE systems by adapting and evolving digital enterprise architectures.

The primary challenge is the standardization and rationalization of the architecture approaches across multiple industry segments in the advancements of diversified DTs. Furthermore, implementing DTs' capabilities imposes customization on the BPs to keep pace with the marketplace and facilitate various types of RTE participants. Eventually, it increases the complexities of the RTE and decreases the maintainability and adaptability of the DTs.

2.1 Investigation of existing RTE approaches

Based on the investigation presented in PW1 and PW10, industry researchers and practitioners have identified five different approaches to solve the relationship between DTs' capabilities and BPs to evolve RTE during the investigation. The following list represents the efforts to manage RTE under the influence of changing dynamics of DTs.

2.1.1 PW1 Investigations

- **Aspect-centric approach**: The aspect-centric approach focuses on developing architecture or transforming existing RTE based on a specific aspect of the integration between participants of the RTE ecosystem [40]. For example, one of the aspects is defining the architecture based on publishing and subscribing the data across the RTE ecosystem with a specific structure to achieve connectivity with the DTs and new data generated to perform the BP.

  Bai Wang et al. [41] developed the event-driven service-oriented architecture to support real-time, concurrency, and event-driven active services execution to compose DT services. The DT services provide actions based on the specific set of conditions associated with the event. Kashif Dara et al. [42] adapt the resource-oriented architecture approach. It recognizes the IoT services based on identified or established BPs for specific RTE. The core components provide the end-to-end integration of Internet of Things systems, focusing on internet-of-thins-aware BPs.

- **Control-centric approach**: The control-centric approach is to identify the rules and policies necessary to manage the integrity between the various technologies, systems, and participants. Typically, the triggering of the rules occurs due to specific events and conditions associated with them. Fadi Al-Turjman et al. [43] proposed a data-gathering framework for data collectors in smart cities to formulate city-wide policies and constraints. An example is the smart city infrastructure, where identification of resource scarcity remains at higher precedence, and policies need to be imposed based on the current utilization of available resources [44].

- **Translation layer-centric approach**: The translation layer maps and advances existing functionalities of the RTE against the DT capabilities to quickly perform the BPs or specific RTE operations instead of leveraging the actual capabilities of the DTs due to the time-to-market requirements and lack of confidence in the newly introduced DTs. The translation layer provision interpretation of allocated responsibilities for specific DTs in terms of already defined BPs [45]. For instance, the functionalities associated with the application need to be performed by the cloud provider platform during either native cloud capabilities or migrating applications to the cloud. An intermediate layer of integration achieves the objective. Pedro Castillejo et al. [46] introduced the integration layer as a bridge for guaranteeing interoperability between different environments and DT services across RTE. It provides the integration of several wearable devices of an enterprise.

2.1.2 PW10 Investigations

- **Digital object-centric approach**: Digital object-centric approach [47] emphasizes developing functionalities based on the characteristic of physical or virtual objects that participates in the RTE. In this approach, the RTE advances by introducing functionalities and their integrity with the other digital objects. The digital twin approach [48] integrates data, models, and other information of a physical asset generated along its life cycle that leverages business opportunities. It bridges the physical and the virtual world and is a simulation tool to understand and model asset performance, predict its behavior, and optimize the operations and services. Sheik Mohammad Mostakim Fattah et al. [49] introduced the notion of a web of objects. It targets the implementation aspects of DT to bring the assorted real-world objects with web applications. The most prominent example is the location service through the mobile agent for the global positioning system of an airline. It continuously emulates the airline's position and updates or integrates with the base station (or airport).

- **Quality-centric approach**: The quality-centric RTE architecture approach [50] accentuates the quality paradigms of either BPs or a set of BPs that collectively formulates the RTE operation. A C Prabhakar et al. [51] attempt to drive the instrument dimensions of electronic service quality through restructuring the dimensions of the RTE business and technology paradigms. The quality paradigms can include the quality of the DT service providing the specific capability to the user or customer. Response time of the particular online order placement can be considered one of the technology-specific quality measures. It can also include customer satisfaction as a commercial quality measure.

2.1.3 Summary: Limitations of Traditional Real-time Enterprise Approaches

All the RTE architecture approaches are at an early stage in identifying DTs' runtime impact and association. The RTE architecture approaches are identified and developed for either a specific use case or solving a specific problem of the RTE. Strikingly, they are not streamlined, standardized, and governed consistently across RTEs. Ultimately, it increases the complexities of maintaining BPs, RTE participants' services, and the accuracy of the information, configuration, or conditions without a centralized view of the RTE ecosystem. Based on the investigation of various existing RTE approaches, the following are the identified limitations of introducing or advancing DTs to the RTE ecosystem.

- The approaches did not consider the diversifications in business logic, interfaces, and data needs between the different participants of the RTE. It changes based on the type of roles during digital activities.
- The traditional architecture approaches lack capabilities to address the impact of customization of the DT functionalities to formulate BP operations.
- The competitive landscape of the digital market needs to develop and deliver technology-savvy products and services to customers instead of providing intermediate solutions.
- Complexities of contextualizing DT functions with BPs increase as more and more technology or custom elements are introduced (or updated) to the DT offerings. Consequently, it also increases the risks. The architecture approaches are unable to manage risks at runtime.

- The key performance indicators (KPIs) associated with the BP or BPs are either undefined or partially defined for new or updated BPs due to a new level of digital activities. It requires changing service level agreements (SLAs) and their association with the KPIs.
- RTE usually engages multiple DT providers and applications to perform various enterprise functions. The ambiguity arises due to the overlapping of the functionalities of DTs. Their integrity in the single business operation is questionable. It requires either governance to be placed or rationalization across RTE.

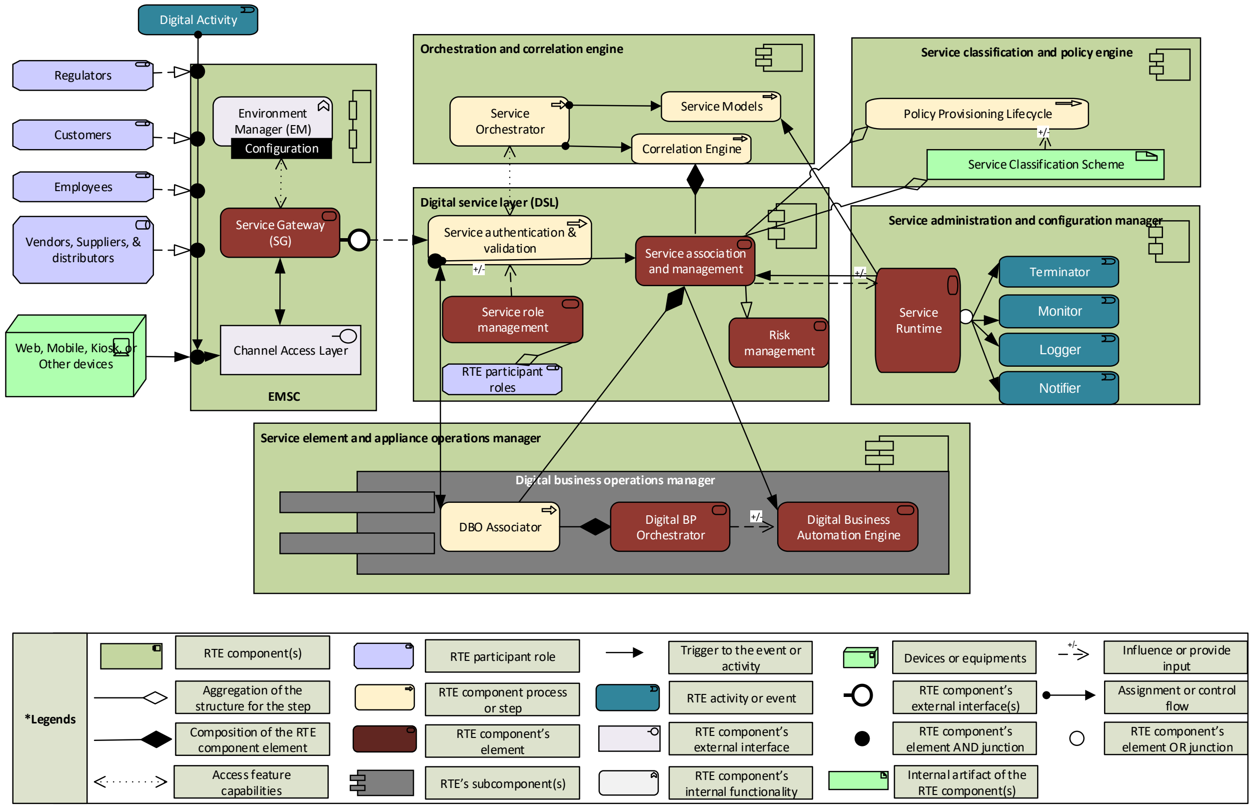
As DT providers are growing, it is vital to overcome this situation by either advancing their BPs with DT functionalities or adapting novel DTs. RTE should have the means to manage the evolving characteristics between DT functionalities and business operations in terms of digital activities and their impact on the businesses.

2.2 RTE architecture framework

The RTE architecture must be able to break down complexities and contextualize the functionalities and operations to the capabilities of DTs. The RTE architecture establishes, integrates, updates, and monitors the relationship between the responsibilities of each RTE component and DTs. The RTE architecture standardizes RTE components' granular level of correspondence with the DT capabilities.

In Figure 3, the RTE architecture and its components utilize the ArchiMate stencils [52]. The overarching architecture framework and corresponding layers were first reported in published work PW12 during the 2nd international conference on IoT-as-a-service in October 2015.

The framework presented in each publication has commonalities across the RTE architecture and also differs based on the DT capabilities or corresponding offerings at the same time. The generic components identified for the RTE architecture framework are Environment Manager, Service Gateway, and Channel Access Layer (EMSC), Digital Service Layer (DSL), Orchestration and Correlation Engine (OCE), Service Classification and Policy Engine (SCPE), Service Element and Appliance Operations Manager (SEAOM), and Service Administration and Configuration Manager (SACM). Each architecture presented in the public work includes one or more components to consistently evolve RTE architecture in the context of DT capabilities and provide measurable advantages.



* ArchiMate legends and stencils are utilized to showcase the relationship between RTE architecture components

Figure 3: Evolving real-time enterprise architecture framework

The following represents the primary research contribution towards developing, deploying and evaluating the RTE architecture utilizing the DT technologies. It considers continuously evolving the RTE architecture framework associated with the upcoming or updated DT capabilities.

- Published work PW1: Multi-agent Cognitive Architecture Framework for IoT
- Published work PW7: Edge policy architecture of mobile edge computing
- Published work PW9: Cloud-enabled trading architecture of the smart city
- Published work PW10: Fragmented architecture of IoT in electronic commerce (eCommerce)
- Published work PW13: Blockchain-driven three domains secure 2.x service fabric architecture framework
- Published work PW20: Industrial IoT Control Framework of Dynamic Multi-Cloud Events and Devices

However, each RTE architecture component presented in Figure 3 requires modifications based on the type of DTs and the industry segment. Table 1 provides the details of the published work for each RTE architecture component. It indicates the overlapping between the published work in terms of the different components necessary for the specific business case of the RTE.

ID	RTE Component	Published Work	Digital Technology	Industry Segment
1	Environment Manager, Service Gateway, and Channel Access Layer (EMSC)	PW17	Mobile edge computing	Smart healthcare system
		PW1	IoT, mobile edge computing, and cognitive computing	Smart manufacturing system
		PW13	Blockchain	Payment technologies
2	Digital Service Layer (DSL)	PW16	Big Data	Electronic commerce platform
		PW10	IoT	Electronic commerce platform
		PW12	IoT	Security alarm system and surveillance camera
		PW13	Blockchain	Payment cards
3	Orchestration and Correlation Engine (OCE)	PW7	Mobile edge computing	Healthcare (in Smart City)
		PW12	IoT	Security alarm system and surveillance camera
4	Service Classification and Policy Engine (SCPE)	PW7	Mobile edge computing	Smart healthcare (in Smart City)
		PW13	Blockchain	Payment technologies
		PW11	Cloud data services	Smart grid metering system
		PW9	Cloud	Smart City ecosystem
		PW20	Industrial IoT 4.x	Smart manufacturing
5	Service Element and Appliance Operations Manager (SEAOM)	PW1	IoT, mobile edge computing, and cognitive computing	Manufacturing
		PW7	Mobile edge computing	Smart healthcare (in Smart City)
6		PW10	IoT	Electronic commerce platform

	Service Administration and Configuration Manager (SACM)	PW14	Software-as-a-Service (Cloud)	Insurance technologies

Table 1: RTE architecture components and the published works

2.3 Environment Manager, Service Gateway, and Channel Access Layer (EMSC)

The primary responsibility of the environment manager is to conduct gateway functionalities for multiple DTs in the RTE ecosystem. It monitors, permits, deprecates, and advances RTE functionalities and applications. It enables various channels and their association with RTE capabilities. The digital channels can be added, removed, and updated based on their utilization in the context of the RTE capability. The example types of the channels are distribution channels, including pure-click, bricks-and-click channels [53], and mobile application channels. Pure-play channels are usually companies that operate solely on the Internet. Bricks-and-click channels combine a physical presence and online selling. Brick-and-click organizations may operate a website that sells products or advertises those it sells in the stores. The service gateway feature enables the configuration of role-based association to the digital channels and connected appliances.

2.3.1 PW17: Service gateway operating modes

The published work PW17, which defines the service gateway, derives the operating modes of communication channels based on the utilization of IoT devices by the end-user of the mobile edge computing ecosystem. These operating modes identify the specific communication paradigms based on the DT's utilization. The service gateway captures the digital activities performed through the communication channels and provides real-time actions. Based on the type of RTE, the service gateway can provide configurable paradigms for the RTE ecosystem and corresponding mobile edge computing services to the users. The configuration implied the cross-domain capabilities in terms of functionalities of IoT devices and their users.

2.3.2 PW1 and PW13: Service gateway functionalities

The heterogeneous cloud environment manager introduced in the published work PW1 conducts gateway functionalities for multiple clouds in the mobile edge computing ecosystem. It monitors, permits, deprecates, and advances heterogeneous cloud for the set of mobile edge computing servers and applications. However, the digital channel director in the published work PW13 provides the means to connect diversified users with the other components of the RTE architecture framework. The customer, issuer, merchant, and acquirer can utilize many ways to perform various activities during the checkout process of the purchases, as indicated in the responsibilities of each component. The digital channel director is responsible for validating and orchestrating these activities. It is the first line of defense against faulty payment activities and transactions. The digital channel director consists of the following components.

- Digital channel authorizer: It authorizes a new or existing digital channel for the payment.
- Digital activity validator: It validates digital activities.
- Digital activity orchestrator: It orchestrates these digital activities in alignment with the checkout process, including receiving payment information and biometrics of the cardholder.
- Digital channel role associator: It associates the role with the Blockchain API manager to recognize the rules implied for the particular digital activity.

2.4 Digital Service Layer (DSL)

DSL’s primary responsibility is to deliver the DT service's capabilities as functionalities, such as wearable health monitoring, smart home security system, and smart grid metering. It empowers specific DT capability and decisions in the form of DT services. DT services differentiate the actions and the data associated as inputs and outputs of those actions. The functionalities aim at achieving aggregate operations. Operations are accountable for coordinating independent functionalities to pursue a DT capability. For instance, the interrelationship between an individual's health monitoring requires actions based on the pre-defined limit of specific real-time paradigms such as blood pressure, diabetes, and pulse rate. These limits vary depending on the various dimensions, including an individual's age, location, health condition, and medication requirements.

The service association and management (SAM), risk management (RIM), service role management (SRM), and service validation and authentication (SVA) are the component of the digital service layer. SAM is responsible for instantiating DBOs associated with the digital activity. It associates BPs to the DT service or set of DT services and is responsible for identifying the classification of DT services classifications associated with the BPs. It provides access and visibility of the service associated with the DT and risk model specified in risk management (RIM).

The SAM component of the DSL can dynamically update different DTs and risks to the DT services (or set of DT services) through service administration and configuration manager. In the example of online credit card approval processing, the post-approval of the credit card requires continuous monitoring and authorizing purchases by individuals in real-time. Service association and management can include a new paradigm to compute the risk associated with future transactions and include attuned paradigms to authorize the payment.

The purpose of RIM is to model the different types of risks associated with the DTs. It identifies, places, and computes risk factors of the specific service or set of services in real-time. Risk management consists of risk factors for the DTs. SVA validates and authenticates services. The RTE can enable or disable specific DT services through SVA. If either legacy service or specific DT service is disabled, it ensures that the participants of the RTE prohibit these services' access. The authentication and authorization of the services are the responsibilities of SVA.

2.4.1 PW10: Fragmented service layer

A fragmented service layer developed in the published work PW10 provides composite IoT services correlated with the electronic commerce dimensions to the different channels and corresponding eCommerce appliances. The fragmented service layer retains the structure of the composite IoT services and the corresponding diversified set of metadata derived at the granular levels of IoT services. Essentially, composite IoT services are derived from a granular level of services to classify into a specific category. The fragmented service layer persists in the internet-of-thing service classification engine and eCommerce dimension correlation engine. For example, introducing an entirely new marketplace for healthcare monitoring devices and the corresponding brand for patient care needs to establish and manage supply-chain of different types with control imposed at multiple levels of transactions. The eCommerce quality dimension offers products and planning services for healthcare devices based on the consumers' specific medical conditions and monitoring criteria. The service includes connectivity with the healthcare provider's network for immediate response identified within the context of the product offering.

IoT service classification engine is the classification engine where composite IoT services are derived and classified to address the specific needs of eCommerce appliances. It characterizes a set of composite IoT services into a particular classification. If there is any necessary diversification, then a separate composite IoT service is developed and deployed with specific paradigms of eCommerce dimensions. The dimension and correlation engine defines the correlation between the eCommerce dimensions and composite IoT services. If there are new eCommerce dimensions, whether or not it leads to new or updated classifications, the eCommerce dimension correlation engine is responsible for managing them.

2.4.2 PW12: Service mediation layer

The IoT service mediation layer in the published work PW12 provides the approach to composing and delivering the IoT services and defining the corresponding operations. The IoT services are invoked either synchronously by responding to service requests or asynchronously by sending notifications according to subscriptions previously made through the service. The service registry registers resource history and metadata associated with the IoT service operations. Role model instance association with IoT service model and specification are also an integral part of the service mediation layer. It provides reusability across multiple BP activities by differentiating IoT services in the presence of the type of role model associated with it. The observatory role model is used to logically trace the physical IoT resource for the IoT service. The operative role model defines actions and alternatives for IoT services during the state change of an IoT device associated with the IoT service. The IoT service manages security alarm devices associated with an observatory role model and an operative role model. However, the purpose of the IoT service changes and the respective model, instance, and utilization differ at runtime.

2.4.3 PW13: Risk factor association manager

The RTE architecture developed in published work PW13 introduces the risk factor association manager (RFM) to identify, place, and compute risk factors associated with the specific transaction or set of transactions in real-time. The risks of online fraudulent transactions increased to 27% in 2019, and 42% of consumers experienced unauthorized payment activities [54]. The results impacted the entire supply chain, including delays in shipments, consumer traffic, and in-store purchases. The risk factor association manager consists of risk factors for the device, browsers, and merchant risk authentication. It can also consist of subcategories of risk factors for each of the data elements associated with the device, browser, and merchant risk authentication during the payment to avoid fraudulent transactions in real-time.

2.4.4 PW16: Dynamic orchestration of rules

The dynamic orchestration of rules within the DT services depends on the various digital activities performed by the RTE participants, as indicated in the published work PW16. Service role management (SRM) provides the accessibility of the service to various participants of the RTE. The DT service involves multiple RTE participants and their roles, such as suppliers, vendors, partners, and consumers. SRM manages the role hierarchy and rules associated with the roles during the DT service execution. The SRM is responsible for dynamically defining, associating, or changing the participant roles for the specific DT service. Typical BPs and orchestration of BPs are associated with the business rules corresponding to the specific static business conditions. At the same time, the dynamic orchestration of the rules associated with the DT service enables RTE to change or update the rules in real-time. For instance, the store can increase or decrease the discount on a specific product based on the outcome of the Big Data enabled real-time analytics of a DT service for the specific brand of product, particular geolocation of the store, and type of customer.

2.5 Orchestration and Correlation Engine (OCE)

The OCE provisions the modeling capabilities of the service specification to the digital service layer. It formalizes the roles and responsibilities of the granular level services. Essentially, it defines the relationship of RTE participants with the specific set of DT services in the form of a service model. The service model correlates the RTE participants with the services utilizing a specific set of DT functionalities. The service orchestrator performs the dynamic orchestration of services based on the DT service's contextual information provided by the DSL to a service model. The service orchestrator's responsibilities also include composite services in correlation with the different digital channels accessed by the RTE participants. Typical BP management and orchestration [55] identify business requirements for performing the RTE operations. The DT functionalities associated with the DT services perform the actual operations identified in the orchestration.

The OCE retains the structure of the composite services and the corresponding diversified set of metadata derived at the granular levels of services. In [56], flexible and scalable metadata management proposed maintaining dependencies on the resources utilized within the services. The OCE leverages metadata management to provide the scheme to manage the context of the DT services. Metadata provides contextual information on the DT functionalities and data services associated with the DT services in the service model. The service model facilitates incremental updates of meta-information. The most prominent example is the "outage_to_restoration_impact" service to formulate the context for the outage-specific functionalities [17]. The healthcare monitoring devices utilize the smart home services and the smart energy services through cloud integration services (or intranet). The framework developed in [57] is to control and manage the network of integrated computing services in cloud environments. It allows the creation, modification, and management of integrated hybrid cloud services with policy-based access to cloud services. The smart home services, smart energy services, and smart healthcare services can be integrated and utilized through a unified platform through orchestration and correlation engine capabilities.

2.5.1 PW7: Mobile edge computing's application programming interfaces

The mobile edge computing's APIs enablement engine in the published work PW7 introduces a cognitive agent. A cognitive agent is the constitution of the decision tree based on the set of conditions and the actions of the specific digital activity (or event) performed by the RTE participants. The API represents the cognitive agent within the mobile edge computing ecosystem. APIs are associated with a set of policies, and they can also represent a standalone set of policies. The cognitive agents are either enforced or subscribed to these APIs based on their role and feature capabilities to specific dimensions such as vertical, consumer type, environment, and connectivity. For example, smart healthcare APIs allow patients with chronic conditions (such as type 2 diabetes) to monitor their health. Patients receive essential reminders about medications, doctor visits, and even new clinical trials based on the health insurance portability and accountability act (HIPAA) policies and corresponding updates [58].

2.5.2 PW12: Service mapper

The IoT service mapper to BP activity layer introduced in the published work PW12 correlates services to BP activities that complement the capabilities of BP aware IoT service. It establishes a common understanding between the utilization of the IoT services concerning the identified and placed BPs. The critical aspects of this layer's functionalities are the continuous updates to the role model and their desired variations based on BP activity and service level agreement monitoring. The managed security alarm device-specific IoT service is associated with the security alarm observatory role utilized within the BP activity of billing and payment inventory checks.

2.6 Service Classification and Policy Engine (SCPE)

The characteristics of RTE differ depending on the types of DT services delivered and evolved. The RTE needs to establish the DT services classification scheme to emphasize the behavioral characteristics of its utilization in various aspects of the RTE. It is an iterative process where DT service classification depends on the numerous dimensions of the RTE ecosystem to define, place, and utilize DT services. Chapter 6 and Chapter 7 detail the steps to identify the DT service classification paradigms and mature the DT service classification in an iterative process. The following are the RTE paradigms to derive the DT service classification schemes (described in Chapter 6 and Chapter 7)

- Types of BPs and BP activities of the RTEs
- Digital activities performed by the RTE participants using the DT services
- DT paradigms associated with the DT services to perform the business operations
- DT services for types of RTE internal and external processes
- Types of RTE policies, controls, and rules associated with DT services
- Categories of incremental risks associated with the DT services
- Characteristics of the utilization of DT services in RTE
- Types of compliances, regulations, and standards to be performed by DT services

The service classification scheme (SCS) is responsible for implementing the DT service classification mechanisms based on the RTE paradigm selected for the DT service classification. The policy provisioning lifecycle (PPL) presented in the published work PW7 is necessary to assign, enforce, and subscribe to policy APIs and maintain uniformity and reliability across RTE.

2.6.1 PW7: Policy provisioning lifecycle phases

Policy provisioning lifecycle phases ensure the rationalization of policy provisioning and corresponding management across RTE. The policy provisioning lifecycle functionalities transpire during the lifetime of a policy API when policies are either modified or upgraded (or downgraded) for the specific DT service or set of DT services under the classification identified within the service classification scheme. Figure 4 provides the phases of the policy provisioning lifecycle and their sequence of implementation.

The DT service classification scheme varies among RTEs depending on the methodologies adopted for the classification. The published work PW10 identifies the detailed methods for DT service classification. Suppose the overlap in the DT service classification exists. In this case, either a new classification or subsequent classification level is introduced based on the anticipated extendibility of the services associated with the classification.

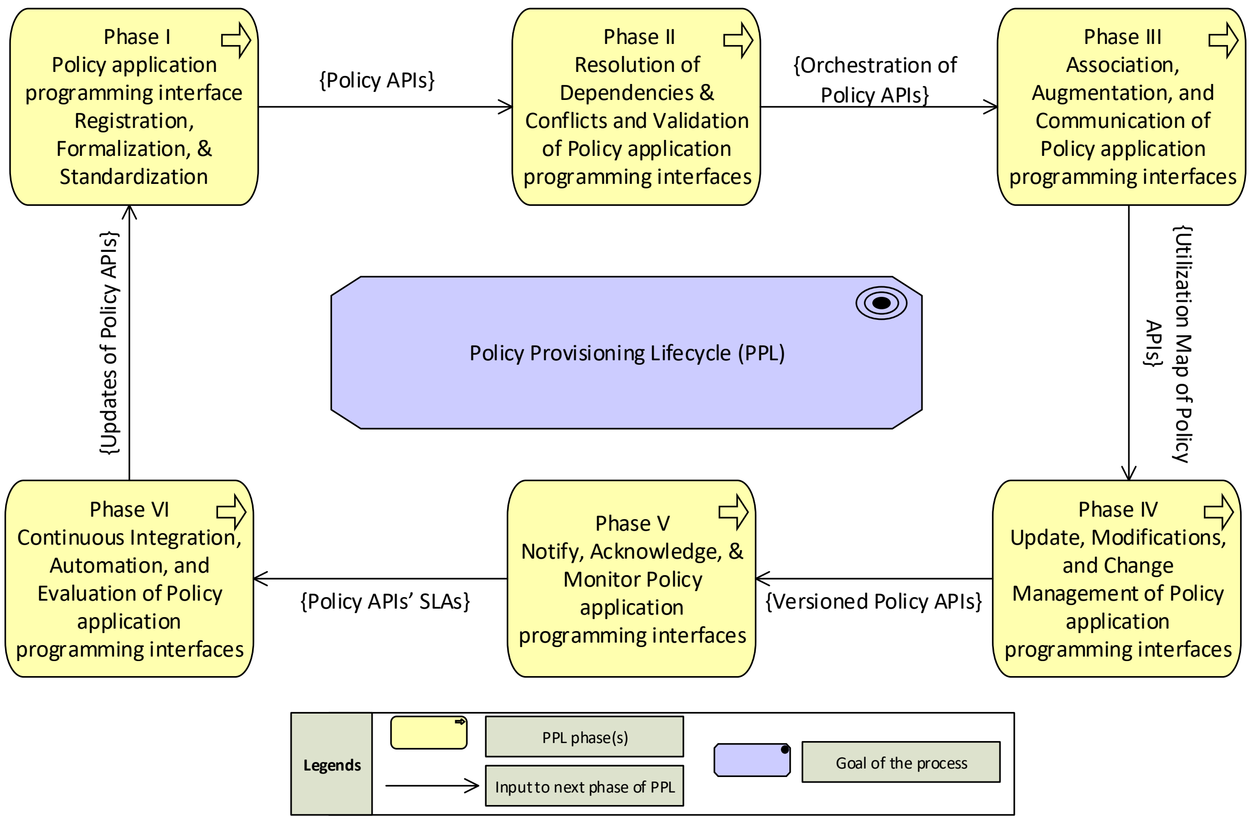


Figure 4: Policy provisioning lifecycle phases

2.6.2 PW13: Blockchain application programming interfaces

Blockchain APIs in the published work PW13 take responsibility for the classification, management, and error handling of services. The classification engine, the role manager, and the tokenization are the essential components of the Blockchain API manager. The classification engine specifies the classification of the services interacting with Blockchain nodes and frictionless payment. The acquirer associated with the merchant (or set of merchants) can define the classification scheme. It depends on the type of transaction, geolocation diversity, type of merchants, device types, mobile applications, consumer types, and other customarily defined classes. The acquirer can select to place classification with multiple dimensions. Blockchain API's tokenization connects the classification engine to recognize risk for the specific classification. It identifies the risk implied for the particular transaction based on the classification specified by the acquirer. However, the transfer of information carried out by the Blockchain API manager occurs using a cryptographic protocol [59] that arrives at a consensus among the Blockchain nodes for updates.

The risk computation (RIC) is calculated for each digital activity performed for a specific transaction. The risk computation is an accumulation of the risks associated with the digital activities of the specific transaction in the risk hierarchy and the risk rating. The risk rating differs based on whether it is the external or internal activity of the RTE. The internal activity is usually at a lower risk rating and lowers in the risk hierarchy. The15 digital activities present the use case of online charitable contribution during the eCommerce transaction. The risk computation is compared against the threshold value to allow the online transaction. It decreases the possibility of fraudulent transactions.

2.6.3 PW11: Composite data services

The runtime framework in the published work PW11 represents a dynamic instance of the composite data services (or consumer services). It provides classes that describe the entities of data associated with the business rules and their interrelationships. The common information model is derived from compliance-specific attributes to hold the structural binding between compliance-aware data services and business rule services. Eventually, the common information model generates consumer services and respective service definitions for the consuming applications. It can select the subset of compliances applicable to deployed data services, avoiding the evaluation of compliances that might not be relevant to the business rule.

2.6.4 PW9: Pervasive cloud trading transaction policy engine

The pervasive cloud trading transaction policy engine in the published work PW9 is the policy engine for the transactions performed. Policies can be either associated with specific digital or supply-chain policies or defined based on the identified paradigms of the DTs. Policies bridge the gap in the transaction. The most prominent example is the tax structure differentiation, where the county tax of a specific smart home (with similar square footage) differs from county to county. In this example, smart home location becomes the policy paradigm to pay the county tax.

2.6.5 PW20: Industrial IoT control framework of dynamic multi-cloud events and devices

The industrial IoT control framework correlates events instantiated from multiple cloud environments for the specific industrial IoT resource devices in the different cloud environments. A hierarchy of the events from multiple clouds is established, derived, or introduced at runtime. The relationship between the environmental factors (example: weather conditions and pollution) and economic factors (example: labor cost and maintenance cost) associated with the events and a set of industrial IoT devices included in performing these events determines the hierarchy levels.

The relationship between the events and industrial IoT devices as services derives the controls. The type of event, the derived controls, and a profiled RTE participant role generate the action plan data for an industrial IoT service execution in a multiple cloud environment. The action plan data is distributed in a multiple cloud environment to indicate the temporal characteristics of the actions performed by a specific industrial IoT device under the particular cloud environment. For example, if a shoe manufacturing organization performs the manufacturing to 3 different geolocation or continents, it can dynamically generate events to switch the manufacturing location at runtime. It depends on the impact on the local environment or even considering the maximum load per day for the site to keep the industrial IoT devices in good condition.

2.7 Service Element and Appliance Operations Manager (SEAOM)

The SEAOM is responsible for the essential functionalities of the service operations. It includes communication paradigms and monitoring the accessibility of the DT services. It collects metadata for the services defined in the digital service layer and models in the orchestration and correlation engine. It determines and selects the right level of deployment in runtime, ensuring relatively independent deployment of DT services. However, each service represents a specific set of functionalities of emerging technologies to be leveraged during the advancements of DTs. It validates that functionalities are achievable by the DT services. For instance, the inclusion of the necessary checks in the service to confirm whether connectivity is available or restored for healthcare devices and service level agreements is adhered to in the outage scenario.

The SEAOM is also responsible for tracking, adding, removing, updating, and quantifying the capacities and capabilities of DT services' applications. It manages the set of applications irrespective of the association of the specific participant of RTEs, including suppliers, producers, administrators, and consumers. It is configured to facilitate progressions of RTE across multiple supply-chain for anticipated or sporadic advancements in technologies necessary due to the competitive characteristic of the marketplace.

The DBOs manager (DBOM) manages DBOs associated with the DT service. The DBOs manager emphasizes managing business operations and corresponding BPs. It consists of the following components.

- Digital business operations associator (DBOA)
- Digital BP orchestrator (DBPO)
- Digital BP automation engine (DBPAE)

Service association and management (SAM) instantiates the specific business operation. The DBOs associator has DBOs and their variations against the digital activity for SAM to initiate the specific business process. The business operations are dependent on the hierarchy of BPs. The digital BP orchestrator has a definition of the BP hierarchy associated with each of the DBOs. The DBOs manager activates a specific BP to run through the digital BP automation engine (DBPAE). The digital BP automation engine interfaces with service association and management to execute specific DT services.

2.7.1 PW1: IoT application programming interface (API) element manager

The IoT API element manager introduces service element and appliance operations manager capabilities in the published work PW1 is responsible for configuring the Microservices. It manages the most basic functionalities and metadata of the Microservices. It determines and selects the right level of deployment for the Microservices and ensures relatively independent deployment in association with the set of IoT APIs. It associates and validates the conditions to run the functionalities and persists the state of the

Microservices associated with the IoT API. For instance, in the case of the smart grid, the Microservice of outage-to-restoration has checks to confirm whether restoration is completed, and the service level agreements adhere to the regulatory conditions of the smart grid's outage scenario.

2.7.2 PW7: Cognitive agent's policy transport layer

The cognitive agent's policy transport layer in the published work PW7 provides mechanisms and protocol to access, communicate, secure, and protect the API integrity of the deployed set of policies. The policy transport layer distributes policy information from a mobile edge computing's radio network controller's API policy accreditation to a group of API policy prosecutions. The policy transport layer also facilitates additional security measures, such as data confidentiality to sensitive APIs. An example is security policy distribution for medical device connectivity to a specific set of patients in the proximity of Wisconsin, USA. The policy transport layer is responsible for flow control policies across cognitive agents, participant consumers, and the mobile edge computing network elements or services.

2.8 Service Administration and Configuration Manager (SACM)

The SACM is responsible for introducing, managing, monitoring, and deprecating services of the digital service layer and corresponding models of orchestration and correlation engine at runtime. Many users or participants dynamically publish services through service runtime. It has a publish-and-subscribe mechanism associating a set of DT-specific feature capabilities to standalone orchestration and correlation engine's service model. The orchestration and correlation engine's service models are either enforced or subscribed based on the operations or feature capabilities to specific criteria such as service classification, type of users, cloud, and connectivity type. For example, monitoring the outage for a particular site and enforcing specific regulations for restoration are the services in a customized cloud environment [60]. The service runtime triggers to terminate the service or notify the users in case of any violations in the service level agreements. The service runtime connects with the orchestration and correlation engine's service model for introducing, managing, monitoring, and deprecating services at runtime. At the same time, it communicates with the digital service layer's service association and management to securely terminate, log, monitor, and notify. The digital service layer's service association and management, in turn, instantiates the appropriate action to the DBOs manager.

The orchestration and correlation engine defines service lifecycle, configuration paradigms, and metadata (or contextual information) defined at this layer for composite and granular services. The service lifecycle also includes service recognition, identification, and discovery, where the existing RTE ecosystem leverages new DTs. Due to the granular level of services, changes to the composite services are also versioned and maintained. It is responsible for migrating and managing services and corresponding dependencies. An example of the custom configuration is specific properties of the smart healthcare environment where users' healthcare data are accessible through the particular security protocol and tokenization mechanism of the private Blockchain ecosystem.

2.8.1 PW10: Service configuration management

In the published work PW10, the IoT service management spectrum manages the lifecycle of composite IoT services. It defines the IoT service lifecycle stages, configuration paradigms, and metadata IoT services in the DT services. The IoT service management spectrum parametrizes the deployment of the IoT services and continuously monitors their performance. It is also responsible for the changeability at runtime through the event-based triggering of the services. It is also responsible for service recognition, identification, and discovery where newly introduced devices or technologies can be leveraged to an existing platform using event-based monitoring. Due to a granular level of DT services, changes to the composite IoT services are versioned, maintained, and migrated within the IoT service management spectrum.

