Shilenge, Musa; Telukdarie, Arnesh

Article

4IR integration of information technology best practice framework in operational technology

Journal of Industrial Engineering and Management (JIEM)

Provided in Cooperation with:
The School of Industrial, Aerospace and Audiovisual Engineering of Terrassa (ESEIAAT), Universitat Politècnica de Catalunya (UPC)

Suggested Citation: Shilenge, Musa; Telukdarie, Arnesh (2021) : 4IR integration of information technology best practice framework in operational technology, Journal of Industrial Engineering and Management (JIEM), ISSN 2013-0953, OmniaScience, Barcelona, Vol. 14, Iss. 3, pp. 457-476, https://doi.org/10.3926/jiem.3429

This Version is available at:
https://hdl.handle.net/10419/261763

OmniaScience

Journal of Industrial Engineering and Management
JIEM, 2021 – 14(3): 457-476 – Online ISSN: 2013-0953 – Print ISSN: 2013-8423
https://doi.org/10.3926/jiem.3429

4IR Integration of Information Technology Best Practice Framework in Operational Technology

Musa Shilenge, Arnesh Telukdarie

University of Johannesburg (South Africa)

musachester@gmail.com, arnesht@uj.ac.za

Received: December 2020
Accepted: March 2021

Abstract:

Purpose: Since inception in the 1970s, Operational Technology (OT) systems were designed to operate in isolation from Information Technology (IT) systems mainly due to differences in objectives relating to Confidentiality, Integrity, Security, and Availability (CISA). Additional IT/OT diverse components include computing speed, and failure severity in terms of safety, environmental, and financial impact. This presents a great challenge in terms of management of the industrial control systems on the facet of its largely IT infrastructure.

The 4IR demands synchronous integration of the worlds of IT and OT with similar services management. Literature analysis indicates that limited research has been conducted on the management of IT and OT as a synergistically integrated set of systems. The focal point of this research is to evaluate if an Information Technology Service Management (ITSM) best practice framework can be integrated into the Operational Technology domain.

Design/methodology/approach: The nature of this study is that it does not seek to gather and analyze numerical data that can be statistically analyzed, hence a qualitative research approach is adopted. A comparative research design with mixed qualitative methods is utilized to analyze and synthesize in a step-wise process the secondary data gathered from academic articles, standards organizations, whitepapers, etc. The employed research methods include constant comparative analysis and benefits case analysis. The proposed and evaluated application case is based on a petrochemical environment with ITSM inclusive of OT.

Findings: After comparative analysis and application case, the research concludes that an IT best practice framework i.e. the Information Technology Infrastructure Library (ITIL) can be integrated, with limited constraints, adapted into the operational technology domain to facilitate the management of OT for service management.

Practical implications: The key benefit of this work is the inclusion of OT in global IT best practices in this Fourth Industrial Revolution (4IR) era. The demand for integrated systems with single service levels can be met.

Originality/value: This paper contributes to ongoing research in IT/OT integration by providing a unique perspective on OT service management in the Fourth Industrial Revolution (4IR). Researchers can utilize the research outcomes to apply ITSM in the OT domain where 4IR technologies have been implemented.

Keywords: 4IR, operational technology, information technology infrastructure library, configuration management

To cite this article:

Shilenge, M., & Telukdarie, A. (2021). 4IR Integration of Information Technology Best Practice Framework in Operational Technology. *Journal of Industrial Engineering and Management*, 14(3), 457-476. https://doi.org/10.3926/jiem.3429

1. Introduction

In this modern-day world, it is unimaginable to contemplate a mass production line that lacks automation of activities using technologically advanced systems. Automated production lines bring efficiency and cost reduction in performing tasks. This is made possible by using operational technologies such as Industrial Control Systems (ICS). The function of an industrial control system is to automatically monitor and control plant facilities (Chapman, Ofner & Pauksztelo, 2016). The term industrial control system is an all-in-one term for describing the Distributed Control System (DCS), Supervisory Control and Data Acquisition (SCADA), and the Programmable Logic Controller (PLC) (Bustamante, Fuertes, Diaz & Toulkeridis, 2016; Chapman et al., 2016). Industrial control systems are a subset of Operational Technology.

Previously, operational technology systems were physically and logically isolated systems within an enterprise. In these beginning stages of the fourth industrial revolution which brings forth technologies such as Cyber-Physical Systems (CPS), Industrial-Internet of Things (IIoT), Big Data Analytics (BDA), cloud computing, blockchain, additive manufacturing, simulation and modeling, semantic technologies, automation and robotics (Ghobakhloo, 2018), operational technology systems must start availing data to other systems within and/or external to the enterprise as part of communication integration effort between enterprise information technology and operational technology systems. This brings the industrial control network and enterprise IT network closer for real-time data and information transfer to the management level for better decision-making (Sopko & Winegardner, 2007).

Industrial control networks (ICN) are designed to maximize operational safety, availability, and reliability, while enterprise IT networks are designed to maximize confidentiality and data integrity (Sopko & Winegardner, 2007). Therefore, in the age of cyber-physical systems and the industrial internet of things, certain aspects of operational technology systems must be implemented and managed using proven best practices from enterprise IT while accounting for the criticality of operational technology systems. Furthermore, Ghobakhloo (2018) stated that it is anticipated that the IIoT and other technology trends will invade all types of operational technologies at various levels. It is crucial to note that IIoT is an industrial version of the Internet of Things (IoT). Therefore, IT protocols will be ubiquitous in the OT domain.

The fourth industrial revolution is no longer hype but an everyday reality. Manufacturing organizations need to embrace the super-competitive environment and uncertain market conditions that are brought forth by the 4IR. Some manufacturing organizations are slowly transforming from traditional manufacturing to service-orientated and entirely digitalized manufacturing.

The origin of this research is based on the third industrial revolution technology i.e. the process automation aspect realized through the implementation of Operational Technology (OT). It is crucial to point out that the fourth industrial revolution advances from the foundation of automation. In the third industrial revolution, information technology emerged and vast research publications in this field are available. One of the outcomes from implementation and research in this field is the information technology best practice frameworks, which are extensively documented. Some of the best practice frameworks are ITIL and Control Objective for Information and related Technologies (COBIT). Both frameworks are leading and widely accepted in the IT industry (Robinson, 2005).