2.8.2 PW14: Service administration

The digital activity Integration model administrator in the published work PW14 administers each digital activity integration model with the four different administration elements: Monitor, Logger, Notifier, and Terminator. It interfaces with a runtime engine to monitor and log the digital activity integration model. It also maintains the versions of the model. A notifier provides alerts to the RTE participants responsible for the digital activities. The terminator stops the execution of the digital activity through a runtime engine. It interns halts the specific DBO.

The primary concern is holding the integrity between the components of the RTE architecture framework presented in Figure 3. The relationships and bindings between the BPs and DT services need consistent definition, derivation, and application across the enterprise through the DBOs. It should provide a consistent way of evolving the RTE considering the runtime characteristics of the RTE. The DBO structure presented in the published work PW14 ensures the unique identification of the DBOs across RTE. The DBO structure maintains the integrity between BPs and DT services depending on DT functionalities and operations.

CHAPTER 3.

PW14 and PW15: RUNTIME OF DIGITAL BUSINESS OPERATIONS

Chapter 2.2 articulates the RTE architecture framework and responsibilities associated with each of the RTE architecture framework components. The RTE architecture components have a specific set of tasks to be performed at runtime in the context of the corresponding BPs and DT services. The proximities of each architecture layer ensure the dynamic insertion and validation of the DT service, the governance, compliances, and validity of the DT services for the diversified set of the RTE functionalities. BPs and the corresponding service operations performing the BP activities drive the characteristics of RTE [61]. It is essential to analyze and manage any new information related to DTs in the perception and input from the BP specification and rationale between the contextual information and BP activity [62]. BPs, BP activities, functionalities of each participant, operations associated with participants, and contextual information of DTs identify the impact factors that are generic enough to recognize from any RTE architecture. It is essential to correlate these individual set of DT services and their context to the BPs across the components of the RTE architecture framework presented in Figure 3. It needs to be uniquely identifiable across the RTE architecture.

The published work PW14 describes the runtime view and the structure of the BP and DT services in the form of a digital activity integration model. The key contribution in the published work PW14 is to identify the physical structure of the DBO model with the composition of the digital activity integration model. The DBO identifier (DBO_ID) in Figure 5 uniquely identifies and represents the correlations between BP and DT services to repeatedly utilize and operationalize Dt services between the RTE architecture framework components at runtime.

As indicated in PW14, the DBO structure contains the correlation between the BPs and DT services. Multiple BPs can be associated with numerous DT services. The orchestration and correlation engine enables the hierarchy when the specific digital channel triggers typical DBO within the RTE architecture framework. The following are the primary elements of the DBO model in Figure 5.

- DBO model (DBO_Model): It holds the structure of the specific or unique DBO and maintains the correlations and dynamic binding between BPs and DT services within the RTE architecture framework in terms of the business operations. It embraces the information of the digital channel, roles, and rules associated with the DBO during runtime.

- BP to DT services link structure (BP_DT_service_Link): The dynamic binding between the BPs and DT services is managed, updated, and performed through the BP to DT services link structure (BP_DT_Service_Link). It consists of a unique BP identifier, associated DT service identifier, and the link type between the specific BP defined in the business operation and the specific DT service. It presents the level of the DT service for the specific BP to formulate the dependencies and sequence of execution of the DT services, that is, DT operations associated with the DT functionalities.
- Business_Operation: The DBO derives the actual RTE's business operation (BO_ID). The multiple BPs and their BP activities constitute the RTE's business operation. The unique business operation identifier represents the specific business operation assigned to the DBO. It ensures the levels of BPs based on their hierarchy at runtime and the expectation in terms of key performance indicators (KPIs) of the BPs.
- BP: The business operations consist of multiple BPs. Each BP is unique in the RTE and recognized with the unique BP identifier (BP_ID). The BP structure also specifies the level of BP in the business operation to determine either the sequence of BP execution, the alternate path for the BP, or concurrent BPs for the business operation in the context.
- BP_Activity: The multiple BP activities and their execution sequence constitute the RTE's BP in the business operation. BP activity identifier (BPA_ID) is the unique identification for the BP activity within the BP. The BP activity structure also specifies the level of BP activity in the BP to determine either the sequence of BP activity execution, the alternate path for the BP activity, or concurrent BP activities for the BP in the context.
- DT service provides the structure to recognize the individual DT service within the RTE architecture. DT service identified (DT_Service_ID) is the unique identification for the specific RTE's DT service. Multiple BPs utilize DT services in the constitution of the business operations. DT service construct traces the DT applications utilizing or offering the DT service. Multiple service level agreements (SLAs), including type, value, and permissible threshold, are associated with DT service. The DT service structure captures the invocation of the specific DT services in the DBO model as a timestamp.

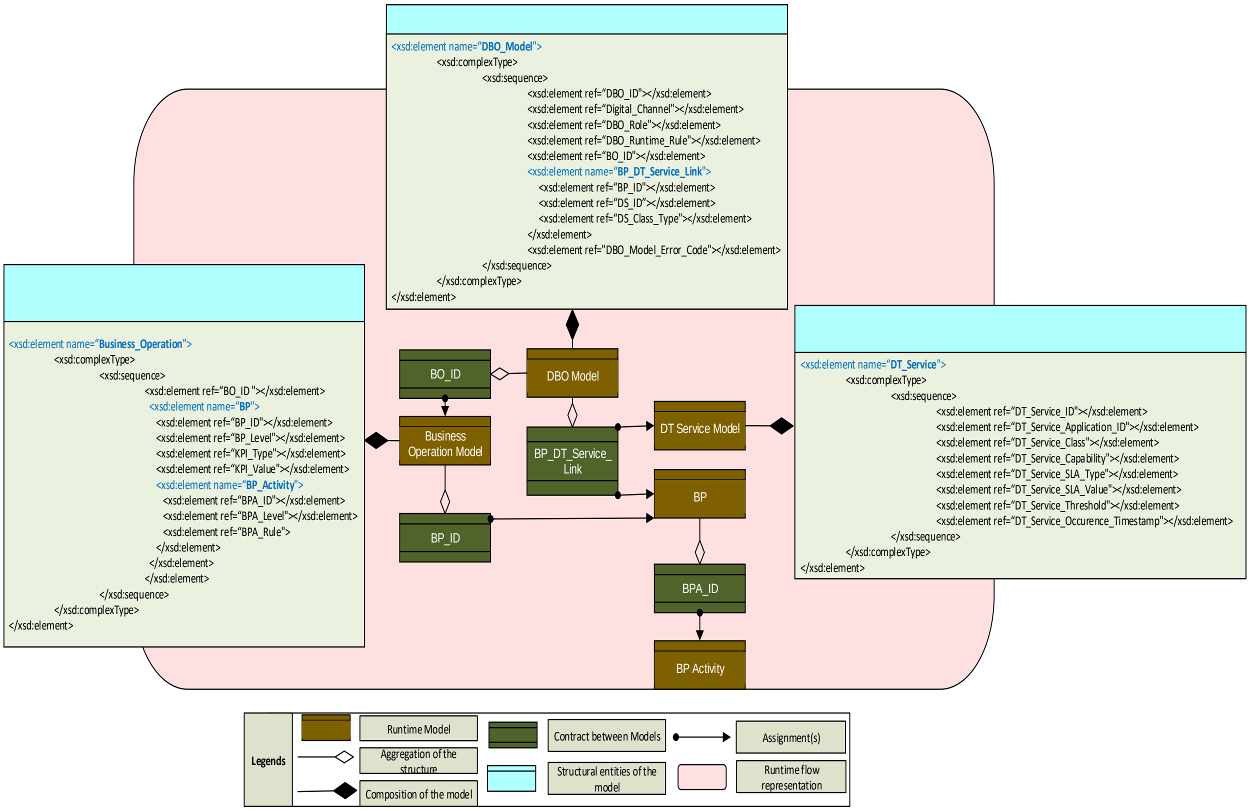


Figure 5: Runtime structure of the DBO model

The digital service layer component of the RTE architecture framework presented in Figure 3 and described in Chapter 2.4 triggers the DT services through the request to orchestration and correlation engine's service model manager described in Chapter 2.5. The DBO model structure connects to a specific BP with the DT service. The digital service layer has call-back services to the orchestration and correlation engine to invoke the DT service or set of DT services. The DBO model contains service level agreements (SLAs), their attributed values, and permissible threshold values in the context of the DT services. The DBO model persists in the parametric value of key performance indicators. Each key performance indicator is associated with BP, indicating the specific BP's operational performance. It captures the actual desired level of the threshold against the key performance indicators assessing the accumulative value of the service level agreements of each associated DT service with the BP in the context of business operation.

The orchestration and correlation engine trace the runtime SLA's values and continuously inform the service administration and configuration manager's service runtime component. The DT service classification (DS_Class) determines the DT service threshold (DS_Threshold) in percentages of specified service level agreement and allowable degradation in the SLA value indicated in the published work PW14. However, the published work PW15 emphasized the digital risk model to identify the correlations between DT services and BPs in the incremental risks associated with the DTs.

Many current risk issues of DBOs are complex, uncertain, or even ambiguous [63] to achieve the SLAs within their threshold value and corresponding measurable KPIs. In most scenarios, the potential benefits and DBO remain interconnected. It raises the need for an RTE operational governance framework that accelerates decisions iteratively and maximizes DBOs' trust in RTE architecture's risk management capabilities. The volatility of DBO is dependent on many factors, including industry segment, line of business, types of target customers, and vendors or suppliers of a specific set of services (or products). The same governance paradigms are not appropriate for every RTE; besides, there is a need to introduce DBO-specific risks. It is neither desirable nor possible for organizations implying DTs to directly leverage governance from a single vendor [64] and [65]. In some cases, RTEs are considering building their governance [66]. Organizations probably understand the need for governance, but they do not know how to implement governance within their identified DBOs.

CHAPTER 4.

PW8 and PW4: RTE OPERATIONAL GOVERNANCE FRAMEWORK

Implications of DTs are multifaceted in terms of locations or devices, for example, sensors capable of automatic data gathering and monitoring. Mobile user interfaces, hybrid cloud services, security, remote authentication, and reusable components could form the foundation of a comprehensive RTE architecture ecosystem. Social networking integration, visualization capabilities, and virtualization may offer the means to explore new communities of consumers and their relationships with the BPs and the DBO model. It is essential to manifest the RTE operational governance during the advancements of the DT services in correlations with BPs for consistently evolving and introducing the DBOs.

However, the evolving requirements of RTE under the advances of DTs are either not defined or partially identified for the DBO and integrity between the set of BPs. It is not apparent to acquire, evolve, and diversify the DT services to formulate and iteratively advance the RTE's DBOs in the principles and purpose recognized in Chapter 3. For example, the global mobile devices' consumer data statistics [66] indicate that 64% of smartphone users expect a website to load with a service level agreement of four seconds or less. However, even though the websites were hosted in a cloud, the service level agreements were either unrecognized or not monitored for the DBO associated with smartphone users to auto-scale and provision enough capacity in the case of peak hours. 40% of mobile device users have turned to a competitor's place for a better mobile experience, and 25% of online customers abandon the cart if a website's navigation is too complex [66]. It indicates that the dimensions to govern the effectiveness of the DBOs to advance DTs are either undefined or unidentified in association with the activities performed by the RTE participants or users.

The key contribution of the PW3 is to introduce RTE operational governance framework. It provides the solution to streamline DBO modeling and its evolution in runtime. Figure 6 illustrates the composition and identifies phases of the RTE operational governance framework to effectively govern and manage DBO across multiple RTE participants. The published work PW4 derives the RTE operational governance framework in the context of RTE's customers. However, the published work PW8 presents the practical implementation and implications of the DBO structure in the eCommerce platform.

Model business imperatives of DBO: The primary reason to introduce DBOs is to accomplish the business imperatives of the BPs in association with the DT capabilities. Accepting online payment through a PayPal account is an example of a business imperative in the context of mobile wallet as a DT capability and payment as BP of the RTE. The initial RTE operational governance framework criteria are to model individual DBO based on the feature capabilities of DT to the niche level of business imperatives. The modeling specification of the DBO includes the specific category of products or services offered by the RTEs, compliances, and constraints associated with them, BPs associated with delivering and managing the RTE products or services offerings, interdependencies with other DBOs, and any identified exceptions to the BPs.

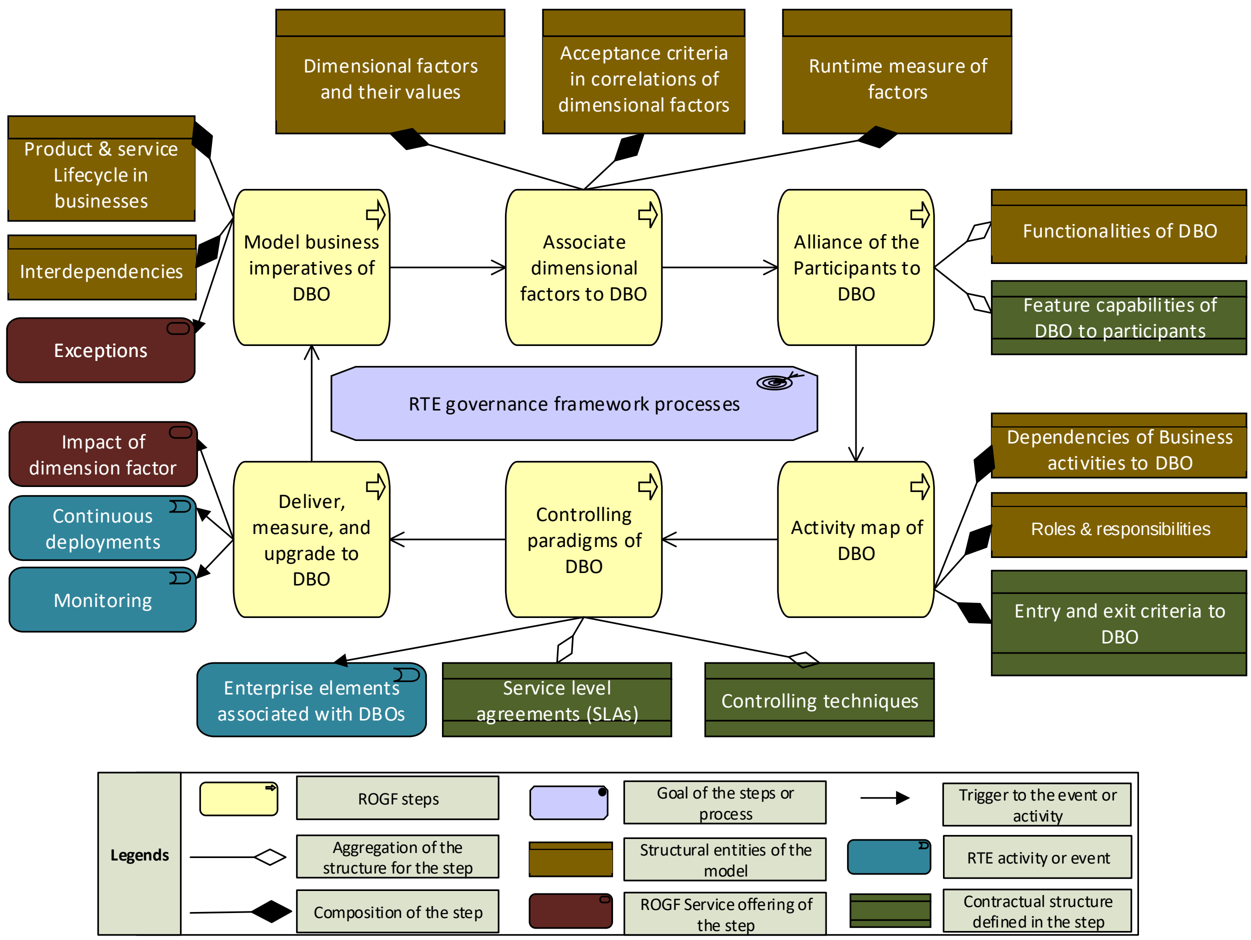


Figure 6: Phases of real-time enterprise operational governance framework

Associate dimensional factors to DBO: The subsequent step is to identify a set of dimensional factors associated with the DBOs based on the analysis performed. An appropriate example of a dimensional factor is privacy under the consumer experience dimension of the online payment DBO. The factors are registered, validated, and authorized before being associated with the DBOs. Multiple DBOs correlate with the dimensional factor, and the opposite is also possible. The following are the essential parameters to specify in this phase.

- Dimensional factors in correlation with DBOs
- Acceptance criteria for the DBOs in the correlation of the dimensional factors.
- Runtime measures of the DBO concerning the dimensional factors and their interdependencies.

Alliance of the RTE participants to DBOs: The alliances between the DBO model and various participants are specified and traced in this phase of the RTE operational governance framework. The alliances are specified in terms of the DTs' functionalities or feature capabilities. The DBO model associates the impacted RTE participants due to DTs, including manufacturers, suppliers, retailers, government agencies, and consumers. Retailers need to have a PayPal account and are willing to accept mobile payment is an example of the alliance between the RTE participant and the DBO model.

Activity map of DBO: Typically, DBO represents the performance of BP activities during the modeling phase. After any commercial transaction using mobile devices, many enterprise elements such as systems, the DBO involves data sources, platforms, infrastructure entities, devices, networks, and third-party components. The DBO model structure can map the BP activities invoking and utilizing the DBO. The BP activity map maintains the enterprise elements involved when performing the specific BP activity. BP activities such as online shopping and electricity bill payment are associated with mobile payment DBO.

Controlling paradigms of DBO: In more stringent BP activities, a DBO must enforce controlling paradigms to the RTE elements of the BP activities. This phase of the RTE operational governance framework is responsible for controlling qualitative and quantitative measures of DBO across the RTE ecosystem. The service level agreements (SLAs) are specified within the parametric aspects of the DBO model in the association with BP activities and corresponding RTE components. For instance, the DT service of mobile payment DBO should send the mobile payment confirmation within one second after accepting the payment.

Deliver, measure, and upgrade to DBO: Each update and deployment of DBO is registered, and the corresponding version of the DBO model is maintained in this phase of the RTE operational governance framework. Continuous evaluation of the Immediate impact areas is based on associated dimensional factors to deploy the DBOs. Business imperatives, BP activities, dimensional factors, relationships with RTE participants, and service level agreements are monitored and validated in each iteration to update DBOs further. The relative measure of these entities is computed using the degree of process classification (DOPC) of the RTE as formulated and evaluated in multiple iterations in Chapter 8.6

The RTE operational governance framework provides the assembly, oversight responsibilities, features, and interdependencies of DBOs and their associated BP activities. The nuts and bolts to implementing the RTE operational governance framework include BP activities, DT's paradigms, RTE processes, and RTE policies that implement governance at the granular level of responsibilities. It leads to the classification of DT services for consistently defining criteria to govern and manage DT functionalities associated with the BP activities. The DT service classification provides methods to measure the integrity of the DBOs within the RTE supply-chain and rationalize the advancement of DBO in uncertainties and adaptation of DT service for the specific purpose or BP. The uncertainties turn into risks for DBOs. It is essential to develop risk management and modeling mechanisms for an RTE to advance BPs associated with the DTs.

The risk assessment and management methodologies for the RTE’s DBOs focus on delivering the feature capabilities in adherence to the marketplace [67] and [63]. Since the operative characteristics of digital businesses are constantly evolving, the perceptions to categorize and monitor individual risk remain ambiguous for the RTEs to manage the integrity of the operational governance framework. Moreover, the RTE operational governance framework maximizes the efficiency and effectiveness of business operations with the ability to scale and adapt DBOs. However, the framework is derived based on a digital transformation viewpoint. It does not continuously assess the risk factors associated with the DBOs during the introduction, update, or advance of DT services. Chapter 5 provides the means to associate and continuously assess the incremental risks of the DBOs.

CHAPTER 5.

PW4: INCREMENTAL RISKS

The RTE operational governance framework presented in the published work PW8 and Figure 6 governs the DBOs in the dimensional factors. Typically, potential future harm to these DBOs' dimensional factors may arise from some present action pronounced as the risk in the RTE. RTE often measures the risk in terms of direct financial loss. However, during digital business management, the risk can be in terms of many other factors such as credibility, trust, prospects, and security. Risk management is a series of steps to identify, address, and eliminate risk items before they become threats to successfully managing digital business and a significant source of expensive revision or investment. DBO is defined as the most granular level of functionality to incorporate specific accessible features or business integration with DT. The incremental risk (IR) is the amount of uncertainty added to or degraded from a risk associated with managing RTE architecture by either incorporating new and updated or eliminating the need to update DBO. The update to DBO can be eliminated through third-party involvement, validating, and conforming to the completeness of DBO or strategic decision not to perform (or partially perform) specific business operations using DT.

The primary contribution of the published work PW4 is the incremental risk modeling framework (IRMF). It correlates incremental risks and their categories to DBOs during deployment of DT services and consequently in runtime management of service models. It provides feasibility for an enterprise to accurately model incremental risks and continuously monitor and update them based on the upgrades to the DBOs. The frequency and intensity of the updates to incremental risks are proportionate to the scope of DBOs required to be updated or deployed in production. The Incremental risk modeling framework also establishes provisions to update policies for individual incremental risks and qualification criteria for the categories of the incremental risks. Figure 7 illustrates the composition and aspects of the incremental risk modeling framework to affectively accommodate the iterative approach for evaluating and updating paradigms of digital business. The incremental risk management framework is presented and evaluated in the published work PW4.

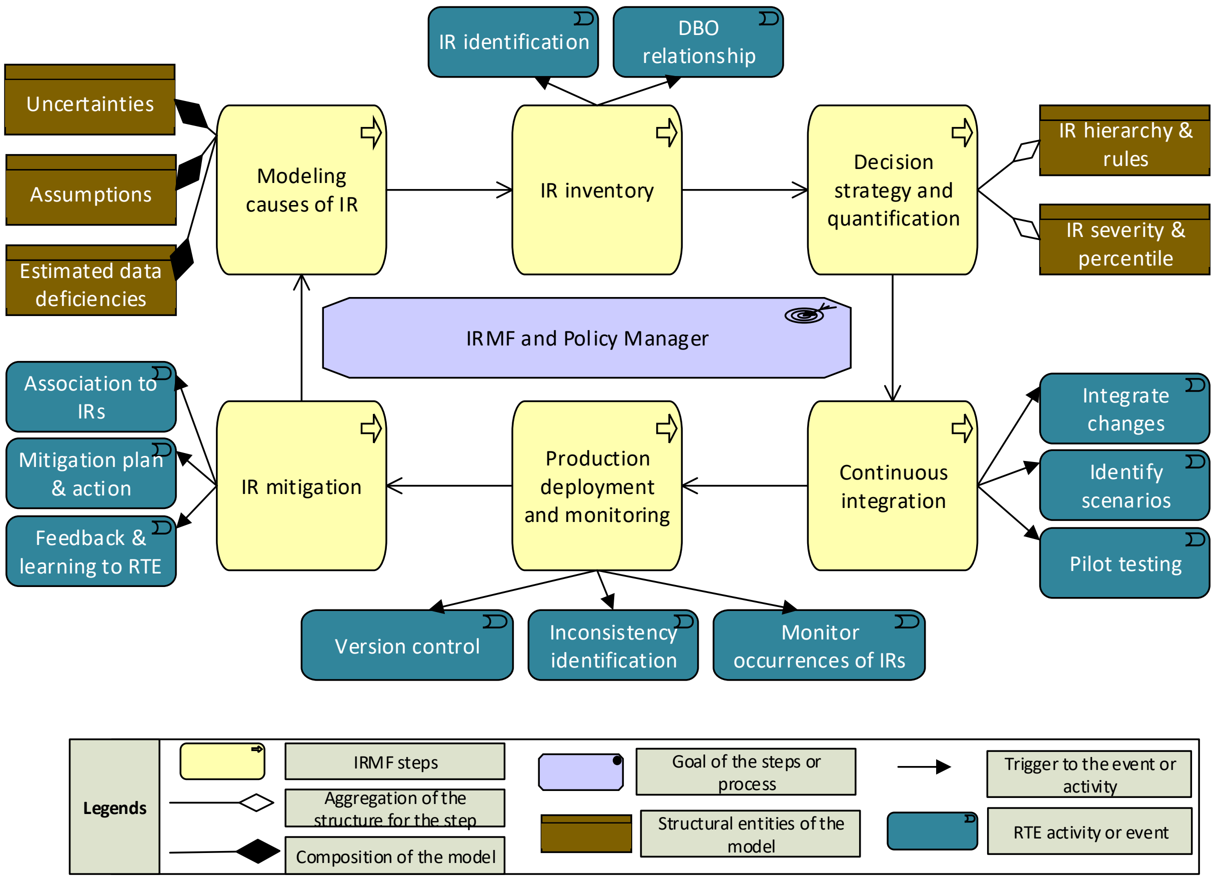


Figure 7: Incremental risk modeling framework

Modeling causes of incremental risks: The first modeling criteria identify the possible causes of the incremental risks. It can be due to uncertainties, assumptions, or estimated data deficiencies. Generally, the causes are modeled based on the situations associated with typical DBO.

Incremental risk inventory: The subsequent step identifies individual incremental risks based on the causes modeled and categorizes them. The incremental risks are registered, validated, and authorized in this step before being added to the inventory. Multiple DBOs can be associated with a single incremental risk and vice versa.

Decision strategy and quantification: This phase is responsible for placing qualitative and quantitative aspects of incremental risks. The scope of DBOs and the digital business goals in the decision log determines the severity of the incremental risks. The hierarchy of decisions and decision rules evolves over the lifetime of the RTE.

Continuous integration: During this phase of the IRMF, the objective is to integrate changes from all the sources associated with updated or newly introduced DBOs, such as customers, vendors, systems, and operations. If there is any need for additional DBO based on the emulated business scenario, it is also determined.

Production deployment and monitoring: It is responsible for deploying parameterization to the production deployment environment. The version control of each DBO and corresponding incremental risks are maintained.

Incremental risk mitigation: It is the final stage of the present cycle of the IRMF before moving to the subsequent iterations. The actual occurrence of incremental risks is analyzed, and corresponding actions are defined at runtime.

Incremental risk attempts to compute the worst-case scenario for an identified timeframe. The values of the incremental risks are placed as the point-in-time risk associated with the DBO in four different categories based on the severity of the risk for specific DBO as described in Chapter 8.1, that is, critical, high, medium, and low. The relative measure to compute the incremental risk is introduced through the percentile of incremental risk (PEIR). It provides an indicative number for the probability of incremental risk occurrences as derived in Chapter 8.1.

While iteratively executing the IRMF and introducing new or updated DT services, the following are the common types of incremental risks in the published work PW4. Further subcategories can be derived based on numerous factors of evolving DBOs.

- **Technology Change Incremental Risk**: The pace of DT change and upgrades are required because of competition and changing marketplace dynamics.
- **Communication Incremental Risk**: It represents the advancements in connectivity and convergence due to the potential of new threats in communication channels and media.
- **Governance Incremental Risk**: Upcoming regulatory and legality of DTs in the assertion of globalization requires recognizing this type of incremental risk.

- **Competitiveness Incremental Risk**: Desired and recognized time-to-market versus the anticipated accuracies in products or services.
- **Consumerization Incremental Risk**: Compromise in consumer satisfaction due to preference for the operational agility to deliver digital business functionalities.

The incremental risk modeling framework will precisely categorize the incremental risks associated with DBOs. However, the question remains open regarding how to identify, assure, and qualify the individual classification of the DT service. Besides, one of the primary distinguishing features between traditional and incremental risk is adding and degrading DBO uncertainties based on the types of associated DT services. Chapter 6 provides the essentials of classifying DT services and logical steps to identify and adapt DT service classification for the RTEs.

CHAPTER 6.

PW10: DIGITAL TECHNOLOGY SERVICE CLASSIFICATIONS

Due to the increasing availability and development of service-oriented architecture [7] and BP platforms [68], RTE services have many facets and characterize numerous aspects. Many service classification techniques are favorable and widely adopted in the industry. The most utilized classification methodology is functional architecture-based services, including platform, data, application, and infrastructure services. Another approach is to classify industry segment-specific services such as healthcare, utility, and payment services. The RTE experiences absence of standards and different rationalizations scheme across multiple departments, groups, or businesses during the advancement or introduction of DTs. It is necessary to introduce and streamline the approach to classify DT services.

Chapter 2.6 describes the responsibilities of service classification and policy engine (SCPE) of the RTE architecture framework illustrated in Figure 3. The service classification scheme (SCS) of the SCPE component is responsible for implementing the DT service classification mechanisms based on the RTE paradigm selected for the DT service classification. However, since each RTE has a different approach to introducing and evolving DT services, RTE needs to establish a process to derive and evolve the DT services classification during advancing or introducing the DTs.

Figure 8 provides the streamlined steps to select the RTE paradigm to derive and evolve DT service classification during either advancing or introducing the DTs. The published work PW10 presents the DT service classification phases.

Characterizing RTE activities (Step 1): Identify the RTE activities and their association in the marketplace involving DTs. The RTE manages the activity map and associated DT capabilities. For instance, the healthcare monitoring marketplace introducing the additional capability to notify the current health condition remotely is an example of the DT capability.

Recognizing RTE paradigms (Step 2): The DBOs are diversified based on the characteristics of DT services to accomplish the goals of a specific RTE paradigm. This diversity needs to be captured into the RTE's activity maps associated with the DT services. For example, the type of BP associated with issuing the mobile-enabled discount coupon for the customer registered online in the loyalty program differs from BP associated with the in-store purchases without the mobile coupon. The purpose of the BP, characteristics of BP activities associated with BPs, and functionalities of DT services in correspondence to BP activities play a significant role in determining the classification of the DT service concerning the BP. The RTE paradigm is BP in this scenario. The DT service classification described in Chapter 6.1 to Chapter 6.5 is derived from the identified RTE paradigms in this step.

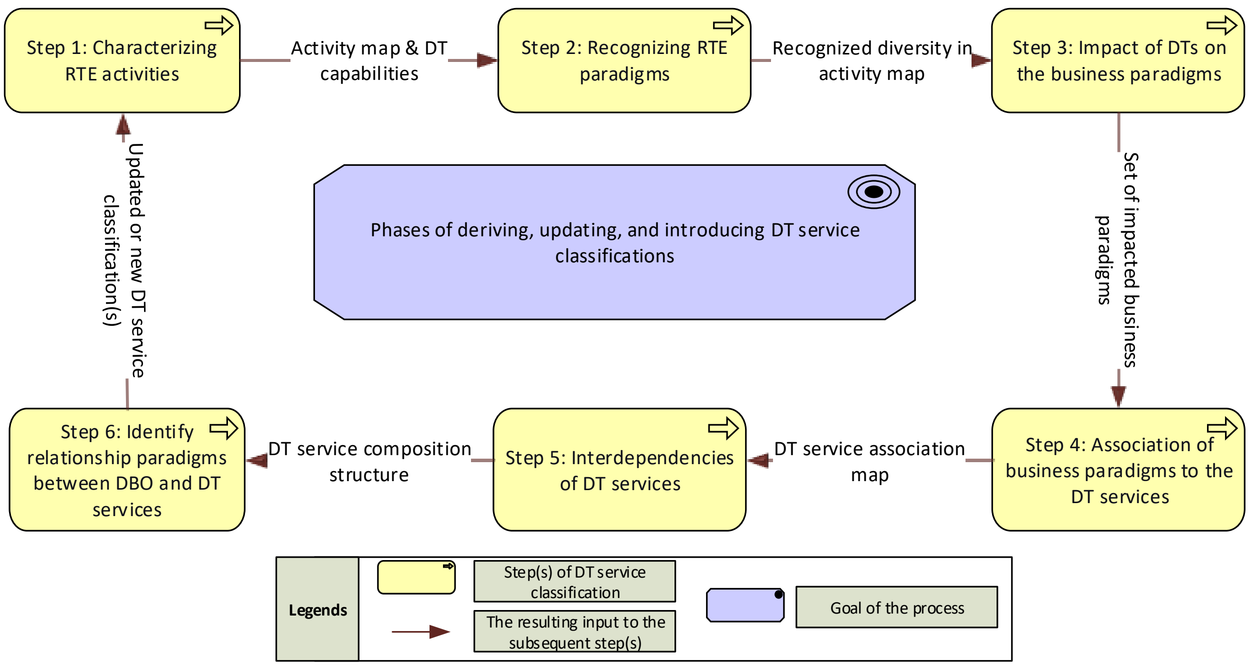


Figure 8: Phases of deriving, updating, and introducing DT service classifications

Impact of DTs on the business paradigms (Step 3): The subsequent step is to capture the effects of advancing or introducing DT and corresponding DT services on the business. The business paradigms can be economical, strategical, or environmental. Capitalization of new products and services, revenue generation due to the introduction of specific DTs, and changes to the tax structure due to online offerings are examples of business paradigms. The most prominent example of the impact of DTs on business paradigms is the introduction of a new eCommerce website instead of partnering with a third party to sell online. The new eCommerce website effectively reduces the overhead of selling and commissions. However, it experiences a reduction in immediate reachability to third-party consumers, resulting in less revenue.

Association of business paradigms to the DT services (Step 4): This phase captures the association of the DT services to the identified business paradigms impacting the RTE. In the above scenario of the new electronic commerce website, capturing the number of items sold and corresponding revenue for the specific timeframe through the online services is an example of an association between business paradigms and DT services. It indicates that the set of DT services is associated with the particular product's volume management in the RTE supply chain.

Interdependencies of DT services (Step 5): Chapter 3 Figure 5 presents the specification of the DT service. Depending on their construct, the DT services can be atomic or composite to associate them with the DBOs. The interdependencies of DT services are required to capture for constituting composite services. The most prominent example is combining the inventory and presenting production cycle information to the actual number of items sold to provide the supply information for the specific product brand. The composite DT service is unique for the DBO and has a unique identifier in the RTE. However, suppose the composite DT services are reutilized differently from the other DBO. In that case, it is accounted for as a separate relationship during the DT service classification and the corresponding evaluation paradigm to assess the DT service classification as indicated in Chapter 8.2 to compute the degree of coverage.

Identify relationship paradigms between DBO and DT services (Step 6): After the association of business paradigms and identification of the interdependencies, the next logical step is to identify the relationship paradigms between the DT services and the multiple DBOs. It will decide the precise classification for the specific DT service. The relationship paradigms between the pricing DBO and the DT service to determine the supply are frequency of production, the ratio of selling a particular product, and the rate of change in pricing.

The DT service classifications can be diversified and customized based on the advancements in DTs and their impact on the DT capabilities. The primary concern is the standardizations of the DT service classification across multiple industry segments and the varied characteristics of DTs capabilities to the recognized RTE paradigms as described in Step 2 of Figure 8. The primary criteria of the recognized RTE paradigm to derive the DT service classification are defined to characterize the impact on business paradigms and identify the relationship paradigms with DBOs. The primary criteria of the recognized RTE paradigms provide the means to specify the DT service classification under the recognized RTE paradigm as described in Chapter 6.1 through Chapter 6.5.

6.1 PW5: DT service classification based on BPs and BP activities

The BP is the RTE paradigm since it is associated with one or more DBOs within the RTE architecture and utilizes diversified DT services. Considering their complexities and the number of BP activities that form the BP, each BP activity needs to depict the behavior of the actual DT service, as indicated in Figure 9. DT service categories are identified based on the characteristics of BP activities associated with the BPs (utilized by the DT service) described in the published work PW5. Additional DT service types can be introduced depending on the progression of RTE in the presence of DTs. Figure 9 provides DT service classification based on the BPs.

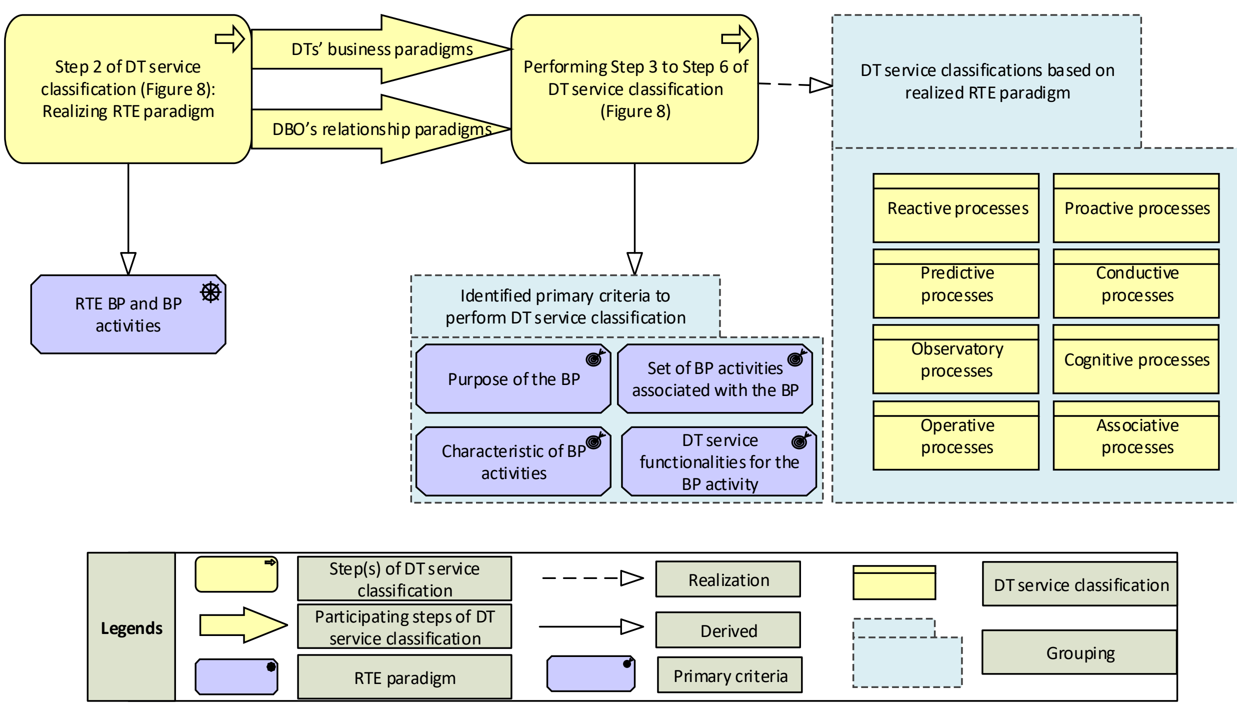


Figure 9: DT service classification based on the BP and BP activities

- **Reactive processes**: BPs with BP activity responding to change propagation at runtime characterizes the reactive processes. Car manufacturer's factory automation was moving from one stage of assembly to another needs to react based on the specific intermediate qualitative conditions of the stage completed is a reactive process.

- **Proactive processes**: They are the set of BPs that deals with the expected occurrence of the BP activities and defines the controls to the BP activities. Runtime policy management and invocation for the human resource department are examples of a proactive process.
- **Predictive processes**: The BP activities of the RTE's BP need to provide the predictive results based on the specific set of information categorized under the predictive process. Hourly weather prediction is an example of a predictive process.
- **Conductive processes**: The BP performing a specific task invoked to complete the sequence instantiating the periodic events are considered a conductive process. The billing to the customer is an example of a conductive process.
- **Observatory processes**: The BP activities to observe specific situation is categorized as observatory process. Monitoring the sale of the product falls in the category of observatory process.
- **Cognitive processes**: The BP contributes to mature RTE in acquiring information and setting conditions based on the paradigms defined to gain appropriate result falls under the cognitive process. Providing discounts based on the consumer's historical purchasing or loyalty points is a BP activity of the cognitive process.
- **Operative processes**: When BP needs to operate based on certain prior conditions to produce the defined set of outcomes, it is an operative process. Automated dental treatment and cleanup is an example of an operative process.
- **Associative processes**: They are generally those BPs that associate BP activities with roles and responsibilities in the RTE. For example, the manager's role differs from the employee. However, during the annual appraisal and assessment activities, they must follow steps in coordination.

6.2 PW6: DT service classification based on digital activities

To provide the actual characteristics of any DBO, it is necessary for each RTE participant and associated DT services need to enable one or more digital activities. Suppose any RTE participant generates ad-hoc activity that is not associated with any digital activity and contributes to responding to digital activity. In that case, the RTE architecture will not recognize the necessity of a specific DBO. The DT services react to the set of events associated with the digital activities to recognize the diversity in DBO, as described in Step 2 of Figure 8. These DT services can be independently built utilizing one or more types of other DT services placed in the RTE. The following is the list of identified categories of DT services depending on their characteristics of responding to an event associated with the digital activity, as indicated in Figure 10.

- **Competency services**: The DT services satisfy the core business offering competencies categorized as competency services. Certain features between different versions of the same product line are generic and essential. However, some features need to be distinguished in the DT service. For example, the difference between a universal life insurance product versus the whole life insurance differs in terms of the premium payment and agreement to the terms of return in real-time.

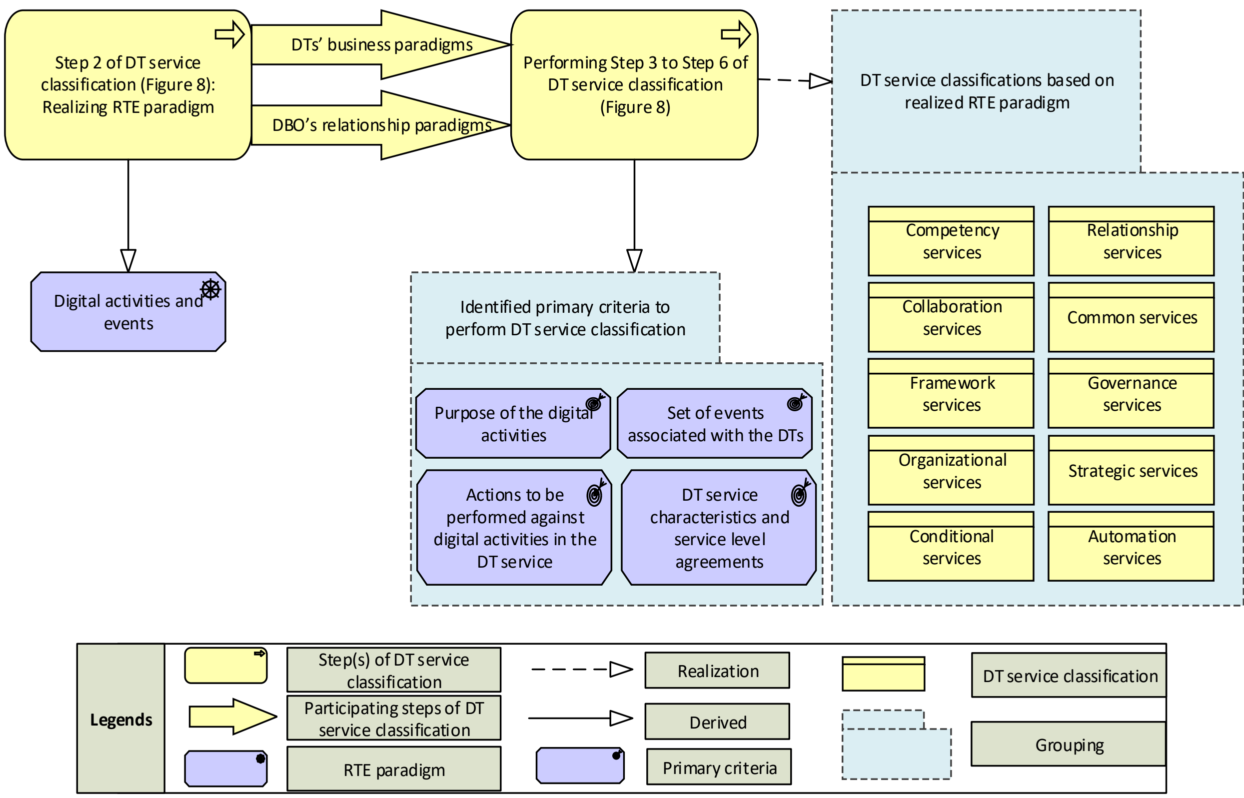


Figure 10: DT service classification based on the digital activities

- **Relationship services**: The relationship service represents the external and internal relationships of the RTE application component with the roles associated with the DT service's functionalities. An example of a relationship service is the relationship of orders placed within the eCommerce platform that includes products by multiple suppliers. The corresponding action needs to differ in the operations of DT service depending on the discount coupons offered by the specific supplier for the specific product. Even the inclusion of the warranty for the specific product offered to the consumer differs from supplier to supplier.

- **Collaboration services**: Any DT service offering collaboration among various RTE application components and BP activities is considered the collaborative service category. For example, a call schedule to receive the customer feedback on their service call or agent experience is an example of the collaborative service. In this example, the participants are the customer, service agent or service, surveyor, data analysis team to formulate insights, and the RTE manager to improve the customer experience.
- **Common services**: When an enterprise gain maturity, it needs to have a standardized audit, log, and monitor capability. This standardized DT service falls in the category of common services. The common services consistently utilize multiple activities with specific objectives to monitor. For instance, *generating invoices* and the *amount paid* for an order are different BP activities. However, the number of items purchased is the same, and they are required to monitor and verify BP activities.
- **Framework services**: The framework services increase awareness of the RTE's technology architecture capabilities. DT service built to search metadata associated with the application, data, platform, or infrastructure services is an example of framework service. The DT service differs in terms of the type of metadata for the variety of services.
- **Governance services**: DT services deployed to ensure the policies, procedures, and defined practices are the governance services. Most diversification to the security-related services, including role-based entitlement, are the participant of governance services.
- **Organizational services**: Organization culture has various impacts on BP activities. DT services that offer a shared understanding of organizational culture and corporate processes are the organizational services. Ordering and utilizing office supplies for different departments is an organizational service. In this example, DT service differs in terms of accessibility of type of supplies to the department.
- **Strategic services**: DT service determines the strategic direction, and corporate goals fall under the strategic services classification. Financial analysis-based selection of marketing segments and budgeting based on available statistics of annual spending are the types of strategic services.
- **Conditional services**: Certain BP activities require special attention and business logic dedicated to the condition. The DT services built, updated, and maintained to accommodate such scenarios

are subject to this classification. A credit card with a special privilege for purchases over-allocated limit is an example of such DT services.

- **Automation services**: Automation services are defined and utilized to introduce the desired level of automation, yielding additional business value for new or existing activities. Typically, automation-related services require stronger bonding and maturity at the activities. The service to send email notifications for the approval versus the service for the online approval process is a typical example of the type of DT service.

6.3 PW10: DT service classification based on DT's business paradigms

RTEs can diversify and customize DBO stemming from DTs' advancements and their impact on the business paradigms. The primary concern is the standardizations and changes to the DT services across multiple industry segments and varied characteristics of DT, and its effect on the diversity of DBOs in terms of business paradigms as described in Step 2 of Figure 8. The DT’s business paradigms include the capitalizing and supply-chain of product or service offerings, including inventory management system, vendor association and management, marketplace collaboration and partnership, and RTE participants of supply-chain management. The following categories are based on the operability of DT services and their direct correlation between DT impact on the DBOs, as depicted in Figure 11.

- **Synergistic**: DT services that formulate the DT paradigms categorizes as synergistic DT services. Radio-frequency identification (RFID) services for inventory management are one of the examples of synergistic DT services.
- **Cooperative**: If DT services cooperate with DT's business paradigms, they are cooperative DT services. The relationship between pricing and the supply of products is considered a cooperative service since pricing must cooperate with the supply equation.
- **Conflictive**: The logical evaluation in electronic commerce operations needs to verify the conflicts between the outcome of the IoT services and the core norms of DT’s business paradigm. In such a scenario, DT services fall into the conflictive category. For example, communication channel agreements conflict in security functionalities due to real-time information of wearable devices' smart services with different methods of performing security functionalities.
- **Cognitive**: The characteristic of cognitive DT services is the embedded decision in DT’s business paradigms based on the intelligence recognized from the available data and information. IoT

services leveraging the Big Data for predictive analytics and corresponding decisions of the eCommerce market model are examples of cognitive DT services.

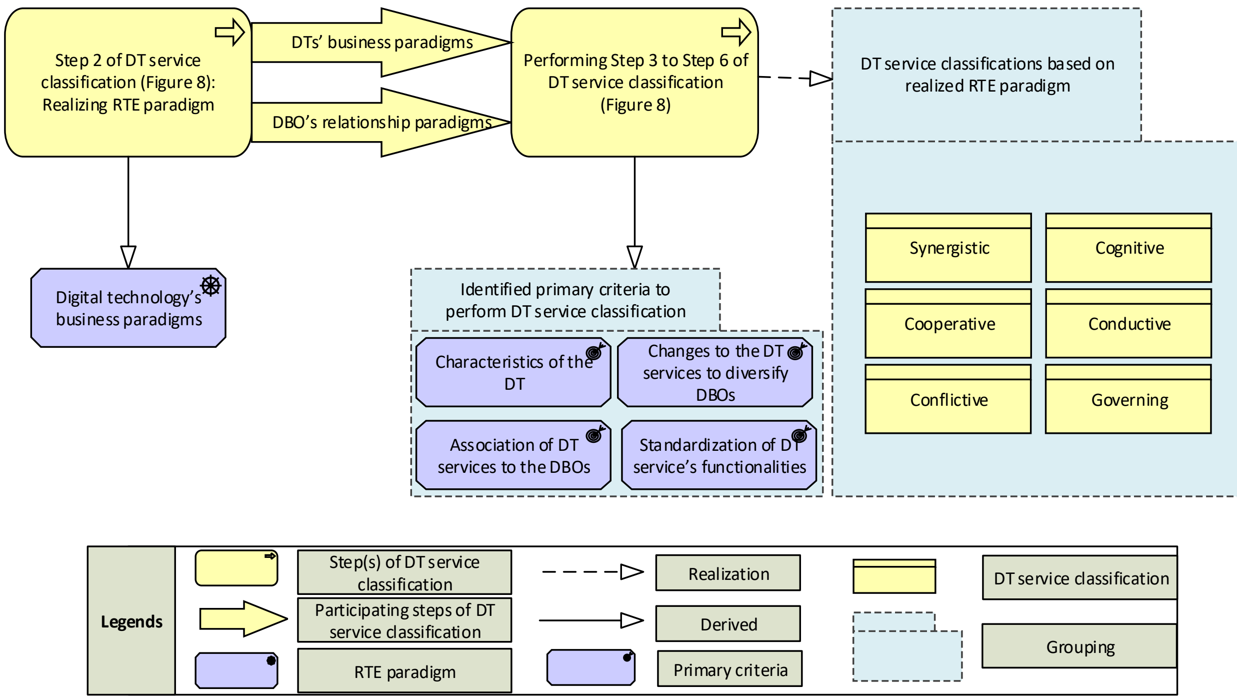


Figure 11: DT service classification based on the DT's business paradigms

- **Conductive**: If eCommerce operations, functions, and actions associated with DT's business paradigms are of the anticipated outcome of the DT services, then DT services are classified under conductive DT service. For example, automated IoT-enabled manufacturing services are dependent on the granular DT services to determine the accurate inventory in production based on the demand and supply ratio.
- **Governing**: When DT services govern the DT's business paradigms, then they are considered governing DT service. The governing of inventory cost based on the reduced manufacturing cycle time captured through IoT service is an example of governing DT service.

6.4 PW8: DT service classification based on RTE processes

The RTE processes differ from the pace of DT adaptation and paradigms of the DBOs associated with the DTs. The primary concern is to determine the correct classifications for the RTE processes that are abstract enough to streamline the implementation across multifaceted RTE participants in the diversity of the DBOs, as described in Figure 8 Step 2. The primary criteria to identify the impact on business paradigms and relationship paradigms with DBO includes responsibilities of RTE process, type of RTE participants performing RTE process, activities of RTE process associated with the DBO, and the service level agreements between the RTE participants. The following are the identified types of the RTE processes in correspondence to deriving DT services classification as indicated in the published work PW8. Figure 12 provides DT service classification based on the RTE's processes.

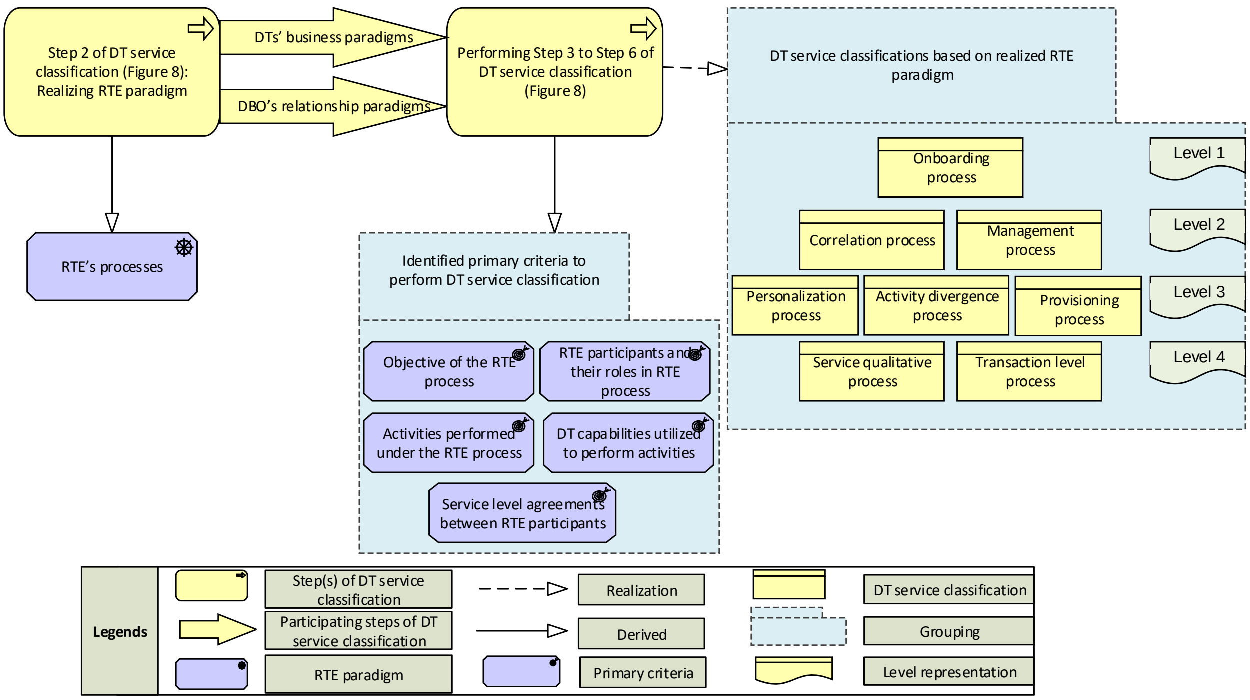


Figure 12: DT service classification based on the RTE processes

- **Onboarding processes**: The processes defined, derived, and implemented to onboard RTE participants, including consumers, retailers, suppliers, distributors, banking, and manufacturers, are categorized at the highest level of the RTE process hierarchy. Introducing a specific supplier to the RTE's supply chain for a product or service is an example of an onboarding process.
- **Correlation processes**: The processes leveraged and built to provide the correlation to DBO for BP activities, participants, dimensional factors, service level agreements, and other external or internal dependencies defined in RTE operational governance framework (Chapter 4) can be categorized as correlation processes. It maintains the integrity and relationship among various types of DBO and subsequent levels of processes within the RTE. The process of associating

privacy paradigms with secure mobile payment during the online transaction for specific business activity is the correlation process.

- **Management processes**: The processes created to manage DBO through the RTE operational governance framework fall under the management process. Upgrading, deploying, and working versions of mobile payment DBO for different BP activities and monitoring corresponding metadata for service level agreements related to the BP activities are the example processes of the management process category.
- **Personalization processes**: The processes placed for the personalization and changing the participants' preferences fall under the personalization process classification. For instance, instantiating alerts for certain types of transactions for retailers is one type of personalization process.
- **Activity divergence processes**: Any process that leads to the divergence into the activity categorized in the activity divergence process. The mobile payment must undergo a payment gateway for utilizing a particular payment method through consumers' mobile devices. It is an example of the activity divergence process.
- **Provisioning processes**: Processes associated with dimensional provisioning factors defined in RTE operational governance framework (Chapter 4) and related resources fall under the provisioning process classification. Leveraging digital signatures and related technologies across RTE participants for authorizing online transactions is an example of the provisioning process.
- **Service qualitative processes**: The processes introduced to either improve, change, or upgrade the quality of the services to the participants of the RTE characterizes the service qualitative processes. It also includes processes to improve scalability, reliability, and performance. Resource allocation and improved quality of the connectivity for mobile web to increase response time and turnaround time are examples of the service quality process.
- **Transaction level processes**: The transaction-level process deals with transactions across multiple participants of the RTE supply chain. Enforcing the prohibition of unauthorized transactions for the specific BP activity associated with mobile payment DBO based on the supplier's or retailer's preferences is the type of transaction-level process.

6.5 PW7: DT service classification based on RTE policies

After establishing the RTE architecture, the primary concerns are the placement and evolution of policy classifications based on the advancements of the RTE ecosystem and the corresponding participation of the DBOs. This chapter identifies initial classifications of the policies based on the policy provisioning lifecycle discussed in Chapter 2.6.1. The subsequent step is to provide these classifications across RTE participants consistently.

The RTE policies are simplified representations of rules to the capabilities and functionalities of DT services. Different illuminating hierarchy of rules within the DBO utilizes different classifications. The DT service classification based on RTE policies emphasizes a precise representation of the characteristics of the RTE policies concerning the DBO. The identified classes of policies and associated DT services to effectively implement the RTE architecture framework are listed below and described in the published work PW7. Figure 13 provides DT service classification based on the RTE policies and the primary criteria to base the diversification in DBOs, as described in Figure 8 Step 2, due to the RTE policies.

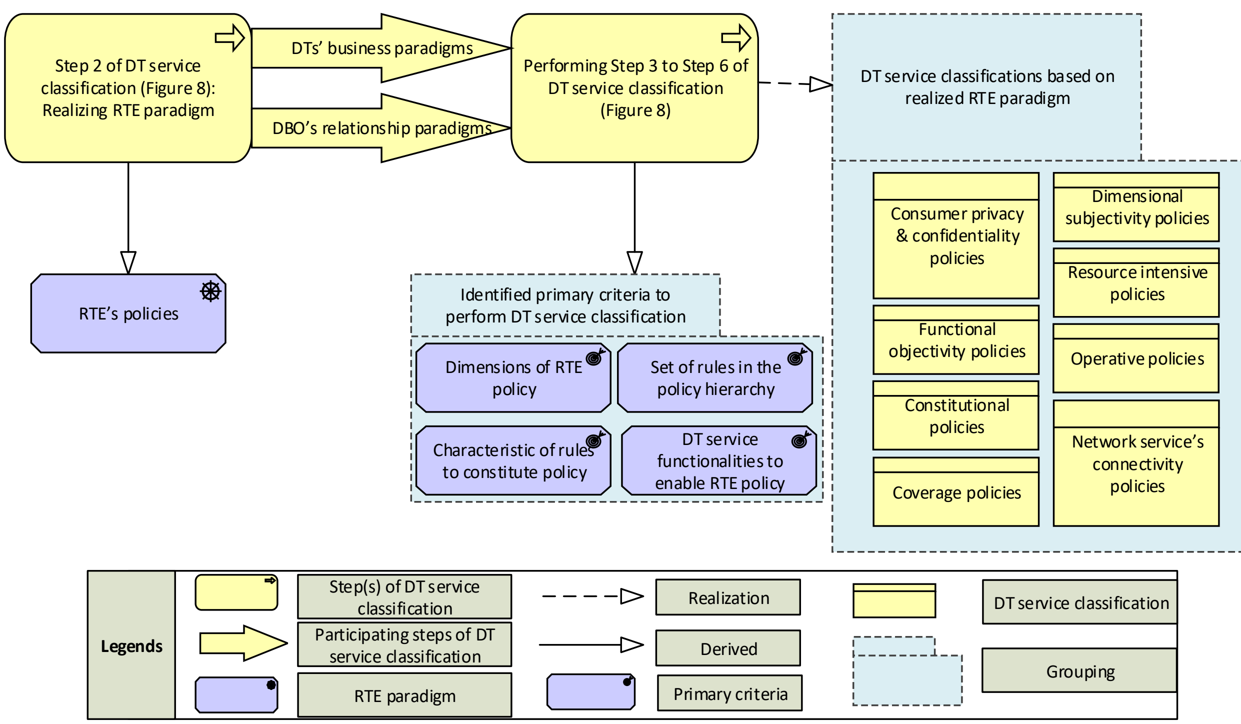


Figure 13: DT service classification based on the RTE policies

- **Consumer privacy and confidentiality policies**: Consumer privacy and confidentiality policies represent policy APIs developed to extend and monitor consumer privacy and confidentiality at various levels. For instance, sharing the patient information with a third party depends on either the patient's approval or the type of entities requesting it (for example, the local justice department or marketing department of a pharmaceutical corporation).
- **Dimensional subjectivity policies**: It is a set of dimensional factors (as described in Chapter 4) specific subjective policies that require to be enforced based on the characteristics of the consumer in consideration of the dimension. The DT service can have the further subsequent level of classifications. For example, the hospital administrator registering and treating the patient in the emergency is not allowed to transfer or discharge patients except with the informed consent or stabilization of the patient's condition requiring transfer based on emergency medical treatment and the active labor act [69].
- **Functional objectivity policies**: Functional objective policies are dimensional factor-specific functional objective principles where the function of the DT service determines the dependencies on the dimension. The difference between functional objective policy and DT service is the dimensional factors with multiple decision points. In the above example, if the patient does not require emergency services, the hospital can transfer, recommend, and discharge based on the patient's Medicare status.
- **Resource intensive policies**: Policies required to utilize any RTE resource, including hardware, software, cloud, external, internal, and network, are considered resource intensive policies. Policies and necessary consent to monitoring the patient's wearable medical devices transmitting and receiving data through RTE connectivity are examples of resource-intensive policies.
- **Constitutional policies**: The constitutional policies-based DT services include those derived from leveraging a specific set of DT services and orchestrations. The overlapping policies to control the car's speed based on the patient's heartbeat count exemplify the constitutional policy-based DT service.
- **Operative policies**: The operative policies are typically any operational constraint of a specific dimensional factor required to enforce in the DT service or corresponding functionalities. The Workload-related quality-of-service policies to the set of DT services are the classic example of the operative policies that also restrict access to the bandwidth consumption by the DT services.

- **Coverage policies**: Usually, the restraining criteria for DTs in terms of any specific dimensional factor fall into coverage policies-based DT service. The most prominent example is the healthcare monitoring DT services are needed to be enforced only for the registered patients.
- **Network service's connectivity policies**: Network service's connectivity policies address the accessibility of network connectivity and corresponding services by any participant network element within RTE. Security policies to access DT services, whether from cloud-to-cloud or cloud-to-on-premise, are classified in this category.

This chapter derives the DT service classifications based on RTE paradigms, including BPs, DT's business paradigms, RTE processes, or RTE policies. The DT services are constantly evolving in synergy with the DT capabilities to advance the RTE architecture. It is necessary to recognize the new or subsequent level of classification of the DT services under the classification of each RTE paradigm. It is also mandatory to continuously evaluate the DT service classification to evolve in the measurable and standardized evaluation paradigms. The different DT service classification mechanism provides a distinct equation to measure the progress of the RTE architecture. Chapter 8 presents the derived methods and equations to evaluate the progress of RTE in the presence of DT service classifications.

CHAPTER 7.

PW3: SCENARIO-BASED CLASSIFICATION OF THE DIGITAL TECHNOLOGY SERVICES

The possible states or changes in the state of the DBO due to the occurrence of specific digital activity instantiated by the RTE participants or invocation of DT service(s) associated with the DBO define as the scenario in the RTE ecosystem. The DBOs and their impact on RTE differ based on DTs' evolving characteristics corresponding to DT services, resulting in the updated or new scenario [70] and [71]. The most prominent example is the online movie rental industry. It gradually introduced the DT services that did not even exist during the traditional way of renting movies from the stores. For instance, the scenario of introducing DT service is to validate and restrict the number of simultaneous logins and devices to stream the video of a rented movie for a specific customer. The other scenario introduces capabilities to evoke the video streaming content when the user paused the video in the previous session. Usually, this type of scenario recognization occurs during the later stages of development after deploying the DTs or the products and services.

All scenarios represent combinations of plausible narratives of the DBO for the specific DT service. Depending on the type of industry vertical, scenarios differ in composition. Scenarios that pursue well-known causal or functional relationships with the DT services tend to vary primarily in their assumptions of either current or future digital activities. Multiple actors and factors accompanying the various scenarios describe the future of utilizing DT services for the specific DBO for the particular digital activity or set of digital activities.

The primary contribution of the published work PW3 is the scenario-based classification of DT services. It provides a mechanism for RTE to rationalize individual DBO and their use of DT services in correspondence to the actual digital activity or the RTE's internal event. Figure 14 presents an approach to identifying categories of scenarios. The published work PW3 presents the steps to identify categories of scenarios. The paramount consent to derive the steps is the DBO to correlate incremental risks, DT capabilities, and industry-specific compliance. The DBOs can be related to multiple DT services and, correspondingly, multiple categories of scenarios that invoke either a specific DT service or a set of DT services. The technique employs six sequential steps to categorize these scenarios as described in the published work PW3 and articulated in Figure 14.

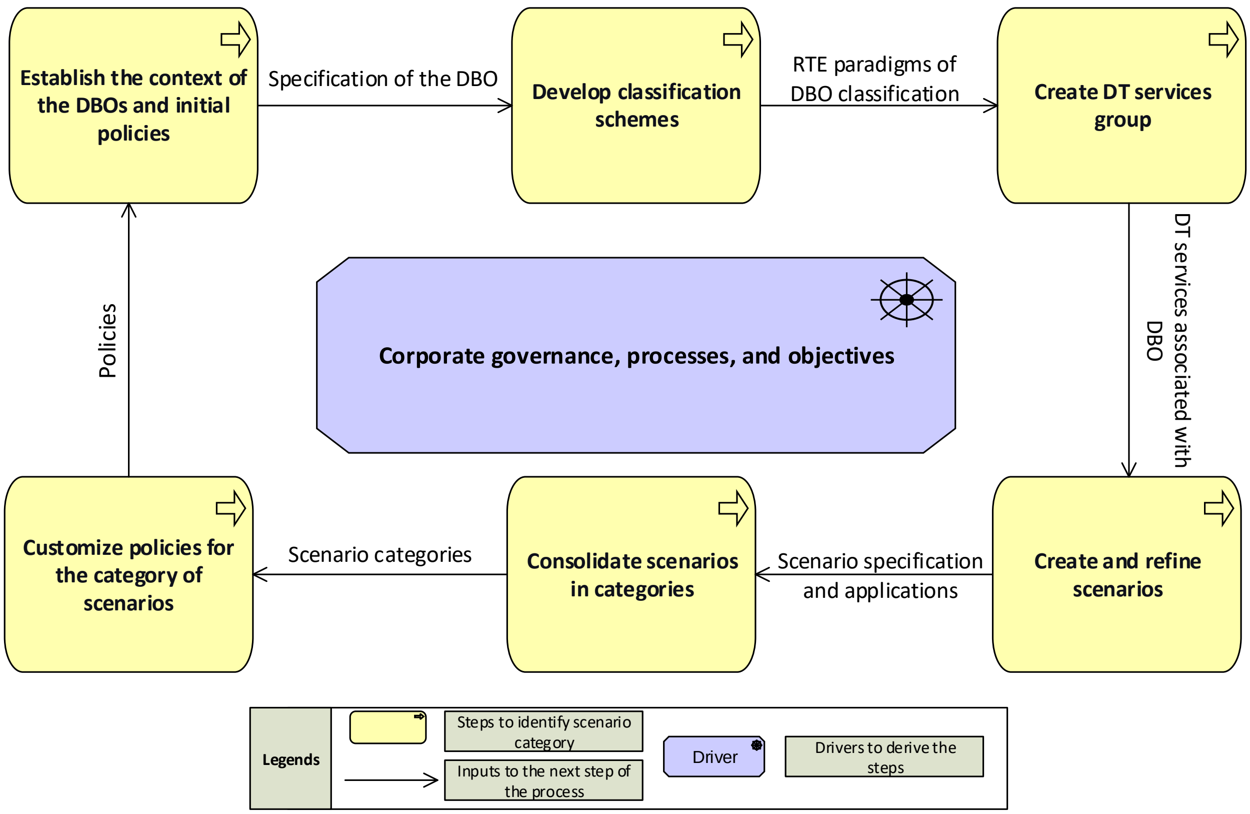


Figure 14: Steps to identify categories of the RTE scenarios

Establish the context of the DBO: Establishing context for the DBO is to collect and record information that will guide the DBOs. One part of establishing context is scoping the DBOs to consider a specific set of DTs. Another aspect is identifying the DT capabilities as DT services to implement the specific set of DBOs. The context of the DBO and corresponding DT capability are scaled to assure that all RTE participants consistently respond to the specific scenario and adhere to the objective of the DBO. In facilitating online movie rental with streaming videos through the internet, the initial DT capability and granular scope for a DBO can be "registering an online account." The policies are employed gradually in the identified context of the DBO. However, it can be employed instantaneously if specific policies are already known while contextualizing the DBO. For example, the DT service for registering an online account needs verification before setting the password for the online account.

Develop classification schemes: The classification scheme categories scenarios and the policies of the DBOs. Typical classification scheme groups scenarios according to goals (example: consumer certification), DBO life-cycle phase (example: manage invoice), the focus of activity (example: process payment), or usage (example: check account balance). The classification schemes also provide a shorthand for discussing groups of scenarios and policies and support efficient communication among RTE participants. Classification schemes developed as input to scenario generation.

Create DT services group: The DT service groups are created based on the similarity in actions performed by DT services in the diversified scenarios. An example is the DT services associated with consumer security at various levels of the DBO. The security can be at the transaction or the application level. The corresponding DT service group remains intact for any type of scenario. However, the severity of the impact differs for transaction-level security versus application-level security.

Create and refine scenarios: The scenarios are generated independently by the DT service groups established in the previous step. In this stage, generating appropriate scenarios that provide broad coverage of DBOs is performed. The initial round elicits a comprehensive range of granular elements of the RTE scenarios. It considers a set of scenarios that address as many DT service groups within the classification scheme as possible by situational analysis that could lead to concerns of a DBO or set of DBOs. The issues could be alleviated if existing corporate policy or control is in place. For example, a concern under administrative privilege could be providing access to unauthorized third-party data. A concern under payment technology could be inconsistent payment gateway use by the third-party vendor providing payment authorization.

Consolidate scenarios in categories: The goal of consolidation is to reconcile and merge the work of the various DT service groups to identify the scenario policies for the RTE. Several dilemmas may arise during the consolidation of scenarios generated by the different DT service groups. They are required to be considered at this stage to identify the categories. Several scenarios across DT service groups appear to be similar since they utilize the same group of DT services. However, they are different, and elements of a scenario conflict with one or more scenarios based on the characteristics of the RTE participants and associated policies. An example of a scenario that generates conflicting policies or mechanisms to address the same situation is the required prohibition of consumers' access to and purchase specific products or services under 16. It is necessary to know the age of the consumer in this case. The example indicates that it needs reconciliation on a case-by-case basis when deriving categories of scenarios.

Customize policies for the category of scenarios: The primary objectives at this stage are to produce a single set of implementable policies and other scenario elements. This step is mandatory and responsible for ensuring that the policies cover the identified RTE scenarios and update the respective policies in adherence to the RTE operational governance framework. For example, manage the accessibility of the products and services prohibited for consumers over age 16.

7.1 PW3: Classification based on incremental risks associated with DT services

The scenarios can be categorized based on the RTE's ability to recognize the incremental risks associated with the DT services and the specific set of actions. The incremental risks are associated with the DBOs, and they formulate the basis to categorize the DT services as described in Figure 8 Step 2. The following represents types of scenarios identified to associate DT services alongside the incremental risks of DBOs as described in the published work PW3 and listed in Figure 15.