Since OT systems have to a great extent the characteristics of traditional IT systems, it follows that certain processes from the field of information technology can be modified and adapted for use in the OT space, since Jie and Li (2011) stipulated that, "The characteristics of an industrial control system as a comprehensive mainstream

information technology have become more apparent." In the 4IR, as mentioned previously, OT systems and information technology will be more interconnected and the approach to service management will shift to be a more involved role within the enterprise. It is important to note that the complexity of the industrial revolutions exponentially increases from one industrial revolution to the next. Thus, IT best practices may fast-track proper and efficient implementation and management of the OT in the fourth industrial revolution. Although, information technology best practice frameworks can only ready operational technology for the technological innovations that are brought forth by the total integration of the enterprise, i.e. 4IR.

The problem statement of this research is as follows: With the introduction of 4IR technologies such as IIoT and CPS in the operational technology space, the OT space is built using equipment/devices that have the qualities of IT systems. This presents a great challenge in terms of management of OT systems on the facet of its largely IT infrastructure.

This research provides a unified theoretical framework that illustrates ITIL best practice processes integrated into OT space. The research seeks to articulate findings on the following questions:

a) What are the global best practice frameworks in IT and what are the critical limitations when applied to OT?
b) How will an information technology best practice framework improve service management in an operational technology environment?

This paper is structured as follows: Section 2 provides a literature review regarding IT best practices, IT/OT integration, etc. Section 3 presents the research methodology used in the inquiry and analysis to ultimately draw a conclusion. Section 4 presents the analysis and discussion that result in the formation of the unified theoretical framework. Section 5 outlines the ITIL application case. Section 6 discusses the projected benefits of ITIL in OT. Section 7 elaborated on the findings with regards to the research questions. Then, section 8 concludes the paper and outlines limitations and future work.

2. Literature Review

2.1. IT Best Practice Frameworks

A best practice is defined as the one and best way of doing something that has worked in the past and is presumed to produce the same outcome in the future (Quayzin, 2011). Best practices must be challenged through the innovation of new ways since best practices have limitations such as bounded rationality, limited validity, limited time until new practices are discovered, and are barriers to innovation (Quayzin, 2011). Some of the benefits of using best practices include cost saving, standardization, and process improvements.

IT best practice frameworks are proven working methods from years of research and practice. Information technology is defined as a whole range of technologies for information processing including software, hardware, communication technologies, and related services (Gartner, 2018). There are two well-known IT best practice frameworks namely ITIL and COBIT that offer guidelines on IT governance and management (Robinson, 2005; Sahibudin, Sharifi & Ayat, 2008). ITIL is mainly a service management framework while COBIT is mainly a governance framework. Of the two frameworks, ITIL is known as the de facto standard and the most widely accepted approach for IT service management in the world (Sahibudin et al., 2008; Bustamante, Fuertes, Diaz & Toulkeridis, 2017; Kozlova, Hasenkamp & Kopanakis, 2012; Mahy, Ouzzif & Bouragba, 2017). ITIL is a collection of best practices organized into 26 processes. The processes are organized under five lifecycle phases, the number of processes in each phase is given in brackets, see Figure 1 (Persse, 2012).

The lifecycle phases are as follows (Persse, 2012): Service strategy – provides processes for directing the form and function of ITSM; Service design – provides a set of process that ensures core services are taken into consideration and aligned with the technical and business needs; Service transition – provides a set of processes that ensures that new or modified services are deployed successfully with minimal downtime and risk of infrastructure inoperability; Service operation – provides a set of processes and functions to ensure information technology services are managed in a manner that results in expected service performance, and lastly Continual Service Improvement (CSI)

– provides a set of process that ensures that an enterprise remains on an ongoing developmental focus on service management improvement through optimization and innovation.

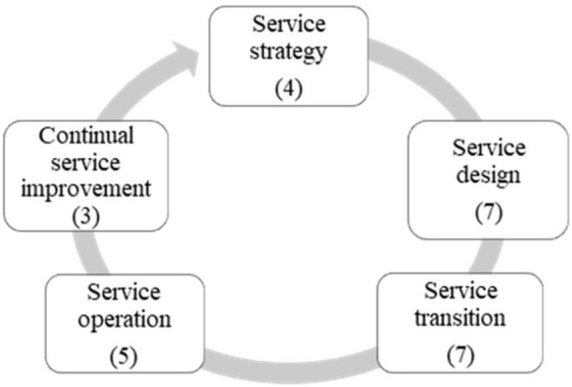

Figure 1. ITIL lifecycle phases

ITIL focuses is on how tasks and business objectives are accomplished using business processes that have defined roles, responsibilities, activities, controls, and performance measurements. All the processes from the ITIL framework do not work in isolation but are linked ultimately forming a web of processes (Lema-Moreta and Calvo-Manzano, 2018). The worldwide implementation of ITIL in prominent companies has been shown to improve the value and quality of rendered IT services (Limanto, Khwarizma, Rumagit, Pietono, Halim & Liawatimena, 2017). ITIL processes are characterized as factory floor processes that form part of day-to-day business operations. The factory floor of interest in this research is that of industrial control systems of the operational technology domain.

2.2. Operational Technology (OT)

According to Fan, Fan, Wang and Zhou (2015), operational technology systems such as industrial control systems are systems composed of various components that facilitate automation of production processes for near-real-time data gathering, control, and monitoring. The rapid development in IT during the third industrial revolution had a direct influence on the developments that occurred in the OT space. Present-day operational technology architectures contain IT equipment such as network servers.

The most critical components in an OT system are the controller, control network, and supervisory control software (Yang & Zhao, 2015). The controller is connected to the sensors, drives, and actuators through the Fieldbus network for gathering and sending data to and from the factory floor (Ray, Harnoor & Hentea, 2010). Research by Galloway and Hancke (2013), Jie and Li (2011), and Vavra and Hromada (2015) found that the interconnectivity between the enterprise IT network and ICN through the control system firewall is becoming more closely linked. This phenomenon is nowadays called IT and OT integration and forms part of the basis of Industry 4.0 technologies in the operational technology space.

2.3. IT/OT Integration

The segregation between IT and OT systems is made possible using as a minimum a network firewall that separates the enterprise zone from the manufacturing zone. IT is defined as the hardware, software, and communication technologies for data exchange for business systems, that is, IT systems are the systems that belong to the enterprise network. While OT systems are found in the manufacturing zone for control and monitoring of devices found in the manufacturing zone (Lewandowski, Pareschi, Pakos & Ragaini, 2018). IT and OT systems are designed with differing focus in terms of protocol structures, failure severity, Quality of Service (QoS), reliability, data composition, operating environment, system architecture, round trip times, and determinism (Galloway & Hancke, 2013).