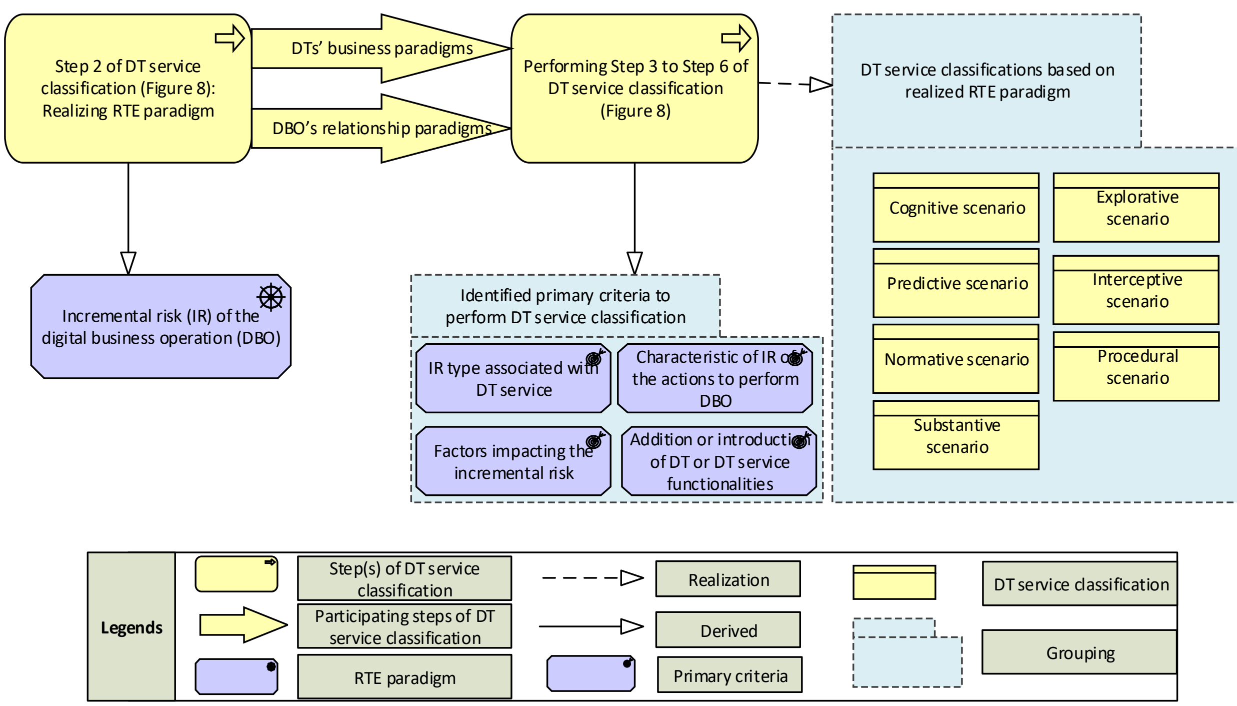


Figure 15: RTE scenario classification based on the incremental risks associated with DT services

- **Explorative scenario**: This type of scenario explores the potential outcomes of DT services under the influence of incremental risks embracing the available knowledge, known processes, or past trends to assess the possibilities. The explorative scenario does not involve significant interventions or paradigm shifts in the RTE. The explorative scenario can also describe future DT service functionalities that bifurcate at some point. An example is the uptake or rejection of a new DT capability or making assumptions about regulation or adaptation of DT during the constitution of the DBO. The simplest form of explorative scenario is a direct extrapolation of past trends.
- **Predictive scenario**: Predictive scenarios give a relatively detailed and quantitative indication of how the RTE reacts to the change under a set of DBOs. Statistical extrapolation of trends or a deterministic model of reality constitutes the predictive scenarios. If the scenario predicts the ambient environmental conditions or human exposures and incremental risks, it is under the predictive scenario category. Anticipating the increase or decrease in the price due to the associated incremental risks is the form of predictive scenarios.
- **Properties scenario**: The properties scenario depicts the alternative futures of DBOs or contrasting trends that might differ from the present due to incremental risks of the DT services. They enable decision-makers to anticipate their reactions to alternative future possibilities, expect timeframes beyond the immediate future, and make choices. They must include a description of the present situation, several alternative futures, and possible pathways connecting the present with images of the results. If DTs are unmatured enough to establish automation of the DBOs, then property scenarios are utilized.
- **Interceptive scenario**: An individual DBO has added responsibilities in interceptive scenarios. The DBO temporizes a static occurrence of incremental risks for additional evaluation in the RTE. It intercepts the typical characteristic of DBO and dynamically adds behaviors without affecting any other RTE architecture components. The interceptive scenario can help manage cross-cutting concerns that access standard features such as logging or validation of RTE participants or users.
- **Substantive scenario**: The substantive scenario focuses on delivering essential functional expectations of groups of DT services. It deliberates the extensibility and maintainability of the DT services under the incremental risks. Substantive scenario facilitates functional and non-functional requirements of the specific business aspect associated with the DBOs. It is to sustain the high priority investment to capture market share and a particular set of consumers. The most prominent example is the fraud prevention mechanisms for eCommerce’s online transactions.

- **Procedural scenario**: The procedural scenario ensures the sequential execution of the functionalities of DT services and resolution of the interdependencies within the specification of the DBOs. It estimates the relative frequency of incremental risks occurrence concerning the DBO, which can be discrete or continuous. The typical example of the procedural scenario is the reaction and procedure to follow during fraud inducement of electronic commerce’s online transactions.

7.2 PW1: Classification based on DT service capability utilization

The scenario classification based on the utilization of DT service capabilities emphasizes precisely representing the characteristics of the DT service capability for the functional aspects of the DBO. It represents identified DT service capability utilization to perform the specific functions that the DBOs anticipate under a specific set of conditions. The DT service capabilities in the diversification of the DBOs determine DT service classification, as illustrated in Figure 8 Step 2. The published work PW1 and Figure 16 depicted the DT service classification based on the DT service capabilities.

- **DT service subscriber**: The DT service subscriber capability has characteristics of implementing the conditions and logic to subscribe to the DT services. It ensures the rationalization of the service requests for a subscriber to utilize the DT service at the correct level of the DTs. For instance, industrial IoT service needs to subscribe to the manufacturing cloud services, ensuring it adheres to supervisory control and data acquisition (SCADA) standardization [72].
- **Information distribution**: The information distribution capability of DT services promotes the information exchange based on a publish/subscribe methodology for the DT services to the RTE or other DT services. The information disseminated through it includes resource utilization, service/unit resolving updates, system status updates, log levels, log entries, and global configuration.
- **Deployment and migration**: The DT services' automated deployment and migration capabilities manage and maintain continuous integration. It carries various types of metadata associated with DT service deployment and migration policies to the DBOs, including versioning and updated association with BPs.
- **User access**: The user access capability specifies users' correlation and authentication information for the DT services. It retains the access policies for DT service or a set of DT services. It can also

specify a group of users that can leverage DT services based on the RTE authorization and authentication criteria associated with the policies.

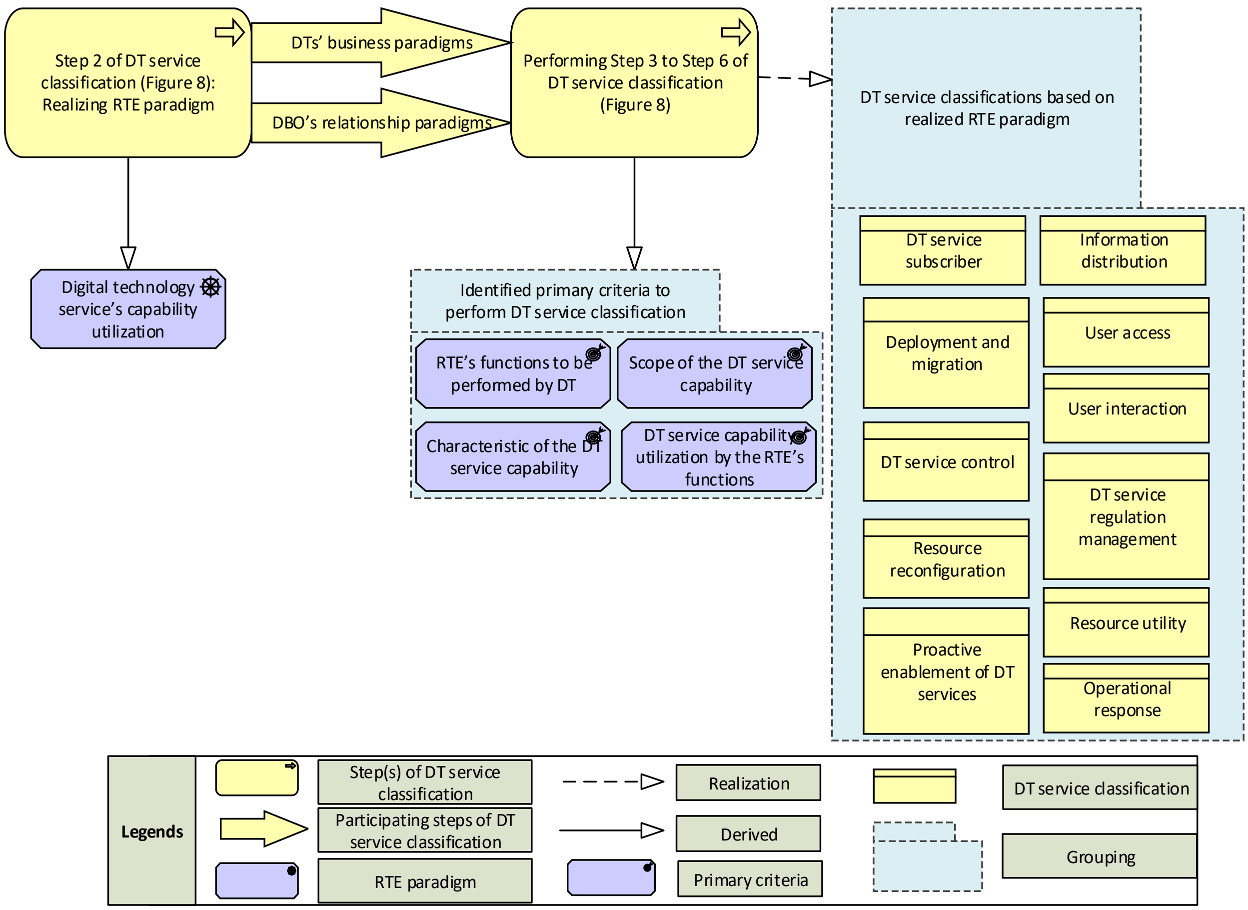


Figure 16: RTE scenario classification based on the DT service's capability utilization

- **DT service control**: DT service control capability derives a degree of control over their actions and internal state corresponding to DT services. DT services should be able to perform tasks based on the specified controls without the direct involvement of the RTE participants. An example is the alerts based on specified limiting factors and actions associated with a specific cloud service for a temperature sensor.
- **User interaction**: Users utilize various devices such as handheld devices, desktops, and tablets. It needs specific user interaction and activities recognition, besides interactions between different applications at the edge. The DT services are responsible for ensuring user interaction activities among other applications and edge user devices.

- **DT service regulation management**: It is a property that regulated industries and their standards cannot keep pace with rapid innovations in DTs. The regulation management capabilities leverage industry-specific regulations and anticipated standards for upcoming DT advancements between DT services and DBOs. For example, the smart grid must accommodate the upcoming regulatory requirements. However, the regulatory requirements of the DTS are currently in draft form by the federal energy regulatory commission (FERC) [73].
- **Resource reconfiguration**: Resource reconfiguration capability specifies, manages, and updates configurations of DT services. RTE participants can change the configuration at runtime. The most prominent example is configuring the wind turbine's rotor blades.
- **Resource utility**: Resource utility capability manages resource utilization and efficiently manages service level agreements between the DT services and corresponding DBOs. The resources may include, however, not limited to data sources, servers or clusters, edge devices, and networks.
- **Proactive enablement**: Proactive enablement capability exhibits opportunities to provide aggregation between DT service and DTs. It enables goal-directed behavioral aspects of the DT service in the DBOs. For instance, the cloud computing paradigm offers flexible and robust storage and computing resources, enabling dynamic data integration and fusion from multiple data sources to DT services at runtime.
- **Operational response**: Operational response perceives the DT service-specific operational environment of the DBOs. RTE anticipates DT services to respond on time to changes in the operational environment of the DBOs, including unavailability of the specific operational service, including external cloud services, security services, monitoring services, logging services, and alerting services.

7.3 PW11: Classification based on compliance-aware DT services

The compliance-aware DT services instantiate a set of rules associated with RTE's DBOs' scenarios. Typically, rules have three parts: events, conditions, and actions. Each aspect can have bound to data set queries, functions, or stored procedures. The basic principles utilized to provide the classification scenarios and business rule composition techniques are the characteristics of rules in compliance-aware DT services. The following are the characteristics of the rules inherited to constitute compliance-aware DT services identified in the published work PW11.

- Symbolic: Independent to represent business-specific decisions in association with the DT services.
- Distributable: It has a set of events, conditions, and action measures redistributed with the compliance-aware DT services.
- Ubiquity: It is compatible with RTE environments and can be extended in the future to support a diversity of scenarios or new scenarios.
- Distributed execution: It supports scenarios for the centrally developed but distributed business rules across the RTE.
- Simplicity: It is easy to integrate, update, and operate. It requires no changes in the existing approaches and practices in the customer landscape.

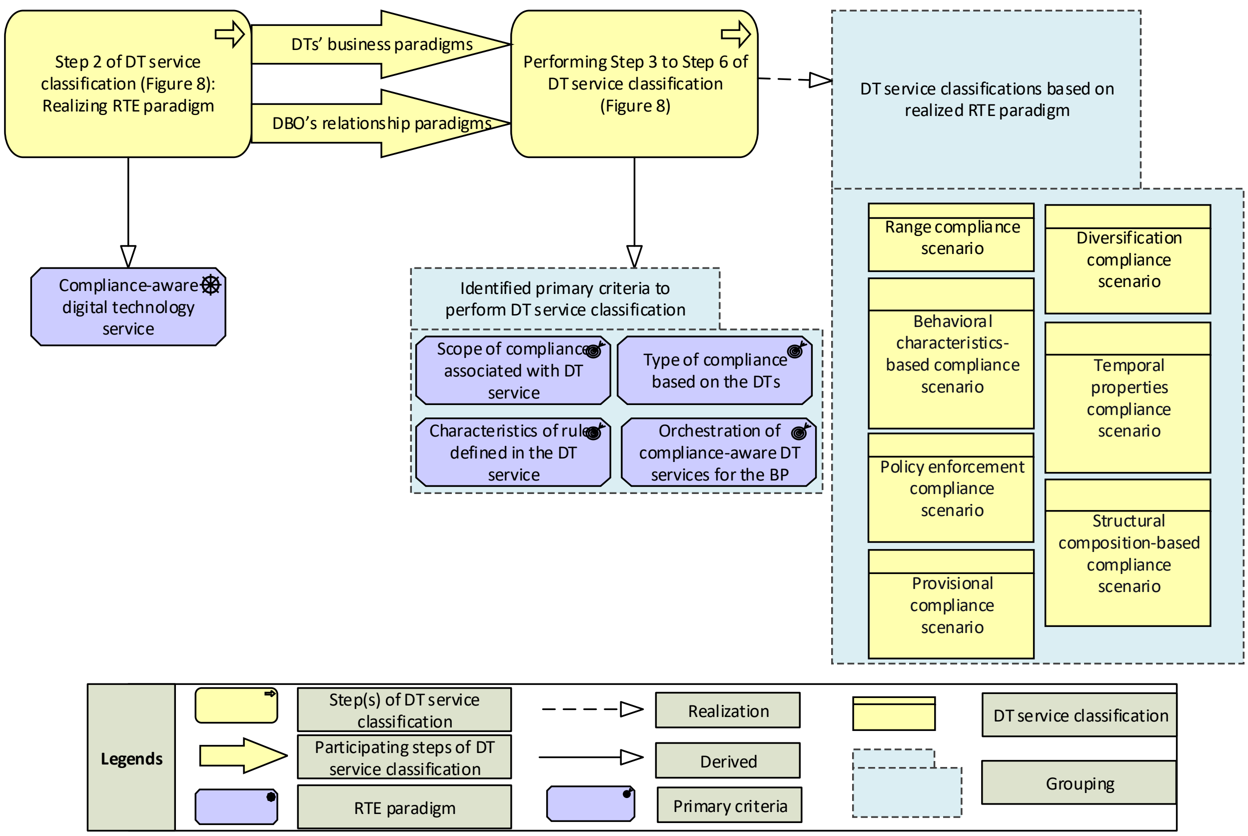


Figure 17: RTE scenario classification based on the compliance-aware DT services

The rule characteristics lead to determining the classification of the scenarios. The published work PW16 describes the method of dynamically constituting and orchestrating the rules in the advancement of DT.

It needs to accommodate a specific type of compliance as a rule or set of rules within the DT services, as depicted in Figure 17. RTE can further expand the classification depending on the progression of the compliances or vicinity of the DBOs within the RTE architecture. Depending on the compliance characteristics related to the scenarios, the following are the scenario classification introduced for the DT services in the RTEs as described in the published work PW11.

- **Range compliance scenario:** The lowest levels of the DT services that inherit rules are generally associated with a range check, whether the date, number or the enumeration defined in the data source. A simple example of the range compliance is that the transaction should be more than $1. However, it should not exceed the limit associated with the credit card. In this example, the limit should be checked for the specific credit card, spawning another DT service.
- **Diversification compliance scenario**: The advancement of the business logic with the specific condition that utilizes particularly identified data set(s) should be considered diversification to the DT service of the rule. The most prominent example is the amendment to contract in adherence to legislation specified by the Texas State can coexist with the dilemma of effective and expiration dates for certain associated retail energy provider accounts specified in amendments. Typically, DT services associated with different versions of the exact compliance are not eligible to be utilized unless a more granular perception is available within the DT services. It makes the DT services and corresponding compliance altogether different from each other.
- **Behavioral characteristics-based compliance scenario**: When DT service depends on human behavior, it should be evolving and flexible enough to accommodate specifics for the presented case. The appropriate example is that the waiver for the late payment differs based on the situation and consistency of the past payment history. The behavioral pattern needs translation into either conditions or actions of the rules. The above example needs to accommodate payment history as a particular condition (placed either as good, weak, or excellent, in terms of enumeration) or as a pre-condition for the rule.
- **Temporal properties-based compliance scenario**: If the events or conditions of rules are associated with timing constraints and are not valid after a specific interval identified using DT services, it falls in the temporal properties-based compliance scenario. For instance, the time limit specifies when to send and receive alert events based on reference timestamps. The RTE can utilize audit logs, temporal service objects, and service level agreements monitoring. Certain temporal aspects are critical, and it should have precise actions in place for DT services. The temporal properties indicate the constraint to an event or upper and lower bound of the timing

aspect of the rule. When the retail energy service provider receives an outage-to-restoration notification after 6:00 PM, it must be processed the next day. The actions to reflect payment adjustment to the account represent temporal properties-based compliance characteristics.

- **Policy enforcement compliance scenario**: The policy framework is a standard terminology that provides policy processing and enforcement features at runtime. RTE can implicitly apply policies to a single rule or a set of rules. The role-based approvals in multiple levels of policies scenario is an example of policy enforcement compliance. The roles-related information needs to be retrieved from underneath data sources or employee's data sets [74]. The RTE can create an enterprise-grade division of categories to enforce the policy framework.
- **Structural composition-based compliance scenario**: Structural binding presented among different DT services or overlaps that need to be precisely identified. The example of offering multiple products to the commercial customer with bundled rate is governed and monitored by the federal energy regulation commission (FERC) [75]. RTE can utilize multiple DT services together to compose rules for various products. However, the conflicts overlap, and additional explicit rules require attribution. Otherwise, it may not provide the expected result. In the above example, multiple products can fall under another product group that can utilize a set of decisions composed of partially binding decisions of the original product type or group.
- **Provisional compliance scenario:** If the compliances are still in development and they are identified based on particular anticipations, assumptions, and customization, then it is characterized as a provisional compliance scenario. The smart grid metering digital initiative is under development by the federal energy regulation commission (FERC), and the RTEs anticipate updates to the security governance paradigms [75].

The notion of each scenario's initial conditions, pre-conditions, and post-conditions forms an absolute entry-point for the rule. DT service-specific conditions and conditions generated due to execution of the DT service. Generally, initial conditions are mandatory to even look at the rule-specific conditions and consequently execute them. Most checks for no values returned from DT service fall in the initial condition category. The RTE much check for facts associated with the rule as initial conditions before checking for pre-conditions. The RTE architecture's digital service layer provides initial conditions in all the DT services related to a specific rule type. Chapter 9 details the continuous evaluation and evolution of scenario-based DT service classification.

CHAPTER 8.

EMPIRICAL EVALUATION OF THE RTE ARCHITECTURE

Due to a lack of maturity and standardization in evaluating the impact of introducing and advancing DTs, the benchmark and evaluation of the RTE architecture are either in the very early stages of identification or nonexistent in practice. This chapter emphasizes providing mechanisms to evaluate the progress of RTE in the presence of evolving DTs.

Chapter 6 discussed the DT service classifications based on the BPs, DT's paradigms, RTE processes, or RTE policies. However, the DT services and classifications constantly evolve in synergy with the DTs and corresponding capabilities to advance the RTE architecture. It is necessary to place and standardize measurements to continuously evaluate and identify criteria to measure the advancements of the RTE architecture during or after the deployment of products or services utilizing new (or updated) capabilities offered by the DTs in terms of DT services. The distinct methods are derived based on the incremental risk classification, identified in Chapter 5, and the DT service classification, identified in Chapter 6, to measure the progress of the RTE architecture. This chapter describes the evaluation properties and experiments for each primary evaluation mechanism.

8.1 PW4: Percentile of incremental risks

The percentile of incremental risk (PEIR) evaluates the incremental risk (IR) categories associated with the DBOs, identified in Chapter 5 during the adaptation or updates of the DTs presented in Chapter 5. It provides an indicative number for the probability of risk occurrences associated with the DBOs under the specific IR category. Table 2 provides the evaluation properties for assessing the PEIR, whereas APPENDIX A.1 details the computing paradigms and results.

Evaluation properties	**Description**
Purpose	The PEIR indicates the RTE architecture's risk management capabilities (Chapter 2.4) based on the identified categories of the IRs (Chapter 5) during the introduction or modifications of the DTs and corresponding DT services.

Characteristic of evaluation	The empirical evaluation computes PEIR for each category of the IR. PEIR emphasizes instrumenting the severity of the IR associated with the DTs to advance the RTE architecture and corresponding DBOs. It computes the relative measures of the risks associated with the DBOs in a specific IR category for the total number of DBOs in the RTE architecture.
Industry vertical	The eCommerce platform's order management system [76] was selected to perform the evaluation.
RTE paradigm(s)	The 6 BPs and the 43 IRs associated with the DBOs were utilized to perform the evaluation. The online registration of the new customers, managing purchase orders, invoicing, and payment were the participant BPs. IR models were built and implemented with project management [77], enterprise architecture [78], and BP management [55] tools.
Production deployment	The experiment included nine production deployment iterations to gradually introduce and evolve 62 DBOs with the selected development and deployment platform [79] and external payment gateway [80].
Results and conclusions	The production deployment in the ninth deployment iteration was found stable in consumer engagement since occurrences of communication, and consumerization IRs were minimal. The occurrence of technology change IR was still higher in the ninth deployment iteration due to the response time associated with the external payment gateway. The pace of updates or introduction of DBOs decreased and stabilized in the later deployment iterations since the deployment rate of new or updated DT services also decreased.
APPENDIX A.1	APPENDIX.A.1 provides the 6 BPs utilized to perform evaluation, computation of the PEIR, the resulting statistics of PEIR for each IR category and overall RTE in the nine production deployment iterations, and the experiment's outcomes.

Table 2: Percentile of incremental risks (PEIR) of DBO: Evaluation properties

8.2 PW5: Degree of coverage: DT service classification based on BPs

The degree of coverage (DoC) evaluates DT service classification based on BPs and BP activities presented in Chapter 6.1. The DoC is the relative measure to indicate the coverage of RTE architecture's functionalities performed by the DBOs and associated DT services. Table 3 provides the evaluation properties for assessing the DoC, whereas APPENDIX A.2 details the computing paradigms and results.

Evaluation properties	Description
Purpose	The DoC directly reflects the number of BPs and BP activities that formulate the RTE architecture's DBO manager (Chapter 2.7) and utilize DT services based on the DT service classifications identified in Chapter 6.1.
Characteristics of evaluation	The DoC provides the relative measure of the RTE's BP activities performed by the DT services in comparison to the previously deployed DT services and the diversification in the BPs or BP activities. The DoC depends on the diversification in the BP activities, the severity of the diversification or change, the number of impacted DBOs, and the dimensional factors of the RTE operation governance framework (Chapter 4).
Industry vertical	The manufacturing supply-chain of industrial IoT devices [81] considered the Big Data as DT services [82] was selected to perform the evaluation. The experiment proactively engaged RTE participants to perform BPs in the manufacturing supply-chain ecosystem [83] to deliver products to consumers.
RTE paradigm(s)	The 42 pre-existing BPs without utilizing DT services were adapted to transform the capturing of the online orders, payment management, manufacturing production plant processes, and dispatching the delivery of products to customers.
Production deployment	The experimentation performed seven production deployment iterations to introduce 23 BP activities and evolve 200 BP activities gradually. Big data architecture pattern [84] and BigData reference architecture's functionalities [82] were utilized to develop and deploy DT services [79].
Results and conclusions	The DoC became steady during the progress from one deployment iteration to subsequent deployment iteration. The reactive and predictive processes requirements were immediately recognized as the DBO manager correlated BP activities with the DT services. However, the associative and cognitive

	processes progressed at pace with the introduction of new DT services. The proactive, conductive, observative, and operative processes remained steady in later stages after the first three deployment iterations. The DoC provides indicative optimization opportunities for RTE architecture and statistical direction to evolve in the marketplace or specific industry vertical.
APPENDIX A.2	APPENDIX.A.2 provides the computation of the DoC in each deployment iteration, the resulting statistics of the DoC for each DT service classification based on the BPs and BP activities and overall RTE in the nine production deployments iterations, and the outcome of the experiment.

Table 3: Degree of coverage (DoC): Evaluation properties

8.3 PW2: Viscosity of DT services based on BPs and BP activities

The viscosity (η) of the DT services evaluates the level of a data services' composition for the DT services associated with the BP and BP activities. The viscosity measures the number of granular data services required to construct the composite DT services associated with the BP activities. The following Table 4 provides the evaluation properties for the viscosity of the DT services, whereas APPENDIX A.3 details the computing paradigms and results.

Evaluation properties	Description
Purpose	DT services' viscosity (η) indicates the efficacies accompanying the RTE architecture's orchestration and correlation engine, presented in Chapter 2.5, to form the service models and orchestrate the data services to cover the BP and BP activities in the composite DT services (or APIs).
Characteristics of evaluation	The degree of API (or composite DT service) coverage (DOAC) was derived to indicate the number of data services supported by the BP activities. However, the capabilities index (CI) measures the variation in the APIs (or composite DT services) relative to the limits of business requirements in each production deployment iteration during the delivery of composite DT services.

	The CI was derived based on the Taguchi capability index [85]. Taguchi capability index was the function of the specification limits, the process, and a provided target.
Industry vertical	The data services of the eCommerce platform's order management system [76] were selected to perform the evaluation.
RTE paradigm(s)	The empirical setup included 85 BPs and 1500 BP activities without using DTs. They were updated to transform the supply chain of the eCommerce partner ecosystem, including onboarding the new supplier (or partner) to dispatching the product(s) from the warehouse.
Production deployment	The experimentation performed seven production deployment iterations to gradually introduce and evolve 242 data services using the DT services development and deployment platform [79].
Results and conclusions	The data services introduced to define the relationships between the data sets were high on viscosity (η) and relatively low on capabilities compared to other data service types during the composition of DT services. The DOAC increases by 46%, indicating the RTE's orchestration and correlation engine evolves service models to compose DT services that correlate with BP activities and their responsibilities.
APPENDIX A.3	APPENDIX.A.3 provides the types of data services, computation of the viscosity, degree of API coverage, capability index, and the results.

Table 4: Viscosity (η) of the DT services: Evaluation properties

8.4 PW10: Degree of fragmentation: DT service classification based on DT's business paradigms

The degree of fragmentation (DoF) evaluates DT service classifications based on DT's business paradigms presented in Chapter 6.3. DoF measures the correlation between DT services and DT's business paradigms numerically. Table 5 provides the evaluation properties for assessing the DoF, whereas APPENDIX A.4 details the computing paradigms and results.

Evaluation properties	Description

Purpose	The DoF assesses the introduction or changes of the DT services due to the external dependencies and data required to formulate the composite DT services in association with the DT services business paradigms derived in Step 2 of Figure 8 in Chapter 6. The DoF indicates the impact of the DT services and their formulation in the RTE's digital service layer presented in Chapter 2.3 based on the DT service classifications identified in Chapter 6.3 using types of BPs and associated BP activities.
Characteristics of evaluation	The DoF provides the relative measure of the impacted RTE's application integration and corresponding composite DT services deployed in previous production deployment iterations to advance the RTE architecture for the internal or external RTE activities. The DoF depends on the DT service correlation factorial (DCF) and correlation impact factor grade (CIGF) during the introduction or changes to the DT services. DCF computes the number of impacted business paradigms associated with the newly introduced or updated DT services. CIGF level indicates the severity of the impact on the business paradigm.
Industry vertical	The eCommerce's online store management of healthcare products and supply-chain of healthcare monitoring accessory products [86] are selected for the experiment.
RTE paradigm(s)	The existing experimental environment included 32 DT business paradigms. The experiment included eight additional DT business paradigms of the eCommerce platform, including pricing, product ontologies, personalization of online stores, digital communication channels, and a dynamic digital market model.
Production deployment	The six production iterations to gradually evolve or introduce DT services. The 25 RTE application integrations (or appliances) and 58 DT services were either migrated or introduced through the DT services development and deployment platform [79].
Results and conclusions	The DoF decreases over the introduction or modifications of DT services, indicating the stabilization of RTE in the advancement of DTs. The DoF of the

	DT service of type governing and synergistic was higher in the initial three iterations. However, it significantly reduced at iteration 6, indicating that these categories of DT services have consistent functional behavior for the specific industry segment. The consistent improvement found in the DoF of cooperative DT service and conductive DT service categories indicates that the DT service for new IoT devices must have minimal generality and abstraction due to the specific divergence required for upcoming advances. The DoF for conflictive and cognitive DT service categories were directly proportional to the number of changes performed to DT services, indicating that they bring the accuracy and desired level of customization to the RTE under the influence of DTs.
APPENDIX A.4	APPENDIX.A.4 provides the computation of the DoF and DCF based on the level of the CIGF in each production deployment iteration, the resulting statistics of DoF for each DT service classification based on the DT's business paradigms and overall RTE in the six production deployment iterations, and the outcome of the experiment.

Table 5: Degree of fragmentation (DoF): Evaluation properties

8.5 PW6: DT services maintainability index: DT services classification based on digital activities

The service-oriented architecture maturity models and governance are applied to more operational aspects of the available services using the agile approach [87] in traditional architecture frameworks [1]. The evaluation presented in [88] and [89] measures the agility of the RTE irrespective of the maintainability of the DT services. However, not much emphasis on evaluating the maintainability of DT services in the uncertainties and advancements of DTs.

The DT service maintainability index (DSMI) evaluates DT service classifications based on digital activities presented in Chapter 6.2. The maintainability index measures whether DT services remain maintainable to account for the progression of the RTE architecture in the presence of a multiplicity of the RTE's digital activities. Table 6 provides the evaluation properties for assessing the DSMI, whereas APPENDIX A.5 details the computing paradigms and results.

Evaluation properties	Description
Purpose	The DSMI provides the indicative performance of the RTE’s DT services in terms of their maintainability in association with the BPs. DSMI essentially specifies the integrity of the RTE’s service appliance and operations manager presented in Chapter 2.8 during the advancement of DTs and corresponding DT services based on the identified DT service classification in Chapter 6.2.
Characteristics of evaluation	The velocity of the RTE represents the rapid changes and updates necessary to achieve the BP requirements due to RTE’s digital activities. Updating or introducing DT services, granular level of DT service operations, BP activities, or sublevel of the BPs can achieve the desired changes and compute the RTE's velocity. The DSMI is the relative measure of the following RTE’s concerns. • Business continuity after the introduction or modification of the DT services. • Operational risks associated with the DT services. • Service level agreements assess the DT services' scalability, reliability, and performance. • Consistency determines the scope of the DT service across multiple BP activities and their performance under different digital activities. • Extensibility and continuous improvement of the DT services based on the required level of customization for the BPs.
Industry vertical	Customer account and order management for the eCommerce platform [90].
RTE paradigm(s)	The experimental evaluation included seven BPs associated with the new customers' online registration, purchase order management, invoicing, account management, payment, and notifications.

Production deployment	The 62 DT services out of the already existing 304 traditional functional services were introduced in four production deployment iterations, mapping the relationship of DT services with BP activities using agile practices [91].
Results and conclusions	The experiments suggest a 58% reduction in velocity in deployment iteration four and a 21% increase in DSMI in deployment iteration four. The result directly illustrates continuous monitoring and improvements in the following areas of the RTE. • It reduced the number of issues reported by the RTE participants. • It provided immediate resolutions of the DT services' failures. • It recognized the accurate utilization of DT services for specific digital activities. • Precisions in test scenarios decrease the velocity of the RTE.
APPENDIX A.5	APPENDIX.A.5 provides the list of BPs utilized during the experiment, the computation of the DSMI in each deployment iteration, and the resulting statistics of DSMI for each DT service classification based on the DT activities and overall RTE in the four production deployment iterations, and the outcome of the experiment.

Table 6: DT services maintainability index: Evaluation properties

8.6 PW8: Degree of process classification: RTE processes-based DT service classification

The degree of process classification (DOPC) evaluates DT service the classifications based on RTE processes presented in Chapter 6.4. It measures the effectiveness of the RTE operational governance framework described in Chapter 4, which corresponds to the correlation between the RTE processes and advancements in DTs to achieve the DBOs. Table 7 provides the evaluation properties for assessing the DOPC, whereas APPENDIX A.6 details the computing paradigms and results.

Evaluation properties	Description
Purpose	The DOPC assesses the introduction or changes to the DBOs due to updates to the RTE processes in association with the DTs and corresponding DT services. DOPC indicates the impact of the RTE processes on the RTE's DBO

	manager described in Chapter 2.7 and the RTE participant's roles defined in the digital service layer (Chapter 2.3) based on the impacted dimensional factors of the DBOs as indicated by the RTE operational governance framework (Chapter 4).
Characteristics of evaluation	The DOPC is the relative measures of the impacted DBOs, dimensional factors of the DBOs, BP activities, RTE participant roles, and service level agreements associated with the DT services during the introduction or modification of RTE processes to update DTs and DT services.
Industry vertical	The rapid progress of RTE offering mobile commerce [92] and [93] has become a powerful trend in digital commerce and online retail industries. Mobile commerce can improve transaction-level productivity and innovate and adapt DTs to offer greater and more general services to diversified supply-chain stakeholders [94] through extensive processes [95]. Mobile commerce operations face many challenges, such as impeded service quality, capacity and necessary diversifications in communications, and loss of revenue due to transaction-level ambiguities [96] and fraudulent refund requests [97]. The RTE operation governance framework can continuously provide feedback to streamline and monitor the corresponding feature capabilities that were either updated or introduced to the mobile commerce platform. The evaluation was performed for the supply chain of pharmacy stores [98] and mobile devices to perform mobile commerce-specific digital activities.
RTE paradigm(s)	The 50 RTE operational governance framework dimensional factors (Chapter 4), the 40 BP activities, the 25 RTE participant roles, and the 90 service level agreements of the mobile banking and payment, communication with pharmacy stores and healthcare providers, and healthcare data analytics were selected to perform the RTE processes.
Production deployment	The experiment performed seven production deployment iterations to gradually introduce and evolve 75 DBOs with the DT services development and deployment platform [79] and external payment gateway [80].

Results and conclusions	The DOPC decreases consistently as RTE's operational governance framework introduces the granular aspects of the RTE processes' service level agreements. The DOPC of the personalization process type was at its peak during the deployment iteration seven, indicating that as RTE participants get more aware of their personalization options, they demanded (or anticipated) the corresponding feature capabilities offered by the DTs. The DOPC of the management processes and activity divergence processes were consistent, indicating that the deployment of the DBOs was at pace with the evolution of DTs. DOPC of service qualitative and transaction-level processes stabilize after initial fluctuation due to applying the RTE operational governance framework.
APPENDIX A.6	APPENDIX.A.6 provides the computation of the DOPC in each deployment iteration, the resulting statistics of DOPC for each DT service classification based on the RTE processes and overall RTE in the seven production deployment iterations, and the outcome of the experiment.

Table 7: Degree of process classification: Evaluation properties

8.7 PW7: Edge policy integrity gradient: DT service classification based on RTE policies

The edge policy integrity gradient (ePIG) evaluates the DT service classification based on RTE policies presented in Chapter 6.5. The edge policy integrity gradient assesses the abilities of DT services to attend to the RTE policies during the introduction or update of the DTs. Table 8 provides the evaluation properties for assessing the ePIG, whereas APPENDIX A.7 details the computing paradigms and results.

Evaluation properties	Description
Purpose	The ePIG assesses the RTE architecture evolution based on the policy provisioning lifecycle phases defined in RTE's service classification and policy engine (Chapter 2.4) based on the DT service classification based on RTE policies presented in Chapter 6.5 during the introduction or update of the DTs and corresponding DT services.

Characteristics of evaluation	The impact factor of the RTE policies was computed based on the RTE policy impact levels of the newly introduced or updated RTE policies. The ePIG is a relative measure of the number of RTE policies introduced or updated, the number of dimension factors introduced or updated, service level agreements violations, and the number of DT services introduced or updated in association with the impact factor.
Industry vertical	The smart healthcare consumer applications [99] and policies [100] were developed and deployed to mobile edge computing platforms (MEC) [101]. The MEC empowers consumer applications and content providers with cloud-computing capabilities and APIs at the edge of the mobile network [102] and [103]. Smart cars [104] and smart homes [19], along with the corresponding healthcare policies, were introduced to evaluate the multiple policies of different regulatory requirements of the diversified verticals in the smart city [105].
RTE paradigm(s)	The 70 RTE policies, 15 participant RTE applications, 12 RTE operational governance framework dimensional factors, and 145 service level agreements associated with the DT services were either introduced or updated to perform the experiments.
Production deployment	The experiment performed eight production deployment iterations to gradually introduce and evolve 70 RTE policies associated with 225 DT services under five diversified heterogeneous cloud environments.
Results and conclusions	The ePIG increases consistently as RTE architecture progresses to introduce the granular aspects of the RTE policies across the DT services. Dimensional subjectivity policies, resource-intensive policies, and coverage policies specific ePIG gradually increased, illustrating that the updating or introduction of new dimensional factors was in pace. However, the consumer privacy and confidentiality policies, operative policies, and network service's connectivity policies specific ePIG significantly increase during the initial stages and stabilize in the later deployment iterations. It is due to the stability of RTE architecture in consideration of new consumers, new IoT devices, and adherence to the regulatory requirements.

	Functional objectivity policies and constitutional policies specific ePIG increase in pace, indicating that the updating, modifying, and introduction of DT services (or APIs) were leveraging reusability at the level of the RTE policies.
APPENDIX A.7	APPENDIX.A.7 provides the computation of the ePIG in each deployment iteration, the resulting statistics of ePIG for each DT service classification based on the RTE policies and overall RTE in the seven production deployment iterations, and the outcome of the experiment.

Table 8: Edge policy integrity gradient: Evaluation properties

CHAPTER 9.

SCENARIO-BASED ASSESSMENT OF THE RTE ARCHITECTURE

The DT service classification presented in Chapter 7 provides the basis for evaluating RTE architecture depending on the identified types of scenarios. The scenario-based classification includes incremental risks associated with the DBOs, utilization of DT service capabilities to perform the DBOs, and compliance-aware DT services of the DBOs. This chapter derives and represents evaluation properties and experimental setup to assess RTE architecture depending on the scenario-based classification of DT services.

9.1 PW3: Inductivity of the scenarios based on the incremental risks

The inductivity (L) evaluates the DT service classification based on the incremental risks (IRs) associated with the DT services. The inductivity measures the change to mitigate the incremental risks while introducing and updating the DT services. Table 9 provides the evaluation properties for assessing the inductivity (L), whereas APPENDIX B.1 details the computing paradigms and results.

Evaluation properties	Description
Purpose	The inductivity (L) assesses the RTE architecture's risk management capabilities, described in Chapter 2.4, in correlation to the digital activities performed by the various types of RTE participants. The inductivity (L) quantifies the impact of the IRs during the updates or introduction of the DBOs based on the DT service classifications derived from the identified categories of IRs in Chapter 7.1.
Characteristics of evaluation	The inductivity is the relative measure of the severity of the IRs associated with the DBOs under a specific category of IRs, the number of impacted DBOs due to the introduction or update of the DT services, consumer applications of the RTEs, BPs, and participant RTE data entities. The consumer applications of the RTEs can include customer portal, call center agent portal, administrative database applications, and vendor-specific applications.

Industry vertical	The eCommerce platform's order management system [76] was selected to perform the evaluation.
RTE paradigm(s)	The 9 BPs of customers' online shopping experience, 12 consumer applications of the RTE, and 22 RTE data entities were either updated or introduced to perform the evaluation.
Production deployment	The experiment carried out eight production deployment iterations to gradually evolve 84 DBOs and manage 78 IRs associated with the DBOs.
Results and conclusions	The inductivity (L) of predictive and properties scenarios decreases before it increases since these scenarios are highly dependent on the DBOs incorporating specific DTs, including predictive analytics and corresponding RTE data entities. The inductivity (L) for the explorative scenarios was stable since the digital marketplace anticipates new regulatory events in pace. However, the inductivity (L) of the substantive and procedural scenarios continuously decreased due to the consistent advancements in DBOs. The characteristics of the cognitive scenarios were unpredictable as they fluctuated dramatically during the deployment of DBOs due to the impact of various factors, including consumer geographical location and purchasing patterns based on the diversity of the population in the region. The inductivity (L) of interceptive scenarios gradually decreased in correlation with the advancements in DBOs due to decreased rate of updates necessary for the DBOs.
APPENDIX B.1	APPENDIX.B.1 provides the detail of the BPs for the experiments, the inductivity (L) computation in each production deployment iteration, the resulting inductivity (L) statistics for each DT service classification based on the IRs for the eight production deployment iterations, and the outcome of the experiment.

Table 9: Inductivity of the scenarios: Evaluation properties

9.2 PW1: Average standard deviations in throughput

The average standard deviations of the DT services' capabilities utilization's throughput measure the performance and response time consistency. Table 10 provides the evaluation properties for assessing the average standard deviation, whereas APPENDIX B.2 details the results of the scenarios generated to introduce DTs' capabilities gradually.

Evaluation properties	Description
Purpose	The average standard deviation in the throughput is the typical approach to measure the service level agreements identified during the RTE operational governance framework (Chapter 4) and is usually captured during the monitoring capabilities of the RTE's service management and administration component described in Chapter 2.8.
Characteristics of evaluation	The average standard deviation in the throughput assesses the performance of the DBOs during the advancements and incorporation of concurrently running DT services in the enablement of multiple DTs' capabilities.
Industry vertical	Mobile edge computing (MEC) [106] manages computational resources across edge users in the diversity of the evolving IoT devices [107] and corresponding APIs in the heterogeneous cloud environment [108]. The DT services were built under the heterogeneous cloud environment [109] and [105] for smart manufacturing [83] and [20] leveraging industrial IoT [81] services. The runtime included 150 mobile network nodes, with each node having 12 cores and 128 GB of memory (2.30 GHz frequency).
RTE paradigm(s)	The following are the approached empirical scenarios to capture the average standard deviation in the throughput of the DT services based on the DT service classification identified in Chapter 7.2. • Scenario 1: No presence of DT services. • Scenario 2: DT services deployment after enabling reconfiguration capabilities, resource utility capabilities, and operational response capabilities. • Scenario 3: DT services deployment after enabling proactive enablement capabilities and all the other DT services deployed in scenario two.

	• Scenario 4: DT services deployed after enabling subscriber capabilities, information distribution capabilities, deployment and migration capabilities, and the capabilities enabled under scenarios two and three. • Scenario 5: DT services deployed after enabling user access capabilities, DT services' control capabilities, user interaction capabilities, and regulation management capabilities, along with all the capabilities enabled under scenario four.
Production deployment	64 DT services out of 80 DT services were dependent on the services offered by the IoT device vendors, heterogeneous cloud, and the MEC. The experiment captured the average standard deviation of throughput of DT services in the enablement of DTs' capabilities for each of the five scenarios in the increment of the 10 DT services.
Results and conclusions	The average standard deviation of throughput increases gradually for scenario two from the production deployment of 10 DT services to the 64 DT services. However, the average standard deviation of throughput is stable for scenario five after minor fluctuations due to the increased dependencies between the DT services. It indicates that DT services take advantage of the auto-scaling capabilities offered by the heterogeneous clouds.
APPENDIX B.2	APPENDIX B.2 presents the average standard deviation in throughput for the identified scenarios, service level agreement violations for the number of concurrent DT services for scenario three to scenario five, and the response latency for scenario one to scenario three.

Table 10: Average standard deviation in throughput: Evaluation properties

9.3 PW11: Degree of divergence and compliance-aware DT services governance index

The degree of divergence (DoD) evaluates the DT service classification based on compliance-aware DT services presented in Chapter 7.3. The DoD indicates the diversification required in the business rules, policies, and controls associated with the DT services. The compliance-aware DT services governance index (CDGI) evaluates the correctness of utilizing the DT services version, ability to prohibit compliance violations, adherence to service level agreements, and responsiveness of the BP activities due to compliance-aware DT services during the updates or introduction of the compliances, regulatory requirements, and industry standards. The following Table 11 provides the evaluation properties for assessing the DoD and CDGI, whereas APPENDIX B.3 details the computing paradigms and results.

Evaluation properties	Description
Purpose	The DoD and CDGI assess the effectiveness of the RTE's service classification and policy engine component, described in Chapter 2.6, in association with the RTE's service element and appliance operations manager component (Chapter 2.7). The RTE's service administration and configuration manager (Chapter 2.8) manages and updates the DT services' compliances, regulatory requirements, and industry standards.
Characteristics of evaluation	The DoD is computed based on the compliance-aware DT services, BP activities utilizing these DT services, the rules associated with the DT services, the number of compliances, and the conflicts between the multiple compliances against the BPs. However, the following are the primary concerns incorporated to formulate the CDGI since it is focused on operational aspects of the compliance-aware DT services. • Diversification of compliance requirements in DT services (DCRD). • The latest version of compliance-aware DT services utilization (LDSU). • Prohibit violations to compliances in DT services (PVCD). • Adherence to RTE's service level agreements (ASLA). • Responsiveness of BP activities to compliance-aware DT services (RBPA).
Industry vertical	The federal energy regulation commission (FERC) [75] for the smart grid-enabled retail energy's regulations with the payment card industry - data security standard (PCI-DSS) [110] and statement on standards for attestation engagements 16 (SSAE 16) [111] for reporting were utilized for the evaluation.
RTE paradigm(s)	The evaluation utilized 7 BPs and 326 existing DT services for the smart grid meter quotation, installation, and activation.

Production deployment	The experimentation performed eight production deployment iterations to evolve 62 BP activities gradually and 64 DT services to capture the DoD and CDGI.
Results and conclusions	The experiment recorded An average of 13% improvements in the DoD. However, the DoD increases significantly during early iterations since DT services include many of the compliances at the early stages of the production deployment. The CDGI increases over the production deployment iterations due to introducing compliance requirements to the DT services within pace. Essentially, it indicates that the greater the number of compliance-aware DT services and their utilization, the greater the level of divergence in the RTE architecture. However, it is vulnerable to consistency and extendibility. Contrarily, the multiple compliances under the single DT service increase the additional level of service level agreements' associations to the single DT service. It, in turn, increases the complexities of RTE architecture. RTE architecture must decide a trade-off during the correlations between compliance requirements, BP activities, DT services, and rules (or policies).
APPENDIX B.3	APPENDIX.B.3 provides the BPs utilized for the experiment, the computation of the DoD and CDGI in each production deployment iteration, the resulting statistics of DoD and CDGI for each DT service classification based on the compliance-aware DT services, and overall RTE in the eight production deployment iterations, and the outcome of the experiment.

Table 11: Degree of divergence and compliance-aware DT service governance index: Evaluation properties

CHAPTER 10.

OVERALL CONCLUSION

Despite recent advancements and available methodologies, real-time enterprises (RTE) face significant challenges in incorporating DTs before realizing the need to establish or update DBOs. The RTEs evolved by integrating, updating, and evolving DTs and BPs. The primary contributions of this research are to introduce RTE architecture, RTE operational governance framework, digital service classification schemes, and methodologies to continuously measure and improve the RTE architecture while keeping pace with the DTs.

The incremental risk modeling framework provides the way to capture uncertainties due to the introduction of DTs and actions to mitigate them in association with DBO. The generic incremental risk modeling framework allows various businesses to analyze, evaluate, and predict pervasive scenarios. It captures the structure and communication between the RTE participants to the identified DBOs and BPs. The primary concerns addressed are articulating DT services' impact on business operations, including inventions, pricing models, and marketing strategies. The methodology to determine types of scenarios assists RTEs by investigating external and internal interventions to manage DBOs efficiently. The RTE architecture framework provides instrumental actions in conjunction with the RTE operational governance framework and incremental risk modeling framework. It evolves the RTE architecture based on rational problem solving to manage incremental risks associated with DTs in correspondence to the BPs. The research work resolves the following primary challenges.

Continuously evolving RTE architecture: The ubiquitous RTE architecture articulated in Figure 3 provides a rationalized approach to establishing, integrating, updating, and monitoring the relationship between DT and BPs in the form of DBOs. The evolving characteristics of RTE architecture are streamlined based on the type of emerging technologies required or advanced, BPs and BP activities, and DBOs and incremental risks associated with them. The RTE operational governance framework provides the approach to streamline the advancement of DBOs in runtime as the inherent capability of RTE architecture orchestration and correlation engine's service model component. The degree of coverage (DoC) continuously identifies the number of BPs of the RTEs associated with the DT services. It provides the measurement of the RTE's pace to introduce DTs to existing BP activities.

Defining and deriving the DT services: The RTE architecture framework introduces the digital service layer. The responsibility of the digital service layer provides the means of modeling the services that leverage DTs in association with the RTE's BPs to constitute the DBOs. It encapsulates the paradigms of DTs, including but not limited to DT capabilities, policies, and resources utilized by DT services based on the RTE participant activities. The digital service layer is extendable to introduce more elements and paradigms to either introduce or update the DT services described in each experiment. The viscosity (η) of DT service defined in published work PW2 provides the measure of business requirements associating the enterprise data entities and corresponding paradigms with the DT services in the form of the data services.

Real-time decisions capabilities: The policy provisioning lifecycle identified in Figure 4 provides an RTE architecture service classification based on the decision criteria embedded in the RTE policies. It gives real-time decisions to RTEs utilizing policies associated with DT services by contextual monitoring in real-time. The policies are derivations of the incremental risks associated with DBOs. The incremental risk modeling framework illustrated in published work PW4 encounters the uncertainties, assumptions, or estimated data deficiencies to operationalize the DT services.

The RTE architecture's service administration and configuration manager executes the specified risk model and computes the risks in real-time for the DT service based on the identified associations by the service association and management. The published work PW4 indicates that the severity of the incremental risks associated with DBOs, and the overall goal of the DT service instantiates the need to introduce or update the policies. The hierarchy of decisions and rules has evolved in policies advocating the identified incremental risks. The results indicate that the weighing and percentile of incremental risk measure the probability of risks during the gradual introduction or updating of DT services to the RTE architecture framework.

DT service composition: The DT services are modeled and constituted within the digital service layer of the RTE architecture framework. However, the dynamic orchestration of the DT services performed within the orchestration and correlation engine of the RTE architecture is based on the context of DT functionalities provided by the digital service layer to the DT service model. The orchestration and correlation engine retains the structure of the composite services in the form of DT services and a corresponding diversified set of metadata derived at the granular levels of services. The degree of fragmentation (DoF) identified in the published work PW10 evaluates and standardizes the RTE architecture in the correlation with DT paradigms based on the definition and classification of DT services. The incremental rate of the degree of fragmentation for DT services provides the measurement of RTE architecture stability in the advancement of DTs.

Manual intervention to the BPs: The service element and appliance operations manager component of the RTE architecture framework provisions the automation of BPs. The digital BP automation engine of the service element and appliance operations manager component presented in Figure 3 determines the level of automation provided with the DT services. It ensures the manual intervention necessary to perform the DBOs. The DT service maintainability index (DSMI) derived in the published work PW6 measures the ability of the RTE to maintain the DT services to account for the digital activities of the diversified types of participants. These digital activities are manual interventions by the diversified types of participants across the RTE ecosystem. It continuously evaluates the level of interactions necessary and whether the DT services remain maintainable in the advancing BOs. It considers the BPs, BP activities, consistency, and service level agreements to evaluate the maintainability of DT services in the presence of digital activities performed by the RTE's participants.

Deploying and changing DT services in real-time: The service administration and configuration manager component of the RTE architecture is responsible for introducing, managing, monitoring, and deprecating services in real-time. It manages the service lifecycle by performing service recognition, identification, and discovery. The RTE ecosystem can leverage newly introduced DTs. Changes to the composite level DT services are versioned and maintained due to the new or updated granular DT services. The inductivity (L) presented in published work PW3 of RTE architecture measures changes performed to mitigate the incremental risks during the deployment of newly introduced or updated DT services.

He RTE

End-to-End DT service provisioning: The DBOs manager component of the RTE architecture establishes the structured DBO models. The structure of the DBO model consistently evolves RTE architecture in the end-to-end perspective of the DT services in correlations with BPs. These DBO models manage the end-to-end DT service provisioning across the RTE. The average standard deviation in throughput was measured gradually by enabling DT services in the different scenarios of the end-to-end capabilities offered by the DT services in the vicinity of the RTE architecture, as illustrated in the published work PW1.

Despite the rationalization of the RTE architecture framework and streamlining of the evolving characteristics of DTs in terms of DT services and BPs, the impact of innovation and disruption in DTs on the RTE and businesses remains unpredictable. The following are the open issues to be considered within RTE architecture.

- Every RTE is different in characteristics, and the RTE architecture leveraging DBO has not yet become a global standard. If the level of automation in the DBOs is incorrect, then the RTE architecture and corresponding operational governance can be vulnerable to manipulations to evolve the DBOs.
- Usually, the novel DTs' compliances, regulations, and standards are introduced after utilization of the DTs and recognition of the advantages offered by the DT services. The early adaptors and implementation of the DBOs to the RTE architecture framework may be susceptible to violations and corresponding legal consequences. The impact and changes due to newly introduced compliances remain unknown and unpredictable. The mechanism needs to be developed to either recognize the upcoming compliances or limit the conditional execution of unauthorized DBOs.
- It is evident that the stakeholders, including the consumers and suppliers, cannot adapt the DTs and corresponding DT capabilities. It is anticipated that the RTE architecture needs to work with both types of participants, that is, participants eager to accelerate the operations utilizing DTs and participants accustomed to the traditional way of performing operations.

The future direction is to explore the subclassification of the identified categories of DT service classification in a large-scale automation initiative. Typically, the connected RTE ecosystem involves the cross-utilization of multiple DTs and corresponding DT services between multiple RTEs and the same participants with multiple roles. The subsequent aspect is to generate subclassifications based on the overlapping characteristics of the various RTEs and the corresponding roles of the RTEs' participants. For instance, the smart city ecosystem includes interconnectivity between smart traffic control systems, emergency response service providers, and smart hospitals during roadside accidents or events. It requires a granular level of classifications to identify the precise impact of the DTs on each of the involved industry verticals since they are interdependent during globalization. The regulatory requirements are evolving based on the advanced automation and interconnections across multiple industry sectors. The multiple standardization bodies are coming together to introduce regulations for the cross-utilization of DTs.

REFERENCES OF THE CONTEXT STATEMENT

[1] F.A. Cummins, Building the Agile Enterprise: with SOA, BPM and MBM, Elsevier, 2010.

[2] R. Eve, "Data Services Platforms–Bringing Order to Chaos," Composite Software, vol. 15, April. 2010.

[3] S. Mithas, A. Tafti and W. Mitchell, "How a firm's competitive environment and digital strategic posture influence digital business strategy," MIS Quarterly, pp. 511-536, 2013.

[4] J. Mendling, I. Weber, W.V.D. Aalst, J.V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C.D. Ciccio, M. Dumas and S. Dustdar, "Blockchains for business process management-challenges and opportunities," ACM Transactions on Management Information Systems (TMIS), vol. 9, pp. 1-16, 2018.

[5] S. Agassi, "The Practical Real-Time Enterprise: Business process evolution in real-time," in The Practical Real-Time Enterprise, Springer, 2005, pp. 193-200.

[6] J. Horkoff and E. Yu, "Evaluating goal achievement in enterprise modeling–an interactive procedure and experiences," in IFIP Working Conference on The Practice of Enterprise Modeling, pp. 145-160, 2009.

[7] D. Petcu and V. Stankovski, "Towards cloud-enabled business process management based on patterns, rules and multiple models," in 2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications, pp. 454-459, 2012.

[8] K.O. Park and C.E. Koh, "Effect of change management capability in real-time environment: an information orientation perspective in supply chain management," Behaviour & Information Technology, vol. 34, pp. 94-104, 2015.

[9] Ç Dilibal, "Development of Edge-IoMT Computing Architecture for Smart Healthcare Monitoring Platform," in 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), pp. 1-4, 2020.

[10] J. Lopez, "Digital Business is Everyone's Business," Forbes.Com, May 7. 2014.

[11] V. Morabito, Trends and challenges in digital business innovation, Springer, 2014.

[12] J. Xu, "Digital enterprise strategy planning and implementation," in Managing Digital Enterprise, Springer, 2014, pp. 51-75.

[13] J. Kiswani, S.M. Dascalu and F.C. Harris Jr, "Cloud-RA: A Reference Architecture for Cloud Based Information Systems." in ICSOFT, pp. 883-888, 2018.

[14] A. Ahmed and E. Ahmed, "A Survey on Mobile Edge Computing," in 10th IEEE International Conference on Intelligent Systems and Control, pp. 1-8, 2016.

[15] J. Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 7, pp. 1645-1660, 2013.

[16] I. Farris, L. Militano, M. Nitti, L. Atzori and A. Lera, "MIFaaS: A Mobile-IoT-Federation-as-a- Service Model for dynamic cooperation of IoT Cloud Providers," Future Generation Computer Systems, pp. 126-137, May. 2017.

[17] S.N. Kulkarni and P. Shingare, "A review on smart grid architecture and implementation challenges," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3285-3290, 2016.

[18] A. Shaik, N. Bowen, J. Bole, G. Kunzi, D. Bruce, A. Abdelgawad and K. Yelamarthi, "Smart car: An IoT based accident detection system," in 2018 IEEE Global Conference on Internet of Things (GCIoT), pp. 1-5, 2018.

[19] H. Papadopoulos, "Designing Smart Home Environments for Unobtrusive Monitoring for Independent Living: The Use Case of USEFIL," International Journal of E-Services and Mobile Applications (IJESMA), vol. 8, pp. 47-63, 2016.

[20] N. Ivezic and V. Srinivasan, "On architecting and composing engineering information services to enable smart manufacturing," Journal of Computing and Information Science in Engineering, vol. 16, 2016.

[21] O. Vermesan and P. Friess, Internet of things-from research and innovation to market deployment, River publishers Aalborg, 2014.

[22] T. Pflanzner and A. Kertész, "A survey of IoT cloud providers," in 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 730-735, 2016.

[23] H. Jeon, H.R. Oh, I. Hwang and J. Kim, "An intelligent dialogue agent for the IoT home," in Workshops at the Thirtieth AAAI Conference on Artificial Intelligence, 2016.

[24] C. Gejke, "A new season in the risk landscape: Connecting the advancement in technology with changes in customer behaviour to enhance the way risk is measured and managed," Journal of Risk Management in Financial Institutions, vol. 11, pp. 148-155, 2018.

[25] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications, vol. 58, pp. 49-69, 2011.

[26] G. Gimpel and G. Westerman, "Shaping the future: Seven enduring principles for fast changing industries," MIT Center for Digital Business, 2012.

[27] Y. S. Pratama, Y. Ruldeviyani, C. E. Noviyanti and E. Kristiani, "Case Study: AppDynamics Application as Business Intelligence to Support Digital Business Operations at PT PGD," in - 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), pp. 577-582, 2020.

[28] M. Hearn and R.G. Brown, "Corda: A distributed ledger," Corda Technical White Paper, vol. 2016, 2016.

[29] Z. Dragičević and S. Bošnjak, "Agile architecture in the digital era: Trends and practices," Strategic Management, vol. 24, pp. 12-33, 2019.

[30] M.J. Anwar and A.Q. Gill, "A review of the seven modelling approaches for digital ecosystem architecture," in 2019 IEEE 21st Conference on Business Informatics (CBI), pp. 94-103, 2019.

[31] A. Josey, ArchiMate® 3.0. 1-A pocket guide, Van Haren, 2017.

[32] J.A. Zachman, "A framework for information systems architecture," IBM Syst J, vol. 38, pp. 454-470, 1999.

[33] P. Saha, "A synergistic assessment of the Federal Enterprise Architecture Framework against GERAM (ISO15704: 2000)," in Handbook of Enterprise Systems Architecture in Practice, IGI Global, 2007, pp. 1-17.

[34] A. Josey, TOGAF® Version 9.1-A Pocket Guide, Van Haren, 2016.

[35] V. Sergeev and V. Solodovnikov, "Using an Adapted Zachman Framework for Enterprise Architecture in the Development of an Industry Methodology of Integrated Supply Chain Planning," Transport and Telecommunication, vol. 21, pp. 203-210, 2020.

[36] O. Noran, P. Turner and P. Bernus, "Towards a Light-weight Enterprise Architecture Approach for Building Transformational Preparedness," 2018.

[37] T. Clark, B.S. Barn and S. Oussena, "Leap: a precise lightweight framework for enterprise architecture," in Proceedings of the 4th India Software Engineering Conference, pp. 85-94, 2011.

[38] M. Johanes and Y.A. Yatmo, "Composing the Layer of Knowledge of Digital Technology in Architecture," in SHS Web of Conferences, pp. 05002, 2018.

[39] A. Zimmermann, R. Schmidt, D. Jugel and M. Möhring, Evolving enterprise architectures for digital transformations, Gesellschaft für Informatik eV, 2015.

[40] M. Sneps-Sneppe and D. Namiot, "On mobile cloud for smart city applications," arXiv Preprint arXiv:1605.02886, 2016.

[41] Z. Laliwala and S. Chaudhary, "Event-driven service-oriented architecture," in 2008 International Conference on Service Systems and Service Management, pp. 1-6, 2008.

[42] K. Dar, A. Taherkordi, H. Baraki, F. Eliassen and K. Geihs, "A resource-oriented integration architecture for the Internet of Things: A business process perspective," Pervasive and Mobile Computing, vol. 20, pp. 145-159, 2015.

[43] F. Al-Turjman, M. Karakoc and M. Gunay, "Path planning for mobile DCs in future cities," Annals of Telecommunications, vol. 72, pp. 119-129, 2017.

[44] International Electrotechnical Commission, "Orchestrating infrastructure for sustainable Smart Cities," 2014.

[45] F. Cicirelli and G. Spezzano, "Concept Hierarchies For Sensor Data Fusion In The Cognitive IoT." in ECMS, pp. 73-79, 2016.

[46] P. Castillejo, J. Martínez, L. López and G. Rubio, "An internet of things approach for managing smart services provided by wearable devices," International Journal of Distributed Sensor Networks, vol. 9, pp. 190813, 2013.

[47] T. Leppänen, J. Riekki, M. Liu, E. Harjula and T. Ojala, "Mobile agents-based smart objects for the internet of things," in Internet of Things Based on Smart Objects, Springer, 2014, pp. 29-48.

[48] D. Hartmann and H. Van der Auweraer, "Digital twins," in Progress in Industrial Mathematics: Success Stories, Springer, 2021, pp. 3-17.

[49] S.M.M. Fattah, H. Kim and I. Chong, "Design of composite virtual objects for service entity creation in WoO based IoT environment," in 2016 International Conference on Information Networking (ICOIN), pp. 372-374, 2016.

[50] X. Jin, S. Chun, J. Jung and K. Lee, "A fast and scalable approach for IoT service selection based on a physical service model," Inf.Syst.Front., vol. 19, pp. 1357-1372, 2017.

[51] M.A. Nasser, R. Islam, I.S. Zainal Abidin, M. Azam and A.C. Prabhakar, "Analysis of e-service quality through online shopping," Research Journal of Business Management, vol. 9, pp. 422-442, 2015.

[52] E. Hosiaisluoma, "ArchiMate Cookbook," 2019.

[53] W.C. Wheaton and E. Tung, "Bricks or Clicks? The Efficiency of Alternative Retail Channels," The Efficiency of Alternative Retail Channels (February 3, 2019), 2019.

[54] M. Guta, "27% of Online Sales End Up Being Fraudulent Transactions," Dec 5. 2019.

[55] C. Richardson and D. Miers, "How the top 10 vendors stack up for next-generation BPM suites," The Forrester Wave: BPM Suites for Enterprise Architecture Professionals, 2013.

[56] A.K. Mandal and A. Sarkar, "A novel meta-information management system for SaaS," International Journal of Cloud Applications and Computing (IJCAC), vol. 9, pp. 1-21, 2019.

[57] G. Breiter and V.K. Naik, "A framework for controlling and managing hybrid cloud service integration," in 2013 IEEE international conference on Cloud engineering (ic2e), pp. 217-224, 2013.

[58] U.S. Congress, "Health information technology for economic and clinical health act," US Department of Health and Human Services, 2009.

[59] S. Goundar, S. Chand, J. Chandra, A. Bhardwaj and F. Saber, "A Taxonomy of Blockchain Applications," in Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends, World Scientific, 2021, pp. 49-71.

[60] O. Avila, C. Paez and D. Correal, "Towards a Maturity Model for Cloud Service Customizing," in International Conference on Applied Informatics, pp. 282-294, 2019.

[61] A. Kos, S. Tomažič, J. Salom, N. Trifunovic, M. Valero and V. Milutinovic, "New benchmarking methodology and programming model for big data processing," International Journal of Distributed Sensor Networks, vol. 11, pp. 271752, 2015.

[62] M. Jafari, M. Fathian, A. Jahani and P. Akhavan, "Exploring the contextual dimensions of organization from knowledge management perspective," Vine, 2008.

[63] A. Baldwin and S. Shiu, "Managing digital risk: Trends, issues, and implications for business," Lloyd's 360 Risk Insight, 2010.

[64] I. Sitima and C.K. Hlatywayo, "A risk metric assessment of scenario-based market risk measures for volatility and risk estimation: Evidence from emerging markets," The South East European Journal of Economics and Business, vol. 9, 2014.

[65] A. Klinke and O. Renn, "Adaptive and integrative governance on risk and uncertainty," Journal of Risk Research, vol. 15, pp. 273-292, 2012.

[66] G. Taylor, "7 Mobile Trends to watch in 2016," March. 2016.

[67] D.S. David, "LL. M., Digital Transformation: New Dimensions of Risk and Risk Mitigation," in European Identity & Cloud Conference 2015, 2015.

[68] R. Khadka, A. Saeidi, A. Idu, J. Hage and S. Jansen, "Legacy to SOA evolution: a systematic literature review," Migrating Legacy Applications: Challenges in Service Oriented Architecture and Cloud Computing Environments, pp. 40-70, 2013.

[69] C. Hsuan, J.R. Horwitz, N.A. Ponce, R.Y. Hsia and J. Needleman, "Complying with the Emergency Medical Treatment and Labor Act (EMTALA): challenges and solutions," Journal of Healthcare Risk Management, vol. 37, pp. 31-41, 2018.

[70] M. Better and F. Glover, "Scenario-based risk management and simulation optimization," Wiley StatsRef: Statistics Reference Online, 2014.

[71] C. Mazri and M. Florin, "No title," IRGC Guidelines for Emerging Risk Governance: Guidance for the Governance of Unfamiliar Risks, 2015.

[72] M. Pipattanasomporn, H. Feroze and S. Rahman, "Multi-agent systems in a distributed smart grid: Design and implementation," in 2009 IEEE/PES Power Systems Conference and Exposition, pp. 1-8, 2009.

[73] Anonymous "Federal Energy Regulatory Commission Strategic Plan FY 2018 to 2022," Federal Energy Regulatory Commission., 2018.

[74] J. Lewis, "How big data means big security changes: Effective identity management in a data-driven world," The DataCenter Journal, 2014.

[75] J. Heeter and L. Bird, "Status and Trends in U.S. Compliance and Voluntary Renewable Energy Certificate Markets," National Renewable Energy Lab (NREL), Golden, CO (United States)., 2011.

[76] M. Shetty, W.J. Shareef, K. Shetty and S. Lohiya, "B2B Order Management System," International Journal of Computer Science and Information Technologies, vol. 6, pp. 1118-1122, 2015.

[77] A. Badiru, A. Badiru and A. Badiru, Industrial project management: Concepts, tools, and techniques, CRC Press, 2007.

[78] J. Schekkerman, "Enterprise architecture tool selection guide," Institute for Enterprise Architecture Developments, 2011.

[79] M.B. Juric, S. Bernhardt, H. Normann, D. Schmiedel, G. Schmutz, M. Simpson and T. Winterberg, Design Principles for Process-driven Architectures Using Oracle BPM and SOA Suite 12c, Packt Publishing Ltd, 2015.

[80] S.D. Dhobe, K.K. Tighare and S.S. Dake, "A review on prevention of fraud in electronic payment gateway using secret code," Int.J.Res.Eng.Sci.Manag, vol. 3, pp. 602-606, 2020.

[81] C. Wang, Z. Bi and L. Da Xu, "IoT and cloud computing in automation of assembly modeling systems," IEEE Transactions on Industrial Informatics, vol. 10, pp. 1426-1434, 2014.

[82] P. Pääkkönen and D. Pakkala, "Reference architecture and classification of technologies, products and services for big data systems," Big Data Research, vol. 2, pp. 166-186, 2015.

[83] P. Helo, M. Suorsa, Y. Hao and P. Anussornnitisarn, "Toward a cloud-based manufacturing execution system for distributed manufacturing," Comput.Ind., vol. 65, pp. 646-656, 2014.

[84] D. Mysore, S. Khupat and S. Jain, "Understanding atomic and composite patterns for big data solutions," Nov 25. 2013.

[85] M. Nataraj, V.P. Arunachalam and G. Ranganathan, "Using risk analysis and Taguchi's method to find optimal conditions of design parameters: a case study," The International Journal of Advanced Manufacturing Technology, vol. 27, pp. 445-454, 2006.

[86] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, B. Kantarci and S. Andreescu, "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges," in 2015 IEEE International Conference on Services Computing, pp. 285-292, 2015.

[87] S.W. Ambler and M. Lines, Disciplined agile delivery: A practitioner's guide to agile software delivery in the enterprise, IBM press, 2012.

[88] A. Qumer and B. Henderson-Sellers, "An evaluation of the degree of agility in six agile methods and its applicability for method engineering," Information and Software Technology, vol. 50, pp. 280-295, 2008.

[89] T. Lui, G. Piccoli and K.C. Desouza, Degrees of agility: implications for information systems design and firm strategy, Burlington, MA: Elsevier Inc, 2007, pp. 122-133.

[90] Z.L. Peng, "Research on the Development of the Integration between IOT and C2C Electronic Commerce," in Applied Mechanics and Materials, pp. 6766-6770, 2014.

[91] I.S. Bajwa, R. Kazmi, S. Mumtaz, M.A. Choudhary and M.S. Naweed, "SOA and BPM Partnership: A paradigm for Dynamic and Flexible Process and IT Management," World Academy of Science, Engineering and Technology, vol. 45, pp. 16-22, 2008.

[92] M. Niranjanamurthy, N. Kavyashree, S. Jagannath and D. Chahar, "Analysis of e-commerce and m-commerce: advantages, limitations and security issues," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, pp. 2360-2370, 2013.

[93] C. Tode, "Mcommerce sales to reach $142 B in 2016: Forrester," Mobile Commerce Daily, 2015.

[94] K. Carey and M. Helfert, "Improving the front end of innovation: The case of mobile commerce services," in International Conference on HCI in Business, Government, and Organizations, pp. 491-501, 2016.