Lewandowski et al. (2018) stated that the future of digitization in industrial control systems rests upon extensive integration of IT and OT systems functionalities and the internet. Furthermore, other studies proposed the integration of all layers within a business to maximize the benefits of unified business processes. Garimella (2018) pointed out that IT/OT integration exists in the industry, but in the intranet, whilst the fourth industrial revolution requires the integration to the internet in the form of industrial internet-of-things. However, integration results in numerous cybersecurity challenges. Another challenge that the industry has recently been facing is the issue of compatibility between IT and OT systems. IT systems are updated more frequently than OT systems, the updates of IT systems are often minor improvements to the software, while OT improvements may require a full shutdown of production or manufacturing plant since online modification exposes the plant to the risk of an unplanned shutdown.

Research by Abe, Fujimoto, Horata, Uchida and Mitsunaga (2016) on security threats of internet-reachable industrial control systems, that is OT systems, has shown that hackers can penetrate an organization through one unsecured organization. It is therefore imperative when implementing integration between enterprises on any level most especially the Enterprise Resource Planning (ERP) level, to consider the risks associated with interfacing enterprises. For instance, other enterprise systems can be systems of a supplier, Subject Matter Expert (SME), Original Equipment Manufacturer (OEM), or an Engineering Contractor (EC).

Cybersecurity is of great concern in IT/OT integration. Several high-profile cybersecurity incidents that quaked the operational technology systems community have been reported. The incidents include amongst others Code red 2001, Blaster 2003, SoBig in 2003, Sasser 2004, Stuxnet 2010, and Havex 2014. The air-gapping/virtual physical isolation methods of the previous century will not be feasible going forward for cybersecurity due to communication integration between IT and OT. Chapman et al. (2016) and Vavra and Hromada (2015) proposed the well-known defense-in-depth approach to counter cyber-attacks. Moreover, Ghobakhloo (2018) suggested that blockchain technology is a suitable method for ensuring secure communication within and external to the enterprise.

2.4. IT Best Practices in the OT Domain

Research by Bustamante et al. (2016, 2017) used IT best practice frameworks in an ICS setting focusing on information security management. While the TOGAF-9 framework was successfully used by Mathew and Pretorius (2017) to investigate critical success factors of Control and Instrumentation (C&I) projects in the power industry. Additionally, Jie and Li (2011) argued that enterprise IT security measures cannot be directly applied to an operational technology system. These instances and limitations highlight the intricacies of dealing with operational technologies as compared to enterprise IT systems.

The notion of applying IT best practice frameworks has not been studied sufficiently thus far, since there is limited research literature. Appreciating the fact that OT personnel are generally unaccustomed with IT frameworks and that the implementation of the relevant processes of the IT frameworks would present paramount challenges due to a steep learning curve. The study by Bustamante et al. (2017) showed that applying information security management from IT in the OT space generates value for an organization when properly adapted. Although Mahy et al. (2017) and Sharifi, Ayat, Rahman and Sahibudin (2008) articulated that implementing IT frameworks is not a simple endeavor due to its many challenges, one of the biggest challenges is changing the organizational culture towards change. It is crucial to note that IT best practices can be applied to any industry that uses IT infrastructure to provide services.

2.5. Frameworks Implementation Approach and Critical Success Factors (CSF)

The frameworks discussed in this paper leaves a choice on the selection of processes that must be implemented in an organization to the process design, implementation, and management unit. For successful implementation, Blumberg, Cater-Steel, Rajaeian and Soar (2019) recommended a socio-technical approach that considers the social and technical aspects of organizational change that comes with ITSM implementations. Many organizations in the study showed effort in trying to find a balance between social and technical aspects by applying appropriate effort on individual components of both aspects. Ahmad, Tarek Amer, Qutaifan and Alhilali (2013) proposed an approach called Unified Theory of Acceptance and Use of Technology (UTAUT) that is accompanied by an ITIL

implementation roadmap for a smooth transition over a specified period. While Kempter (2019) proposed an ITIL Process Map which constitutes a series of implementation steps.

Studies by Sharifi et al. (2008), Blumberg et al. (2019), Ahmad et al. (2013) and Pollard and Cater-Steel (2009) looked into the critical success factors that are common in successful ITIL implementation which are as follows: Top management support; communication and cooperation; ITIL awareness and training; interdepartmental collaboration; process priority; software tools selection; proper change management; customer/end-user orientation; appointment of expert consultants; maintaining momentum, project management; and monitoring and evaluation. All the critical success factors must work together in unison and receive appropriate effort. Most of the CSFs are not related to the technology but the user acceptance and appreciation of the ITIL framework and its benefits (Ahmad et al., 2013). ITIL implementation projects often become a long process since organizations are not willing to alter current running and established processes until the benefits of the change have been proven (Isaksson, Harjunkoski & Sand, 2018).

3. Research Methodology

This research does not seek to collect and analyze any numerical data as it seeks to generate theory. Thus, the selected research approach is qualitative in nature. It is crucial to note that qualitative data is not numerical, but descriptive (Flick, 2009). The research design adopted is the comparative design which expresses the logic of comparison amongst two or more contrasting situations (Bryman, Bell, Hirschsohn, dos Santos, du Toit & Masenge, 2014). The intent is to extend the literature review presented in Section 2 through secondary data gathering, analysis, and synthesis to formulate a framework.

Mixed research methods are used in this study, including constant comparative analysis and a benefits case study. This approach is satisfactory since it aims to identify gaps in the current OT landscape, compare the field of IT and OT, and analyze benefits from the application case of ITSM in the OT domain to close the identified shortfalls.

The secondary data/information sources include academic articles, standards, whitepapers, and other sources. The mixed research method is selected since the review of other research designs and methods proved the alternatives are inadequate in addressing the research questions. The main factor is that OT personnel are generally unfamiliar with IT best practice frameworks apart from knowledge of basic IT systems setup and administration, for instance, OT database administration. This research seeks to introduce a new transdisciplinary approach to OT services management.

The constant comparative analysis is used for data analysis, synthesis, and discussion of various models/frameworks based on theory extracted from the narrative literature review. Comparative research strives to obtain similarities between events, methods, and techniques (Rajasekar, Philominathan & Chinnathambi, 2013). The constant comparative analysis is suitable in this instance since the research seeks to analyze models to find similarities and differences thereby identifying shortfalls in the existing models to then propose a unified theoretical framework. The models compared are ISA-95, ISA-99, and ITIL based on the ISO/IEC-15288 system lifecycle model.

Bryman et al. (2014) stipulated that case studies can be used for generating and testing theory, in this study the benefits case analysis is utilized to model and analyze a typical IT best practice in the OT space.

The research methodology steps followed to answer research questions are shown in Figure 2 below.

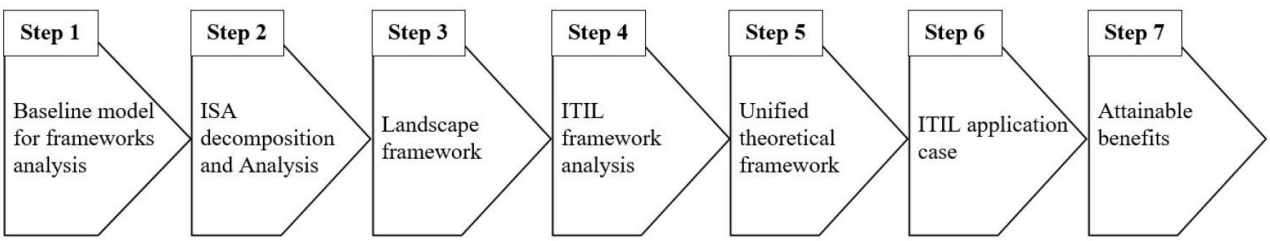

Figure 2. Research methodology

The research methodology steps are outlined below.

Step 1 - Baseline model for frameworks analysis: The ISO/IEC-15288 system engineering lifecycle model which is used as a baseline of comparison is presented and outlined. The ISO/IEC-15288 system lifecycle model is compared to the industrial control systems standard models (ISA-95 and ISA-99) and the ITIL information technology best practice framework in the following methodology steps.

Step 2 - ISA decomposition and analysis: The ISA-95 enterprise-control integration model is analyzed. The shortfalls identified in ISA-95 in terms of cybersecurity are addressed by the ISA-99 model. The ISA-99 model provides the zones and conduits model and the defense-in-depth approach, just to mention a few, to describe cybersecurity concerns and solutions regarding designing and building into the Industrial Control Network (ICN). ISA-95 and ISA-99 are then compared to the ISO/IEC-15288 system lifecycle model to highlight ISA-95 and ISA-99 focus areas based on the system lifecycle stages.

Step 3 - Landscape framework: A landscape framework that identifies and highlights the shortfalls in the ISA-95 and ISA-99 models is presented. For the landscape framework to be sustainable in the long run in the 4IR environment, a framework is proposed to close the gaps identified in the landscape framework from the service management and design perspective based on the baseline from Step 1.

Step 4 - ITIL framework analysis: The ITIL framework is decomposed based on literature and step 1 to evaluate the applicability of ITIL processes in the operational technology space based on the landscape framework from step 3, then ITIL processes are aligned to the OT landscape framework. This forms part of the service management function in OT using ITIL.

Step 5 - Unified theoretical framework: A theoretical framework that unifies ISA-95, ISA-99, and ITIL model based on the landscape framework and Step 1 is presented. Its purpose is to realize the unification of the models/frameworks. Furthermore, the properties of ITIL processes in comparison to OT processes are presented.

Step 6 - ITIL application case: An application case of an IT best practice, in this research the service asset and configuration management process, is applied to the OT space. The application case is proposed to illustrate the abstractions of this research. Furthermore, benefits analysis follows the application case.

Step 7 - Attainable/Projected benefits discussion: The accomplishment of the research objectives and attainable benefits from the developed unified theoretical framework are discussed.

The research questions are addressed by the steps outlined in Figure 2 as follows:

Research question one: The constant comparative analysis of steps 1 to 4 together with the narrative literature presented in section 2.

Research question two: The constant comparative analysis and benefits case analysis of steps 5 to 7.

The abovementioned research methodology is followed step-by-step in the following sections.

4. Analysis and Discussion

4.1. Baseline Framework

The analysis commences with establishing a baseline for analysis which is the ISO/IEC-15288 systems lifecycle model. ISO/IEC-15288 is a model of the lifecycle of any man-made system (ISO/IEC/IEEE-15288, 2015). The systems engineering lifecycle is used as a basis for comparative analysis since it provides guidance for the engineering of complex systems. The system lifecycle is a stepwise evolution of a new system from concept through development and on to production, operation, and ultimately disposal. The system lifecycle model is made up of six stages namely concept, development, production, utilization, support, and retirement (Kossiakoff, Sweet, Seymour & Biemer, 2011). The model is used in this research as a basis for the analysis and decomposition of ISA-95, ISA-99, and the ITIL framework. The system lifecycle model is used for framing the basis of the theoretical framework that results from this research.

4.2. ISA-95 and ISA-99 Decomposition and Analysis

4.2.1. ISA-95 Enterprise - Control System Integration

ISA-95 defines the Manufacturing Execution System (MES) activities and data exchanges to and from ERP and the Industrial Automation and Control Systems (IACS) domain (Kannan, Suri, Cadavid, Barosan, Brand, Alferez et al., 2017). The ISA-95 functional hierarchy detail that the components of an OT belong to levels zero to three. ISA-95 categorizes and illustrates the flow of data/information between its layers through object models. This is useful during the design of information workflows for an architecture that depicts the integration between business and manufacturing execution systems. It is quite a setback that ISA-95 does not detail the activities or function of level zero to three where OT systems are classified. In modern times, the shortfall of the ISA-95 architecture is that it is only focused on vertical information integration within an enterprise which makes it insufficient for use in future Industry 4.0 implementations that takes into account horizontal information integration (Jiang, 2017).

4.2.2. ISA-99 Industrial Communication Networks - Network and System Security

The ISA-99 standard focuses on the cybersecurity aspect of operational technology systems. It is specifically this facet that complements ISA-95 on cybersecurity regarding data exchanges between the ERP and ICAS domain. ISA-99 provides the Cybersecurity Management System (CSMS) and Security Level Lifecycle Management (SLLM) amongst other models for planning, implementation, and management of cybersecurity in OT deployments. ISA-99 urges that organizations form an overall program that combines the capabilities of IT personnel with those of OT personnel to collaboratively plan and manage cybersecurity.

4.3. Landscape Framework

The landscape illustrates how ISA-95 and ISA-99 align with ISO/IEC-15288 system lifecycle model as summarized in Table 1 columns 1 to 3, and within the dotted shape in Figure 3. The landscape outlines that ISA-95 is only for the development stage of the system lifecycle, while ISA-99 spans the entire lifecycle except for the retirement stage. ISA-99 SLLM outlines the activities undertaken from the conceptual stage through to maintenance. While the ISA-95 Manufacturing Operation and Control (MO&C) model does not address activities that must be undertaken in the OT domain. Therefore, the landscape presents shortfalls concerning the management of non-cyber security activities of the operational technology domain.