[95] M.Y. Shen, C.Y. Liu and B. Huang, "A development strategy of m-commerce against mobile internet," in Advanced Materials Research, pp. 1092-1096, 2013.

[96] R. Yadav, S.K. Sharma and A. Tarhini, "A multi-analytical approach to understand and predict the mobile commerce adoption," Journal of Enterprise Information Management, 2016.

[97] M. Macinas, "Study: Mobile Commerce Fraud Cost up 18 Percent," Jan 19. 2015.

[98] R. Alamelu, R. Amudha, L.C.S. Motha and R. Nalini, "Online pharma retail is a promising/unpromising avenue: An Indian context," Asian Journal of Pharmaceutical and Clinical Research, vol. 9, pp. 26-29, 2016.

[99] J.C. Mandel, D.A. Kreda, K.D. Mandl, I.S. Kohane and R.B. Ramoni, "SMART on FHIR: a standards-based, interoperable apps platform for electronic health records," Journal of the American Medical Informatics Association, vol. 23, pp. 899-908, 2016.

[100] L. Edwards, "Privacy, security and data protection in smart cities: A critical EU law perspective," Eur.Data Prot.L.Rev., vol. 2, pp. 28, 2016.

[101] Y.C. Hu, M. Patel, D. Sabella, N. Sprecher and V. Young, "Mobile edge computing—A key technology towards 5G," ETSI White Paper, vol. 11, pp. 1-16, 2015.

[102] P. Mach and Z. Becvar, "Cloud-aware power control for real-time application offloading in mobile edge computing," Transactions on Emerging Telecommunications Technologies, vol. 27, pp. 648-661, 2016.

[103] Y. Jararweh, A. Doulat, A. Darabseh, M. Alsmirat, M. Al-Ayyoub and E. Benkhelifa, "SDMEC: Software defined system for mobile edge computing," in 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), pp. 88-93, 2016.

[104] M.I. Mamun, A. Rahman, M.A. Khaleque, M.F. Mridha and M.A. Hamid, "Healthcare monitoring system inside self-driving smart car in 5g cellular network," in 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), pp. 1515-1520, 2019.

[105] P. Potvin, H.G. Gamardo, K. Nguyen and M. Cheriet, "Hyper heterogeneous cloud-based IMS software architecture: A proof-of-concept and empirical analysis," in Smart City 360°, Springer, 2016, pp. 250-262.

[106] M. Peng, Y. Li, Z. Zhao and C. Wang, "System architecture and key technologies for 5G heterogeneous cloud radio access networks," IEEE Network, vol. 29, pp. 6-14, 2015.

[107] S. Dey, A. Mukherjee, H.S. Paul and A. Pal, "Challenges of using edge devices in IoT computation grids," in 2013 International Conference on Parallel and Distributed Systems, pp. 564-569, 2013.

[108] M. Kovatsch, S. Mayer and B. Ostermaier, "Moving application logic from the firmware to the cloud: Towards the thin server architecture for the internet of things," in 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 751-756, 2012.

[109] I. Mansour, R. Sahandi, K. Cooper and A. Warman, "Interoperability in the heterogeneous cloud environment: a survey of recent user-centric approaches," in Proceedings of the International Conference on Internet of things and Cloud Computing, pp. 1-7, 2016.

[110] J. Rees, "The challenges of PCI DSS compliance," Computer Fraud & Security, vol. 2010, pp. 14-16, 2010.

[111] A. Sinha, A. Jaiswal, R. Gupta and V.K. Chaurasiya, "SAS 70 to SSAE 16/ISAE 3402: An insight into outsourcing security and process controls, and significance of new service audit standards," Issn 1931-0285 Cd Issn 1941-9589 Online, pp. 315, 2011.

[112] A. Krylovskiy, M. Jahn and E. Patti, "Designing a smart city internet of things platform with microservice architecture," in 2015 3rd International Conference on Future Internet of Things and Cloud, pp. 25-30, 2015.

APPENDIX A: RTE architecture's experiments and results

APPENDIX A.1: PW4: Percentile of incremental risks (PEIR)

The experimental evaluation of PEIR included six diversified BPs and 62 DBOs, as indicated in published work PW4). The DBOs are associated with one or more of the BPs identified below.

BP# 1: Online customer enrollment. The registration and account validation are examples of DBOs inheriting BP# 1.
BP# 2: Manage customer information, inquiry, and history. Customer payment history is the type of DBO within the arsenal of this BP.
BP# 3: Manage purchase orders. Addition, removal, and updating the item from a purchase order constitute BP #2's DBOs.
BP# 4: Online billing and invoicing. Generating invoices is an example of the DBO of BP# 3.
BP# 5: Payment processing and account receivable. The bank's credit card payment processing is the most prominent DBO for BP# 5.
BP# 6: Online notification and acceptance of terms. Updating payment terms is the DBO that can utilize this BP.

The incremental risks (IRs) are used to attempt to compute the worst-case scenario for the identified timeframe. The production deployment iterations are typically set for four weeks to capture and iterate the DBOs and update the associated IRs. Severity levels are assigned to each identified IR. Although the RTE can define their levels and interpretation of severity levels (ISL), the four levels of IR severity were utilized during the evaluation. They are listed below.

- **ISL1 (critical)**: When the IR is anticipated to be critical and interrupts continuity in day-to-day business, it is assigned with an ISL1 severity level. The assigned value for ISL1 is at the highest level, that is, ISLV1 =1, since it signifies disruption of the DBOs. It implies that the BP may fail and cannot recover the impairment due to the failure. It will directly impact the various stakeholders associated with DBO.
- **ISL2 (high)**: If the backend operational level failure occurs due to connectivity or resource unavailability, the IR is assigned to the ISL2 severity level. The assigned value for ISL2 is relatively

lower than the ISL1 level to the DBOs, that is, ISLV2 = 0.7 since the RTE can still recover revenue due to manual support or corrective actions.

- **ISL3 (medium)**: If the IR is determined to violate one or more specified service level agreements, it is assigned with the ISL3 severity level. The ISL3 is 60% lower in impact than ISL1. It is the reason he assigned value to ISL3 is 0.4, that is, ISLV = 0.4. The IRs associated with ISL3 are fully recoverable without manual intervention, and stakeholders can continue utilizing DT services with minimal interruptions.
- **ISL4 (low)**: The customer or vendor anticipates a minor request for an additional feature or add-on capability from the DBO, then the IR is assigned with the ISL4 severity level. IRs associated with ISL4 do not cause any significant challenges. However, it requires correction in subsequent advancements of the corresponding DBOs. The incremental risk associated with ISL4 is assigned the value of 0.2 since the impact is much lower than ISL1 (80% lower); ISL4 = 0.2.

The average weighing AW<IR category> in Equation 1 represents the average severity of all the IRs of the specific category of IR specified in Chapter 5. The following are the terminologies utilized to formulate Equation 1.

- ISLV<i> represents the finite value of the severity level "i" for the specific IR category.
- #IR<i><IR category>: It is the number of IRs identified for the specific category with the severity level "i" in the current production deployment iteration.
- "n": The number of levels defined for the severity in the present iteration, ISL1 to ISL4. The (n = 4) for this evaluation.
- #IR<IR category>: The number of IRs identified for the specific category (5 categories described in Chapter 5) in the current production deployment iteration.

$$\boldsymbol{AW < IR\ category >} = \frac{\sum_{i=1}^{n} [\boldsymbol{ISLV{<}i{>}}] \times [\boldsymbol{\#IR{<}i{>}{<}IR\ category{>}}]}{\boldsymbol{\#IR{<}IR\ category{>}}} \quad (1)$$

The PEIR for the specific IR category is dependent on the $AW < IR\ category >$ and the number DBOs impacted due to the particular category of incremental risk. For example, a security breach does not need to occur on all online transactions due to the introduction of cloud migration. A security breach probability is much lower than the probability of Big data analytics-specific risks. The PEIR provides the measure of actual violations of the service level agreements based on the occurrence of the IR after deploying the particular set of DT services associated with the DBOs. If the DBOs include multiple IRs from the multiple IR categories, they are considered for the corresponding IRs to provide accuracy in computing the PEIR. Equation 2 represents the percentile of IR for each category of IR, that is, PEIR<IR Category>. The following are the terminologies utilized for Equation 2.

- #DBO: The number of RTE's DBOs in the current production deployment iteration.
- #DBO <IR category>: The number of DBOs associated with the specific category of IRs in the current production deployment iteration.
- #IRs: The number of IRs in the current production deployment iteration.
- #IR<IR category>: The number of IRs of the specific IR category in the current production deployment iteration.
- AW<IR category>: The average weighing of the IRs computed using Equation 1 for the specific category of IR in the current production deployment iteration.
- "p": The number of IR category paradigms utilized to compute the PEIR. The value of p is three since AW<IR Category>, IR<IR Category>, and DBO<IR Category> were utilized to compute PEIR.

$$PEIR < IR\ category > = \frac{(AW{<}IR\ category{>} \times \#IR{<}IR\ category{>} \times \#DBO{<}IR\ category{>}) \times 10^{p}}{\#IR \times \#DBO} \quad (2)$$

Figure 18 provides the PEIR for each IR category, and the number of DBOs deployed in each production deployment iteration from iteration#1 to iteration# 8.

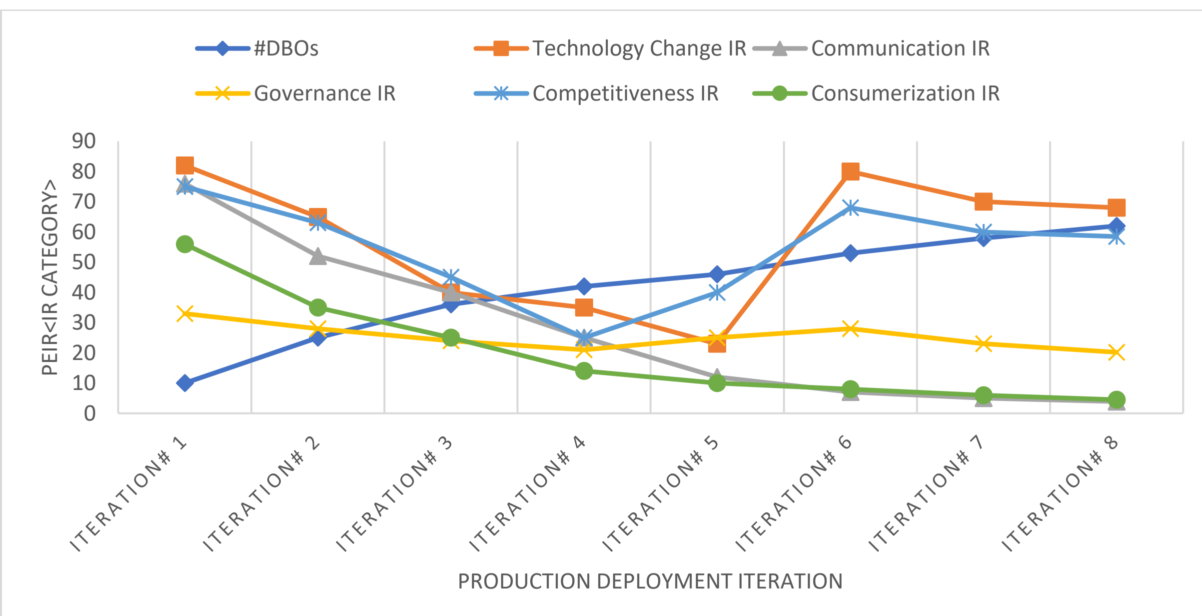


Figure 18: PEIR<IR category> form the production deployment iteration# 1 to 8

Table 12 represents the absolute values of PEIR captured for each category of the IR in the production deployment iteration 9. The number of actual unique service level agreement (SLA) violation occurrences due to identified IRs in the specific IR category is observed and specified in Table 12.

IR category	IR category paradigms				
	#IRs	**#DBOs**	**AW**	**PEIR**	**Actual violations of the SLAs due to IRs**
Technology Change Incremental Risk	14	18	0.72	68	5
Communication Incremental Risk	4	7	0.375	3.9	0
Governance Incremental Risk	8	12	0.56	20.2	3
Competitiveness Incremental Risk	12	20	0.65	58.5	6
Consumerization Incremental Risk	5	5	0.48	4.5	1

Table 12: PEIR<IR category> in production deployment iteration# 9

APPENDIX A.2: PW5: Degree of coverage (DoC)

The Big data architecture pattern [84] was adopted as a potential DT for the RTE to measure the DoC. Each production deployment iteration completes the phases to associate Big data architecture patterns with BP activities. The BP activities are introduced or updated based on the necessary Big data functionalities captured in the DT services. The mapping between the Big data architecture patterns and BP activities determines the diversification behavior in the DBOs. The focus of the BP activities was actual transactions and associated properties in utilizing analytical data. The most prominent example is the real-time inspection of any potential fraud or compromised privacy during the online payment processing based on the past transactions' history and location of the transaction.

The severity levels have been assigned to each diversification introduced or updated to the DT services associated with the DBOs. Although the RTEs can define their severity levels and interpretation of severity levels, the following five levels of severity are defined to evaluate the DoC.

- **Severity Level 1 (Critical)**: If diversification in DT service is anticipated to be critical and interrupts continuity in day-to-day business, then it is categorized in severity level 1 (SL1). For instance, the unavailability of the DT service providing functionality to retrieve the mission-critical data and transaction history to perform and validate the transaction is at SL1. It has the highest level of the finite value assigned, that is, severity level value 1 (SLV1) = 1, to indicate the level of criticality.

- **Severity Level 2 (Major)**: If RTE expects one or more functional failures due to DT service, it is considered severity level 2 (SL2). For example, anticipated error due to incorrect validation criteria for the online transaction is an example of SL2. It has a lower impact than SL1. However, a significant impact may allow inaccurate or erroneous online transactions. Typically, it is 20% less severe than SL1. The severity level value 2 (SLV2) has been assigned with a finite value of 0.8 (SLV2 = 0.8).
- **Severity Level 3 (Intermediate)**: When DT service is estimated to violate one or more service level agreements, it has been assigned severity level 3 (SL3). An example of a service level agreement is the real-time online transaction with an anticipated time to complete the authorization in 30 milliseconds. The SL3 is 40% less severe than SL1. The severity level value 3 (SLV3) has been assigned with a finite value of 0.6 (SLV3 = 0.6).
- **Severity Level 4 (Minor)**: If there is an anticipation of a request for an additional feature or add-on capability in the DT service, however, it is yet to be included, then DT service has been assigned with severity level 4 (SL4). The most prominent example of SL4 is blocking the donation with the online transaction during online shopping due to the undeployed capabilities offered by the eCommerce platform. Typically, SL4-related issues are recoverable and 60% less severe than SL1. The severity level value 4 (SLV4) has been assigned with a finite value of 0.4 (SLV4 = 0.4).
- **Severity Level 5 (Negligible)**: If the RTE expects to include a specific extension for the monitory aspect of DT services, then it falls into severity level 5 (SL5). For instance, the inability to instantiate the customer requires a survey to be filled out after the customer service call is considered at SL5. It has practically minimal to no impact and is 80% less severe than the SL1. The severity level value 5 (SLV5) has been assigned with a finite value of 0.2 (SLV5 = 0.2).

Equation 3 provides the formulae to compute AWOP<DT Service Classification>, the average weighing of the changes to all the BP activities associated with the DBO for specific DT service classification presented in Chapter 6.1. The following are the terminologies utilized to formulate the AWOP<DT Service Classification>.

- AWOP<DT Service Classification>: Average weighing of the changes to all the BP activities associated with the DBO for specific DT service classification presented in Chapter 6.1.
- #DBO: The number of times that the DBOs need to be either diversified or updated.

- SLV<j>: The severity level associated with the DT service of the DBO under the specific DT service category. If the multiple DT services are associated with the DBO, it is counted separately in the equation.

$$AWOP < DT\ service\ category > = \frac{\sum_{j=1}^{\#DBO}[SLV<j>]}{\#DBO} \quad (3)$$

Equation 4 provides the formulae to compute the AWFN<DT service category>, the average weighing of the changes to DT service and its functionalities under the specific DT service category in the consideration. The following are the terminologies utilized to formulate the AWFN<DT service category>.

- AWFN<DT service category>: average weighing of the changes to DT service and its functionalities under the specific DT service category in the consideration.
- #DFN represents the number of DT service functionalities that need to be either diversified or updated.
- SLV<j>: The severity level associated with the DT service functionality under the specific DT service category. If the multiple DT service's functionalities are associated with the DBO, it is counted separately.

$$AWFN < DT\ service\ category > = \frac{\sum_{i=1}^{\#DFN}[SLV<i>]}{\#DFN} \quad (4)$$

In Equation 5, DoC<DT service category><Iteration (N)> represents the DoC for a specific DT service category in the current production deployment iteration (that is, N is 7 for the production deployment iteration number 7). Essentially, each production deployment iteration has a dependency on the previous iteration of updates and diversification in the DT services. DoC<DT service category><Iteration (N-1)> represents the DoC computed in the previous iteration. The following are the terminologies utilized to formulate the DoC<DT service category><Iteration (N)>. The DoC of the previous production deployment iteration for the very first production deployment iteration is essentially 0.

- DoC<DT service category><Iteration (N)>: DoC for a specific DT service category in the current production deployment iteration.
- DoC<DT service category><Iteration (N-1)>: The DoC computed in the previous production deployment iteration.

- #FN: The number of DT service functionalities participating in the BP activities of a specific DT service category.
- #DFN: The number of diversified or newly introduced DT service functionalities.
- #OP: The number of RTE operations that participate in the BP activities of the DT service category.
- #DBO: The number of diversified or newly introduced digital business operations.
- #DM: The number of dimension models that participate in the correlation between Big data architecture patterns and BP activities of the DT service category.
- #DDM: The number of DT service category diversified or newly introduced dimension models.
- #BPA: The number of BP activities that participate in qualifying corresponding BP in the DT service category.
- #BDAP_BPA: The number of BP activities diversified, newly associated, or introduced to RTE for the specific DT service functionality.
- "p": The number of paradigms considered to evaluate the DoC in the presence of DTs. In this experiment, the value of p = 4, that is, #BPA, #FN, #OP, and #DM.

$$DoC < DT\ service\ category >< Iteration(N) > =$$

$$DoC < DT\ service\ category >< Iteration(N-1) >$$

$$+$$

$$\left(\left(\left(\frac{\#BDAP\_BPA}{\#BPA}\right) + \left(\frac{\#DBO}{\#OP}\right) + \left(\frac{\#DFN}{\#FN}\right) + \left(\frac{\#DDM}{\#DM}\right)\right) < DT\ service\ category >\right) \times \frac{10^{p-2}}{p} \quad (5)$$

Table 13 represents the experimental data at the end of the DT service category's production deployment iteration# 7. The following terminologies are utilized to represent the DoC.

- DoC(N): DoC<DT service category><Iteration (N)>.
- DoC(N-1): DoC<DT service category><Iteration (N-1)>.

DT service category	***#BDAP_ BPA (#BPA)***	***AWFN***	***#DFN (#FN)***	***AW OP***	***#DBO (#OP)***	***#DDM (#DM)***	***DoC (N-1)***	**DoC (N)**
Reactive processes	10 (55)	6	18 (115)	3	6 (68)	3 (18)	242.2	280.85
Proactive processes	4 (42)	4	5 (76)	2	1 (62)	1 (12)	178.32	190.16
Predictive processes	8 (35)	2	14 (52)	2	7 (23)	4 (23)	211.77	250.5
Conductive processes	2 (28)	6.5	2 (34)	0	0 (23)	0 (6)	169.42	180.76

DT service category	*#BDAP_BPA (#BPA)*	*AWFN*	*#DFN (#FN)*	*AW OP*	*#DBO (#OP)*	*#DDM (#DM)*	*DoC (N-1)*	**DoC (N)**
Observatory processes	3 (25)	2	3 (38)	0	0 (12)	0 (19)	153.61	160.55
Cognitive processes	5 (21)	4.5	5 (38)	2	1 (35)	2 (10)	188.1	215.28
Operative processes	1 (45)	7	2 (98)	4	2 (82)	0 (25)	223.01	229.57
Associative processes	4 (26)	4	6 (62)	2	1 (15)	0 (12)	188.35	205.2
Average degree of coverage							**194.35**	**214.11**

Table 13: DoC computation in the production deployment iteration# 7

Figure 19 illustrates the progress of the DoC and the evolution of each identified DT service category from the production deployment iteration 1 through production deployment iteration 7.

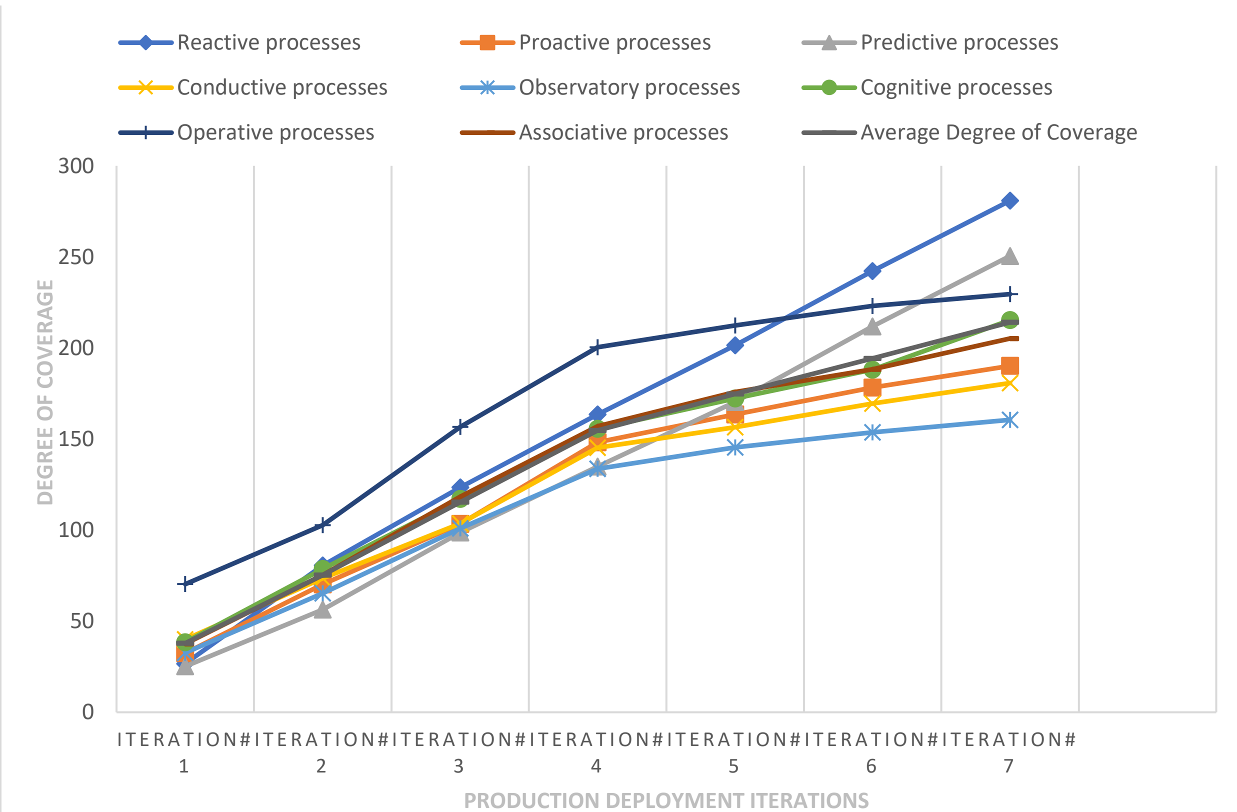


Figure 19: DoC evaluation in the production deployment iterations # 1 to #7

APPENDIX A.3: PW2: Viscosity (η) of the DT services

The BP activities associated with DT services use multiple data services in this experiment. Each data service combines one or more data sets and functionalities performed to the data sets to measure the viscosity (η). Logical data services are composed of multiple canonical and physical data services. For instance, the account reconciliation data service is the logical data service utilizing account information physical data service and general ledger entries as canonical data service. The viscosity of data services is the ratio of a total number of physical and canonical data services against the corresponding number of logical data services as DT services.

The computation of viscosity (η) is presented in Equation 6. The following terminologies are utilized to formulate viscosity (η).

- #LDS: The number of logical data services to compose the data services category.
- #PDS: the number of physical data services (PDS) utilized within the logical data services (LDS).
- #CDS: The number of canonical data services (CDS) used within the logical data services (LDS).
- #C_PDS: The number of physical data services used by the canonical data services.

$$\eta = \left(\sum_{i=1}^{\#LDS}[\ \#PDSi\ +\ \#CDSi\ +\ \#C\_PDSi\ ]\right)/LDS \quad (6)$$

The following represent logical data services (LDS) categories based on their characteristics to formulate DT services.

- **RTE data entity management service**: Data service manages the RTE's participant data entities. Managing or updating customer account information is an example of an RTE data entity management service.
- **Provisioning data service**: Data service encapsulates data changes of the RTE application(s) and introduces modes of operations for BPs. For example, the delivery mode determined for the online order based on the customer's delivery address is a provisioning data service.
- **Relationship data service**: Data service carrying information to specify and retain the relationship between the entities of RTE. For instance, the data service managing the relationship between the customer's account information and the online order instantiated by the customer is an example of relationship data service.
- **Association data service**: Data service placing and providing an association between inter or intra-RTE data entities to the external participants such as vendors, suppliers, and customers of RTE. The association of the RTE to the shipping company for order fulfillment is an example of an association data service.

- **Governance data service**: Data service specific to data quality, policies, security, and other regulatory aspects of RTE. For instance, address verification and payment validation are governance data services.

The composite DT services are developed in the form of APIs with multiple types of data services. The degree of API coverage (DOAC) indicates the number of data services supported by the BP activities within these APIs. The BP activities are associated with the BP and corresponding DBOs. The following are the terminologies utilized to formulate the DOAC in Equation 7.

- #BA: The number of BP activities defined and placed within the BP for the specific data service type. If the BP activity utilizes multiple data services, they are counted for each data service type separately for the accuracy in computing DOAC.
- #DS: The number of data services utilized to accomplish the BP activity for the specific data service type.
- #BP: The number of BPs using the APIs associated with the BP activities that fall under the specific data service type.
- DS type: Identified data service types associated with the APIs to perform BP activities.

$$DOAC < DS\ type > = \frac{\sum_{k=1}^{\#BP}[(\sum_{j=1}^{\#BAk}[\#DSj\ ])/\#BAk]}{\#BP} \quad (7)$$

The capabilities index (CI) measures the amount of variation in the APIs relative to the limits of business requirements during the advancements of BPs using DTs. The CI is derived based on the Taguchi capability index [85]. Taguchi CI is the function of the specification limits, the process, and a provided target. In Equation 8, the CI considers the specification limit as presenting the level of alteration in business requirements due to the updated or newly introduced data services for the specific data service type, corresponding changes in the present deployment iteration, and variations in the BPs. The following are the terminologies utilized to derive the CI for the specific type of data services.

- B_USL: The upper bound limit of the number of business requirements.
- B_LSL: The lower bound number of alterations in business requirements to advance the BP activities based on the introduction or update of the DTs.
- (B_USL – B_LSL) provides a finite number indicating allowable BP variations in the effect of APIs' changes dedicated to data service type (or DT service type).
- "T" is the target state mean of the number of changes to data services during the current

deployment iteration.

- "µ": The mean number of changes to data services.
- The actual variability of the data services is expressed as a standard deviation, σ. Standard deviation is computed for each deployment iteration relative to the variability of data services captured during the previous deployment iteration.
- DS type: Identified data service types associated with the APIs to perform BP activities.

$$CI < DS\ type > = \frac{B_U SL - B_L SL}{6\sigma \sqrt{1 + ((\mu - T)/\sigma)^2}} \quad (8)$$

Table 14 provides the experimental evaluation in an order management system where each data service category is measured in Equation 6, Equation 7, and Equation 8. The 1.3 value of standard deviation σ in Table 14 represents the increased (or decreased) variability of 37.54% in the utilization of data services compared to previous production deployment iterations. It represents the measures of each type of data service.

Data Service Type (#DS)	**Viscosity (η)**	**DOAC<DS type>**	**CI<DS type> σ = 1.3**
RTE data entity management (23)	6	7.5	1.8
Provisioning (21)	7	8	1.33
Relationship (18)	8.5	4.33	0.83
Association (12)	3	6.5	2.05
Governance (15)	4	5.5	1.66

Table 14: The Viscosity (η), DOAC, and CI of the data services

APPENDIX A.4: PW10: Degree of fragmentation (DoF)

The degree of fragmentation (DoF) is introduced to evaluate and standardize the RTE architecture corresponding to the correlation between DT services and DT's business paradigms, as indicated in Chapter 6.3. The example DT's business paradigms for the eCommerce industry are pricing, digital market model, visualization, personalization, product ontologies, communication channel, and privacy. The evaluation of DoF considers the use case of adding a supply-chain of healthcare monitoring accessory products [86] to the existing eCommerce marketplace in this experiment. Correlation Impact Factor Grade

(CIFG) represents the criticality of the correlation between the DT's business paradigm and the DT services. The following describes the levels of CIGF.

- **Correlation impact factor grade level 1 (CIFG1):** If the impact of DT's business paradigm is very high on the DT services, then the DT's business paradigm for the specific DT service category is at the CIFG level 1, that is, CIFG1. The most prominent example is the market model in the eCommerce platform. The online offering of a new healthcare accessory that monitors multiple conditions to the global marketplace changes the market model for the existing healthcare accessories for individual conditions is an example of CIFG1. It has the highest level of the finite value assigned as "10", that is, CIFG1 = 10, to indicate the level of criticality.
- **Correlation impact factor grade level 2 (CIFG2):** If IoT services are independently associated with the DT's business paradigm to meet the requirement of the RTE, then the specific DT's business paradigm is in CIFG2. The pricing paradigm based on the supplier's readiness and the baseline cost of the healthcare product offerings is an example of CIFG2. The finite value assigned for the CIFG2 is "8" since it has a 20% lower impact than CIFG1.
- **Correlation impact factor grade level 3 (CIFG3):** If DT services are collaborated to perform specific market activity utilizing any digital channels for a particular DT's business paradigm, it falls under CIFG3. The personalization offered to the third-party product advertising on the eCommerce platform is an excellent example of a CIFG 3. The designated finite value for CIFG3 is "5" since it has a 50% lower impact than CIFG1.
- **Correlation impact factor grade level 4 (CIFG4):** If the DT services have many external dependencies, then the DT's business paradigm is considered at CIFG4. For example, the visualization offered to view the anticipated product inventory for the specific timeframe from the manufacturers is categorized in the CIFG4. The finite value of the CIFG4 is "2" since it has an 80% lower impact than CIFG1.

Equation 9 represents the DT service correlation factorial (DCF) formulation for each DT service category identified in Chapter 6.3.

- #ED: The number of DT's business paradigms as eCommerce dimension (ED), associated with the specific DT service category.
- #IED: The number of DT's business paradigms, as eCommerce dimensions (IED), are impacted due to the introduction or modification of DT services under the specific DT service category.

$$DCF_{<DT\ service\ category>} = \frac{\left[\sum_{i=1}^{\#IED} CIFG_i\right]}{\#ED} \quad (9)$$

The following are the factors identified to derive a degree of fragmentation (DoF) for the supply chain of the introduction of healthcare accessories to the eCommerce marketplace.

- Market activities (MA): The market activities recognized by the eCommerce platform
- eCommerce appliances (EA): The applications developed and utilized to formulate the end-to-end eCommerce platform.
- Composite IoT services (IoS): Composite DT services utilize granular DT services to perform specific eCommerce functionality.
- Entities associated with IoT or DT services (EIS): EIS represents the data entities of information associated with the DT services to perform the specific eCommerce functionality.
- IoT service (or DT service) dependencies to external participants of eCommerce platform (IDX): The action to be performed by the external participants to complete specific eCommerce functionality.

Equation 10 presents the computation of the DoF for the specific DT service category during the current production deployment iteration of the RTE architecture.

$$DoF_{<DT\ service\ category>} = DCF_{<DT\ service\ category>} \times \frac{[tMA + tEA + tIoS + tEIoS + tIDX] \times 10^{t-2}}{t} \quad (10)$$

- "t" represents the number of criteria considered to quantify the measures of the degree of fragmentation. In this case, the value of "t" is "5", the five paradigms listed above.
- tMA: It is the ratio of impacted or introduced market activities due to the IoT services of the specific DT service category over the total number of market activities associated with the specific DT service category.
- tEA: It is the ratio of impacted or introduced eCommerce appliances due to the IoT services of the specific DT service category over the total number of IoT services associated with the specific DT service category.
- tIoS: The ratio of impacted or introduced IoT services of the specific DT service category over the total number of IoT services associated with the specific DT service category.

- tEIoS: The ratio of impacted or introduced data entities due to the IoT services of the specific DT service category over the total number of data entities associated with the specific DT service category.
- tIDX: It is the ratio of impacted or introduced external dependencies due to the DT service category's internet-of-things services (#IIDX) over the total number of external dependencies of the DT service category.

During the computation, if the market activity, eCommerce appliance, data entity, and IoT service dependency are impacted or introduced for the multiple DT service categories, they are considered separately for each DoF<DT service category> in the RTE. The RTE's DoF is computed as a DoF average for all the identified DT service categories, as indicated in Table 15. Table 15 represents the DoF for the sixth production deployment iteration of the RTE based on Equation 10.

DT service classification	**Paradigms to Evaluate DoF**						
	DCF <DT service classification>	**tMA**	**tEA**	**tIoS**	**tEIoS**	**tIDX**	**DoF <DT service category>**
Synergistic	0.3	0.02	0.1	0.02	0.03	0.03	12
Cooperative	0.5	0.2	0.14	0.15	0.04	0.025	55.5
Conflictive	0.15	0.15	0.035	0.2	0.02	0.1	15.15
Cognitive	0.2	0.2	0.15	0.18	0.05	0.01	23.6
Conductive	0.7	0.1	0.2	0.08	0.028	0	57.12
Governing	0.15	0.01	0	0.1	0.015	0.05	5.25
RTE’s Degree of Fragmentation (DoF)							**28.10**

Table 15: DoF during the sixth production deployment iteration

Figure 20 presents the DoF of each DT service category from the production deployment iteration 1 to iteration 6.

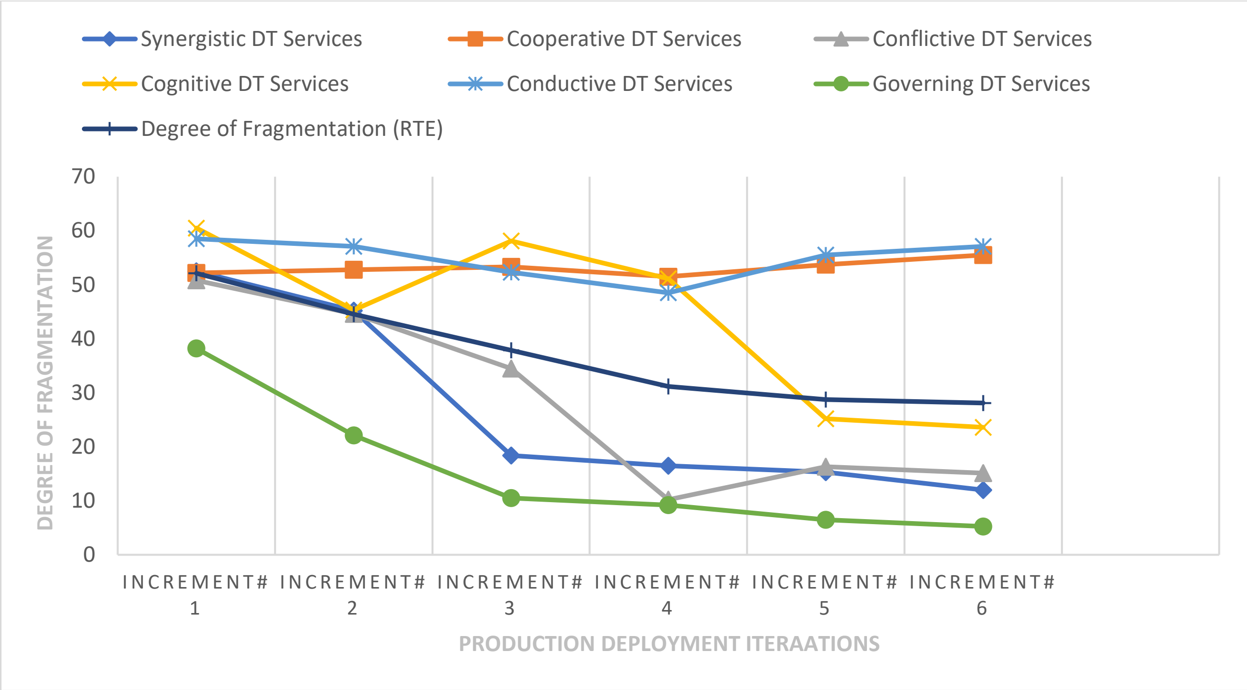


Figure 20: DoF evaluation in the production deployment iteration# 1 to #6

APPENDIX A.5: PW6: DT services maintainability index (DSMI)

The thrust of evaluating the DT service maintainability index is to derive the relationship between the BP activities and DT services to perform and provide actions to the specific set of digital activities. For instance, DT services must complete customer validation before acknowledging the successful registration to the eCommerce platform; else, it introduces the risk of unauthorized access to the customer account. The following are the BPs selected for the experiment.

BP# 1: Customer enrollment and registration. The BP is to enroll new customers or register existing customers to the eCommerce platform. The customer validation and account creation BP activities are part of this BP.

BP# 2: Manage customer information, inquiry, and history. The BP manages the customer information. It has various access levels, including the customer, call center agent, and administration, to update and retrieve the customer information for different purposes.

BP# 3: Purchase order management. The BP is to manage the purchase order. It includes selecting the items, online shopping cart management, and the checkout process for the eCommerce platform customer.

BP# 4: Payment processing and account receivables. The BP is for the payment processing, shipping, vendor management, and account receivable.

BP# 5: Invoicing. It is the BP of managing invoices and returning procedures of the already purchased items.

BP# 6: Notification and acceptance of terms. The BP includes notification and acceptance of the terms for compliance reasons to access the online capabilities of the eCommerce platform. The RTE can configure the level of notifications for individual customers based on the customers' preferences. For example, RTE administration can set order delivery notifications to either customer’s email address or mobile messaging.

BP# 7: Account management. The customer can manage the account through this BP. The RTE administrator and the customer can upgrade to the premium services. The authorized user can change other customers’ profile information through this BP. For example, the address change for the customer.

The velocity (V) of the RTE represents the rapid changes and updates necessary to achieve the BP requirements. Updating or introducing DT services, granular level of DT service operations, BP activities, or sublevel of the BPs can achieve the desired changes. Correspondingly, the velocity is based on four types of ratios as specified below. The ratios represent the level of change necessary to achieve the goals of BP requirements.

- DT services’ ratio (DSR): The DSR represents the number of DT services introduced to the RTE to perform the DT activities over a total number of existing DT services.
- DT service operations' Ratio (OPR): The OPR represents the number of DT service operations introduced to the RTE to perform the digital activities over a total number of existing DT services' operations.
- BP activities’ ratio (AR): The AR represents the number of BP activities introduced to the RTE to perform the digital activities over a total number of existing BP activities.
- Sublevel BPs’ ratio (SBR): The SBR represents the number of sublevel BPs introduced to the RTE to perform the DT activities over a total number of existing sublevel BPs.

$$V = \frac{\sum_{BP=1}^{\#BPs} m\times DSR + l\times OPR + h\times AR + c\times SBR}{\#BPs} \quad (11)$$

The velocity evaluation presented in Equation 11 introduces the impact factor corresponding to each ratio, that is, c (critical), h (high), m (medium), and l (low). The assigned values for the impact factors are c = 10, h = 7, m = 4, and l = 2 to indicate finite value for the severity of update. The following describes the levels of impact factor and their utilization.

- **c (critical):** If the sublevel BP is introduced to meet specific compliance, regulation, or standard, then it falls under the critical category. For example, payment information verification BP is the sublevel BP since it has the highest impact on the customer's online purchasing experience. It is the reason the BP sublevel introduction and modification has a critical impact factor, and it is assigned the highest impact factor value, that is, 10.
- **h (high):** The impact of introducing or updating the BP activity is higher than introducing the DT services and DT service operations. However, the impact is lower than introducing the sublevel BPs. For example, the BP activity to set up the payment notification has a lower impact than payment verification BP. However, it has a higher impact than notifying the completion of a transaction. Typically, these BP activities are 30% lower than the sublevel BPs. It is the reason; that the high impact category has an assigned value of 7 (30% less than the critical category of the impact).
- **m (medium):** The impact of introducing or updating the DT services is higher than introducing the DT services' operations. However, the impact is lower than introducing the BP activities. For example, the DT service to send a reminder for the payment has a lower impact than setting up the autopayment. However, higher impact than the call back function after sending the reminder for the payment. Typically, the impact of DT services is 60% lower than the sublevel BPs, and it has an assigned value of 4 (60% less than the critical category of the impact).
- **l (low):** The impact of introducing or updating the DT services' operations is lower than introducing DT services. It has the lowest level of changes and granular level of operations. For example, acknowledgment of notification sent to the customer's mobile devices. Typically, the impact of DT services' operations is 80% lower than the sublevel BPs, and it has an assigned value of 2 (80% less than the critical category of the impact).

DT services' operations, DT services, BP activities, and sublevel BPs reused across multiple BPs are counted for accuracy to evaluate velocity. Table 16 provides an implementation-based analysis and computed velocity of BP requirements' fourth production deployment iteration corresponding to the identified BPs (as described above). The following are the acronyms utilized in Table 16.

- #DTS: Total number of participants' DT services for the BP.
- #OP: Accumulative number of DT services' operations involved.
- #A: Total number of BP activities for the BP.
- #SBP: Total number of sublevel BPs of the BP.
- #ACS: Sum of new and updated DT services to the BP in the production deployment iteration 4.
- #AOP: Sum of the new and updated number of DT services' operations introduced to the BP in the production deployment iteration 4.
- #AA: Sum of new and updated BP activities introduced to the BP in the production deployment iteration 4.
- #ASBP: Sum of new and updated sublevel BPs introduced to the BP in the production deployment iteration 4.

There is no maximum limit set for the velocity (V). However, the current production deployment iteration's velocity (V) score is considered the baseline for subsequent deployment iterations.

BP#	#DTS (#ACS)	# OP (#AOP)	#A (#AA)	#SBP (#ASBP)
1	7(0)	20(2)	8(1)	2(0)
2	12(3)	28(7)	15(0)	3(0)
3	18(4)	42(7)	22(2)	5(1)
4	8(2)	15(3)	15(2)	3(0)
5	5(1)	12(2)	10(1)	3(0)
6	3(0)	8(1)	7(0)	1(0)
7	9(2)	16(3)	14(1)	2(0)
V = 1.52				

Table 16: Velocity (V) of the RTE in the production deployment iteration# 4

The DT services maintainability index (DSMI) computes and continuously monitors the maintainability of DT services. The paradigms to formulate the DT services maintainability index is described below for the types of DT services.

Business continuity (BUC): Business continuity determines whether the introduced or updated DT services can continue the day-to-day business activities after the deployment (or iteration). The evaluation criterion for the business continuity paradigm is to monitor the number of unique support tickets created for the type of DT services in the context. For example, new customer registration provides errors due to inaccuracies in validating customer account numbers or customer identification. The inverted ratio for business continuity specific to DT services associated with the DT service type is derived below.

- #ST<DT service category>: Number of unique support tickets by the customers in the current production deployment iteration for a specific DT service category.
- #DTS<DT service category>: Number of DT service deployers for the specific DT service category in the current production deployment iteration.

$$iBUC < DT\ service\ category > \\ = (\#ST < DT\ service\ category > / \#DTS < DT\ service\ category >)$$

Operational risk (ORI): Operational risks evaluate the DT service level continuation of the RTE operations. RTE traces the number of failures that occurred for the DT services in the production of the present deployment iteration. A specific example is the change purchase order request specific DT service failed due to unambiguous conditions within dedicated DT services. The inverted ratio for ORI specific to DT services associated with the DT service type is derived below.

- #OF<DT service category>: Number of unique operational failures in the current production deployment iteration for a specific DT service category.
- #DTS<DT service category>: Number of DT service deployers for the specific DT service category in the current production deployment iteration.

$$iORI < DT\ service\ category > \\ = (\#OF < DT\ service\ category > / \#DTS < DT\ service\ category >)$$

The ratio of operational risk is generated by comparing with the failures of the previous deployment iteration. The DT services header contains the probability of failures, and it is automated to gain indicative operational risk at runtime.

Service level agreement factorization (SPR): Service level agreement factorization accumulates scalability, reliability, and performance (SPR). The service level agreement is defined considering the desired level of scalability, reliability, and performance anticipated for each DT service category. The SPR is identified based on the number of violations by the category of DT services in the current production deployment iteration. The four-second delay (when the service level agreement is set for three seconds) in sending confirmation to the vendor for the specific product due to heavy traffic is an example of a service level agreements violation. The inverted ratio for SPR specific to the set of DT services associated with the DT service category is derived below.

- #SPR<DT service category>: The number of unique scalability, reliability, and performance-specific service level agreement violations in the current production deployment iteration for a specific DT service category.
- #DTS<DT service category>: Number of DT service deployers for the specific DT service category in the current production deployment iteration.

$$iSPR < DT\ service\ category > \\ = (\#SPR < DT\ service\ category > / \#DTS < DT\ service\ category >)$$

Consistency (COS): RTE can evaluate consistency in many different aspects. The primary objective of this criteria is to assess the scope of the DT service across multiple BP activities. Due to the BP requirements, the specification of the DT service needs to incorporate high-level interactions with RTE data entities and underneath events of BP activities. The consistency of DT service is being derived based on the number of BP activities utilizing the specific type of DT services in consideration. The most prominent example is order delivery confirmation, and status needs to send to customer, vendor, and account receivables. The inverted ratio for consistency specific to the set of DT services associated with the DT service type is derived below.

- #BPA<DT service category>: Number of BP activities utilizing DT services in the current production deployment iteration for a specific DT service category.
- #DTS<DT service category>: Number of DT service deployers for the specific DT service category in the current production deployment iteration.

$$iCOS < DT\ service\ category > \\ = (\#BPA < DT\ service\ category > / \#DTS < DT\ service\ category >)$$

Extendibility and continuous improvements (ECI): Extensibility and continuous improvement of the DT services are evaluated based on customization required to accomplish BP requirements. The number of additional custom modeling and implementation needed in the context of BP activity and the RTE data entity. The primary objective is whether respective DT services can accommodate these customizations within the dilemma of their dependencies with existing RTE data entities. For example, if the payment is not received within six months, it needs to be sent for collection, and the vendor also needs to be notified. It is an example of the extendibility of DT services associated with payment processing and account receivable BP. The inverted ratio for extendibility and continuous improvement specific to the set of DT services associated with the DT service type is derived below.

- #ABPAF<DT service category>: Number of alternate BP flows accustomed in DT services in the current production deployment iteration for a specific DT service category.
- #DTS<DT service category>: Number of DT service deployers for the specific DT service category in the current production deployment iteration.

$$iECI < DT\ service\ category > \\ = (\#ABPAF < DT\ service\ category > / \#DTS < DT\ service\ category >)$$

"*n*": The number of DT service types identified in the RTE. It is 10 in this case, as indicated in Chapter 6.2 and published work PW6.

#Paradigms: The number of paradigms to impact the DT service maintainability index (DSMI) is 5, as described above, that is, BUC, ORI, SPR, COS, and ECI.

The inverted DT service maintainability index (iDSMI) is computed based on Equation 12.

$$iDSMI = (1\ /\ DSMI) = \frac{\left[\frac{\sum_1^n iBUC}{n}\right]+\left[\frac{\sum_1^n iORI}{n}\right]+\left[\frac{\sum_1^n iSPR}{n}\right]+\left[\frac{\sum_1^n iCOS}{n}\right]+\left[\frac{\sum_1^n iECI}{n}\right]}{\#Paradigms} \quad (12)$$

Table 17 below presents the DT service maintainability index computed in the production deployment iteration 4 for the identified and deployed BPs.

Paradigm / DT service category (#DTS)	iBUC	iORI	iSPR	iCOS	iECI
Competency (6)	0.33	0.83	0.5	0.5	0.67
Relationship (12)	0.25	0.67	0.5	1.5	0.5
Collaboration (4)	0.25	0	0.25	0.5	0.25
Common (7)	0.29	0.14	0.42	2	0.29
Framework (8)	0.5	0.25	0.75	0.5	0.38
Governance (6)	0.33	0.5	0.33	1.5	0.83
Organizational (7)	0.29	0.14	0.42	0.71	0.86
Strategic (7)	0.14	0	0.14	1	0.42
Conditional (5)	0.6	0.8	0.4	0.4	0.2
Automation (3)	0.33	0.67	1.67	0.67	2
DSMI (of the production deployment Iteration# 4) = 1.76					

Table 17: DT service maintainability index (DSMI) in the production deployment iteration# 4

Figure 21 provides the progress of velocity (V) and DT service maintainability index (DSMI) through production deployment iterations 1 to 4 for the identified 7 BPs deployed, advanced, and monitored.

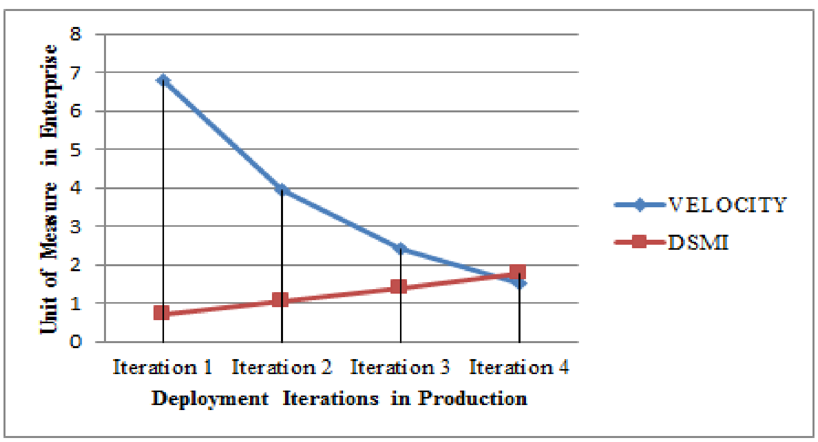


Figure 21: The Velocity (V) and the DSMI in the production deployment iterations 1 to 4

APPENDIX A.6: PW8: Degree of process classification (DOPC)

The degree of process classification (DOPC) evaluates the RTE operational governance framework corresponding to the correlation between the classification of processes and advancements in mobile commerce operations. A pharmacy store's supply chain use case is developed to illustrate the evolving characteristics of DOPC. The evaluation included healthcare or mobile devices and DT services (including mobile banking, social networking integration, and analytics) across existing mobile commerce operation models utilizing the RTE operational governance framework for the pharmacy store's customers. An example of mobile commerce operations is payment processing through the secure payment gateway. However, there are dimension factors associated with each mobile commerce operation. An appropriate illustration of a dimensional factor is the security of payment information during payment processing. The dimension factor represents dependency on DT's advancements in mobile commerce, such as mobile payment processing. Multiple mobile commerce operations can be associated with dimensional factors, and vice versa is also possible. The mobile commerce operations are a participant of the BP activities. Each BP activity is associated with RTE participants and service level agreements to ensure the performance of mobile commerce operations.

Equation 13 represents the method to evaluate the DOPC for each DT service classification. Based on the RTE processes based on the DT service categories identified in Chapter 6.4 and published work PW8. Following are the interpretation of each term indicated to derive a DOPC for each RTE process classification.

- rMCOM: The ratio of the impacted (or new) DBOs and the total number of DBOs corresponding to the update or introduction of DT services of the specific DT service category for the RTE processes.
- rDF is the ratio of the impacted (or new) dimension factors and the total number of dimensional factors corresponding to the update or introduction of the DBOs for the specific DT service category.
- rBA is the ratio of the impacted (or new) BP activities and the total number of BP activities corresponding to the update or introduction of the DBOs for the specific DT service category.
- rRPT is the ratio of the impacted (or new) types of RTE participant roles and the total number of RTE participant roles corresponding to the update or introduction of the DBOs for the specific DT service category.

- rSLA is the ratio of the impacted (or new) service level agreements and the total number of service level agreements defined corresponding to the update or introduction of the DBOs for the specific DT service category.
- **"*r*"** is the number of paradigms to evaluate the degree of process classification for specific RTE process classification (*r* = 5 for rMCOM, rDF, rBA, rRPT, and rSLA).

$$DOPC_{<DT\ service\ classification>} = \frac{[rMCOM + rDF + rBA + rPT + rSLA] \times 10^{r-2}}{r} \quad (13)$$

Equation 14 presents the approach to computing the DOPC of mobile commerce for the current production deployment iteration. The **"*n*"** represents the total number of DT service classifications based on the RTE processes (*n* = 8 as indicated in Chapter 6.4), and **"l"** is the level of the RTE process in the hierarchy of RTE processes. The RTEs can derive levels of RTE processes based on a number of different criteria. The four levels of RTE processes are defined for the experimental evaluation based on the order of invocation of the DT services associated with the RTE process, as indicated in Chapter 6.4 Figure 12.

$$DOPC = \frac{\left[\sum_{i=1}^{n} DOPC_i \times {}^{1}/_{l_i}\right]}{n} \quad (14)$$

Table 18 provides the degree of process classification for each RTE process classification and DOPC of the mobile commerce ecosystem in production deployment iteration 7. At the end of iteration 7, mobile commerce was operating under 75 mobile commerce-specific DBOs, 50-dimensional factors, 40 business activities, 25 participant roles, and 90 service level agreements.

RTE process Classification	**Paradigms to Evaluate DOPC**					
	rMCOM	**rDF**	**rBA**	**rRPT**	**rSLA**	***DOPC <RTE Process Classification>***
Onboarding processes	0.027	0.02	0.025	0	0.044	23.2
Correlation processes	0.12	0.04	0.125	0.08	0.133	99.6
Management processes	0.08	0.06	0.05	0.04	0.089	63.8
Personalization processes	0.24	0.12	0.2	0.24	0.167	193.4
Activity divergence processes	0.04	0.04	0.25	0.08	0.0556	93.12
Provisioning processes	0.013	0.1	0.125	0.04	0.033	62.2

RTE process Classification	Paradigms to Evaluate DOPC					
	rMCOM	rDF	rBA	rRPT	rSLA	*DOPC <RTE Process Classification>*
Service qualitative processes	0.04	0.06	0.075	0.08	0.22	95
Transaction level processes	0.08	0.08	0.1	0.12	0.167	109.4
DOPC for mobile commerce						**34.03**

Table 18: DOPC in the production deployment iteration# 7

Figure 22 presents the progress of the DOPC from the production deployment iteration 1 to the production deployment iteration 7 for each DT service classification based on RTE processes.

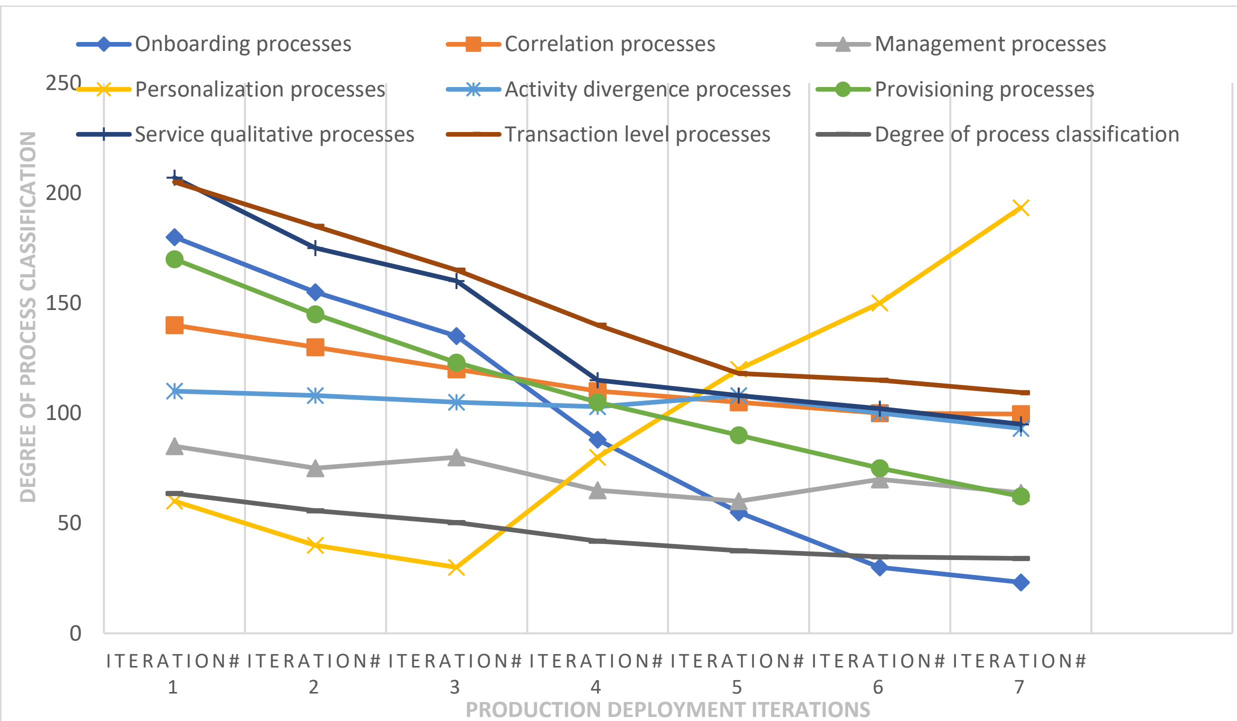


Figure 22: DOPC of mobile commerce in the production deployment iterations # 1 to 7

APPENDIX A.7: PW7: Edge policy integrity gradient (ePIG)

Provisioning the RTE's policies in the APIs or DT services is novel, and there is no standard way of evaluating the effectiveness of the policy-based DT services. The edge policy integrity gradient (ePIG) measures RTE architecture evolution based on the identified categories of DT services from the policy provisioning lifecycle phases in Chapter 2.6.1 Figure 4 and published work PW7. The use case of smart healthcare implied the RTE architecture components and the policy provisioning lifecycle defined in Chapter 2.6.1 to illustrate the ePIG. Chapter 6.5 and the published work PW7 describe DT services' identified categories based on the RTE policies.

The policy impact level (PIL) is the terminology to formulate the impact of policy APIs (or DT services) at each phase of the policy provisioning lifecycle (PPL). Policy impact level 1 corresponds to the policy provisioning lifecycle phase I. If the policy API impacts the already defined registration, formalization, and standardization, then the policy API's impact level is at the highest policy impact level 1. Policy impact level 2 is for the effect of policy API at policy provisioning lifecycle phase II. Similarly, policy impact levels 3, 4, 5, and 6 were derived for the impact of policy application programming interfaces at policy provisioning lifecycle phases III, IV, V, and VI, respectively. The finite policy impact level value (PILV) for each policy impact level 1 through level 6 is assigned to impact policy provisioning lifecycle phases to quantify the diversity of policy application programming interfaces.

- **Policy impact level value 1 (PILV1)** is associated with the policy impact level 1 and, in turn, with the policy provisioning lifecycle (PPL) phase I described in Chapter 2.6.1 Figure 4. The highest possible finite value associated with policy impact level 1 is 1.0 since it has the highest impact on the RTE, PILV1 = 1.0. For instance, standardizing access to the network resource configuration impacts the runtime system resource utilization and causes operational failures.
- **Policy impact level value 2 (PILV2)** is associated with the policy impact level 2 and, in turn, with the policy provisioning lifecycle (PPL) phase II described in Chapter 2.6.1 Figure 4. The finite value associated with policy impact level 2 is 0.8, PILV2 = 0.8. Typically, resolving the dependencies through application programming interfaces increases extendibility and introduces consistency across RTE. It has 20% less impact over policy impact level 1.
- **Policy impact level value 3 (PILV3)** is associated with the policy impact level 3 and, in turn, with the policy provisioning lifecycle (PPL) phase III described in Chapter 2.6.1 Figure 4. The finite value associated with policy impact level 3 is 0.6, PILV3 = 0.6. The interconnectivity paradigms are defined in policy provisioning lifecycle phase III. It has a higher impact on notification and acknowledgment; however, lower impact than resolving the dependencies across the RTE architecture through application programming interfaces.

- **Policy impact level value 4 (PILV4)** is associated with the policy impact level 4 and, in turn, with the policy provisioning lifecycle (PPL) phase IV described in Chapter 2.6.1 Figure 4. The finite value associated with policy impact level 4 is 0.4, PILV4 = 0.4. The runtime changes to the policies are accomplished in policy provisioning lifecycle Phase IV. It has 60% less impact than introducing the policy application programming interfaces since essential standardization is already established in policy provisioning lifecycle phase I.
- **Policy impact level value 5 (PILV5)** is associated with the policy impact level 5 and, in turn, with the policy provisioning lifecycle (PPL) phase V described in Chapter 2.6.1 Figure 4. The finite value associated with policy impact level 5 is 0.2, PILV5 = 0.2. The notifications are configurable through policy application programming interfaces. It has a much lower impact (80% lower) than enforcing regulatory requirements in policy provisioning lifecycle phase I.
- **Policy impact level value 6 (PILV6)** is associated with the policy impact level 6 and, in turn, with the policy provisioning lifecycle (PPL) phase VI described in Chapter 2.6.1 Figure 4. The finite value associated with policy impact level 1 is 0.1, PILV6 = 0.1. Automation has the lowest impact; however, it brings consistency across policy application programming interfaces. It has 90% less impact over standardization since RTE can use only automation efficiently after the standardization.

Equation 15 provides the formulae to compute the average impact factor (IF<c >) of the updated or newly introduced policies. #cPA represents the number of policies associated with the specific DT service category required to be updated or introduced. Each policy can fall only into one DT service classification. A single policy-based DT service can impact multiple policy provisioning lifecycle phases. In such cases, the average is considered for computing the impact factor of the specific DT service category (IF<c>). For instance, if a specific policy associated with the DT service category is impacting policy provisioning lifecycle phase I and policy provisioning lifecycle phase IV, then ((PILV1 + PILV4)/2), that is, "0.7" in finite value, is placed in Equation 15.

$$IF < c > = \frac{\sum_{i=1}^{\#cPA}[PILV<i>]}{\#cPA} \quad (15)$$

Equation 16 represents the method for evaluating the edge policy integrity gradient for each DT service category (ePIG<c>) identified in Chapter 6.5. the variability of the RTE architecture for mobile edge computing depends on the policies, DT services deployed as APIs, participant application under the RTE architecture components, dimensional factors of the RTE operational governance framework (Chapter 4), and the service level agreements. The following five paradigms are considered to assess ePIG<c>.

- #PA is the number of policies associated with the specific DT service category.
- #cPA is the total number of either new or updated policies associated with the specific DT service category.
- #API is the total number of APIs (or DT services) in the current production deployment iteration for the DT service category.
- #cAPI is the number of APIs (or DT services) either introduced or updated in the current production deployment iteration for the DT service category.
- #CA is the total number of participant applications in the current production deployment iteration for the DT service category.
- #cCA is newly introduced or updated participant applications in the current production deployment iteration for the DT service category.
- #DIM presents the total number of dimensional factors in the current production deployment iteration for the DT service category.
- #cDIM is the number of dimensional factors introduced or updated in the current production deployment iteration for the DT service category.
- #SLA is the total number of service level agreements associated with the policies for the DT service category in the current production deployment iteration.
- #cSLA is the number of service level agreements violated in the current production deployment iteration associated with the policies associated with the DT service categories.
- "r" represents the number of paradigms to evaluate each DT service classification's edge policy integrity gradient. The value of "r" is five since the above paradigms derive the ePIG, that is, #PA, #API, #CA, #DIM, and #SLA.

$$ePIG < c > = \frac{IF{<}c{>}\times(\#PA\times\#API\times\#CA\times\#DIM\times\#SLA)}{\#cPA\times\#cAPI\times\#cCA\times\#cDIM\times\#cSLA\times 10^{r-1}} \quad (16)$$

Based on Equation 16, if the policy is not updated or introduced for the specific DT service category, the denominator in Equation 16 will not have any values for any of the paradigms. The ePIG for each DT service category will be at its peak. Table 12 provides the values of all the paradigms specified in Equation 16 for each identified DT service category (Chapter 6.4) in the production deployment iteration 8. At the production deployment Iteration 8, 70 policy-based DT services, 225 total DT services, 15 RTE participants, 12-dimension factors, and 145 service level agreements were recorded.

Policy classification		**Paradigms to derive ePIG**					
	IF <c>	#cPA	#cAPI	#cCA	#cDIM	#cSLA	*ePIG <c>*
Consumer privacy and confidentiality policies	0.5	1	5	3	2	4	171.28
Dimensional subjectivity policies	0.45	2	5	1	3	8	77.08
Functional objectivity policies	0.65	3	6	2	3	3	82.47
Resource intensive policies	0.6	3	3	3	2	5	91.35
Constitutional policies	0.55	4	7	4	1	2	100.93
Operative policies	0.7	1	5	3	1	10	191.84
Coverage policies	0.4	2	3	4	2	3	114.19
Network service's connectivity policies	0.75	1	9	3	1	6	190.31
	ePIG of RTE						127.43

Table 19: ePIG of RTE in the production deployment iteration 8

Figure 23 presents the progress of the edge policy integrity gradient for each DT service category and the overall edge policy integrity gradient of mobile edge computing from the production deployment iteration 1 to the production deployment iteration 8.

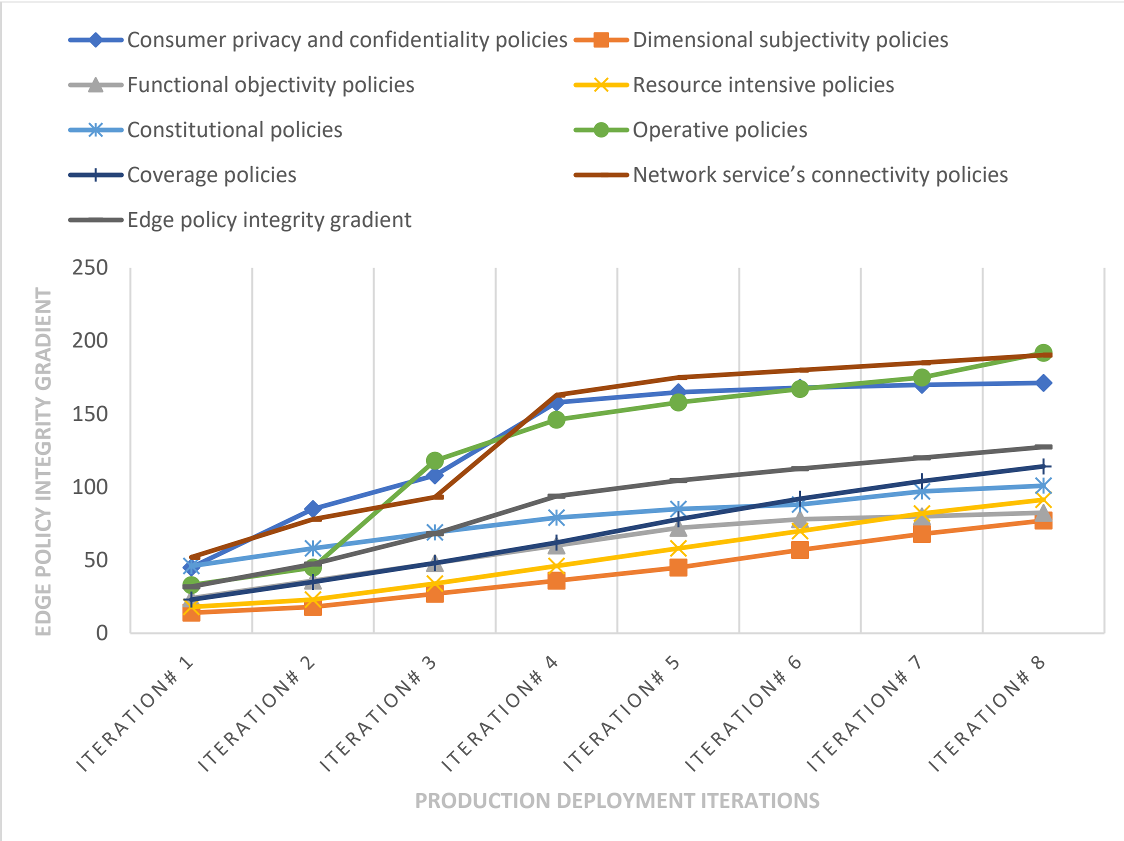


Figure 23: Progression of ePIG in the production deployment iteration# 1 to 8

APPENDIX B: RTE architecture's scenario-based experiments and results

APPENDIX B.1: PW3: Inductivity (L) of the RTE scenarios

The inductivity (L) of the RTE architecture, identified in the published work PW3, provides the measure of changes performed to mitigate the incremental risks during the introduction and updates of the DT services. The DBOs and corresponding identified scenarios are associated with one or more of the following BPs to practically evaluate the inductivity (L) of the RTE architecture.

BP# 1: Online customer enrollment. The registration and account validation DBOs utilize this BP.
BP# 2: Manage customer information, inquiry, and history. Customer payment history is the type of the DBO utilizing this BP.
BP# 3: Manage purchase orders. Removing the item from a purchase order is an example of a DBO utilizing this BP.
BP# 4: Delivery of product and service. Assigning a vendor to deliver a specific product is the DBO utilizing this BP.
BP# 5: Manage inventory. Supplier removing a number of items from inventory after delivery is an example of the DBO utilizing this BP.
BP# 6: Online billing and invoicing. Generating invoices is an example of the DBO utilizing this BP.
BP# 7: Payment processing and account receivable. The bank's credit card payment processing is a type of the DBO utilizing this BP.
BP# 8: Online notification and acceptance of terms. Updating payment term is the DBO utilizing this BP.
BP# 9: Online support and resolution. Requesting a different address is an example of a DBO utilizing this BP.

Scenarios attempt to compute the worst-case possibility considering all the participants of the RTE in the provided timeframe. The production deployment iterations were typically set for 4 to 5 weeks to capture and iterate scenario categories and associated incremental risks (IRs) using the incremental risk governance framework. The empirical evaluation was completed in eight production deployment iterations. The severity levels were assigned to each identified incremental risk. Although RTE can define its severity levels and interpret the severity levels, the following five severity levels of incremental risks were determined and utilized to assess the inductivity (L) of the RTE architecture.

- **Incremental risk severity level 1 (catastrophic)**: If the incremental risk is anticipated to be critical and interrupts continuity in the day-to-day business for the specific scenario's DBO, then it is categorized under incremental risk severity level 1. It has the highest level of the value assigned. The incremental risk severity level value (ISLV) 1 has set the finite value of 1 (ISLV1 = 1) to indicate the highest criticality level.
- **Incremental risk severity level 2 (significant)**: If the operational level failure of the RTE's DBO is possible due to an incremental risk, it has been identified as incremental risk level 2. Usually, the incremental risks associated with the scenario categorized under incremental risk severity level 2 are relatively less than those under incremental risk severity level 1. However, it has a significant impact as it may allow erroneous transactions. Typically, it is 20% less severe than the incremental risk severity level 1; incremental risk severity level value 2 (ISLV2) has been assigned with a finite value of 0.8 (ISLV2 = 0.8).
- **Incremental risk severity level 3 (moderate)**: An incremental risk is estimated to violate one or more specified service level agreements for the DBO of a specific scenario category. It is categorized under incremental risk severity level 3. The incremental risk associated with the scenario is usually 40% less severe than the incremental risk severity level 1; that is, severity level value 3 (ISLV3) has been assigned with a finite value of 0.6 (ISLV3 = 0.6).
- **Incremental risk severity level 4 (low)**: If there is an anticipation of a request for an additional feature or add-on capability for the DBO of a specific scenario category, then the risk associated with the scenario is categorized in incremental risk severity level 4. Typically, it is recoverable and usually 60% less severe than the incremental risk severity level 1; incremental risk severity level value 4 (ISLV4) has been assigned with a finite value of 0.4 (ISLV4 = 0.4).
- **Incremental risk severity level 5 (negligible)**: If the particular extension has expected to include monitory help for consumers within the DBO of a specific scenario category, it falls into incremental risk severity level 5. It has practically minimal to no impact and is usually 80% less severe than the incremental risk severity level 1; incremental risk severity level value 5 (ISLV5) has been assigned with a finite value of 0.2 (ISLV5 = 0.2).