ISO/IEC-15288 Lifecycle Stage	OT/ICS		IT
	ISA-95	ISA-99	ITIL
Concept	-	SL Assess phase/CSMS Risk analysis	Service strategy
Development	MO&C	SL Develop and implement phase/ Addressing risk with the CSMS	Service design
Production	-	SL Develop and implement phase/Addressing risk with the CSMS	Service transition
Utilization	-	Monitoring and improving CSMS	Service operation
Support	-	SL Maintenance phase/ Monitoring and improving CSMS	Service operation and CSI
Retirement	-	-	-

Table 1. Comparison of ISA-95, ISA-99, and ITIL to ISO/IEC-15288 system lifecycle stages

The shortfalls of the landscape framework regarding the design and operation of operational technology management are as follows:

- The framework does not specify how activities and functions must be performed. The landscape framework focuses on the operations and integration from the perspective of MO&C; hence it is not Industry 4.0 ready.
- The framework does not fully emphasize roles and responsibilities on activities and functions.
- The framework does not address aspects of continual improvement in the operational technology domain.

- The framework lacks the cogent unification of the different components/activities of the operational technology domain.
- The framework does not address the business processes facet of operational technology management systems. Only cybersecurity through ISA-99 addresses the IT facet of the ISA-95 hierarchy.

4.4. ITIL Framework Analysis

The landscape framework showed that ISA-95 and ISA-99 scarcely address the activities of the OT space, specific to service management. Hence, for the landscape framework to be utilizable and sustainable in the era of fourth industrial technologies such as CPS and IIoT for the benefit of OT, the ITIL service management framework is proposed as an operations model. The purpose of ITIL, in this case, is to support and maintain OT services and business processes as depicted by the circular arrow in Figure 3. Thus, ultimately addressing the shortfalls identified in the landscape framework.

4.5. Unified Theoretical Framework (UTF)

The unified theoretical framework highlights ITIL's area of focus in the operational technology domain. ISO/IEC-15288 states that it is compatible with IT service management systems, in this case, ITIL, moreover it is compatible with the information security management system of ISO/IEC-27000 (ISO/IEC/IEEE-15288, 2015). It is crucial to note that ISA-99 is derived from information security management systems of ISO/IEC-27000. Additionally, ISA-99 encourages that OT and IT staff to find synergies in managing cybersecurity within an organization. This collaborative relationship is illustrated by the unified theoretical framework. Although the unified theoretical framework does not address the retirement stage of ISO/IEC-15288 it fosters continuous improvement through formal change management processes. Furthermore, the unified theoretical framework demonstrates that ISA-99 and ITIL follow similar lifecycle stages as outlined by ISO/IEC-15288, see Figure 3.

ITIL integration into the OT space partly brings business process optimization answers the literature gap highlighted by Medoh and Telukdarie (2016) that highlighted that immense effort has been directed at ERP business process automation discounting MES and OT processes. The adaptation and implementation of ITIL must complement and improve the current state of the OT operations in various ways since ITIL aligns business objectives, people, processes, and technology (Enose, 2012). Furthermore, it is crucial to reiterate that not all ITIL processes need to be implemented at the same time since implementing all processes at once proved to be very costly and time-consuming (Ahmad et al., 2013). The unified theoretical framework addresses the shortfalls identified in the landscape framework as follows:

- The introduction of the proposed ITIL framework in the OT space assists with identifying processes that requires implementation in an OT organization and provides sample business process flow diagrams that are utilized as a starting point for OT business process development.
- ITIL emphasizes the Responsible, Accountable, Consulted, and Informed (RACI) matrix for each business process to clarify roles and responsibilities to avoid conflict.
- The ITIL lifecycle stages form a continuous cycle through continual service improvement across all stages.
- The ITIL framework proposed that an organization develop a service catalog that contains all the services and processes of the organization. The consolidation of the various processes into a single portfolio is beneficial for OT process visibility and information display for better decision making.
- ITIL brings the service management aspect to the OT environment in preparation for the age of digitalization.

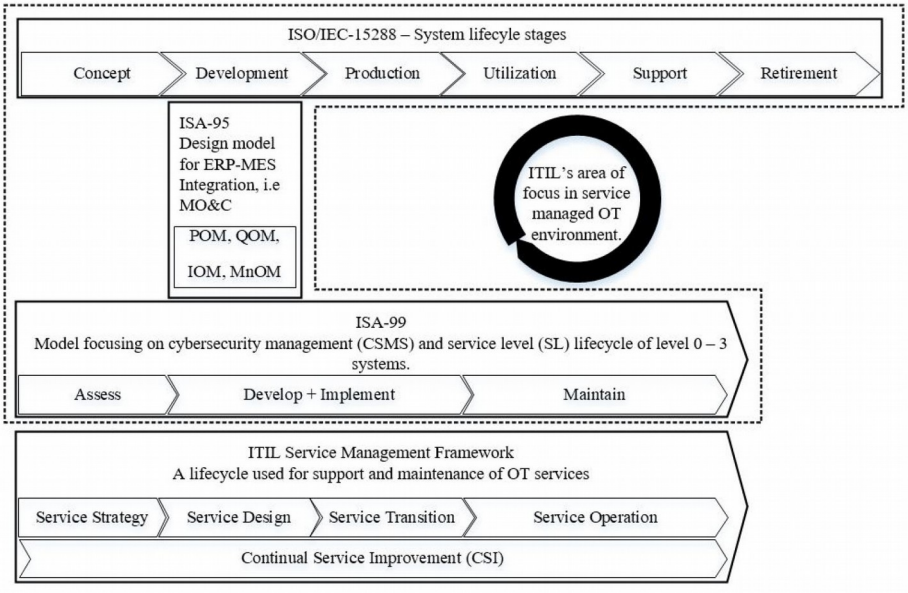

Figure 3. The unified theoretical framework, i.e. the landscape framework with ITIL adapted to OT

4.6. Alignment of ITIL and OT Processes

Research has shown that there are differences between OT processes and IT processes in terms of the application environment, process priority, process interfaces, organization-wide standardization, process performance tracking, business strategy alignment, process software tools, and process innovation. The differences are summarized in Table 2.

The work by Kozlova et al. (2012) is extended by mapping ITIL processes to traditional operational technology processes as shown in Table 3 to Table 7.

Portfolio and project management in the OT domain is carried out using the widely known PMBOK, while OT portfolio and project management are carried out using various flexible project management methodologies such as Agile project management, PMBOK, etc. In the aspect of service, OT undertakes neither service portfolio nor project management.

Characteristic	OT	IT
Environment	Manufacturing environment	Business environment
Process priority	Plant availability	Information confidentiality and service availability
Process interfaces	Mostly isolated	Interdependent processes
Organization-wide standardization	Minimal standardization often localized within business/plant units	Highly standardized and documented
Process performance tracking	Moderate	Highly tracked as part of the continual process improvement effort
Business strategy alignment	Minimal aligned with operations	Highly concerned with strategic alignment
Process software tools	Moderately specialized	Highly specialized
Process innovation	Low	High

Table 2. Comparison between OT and IT processes

ITIL		OT
Service Strategy	Financial management	-
	Demand management	-
	Strategy Operations	-
	Service portfolio management and Project management	Portfolio and project management

Table 3. High-level service strategy ITIL - OT mapping

ITIL		OT
Service Design	Continuity management	-
	Availability management	Predictive maintenance
	Capacity management	Capacity management
	Server level management	Server level management
	Supplier management	-
	Information security management	Industrial automation and control systems security
	Service catalog management	-

Table 4. High-level service design ITIL - OT mapping

ITIL		OT
Service transition	Service asset and configuration management	Asset management
	Release and deployment management	-
	Change management	Management of change
	Knowledge management	-
	Service validation and testing	-
	Service evaluation	-
	Transition planning and support	-

Table 5. High-level service transition ITIL - OT mapping

Service Level Management (SLM) is performed in a similar manner in both the information technology and operational technology domains. Both domains have Service Level Agreements (SLA) and Operational Level Agreement (OLA) in place for handling internal and external clients and service providers. The only difference lies in the SLA turnaround times, for the OT domain the turnaround time is less than an hour, while in the IT domain it is in the range of days.

The IACSS of the operational technology space is derived from the cybersecurity standards from the information technology space, that is, ISO/IEC-27000 series (ISA-99, 2019). The ISA-99 standard also encourages synergy between OT and IT personnel in the management of enterprise-wide cybersecurity.

Asset management practice guided by ISO-55000 (Formerly, PAS 55) is well-established in the OT domain with ERP systems in place to handle workflows and data storage. However, there are coherent configuration management practices. The IT domain enjoys the combination of asset and configuration management for assets as described in the ITIL best practice framework. The OT domain could benefit immensely from a configuration management system and process. This research aims to explore and expand on this ITIL best practice.

The change management practice is matured in both the IT and OT domains since change forms part of the fabric of organizational processes as highlighted in ITIL best practice framework for the IT domain, and ISO-45001 for the OT domain in which safety of personnel, environment, and monetary loss are paramount factors.

ITIL		OT
Service Operation	Incident management	Repair and restoration
	Problem management	Proactive maintenance
	Access management	Access management
	Request fulfillment	-
	Event management	-

Table 6. High-level service operation ITIL - OT mapping

ITIL		OT
Continual Service Improvement	7 step improvement process	-
	Service measurement	-
	Service reporting	-

Table 7. High-level continual service improvement ITIL - OT mapping

Most often operational technology assets malfunction and thus require repairs and in other cases restoration to re-establish a good working order. While incident management works on handling incidents as they occur to comply with defined and agreed SLAs/OLAs. The two processes handle incidents except that the ITIL process introduces process owner, process KPIs, policies, and roles and responsibilities.

Proactive maintenance focuses on correcting root-causes of failure to avoid future failures due to the root-cause. Thus, proactive maintenance is a form of preventive maintenance while problem management focuses on preventing incidents from occurring, especially incidents that previously occurred multiple times. Both processes from the two domains address similar concerns.

Access management is performed in both the IT and OT domain to facilitate access to secured facilities such as data centers and engineering rooms, and engineering systems access such as hardware and software applications passcodes or biometric recognition. On the application level, user access is managed by a domain controller to authenticate and authorize users using role-based access in both the OT and IT domains.

Continual improvement is an on-going effort guided by ITIL and other IT best practice frameworks. While in the OT domain, continuous improvement is guided by industrial continuous improvement frameworks such as Lean Six sigma. The OT domain can benefit immensely from the ITIL approach in terms of continual services and business process improvement.

Table 3 to Table 7 depicted a mapping between IT and OT processes. It is important to note that ITIL does not prescribe what and which processes must be implemented, it does not set obligatory requirements (Persse, 2012), but only provide best practices and guidelines for implementation. The processes links with other ITIL processes through process inputs and outputs ultimately forming a web of processes.

5. ITIL Asset Configuration Management Case

Configuration management is an ITIL best practice process that specifies, tracks, and controls the lifecycle of all the individual configuration items in an IT system. Changes to the configuration items are performed using a systematic change management process. A Configuration Items (CI) is defined as the fundamental unit of a configuration management system such as hardware, software, people, location, etc. The use of a Configuration Management Database (CMDB) is part of ITIL's infrastructure operations and support processes. Pantoni, Mossin and Donarires (2007) stipulated that configuration management is a common practice in complex technology-based endeavors. A CMDB contains all the relevant information about the CIs used in an organization to provide services and the relationships between the CIs.

This research proposes the adoption and adaptation of the configuration management process from ITIL into the OT domain for the management of individual configuration items such as network servers, network switches,

workstations, controllers, and field devices. A CMDB is a high-priority system to illustrate the value of a configuration management system in the operational technology domain.

Figure 4 depicts the ISA-95 system hierarchy levels with CMDB deployment at various levels of the enterprise highlighted by rectangles connected by the upward arrow from level 0 to level 4. The distinction between IT and OT is shown on the far-right. The deployment strategy of OT CMDB is as follows:

- Field Device Managers (FDM) are used to collect CI data from various vendor instruments and devices such as transmitters, analyzers, actuators, and drives. It is important for data security that field equipment configurations are password protected to prevent unauthorized configuration changes.
- OT CMDB: A CMDB agent of the Configuration Management System (CMS) software is used to collect CI data of ethernet-reachable devices on the Process Control Network (PCN) such as PLC, SCADA, DCS, Engineering station, operator station, application server, etc. Any changes to the parameters and programmable logic must be accepted by the system via a passcode cybersecurity system or biometric recognition to prevent unauthorized changes by personnel, computer viruses, and malware, and the change must be recorded in a change record. Additionally, CI data stored in the field device managers are Extracted, Transformed, and Loaded (ETL) into the OT CMDB which is the master operational technology CI database. Furthermore, the OT CMDB accepts manually entered data by system administrators.
- An OT CMDB positioned in the enterprise Demilitarized Zone (DMZ) receives the latest CI data from the OT CMDB via the control system firewall through database replication. The CI data in level 3 is utilized by the MES and ERP systems of level 4. In level 4, the OT CI data is combined with IT CMDB in the Enterprise-wide CMDB (ECMDB) used by ERP systems, as a result, an enterprise-wide CI database is created.