The average weighing for the category of scenario is computed based on the number of DBOs, the corresponding number of incremental risks associated with the specific category of scenario, and the severity level determined for the incremental risks. Equation 17 presents the average weighing (AW) of the scenario category in consideration.

- "n" represents the number of levels defined for the severity in the present iteration (n = 5 for ISLV1 to ISLV5).
- #IR<sc> is the total number of incremental risks of the DBOs within the scenario category in the current production deployment iteration.
- #IR<sc><ISL> is the number of incremental risks that fall into the specific incremental severity level in the context of the scenario category or <sc> for the current production deployment iteration.
- ISLV<sc> has an assigned value based on the level of the incremental risk severity for the specific category of scenarios.

$$AW < sc > = \frac{\sum_{i=1}^{n}[ISLV<i>]\times[\#IR<i><ISL>]}{\#IR<sc>} \quad (17)$$

The inductivity of the DBOs associated with the specific category of scenarios (L<sc>) is identified in Equation 18, providing an indicative number for the probability of scenario occurrences (for the specific category). In Equation 18, the following is the terminology utilized to formulate the inductivity (L).

- #DBO represents the total number of DBOs in the current production deployment iteration.
- #BPs represent the total number of BPs in the current production deployment iteration.
- #CAs are the total number of consumer applications in the current deployment iteration.
- #EEs is the total number of RTE data entities in the current production deployment iteration.
- #DBOs<sc> is the number of DBOs associated with the specific scenario category during the current production deployment iteration.
- #BPs<sc> is the number of BPs related to the particular scenario category during the current production deployment iteration.
- #CAs<sc> is the number of consumer applications associated with the specific scenario category during the current production deployment iteration.
- #EEs<sc> is the number of RTE entities related to the scenario category during the current production deployment iteration.
- *"p"* presents a number of paradigms in consideration (p = 4 for the paradigms DBO, BPs, CAs, and EEs).
- AW<sc> computed using Equation 17 for the specific category of scenario in the current production deployment iteration.

$$L < sc > = \frac{(AW<sc>\times\#DBO<sc>\times\#BPs<sc>\times\#CAs<sc>\times\#EEs<sc>)\times 10^{p-1}}{\#DBOs\times\#BPs\times\#CAs\times\#EEs} \quad (18)$$

Table 20 represents the L<sc> recording of the production deployment iteration 8 of the categories of scenarios and associated DBOs. If the DBO participates in multiple scenario categories, they are considered in both categories to provide accuracy while analyzing the impact. Similarly, if the same incremental risks are present in the DBOs for a single scenario, it is considered various times to compute the weighing of the scenario category.

Scenario category	**Scenario category paradigms**						
	#IRs	**AW**	**#DBOs**	**#BPs**	**#CAs**	**#EEs**	**L<sc>**
Cognitive scenarios	12	0.6	18	5	7	10	18.93
Explorative scenarios	14	0.7	23	6	8	12	46.46
Predictive scenarios	18	0.65	20	7	9	16	65.65
Normative scenarios	10	0.48	14	9	9	8	21.82
Interceptive scenarios	8	0.56	10	7	5	15	14.73
Substantive scenarios	7	0.4	8	4	4	9	2.3
Procedural scenarios	9	0.34	12	6	7	13	11.16

Table 20: Inductivity (L) of scenario categories in the production deployment iteration# 8

Figure 24 provides the total number of DBOs in each deployment iteration and the inductivity of each category of scenarios for the corresponding iterations. It is apparent from the presented analysis in Figure 24 that each category of scenarios has a different pace of inductivity (L) and respective probability of incremental risks' occurrence rate.

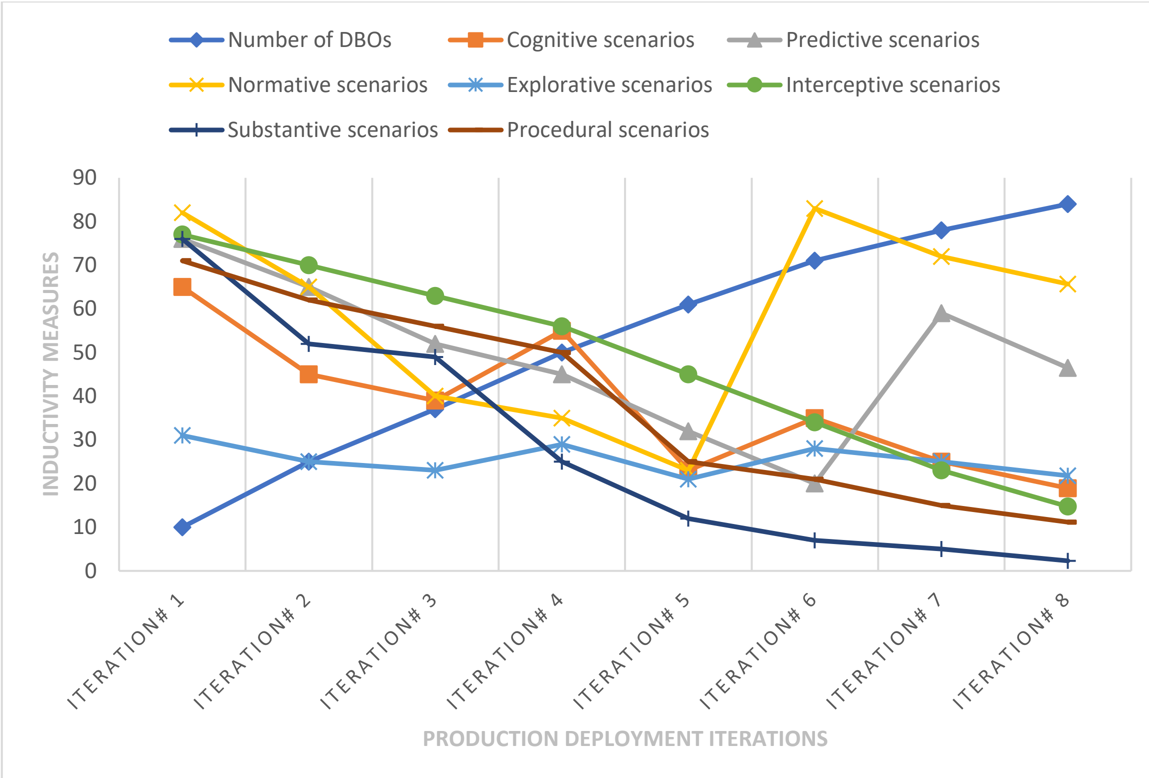


Figure 24: The inductivity (L) in the production deployment iterations # 1 to 8

APPENDIX B.2: PW1: Average standard deviation in throughput

When mobile edge computing resources run over virtual infrastructures [106], adding flexible and scalable resource management capabilities, it transforms into a heterogeneous cloud computing environment [109]. The environment enables users to publish DT services, allowing data processing and storage to move from the devices to a centralized computing platform in the heterogeneous cloud platform. Other users accessed these DT services over the wireless connection based on a thin native client or web browser. Essentially, it is an infrastructure where the DT services, data storage, and data processing occur outside the devices.

A fundamental problem is the complete delegation of the DT services and corresponding heterogeneous cloud users that require autonomous intelligence from clients to the heterogeneous cloud. The heterogeneity of the clouds, nature of knowledge generated, and heterogeneity of data processing are the inherent concerns of any RTE. It is viewed as a computational grid consisting of many DT services generating cognitive information-base for processing.

DT services can carry out specific tasks for a set of DT services. They have a degree of intelligence that permits RTE to perform part of their task autonomously. To evaluate the implications of the scenarios derived based on DT service capability utilization, an integrated heterogeneous cloud environment for smart manufacturing is implemented during experimentation in the published work PW1. Diversifications in heterogeneous clouds are primarily focused on manufacturing supply-chain management and industrial IoT cloud based on the identified DT service capability utilization categories in Chapter 7.2. It consists of 150 nodes, with each node having 12 cores and 128 GB of memory (2.30 GHz frequency).

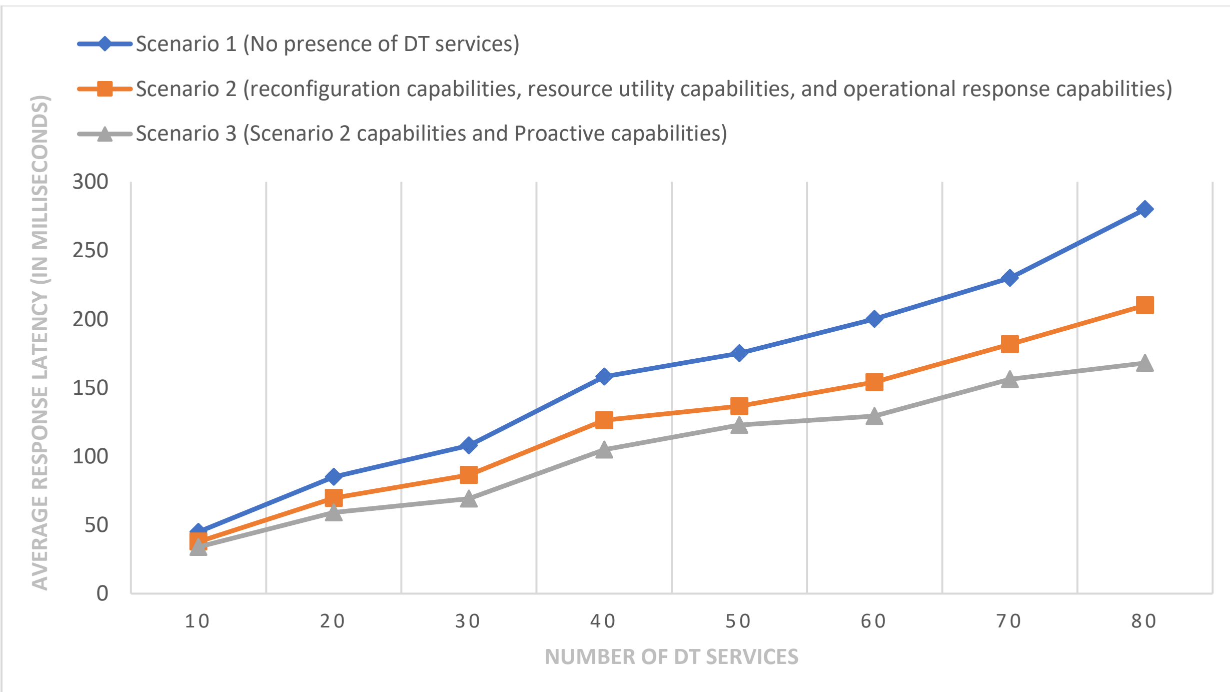


Figure 25: Response latency and number of DT services

The first level of feature capabilities to enable or disable a set of IoT APIs (as DT services) is introduced for evaluating the impact of resource reconfiguration capability, resource utility capability, operational response capability, and proactive enablement of DT services capabilities. The RTE measures the DT services' response latencies during integrating IoT APIs (as DT services) between the system resources through abstracting Microservices [112]. Additionally, the access latency captured from the mobile edge computing communication channels for all three scenarios considering resource access over the heterogeneous cloud. The following are the approached scenarios.

- Scenario 1: No presence of DT services.
- Scenario 2: Enabling DT services developed and deployed to provide reconfiguration, resource utility, and operational response capabilities.
- Scenario 3: Enabling DT services developed and deployed to provide proactive capabilities with all the other DT services developed and deployed in scenario 2.

The response latency reduces as DT services develop and deploy for resource utility capabilities. The response latency has a higher rejection rate as more IoT APIs were introduced in the form of DT services. In scenario 2, it starts at a 16 % reduction in response. However, it was at a 25% reduction when all the IoT APIs were introduced to the RTE. It further improves the result by 10% to 20% depending on the dependencies between resources in scenario 3.

Another assessment was performed to evaluate the concurrent IoT APIs (DT services) and corresponding violations of service level agreements. The following are the service level agreements considered to capture the service level agreement violations due to concurrent IoT APIs in the mobile edge computing

- Accessibility of the DT services (or IoT devices).
- Response time of the DT services.
- Availability of the DT services.
- Quality of the DT services.
- Quantity of the information received through the DT services.

Adapting the same set of paradigms described in scenario 3, RTE recorded the service level agreement violations for running IoT APIs concurrently. Scenario 4 evaluates the impact of DT services developed and deployed to introduce DT service subscriber capability, information distribution capability, deployment and migration capability, and the DT services deployed in scenario two and scenario 3. Scenario 5 includes DT services developed and deployed to provide user access capability, DT service control capability, user interaction capability, and DT service regulation management capability.

- Scenario 4: Enabling DT services developed and deployed to introduce subscriber capabilities, information distribution capabilities, deployment and migration capabilities, and DT services deployed in scenarios 2 and 3.

- Scenario 5: Enabling DT services developed and deployed to provide user access capabilities, DT services' control capabilities, user interaction capabilities, and regulation management capabilities, along with all the DT services deployed in scenario 4.

Figure 26 presents the recorded statistics of the service level agreement violations in the specified scenarios under the same external influences and internal bindings within the mobile edge computing.

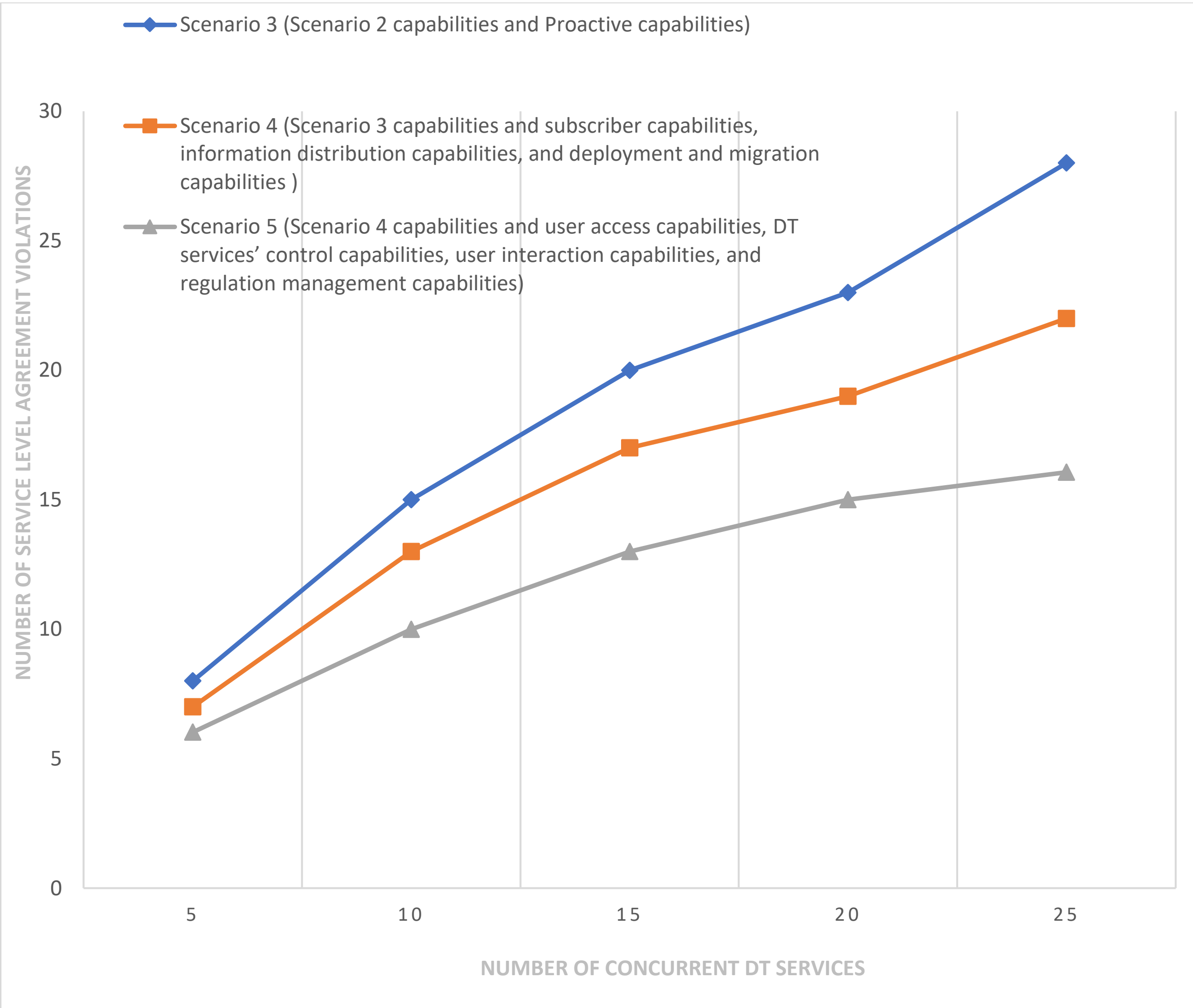


Figure 26: The service level agreement violations and number of concurrent DT services

As the number of concurrent DT services increases, the service level agreement violations also increase. After introducing the DT service subscriber capability, information distribution capability, and deployment and migration capability, the service level agreement violations decrease by 15%. The reduction in the service level agreement violations is uniform. However, during scenario 5, there is a significant reduction in the service level agreement violations as the concurrent DT services increase. It begins with a 14% decrease in service level agreement violations over scenario four and ends with a 27% during the maximum number of possible DT services in concurrency. The resource utilization at all the three distinguished levels of service level agreements is predictable based on the anticipated runtime concurrency of DT services.

Eventually, the average standard deviation in throughput is measured gradually by enabling DT services in scenarios 2 to 5. 64 DT services depend on the action plan associated with the DBOs, as indicated in Figure 27. The average standard deviation in throughput increases gradually for scenario 2. However, it becomes stable for scenario five after a minor level of fluctuations due to increased dependencies. It indicates that DT services introduce auto-scaling capabilities.

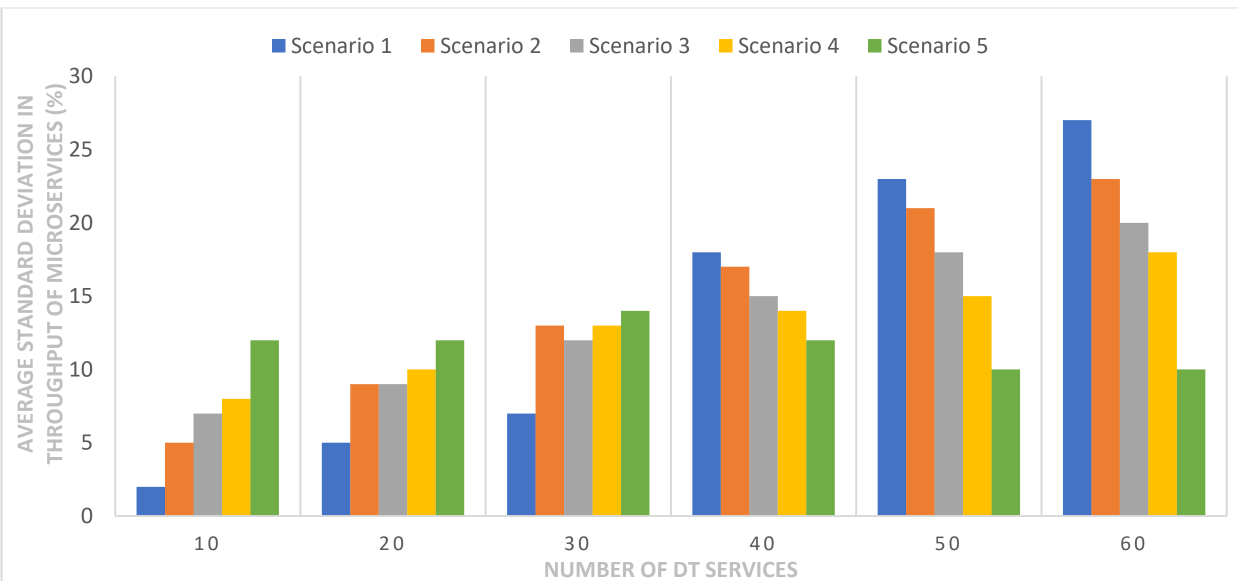


Figure 27: The average standard deviation in throughput and DT services

APPENDIX B.3: PW11: Degree of divergence (DoD) and compliance-aware DT services governance index (CDGI)

RTEs can support multiple lines of products and services that can also generate conflicts in compliances due to the standards and regulations requirements for each line of product or service. For instance, the health insurance portability and accountability act (HIPAA) [61] and payment card industry – data security standard (PCI-DSS) [121] have different sets of compliance requirements. Government committees intended the HIPAA to protect citizen data for the healthcare industry. The private sector developed the PCI-DSS to reduce fraud-related costs regarding card data loss. The HIPAA restricts healthcare insurance providers from disclosing the customer's personal information, including the bank account number and national identification number. RTE offering health insurance and payment services (or payment towards reward programs) needs to recognize and manage the privacy aspects of both the compliances separately. The degree of divergence (DoD) and compliance-aware DT service governance index (CDGI) assesses the effectiveness of the RTEs in managing and updating the compliances, regulatory requirements, and the industry standards within the DT services in the multitude of existing and upcoming standards and regulatory specifications.

The experimental evaluation includes retail energy sectors required to utilize the federal energy regulation commission (FERC) [75] for the smart grid with the payment card industry regulations - data security standard (PCI-DSS) [110] and statement on standards for attestation engagements 16 (SSAE 16) [111] for the reporting. The assessment included eight iterations of the development, updates, and deployment conducted for the following 7 BPs. The average duration of each deployment iteration is 4 to 5 weeks. The BP activities and DT services are derived based on the identified regulations and compliance requirements.

BP# 1: Smart grid meter quotation, installation, and activation
BP# 2: Manage consumer account for smart grid meter information, inquiry, and history
BP# 3: Billing and invoicing to the consumer
BP# 4: Payment processing and account receivables
BP# 5: Real-time monitoring and provisioning of smart grid meters
BP# 6: Notification and reporting of smart grid meter activities
BP# 7: Outage and restoration of smart grid meters

Equation 19 represents the scorecard to measure the DoD in the business rules that are incorporated in the DT services. The goal of scoring the DoD is to identify the level of diversification required for DT services to accommodate new or updated compliances and regulatory requirements. The DT services can inherit conflicts in compliances due to the standards and regulations requirements for each product or service line. For instance, the privacy regulations to protect FERC's customer data [75] differ from the PCI-DSS standard [110] since PCI-DSS needs to monitor customers' payment information for any fraudulent activities proactively. Each standard is specifically designed for different types of information. RTE offering retail energy and payment services needs to recognize and separately manage the privacy aspects of both the compliances. The following is the terminology to represent the score for the DoD in Equation 19.

- #DTS: It represents the number of compliance-aware DT services for the BPs in the current production deployment iteration.
- #BP Activities: It represents the number of BP activities associated with the BPs considered to participate in the RTE in the current production deployment iteration.
- #BRs: The number of business rules instantiated along each BP activity associated with the BPs in the current production deployment iteration.
- #Compliances: It represents the number of compliances required in adherence during the operationalization of the DT services in the current production deployment iteration.
- #Conflicts: It represents the number of conflicts between the multiple compliances or regulations supported by the DT services in the current production deployment iteration.

$$DoD = \frac{\sum_{BP=1}^{\#BPs} \frac{\#DS/(\#Compliances+\#Conflicts)}{\#BRs/\#BP\,Activities}}{\#BPs} \quad (19)$$

Table 21 provides an implementation-based analysis and compliance scenario of the FERC, PCI-DSS, and SSAE 16 of the production deployment iteration# 8. After each update, the DoD can be evaluated to accommodate new or upcoming compliance requirements to understand the level of changes to the rules associated with DT services. Higher the degree of divergence, the higher the adherence and maintainability of the compliances associated with the DT services.

BP#	**#BP Activities**	**#BRs: # of business rules**	**#Compliances (#Conflicts)**	**#DS: # of compliance-aware DT services**	**DoD**
1	7	12	13(3)	15	0.39
2	10	7	8(3)	13	1.68
3	6	10	11(2)	17	0.78
4	12	17	13(5)	19	0.75
5	6	9	7(2)	12	0.89
6	7	6	5(2)	6	1
7	14	16	18(3)	23	0.96
Degree of divergence (RTE)					1.075

Table 21: Degree of divergence in the production deployment iteration# 8

The compliance-aware DT services governance index (CDGI) computes and continuously monitors the governance of compliance-aware DT services. The paradigms to formulate CDGI are described below for a set of DT services for each type of compliance scenario category. The compliance-aware DT services governance index is presented in the published work PW11. The following are the primary governance concerns incorporated to formulate the CDGI since it is focused on operational aspects of the compliance-aware DT services.

Diversification of compliance requirements in DT services (DCRD): Continuous improvement of the DT services is evaluated based on the customization required to accomplish compliance requirements. The DCRD is computed considering the number of additional custom compliance needed in the BP activities. It is the number of alternate service operations accustomed in the DT services of the compliance scenario category over the total number of service operations in the DT services deployed for the compliance scenario category. The DCRC for the specific compliance scenario category is derived using the following ratio.

- #SO: The number of alternate service operations accustomed in DT services of the specific compliance scenario category.
- #tSO: The total number of the service operations in the DT services of the specific compliance scenario category.

$$DCDR < CS\ category >= \#SO/\#tSO$$

The latest version of compliance-aware DT services utilization (LDSU): The vendors, partners, employees, and customers must utilize the newest version of the compliance-aware DT services. However, certain parties and consumers of DT services of an enterprise could not upgrade and continue utilizing the previous version of the DT services due to structural and integration challenges. The LDSU is the number of consumers using the latest versions of DT services of the compliance scenario category over the total number of consumers for DT services. The LDSU for the specific compliance scenario category is derived using the following ratio.

- #LD: The number of the consumers using the latest versions of DT services of the specific compliance scenario category.
- #tLD: The total number of the consumers using the latest versions of the DT services of the specific compliance scenario category.

$$LDSU < CS\ category >=\ \#LD/\#tLD$$

Prohibit violations to compliances in DT services (PVCD): The DT services are placed based on logical attributions of compliances, and it validates the business rule-specific conditions. However, open-ended compliance attributes may trigger violations by the consumers. The PVCD evaluates the number of times DT services prohibit such attempts. The number of times DT services prohibited violations of compliances over the number of times consumers attempted to violate compliances. The PVCD for the specific compliance scenario category is derived using the following ratio.

- #PV: The number of times the DT services of the specific compliance scenario category prohibited violations of compliances.
- #tPV: The total number of times that consumers attempted to violate compliance with the DT services of the specific compliance scenario category.

$$PVCD < CS\ category >=\ \#PV/\#tPV$$

Adherence to RTE's service level agreements (ASLA): It determines the number of times the set of compliance-aware DT services of a specific compliance scenario category meets the identified and placed service level agreements for the RTE data entities or data source in use. The number of service level agreements accomplished over the number of DT services deployed for the compliance scenario category. The ASLA for the specific compliance scenario category is derived using the following ratio.

- #AS: The number of SLAs accomplished by the DT services of the specific compliance scenario category for the RTE data entities.
- #tAS: The total number of the DT services deployed for the specific compliance scenario category.

$$ASLA < CS\ category >=\ \#AS/\#tAS$$

Responsiveness of BP activities to compliance-aware DT services (RBPA): It may not be possible for the RTEs to be aware of all the changes to the standards due to upcoming DTs and provide complete BP activities specifications for the DT services. It is the number of responses by DT services to the BP activities over the total number of anticipated responses by DT services to the BP activities. The RBPA for the specific compliance scenario category is derived using the following ratio.

- #RBA: The number of responses by the DT services of the specific compliance scenario category to the BP activities.
- #tRBA: The total number of anticipated responses by the DT services of the specific compliance scenario category to the BP activities.

$$RBPA < CS\ category >= \#RBA/\#tRBA$$

"***n***": The number of compliance scenario categories identified in the RTE (n=7 based on Chapter 7.3).

"i": It represents the compliance scenario category currently considering the RTE's CDGI.

#Paradigms: The number of paradigms to impact the compliance-aware DT services governance index is five, as stated above, that is, DCRD, LDSU, ASLA, and RBPA.

The RTE can compute the compliance-aware DT services governance index (CDGI) based on Equation 20. The CDGI is the accumulation of all the RTE governance paradigms identified to evaluate compliance scenario categories.

$$CDGI = \frac{\left[\frac{\sum_1^n DCRD}{n}\right]+\left[\frac{\sum_1^n LDSU}{n}\right]+\left[\frac{\sum_1^n PVCD}{n}\right]+\left[\frac{\sum_1^n ALSA}{n}\right]+\left[\frac{\sum_1^n RBPA}{n}\right]}{\#Paradigms} \quad (20)$$

Figure 28 provides the progress of DoD and CDGI through the production deployment iteration 8.

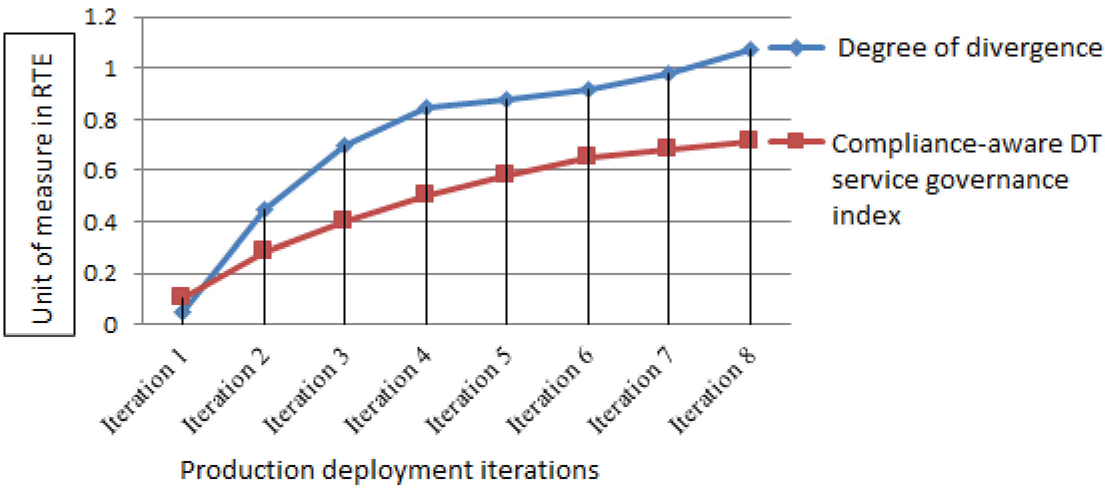


Figure 28: The CDGI and DoD in the production deployment iterations # 1 to 8

APPENDIX C: Definition of standard terminologies

Terminology	Definition
Application Programming Interface (API)	Application programming interface (API) is the integration between multiple systems, software, applications, and technologies. It establishes protocols and enables communication between diversified enterprise elements.
Business Process (BP)	Business process (BP) is the collection of business process activities (or tasks) that an enterprise performs for operations and management, including order processing, customer acquisition, budgeting, expense management, customer support, and marketing.
Business Process Activity (BPA)	The business process activity (BPA) is the set of structured events associated with the specific step within the business process to perform the desired action to progress the business process.
Consumer Applications (CAs)	Consumer application is the software developed, deployed, customized, and integrated to perform a specific task for the consumer. Consumer application provides interactions with different types of consumers of the enterprise.
Digital Business Operation (DBO)	The DBO presents the core operations performed utilizing digital technologies. It creates new value for the RTE's participants and the internal capabilities that support the enterprise's core operations.
Digital Technology (DT)	Emerging technologies provisioning end-to-end business processes (BPs), proactively engaging a diversified set of the RTE participants and advancing interactive services defined as digital technologies (DTs).
Digital Technology Service	The functional or operational services and application programming interfaces are derived from the capabilities of digital technologies to perform specific tasks. Digital technology

	services can be data services, cloud services, internet-of-things, and consumer application services.
Enterprise Entity	Any entity participates in functionalizing, operationalizing, capitalizing, or utilizing the enterprise service and product offerings.
Incremental Risk (IR)	The incremental risk (IR) is the amount of uncertainty added to or degraded from a risk associated with managing the RTE architecture by incorporating new and updated DBOs or eliminating the need to update the DBOs.
Key Performance Indicator (KPI)	A key performance indicator is a measurable value that demonstrates the effectiveness of an enterprise in achieving the goals of BPs. Enterprises use KPIs at multiple levels to evaluate their success in reaching the business objectives.
Real-time Enterprise (RTE)	Enterprises respond to the business and technology changes in real-time. Real-time enterprises are acceding to enterprises' responsive characteristics to the functional and operational changes.
Real-time Enterprise Operational Governance	The RTE operational governance performs the key operating decisions made by the RTE's business operations following the policies. It presents governing criteria to operate real-time enterprises in response to the business operations.
Service Level Agreement (SLA)	An SLA is an operating agreement between the technology platforms, vendors, partners, customers, suppliers, and the other RTE participants. It defines the evaluation criteria used to measure the level of services provided by any part of the RTE.

APPENDIX D: Primary researcher profile

Vikas Suvratkumar Shah is a Chief Architect at Knights of Columbus. Over the past 25+ years, he has led multiple products and solutions at numerous real-time enterprises, including Ernst & Young US LLP, Wipro Technologies, Symphony Services, Samsung India Software Operation Pvt. Ltd., and Fujitsu Network Communication. Vikas is pursuing a Doctor of Philosophy in Computer Science from Middlesex University. He received his Master of Science degree in computer science from Worcester Polytechnic Institute and a Bachelor of Engineering in computer engineering from Mumbai. He has 23+ international publications and patents in Real-time Enterprises, Blockchain, Smart City, Incremental Risk Management, Data Science, IoT, Cloud Computing, Mobile Edge Computing, and Integration Architecture. Vikas ran multiple strategic initiatives of emerging technologies and digital transformation at diversified scales, including global organizations, startups, and consulting. He is also extensively supporting pre-sales and marketing. Vikas is the recognized senior committee member, technologist, and speaker at numerous global conferences and events.

- ORCID: https://orcid.org/0000-0001-7248-2465
- Google Scholar Profile: https://scholar.google.com/citations?user=zCliOasAAAAJ&hl=en
- ResearchGate Profile: https://www.researchgate.net/profile/Vikas-Shah-6
- LinkedIn Profile: https://www.linkedin.com/in/vikas-shah-a6b81a162/
- American Journal of Computer Science and Technology Editorial Board Member: http://ajocsat.com/editorialboard
- Winner of Top Global Chief Architect 2020 Award (ICMG International LLC & Associates): https://www.architecturerating.com/chief-architect-2020

WORK EXPERIENCE

KNIGHTS OF COLUMBUS, NEW HAVEN, CT, USA — JUL 2019 – PRESENT

Chief Architect

ERNST AND YOUNG LLP, PHILADELPHIA, PA, USA — NOV 2017 – JUN 2017

FSO Technology & Architecture Advisor

WIPRO TECHNOLOGIES, PHOENIXVILLE, PA, USA — OCT 2013 – OCT 2017

Chief Architect (Connected Enterprise Services)

DNS Global Solutions Inc., Northridge, CA, USA — Aug 2012 – Sep 2013

Chief Technology Officer

Multivision Inc., Fairfax, VA, USA — Aug 2007 – Jul 2012

Chief Enterprise Architect

Sortes Technologies Inc. Nortel Co., Brampton, ON. — Aug 2005 – Jun 2007

Sr. Enterprise Architect/ Founder

Symphony Information Resources Inc., India — Dec 2003 – Jul 2005

Enterprise Architect / Product Manager

Samsung, Bangalore, India — Feb 2003 – Dec 2003

Project Leader (LE III)

ICSS Inc – Intel Corporation, Hillsboro, OR — Sep 2001 – Jan 2003

Lead Software Architect

Ajilon Consulting Services, Somerset, NJ — Aug 1999 – Aug 2001

Senior Software Engineer

Fujitsu Nexion, Acton, MA. — May 1998 – Jul 1999

Software Engineer (ATM Cell Switch)

Worcester Polytechnic Institute, Worcester, MA — Aug 1996 – May 1998

Researcher – Active and Real-time Database Systems

Tata Consultancy Services, Mumbai, India — Dec 1995 – Aug 1996

Assistant Systems Analyst - Positive Train Separation (GE-Harris)

SAMEER (Research Center– Gov. of India), Mumbai — Jun 1994 – May 1995

Trainee Engineer - Time Series Prediction Using Neural Network