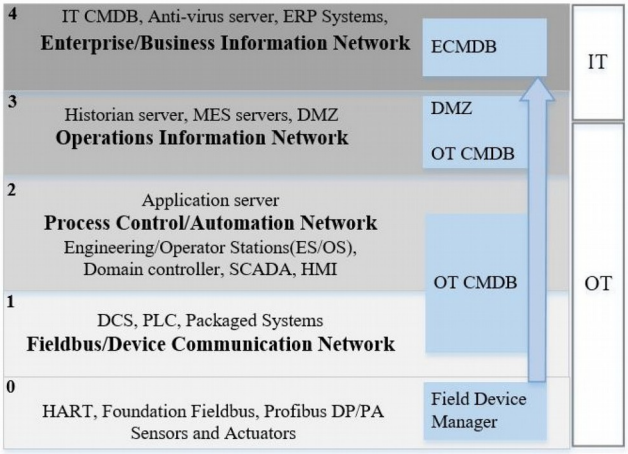

Figure 4. Proposed application of CMDB in the OT domain (Modified ISA-95)

5.1. Structure of Asset Configuration Data

Level 0 assets: The assets logged in the vendor-specific Field Device Manager (FDM) includes that of transmitters, analyzers, actuators, converters, drives, wireless gateways, analyzers, and more. The following configuration items are stored in the FDM: Device tag, device address, model, manufacturer, serial number, asset location, asset area description, asset application system, status, asset business unit, asset department, ownership, device criticality, datasheet information, etc. FDMs are also called field information managers.

Level 1 and 2 assets: Assets logged in the OT CMDB include controllers, network servers, engineering stations, operator stations, network firewalls, network gateways, etc. The level 1 FDM asset data is logged through the ETL process into the OT CMDB at levels 1 and 2 as indicated by the upward arrow in Figure 4. The following configuration items are stored in the OT CMDB: Hostname, IP address, CI type, manufacturer, model, asset tag, serial number, operating system, application software, number of processors, number of cores, processor type, total

memory, total storage space, status, asset location, asset area description, asset business unit, asset department, ownership, business application, business function, business criticality, in-service date, business owner, technical owner, application owner, etc.

Level 3 and 4: The OT CMDB data of level 2 is replicated in the OT CMDB located inside the DMZ. Since the OT CMDB contains configuration data of levels 0, 1, and 2, the OT data is made available to MES systems of level 3 and interface through the operations information network to the ECMDB. The IT CMDB of level 4 and OT CMDB in the DMZ are subscribers to the ECMDB. The ECMDB is used by enterprise systems and can be accessed via personal computers after authentication and authorization by the relevant domain server. The ECMDB configuration items data is available to ERP systems for processing and use by data analytics and business intelligence software packages.

The key objective of a centralized CMDB is to store data and manage change in terms of hardware, software, locations, people, etc., using a change management process. The change process ensures that the risks associated with disruptions to normal OT operations are minimized and managed. The practical enablement of the CMDB through an application case is presented in Figure 5, see below.

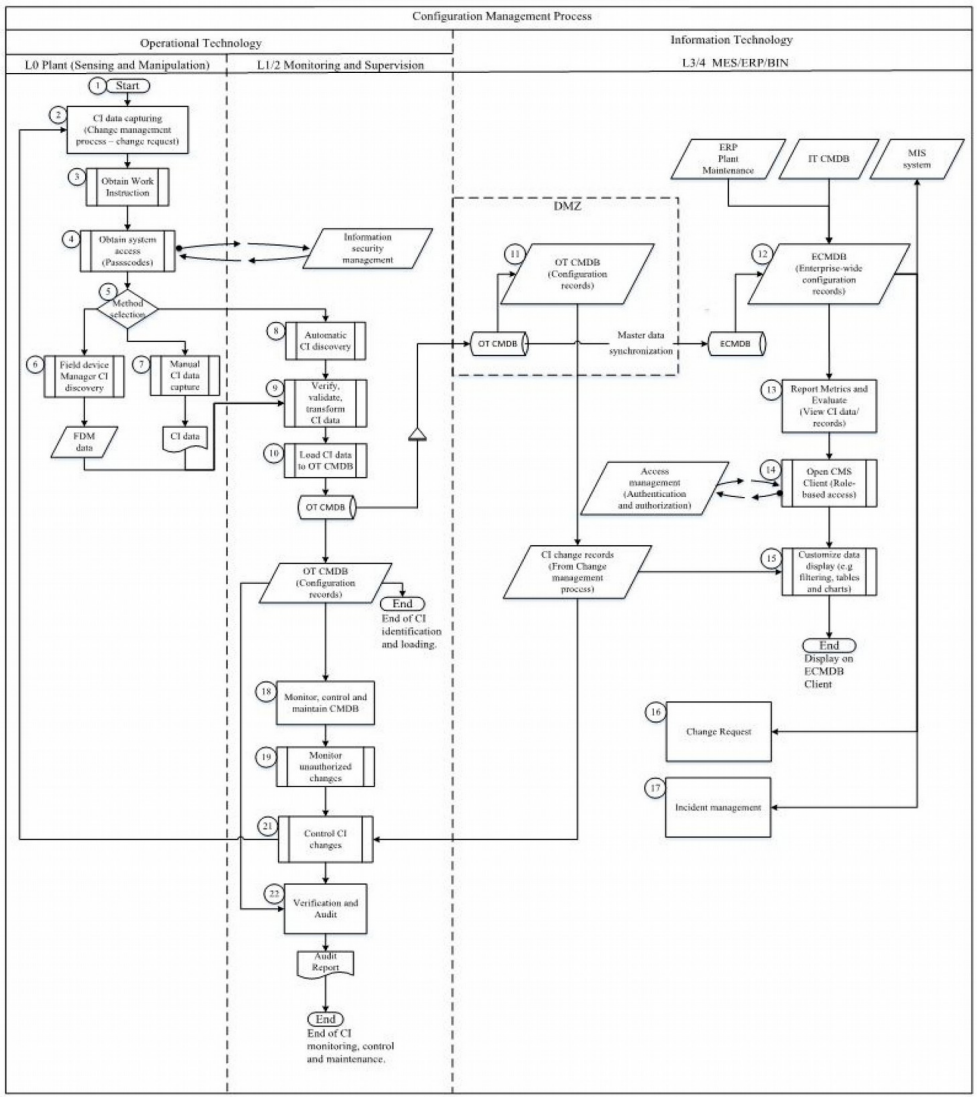

Figure 5. Sample OT configuration management process

An OT CMDB presented in this research is a service-managed function of the organization. Therefore, it is monitored, controlled, and maintained using a change management process that begins with a change request. Step 1 to 10 of Figure 5 illustrates the tasks that are involved in the creation of a CI from the change request to database update for both level 0 and 1 assets. From the same Figure 5, step 11 to 17 takes place in level 3 to 4 of the ISA-95 system hierarchy presented in Figure 4, the tasks are for the acquisition of OT CMDB data and synchronization to the ECMDB for use by level 3 and 4 systems. Steps 13 to 15 highlight the data retrieval process from a user's Personal Computer (PC) as an ECMDB client through an application system. Steps 16 and 17 depict the link between ECMDB and other ITIL and OT processes that require ECMDB data as trigger events or secondary data. Furthermore, step 18 to 22 illustrates the process of managing and auditing of the OT CMDB using a configuration management system application.

Through the business process outlined in Figure 5, a unified support system for OT CMDB is shown. Thus, it demonstrates that ITIL can be successfully integrated into the operational technology domain. Since ITIL processes are interlinked and interdependent, more ITIL processes can be explored in the OT domain, however not overlooking the criticality of OT systems compared to IT systems in the organization in terms of confidentiality, integrity, security, and availability.

6. Projected Benefits of IT Best Practice Framework in OT Domain

The integration of the ITIL service management framework in the OT domain comes with various benefits for the OT organization. Below are the projected benefits:

- Improved strategic alignment (sensor to ERP) between business and the OT department and aligns people, processes, and technology infrastructure assets.
- Reduces costs and wastage through business process integration and standardization.
- Through process interfaces, the unified theoretical framework promotes the involvement of both OT and IT personnel in the implementation of OT CMDB, CSMS, and other relevant collaborations in future 4IR business processes.
- Use of service management tools with advanced analytic features to assist with an overall view of service and process performance across the enterprise. Thus, increasing visibility and assisting the OT organization with analysis of equipment behavioral patterns and better decision making.
- Provides the capability of communication integration to avail more data to the Management Information System (MIS) and ERP systems used by decision-makers.
- The OT domain through ITIL aligns with third-party frameworks such as PMBOK, COBIT, ISO/IEC-55000, TOGAF9, IS0-27001/2, and many more.
- The process performance data assist with business process optimization and selection of the most suitable maintenance strategies. Furthermore, personnel performance is deduced from service and/or process Key Performance Indicators (KPI).
- Clarity of roles and responsibilities, i.e. RACI matrix of various role-players is defined, and governance becomes easily enforceable.
- The unified theoretical framework brings a dynamic assessment of security infrastructure and proactive protection against cyber-attacks, for example, through the use of OT CMDB outline in Figure 5.

7. Findings

7.1. What are the Global Best Practice Frameworks in IT and What Are the Critical Limitations When Applied to OT?

ITIL is a process-oriented framework for information technology service management (Mahy et al., 2017). Furthermore, ITIL is the de facto standard and widely used information technology best practice framework for service management (Sahibudin et al., 2008; Bustamante et al., 2017; Kozlova et al., 2012; Mahy et al., 2017). It is evident from this research that ITIL fills the shortfalls found in the OT operations regarding management processes, in this case, service provision processes. Current operational technology systems are heavily constituted with IT infrastructure components and proliferation is inevitable in the 4IR. Literature illustrated that today's OT

systems are constructed from IT equipment despite differing perspectives regarding failure severity, quality of service, computing power, information/data CISA and that the definition of OT is identical to that of IT. Research has shown that OT in Industry 4.0 will require more smart devices in the control zone (Controllers, sensors, actuators, and drives) to improve data collection and command execution since digital systems have high precision compared to analog systems that are currently installed in OT around the world.

The unified theoretical framework developed in this research illustrates where in the lifecycle of operational technology systems is the ITIL framework most applicable since it closes the shortfalls identified in the landscape framework related to support, operation, and maintenance of OT services and processes. Literature also pointed out that ITIL principles are not only applicable to the IT environment but to other fields that strive to find alignment to business needs to realize effective change and growth.

The critical limitations of ITIL best practice when applied in OT are as follows: The business value of IT best practice processes in the OT domain is challenging to prove to OT management since OT is a technologically slow-paced environment with robust business processes aimed at maximizing plant uptime, the safety of personnel, environment and financial capital; Culture shift and resistance to change limits the full-scale implementation of IT best practice processes even in the IT environment; IT best practice terminology brought forth by frameworks such as ITIL is foreign to the OT domain and result in a steep learning curve for non-IT staff; The cost, time and effort investment required to implement IT best practices can result in OT personnel relapsing to the old work practices; ITSM implementation in IT is challenging often resulting in project failure, and in the OT domain it is expected to be more challenging; and ITSM increases the administration burden to OT personnel that are preoccupied with production and safety targets. Once ITSM is formalized and in full operation in the OT domain in the 4IR context, the management of CPS and IIoT can be significantly improved.

7.2. How Will IT Best Practice Framework Implementation Improve Service Management in an Operational Technology Environment?

ITIL contains a set of best practice processes and employs a process model that considers the process, process enablers, process control, process inputs, triggers, and outputs to create business processes for service management, of which some were found applicable in the operational technology space. Additionally, ITIL consist of a lifecycle made-up of staged phases. The processes contained in each ITIL phase are implemented in organizations based on the needs and objectives set by the organization's top management. ITIL also presents a sample of process flow diagrams that serve as templates for applying ITIL principles and processes. Some of the ITIL processes such as incident management, problem management, and service and asset configuration management have widely been documented in research and implementation. An application case of an OT CMDB illustrates how an ITIL best practice process can be applied in the OT space. IT service management makes OT streamline its services to be cost-effective and more efficient through effective monitoring of process performance using metrics and indicators.

8. Conclusion, Limitations, and Future Work

Apart from answering the research questions as outlined in the findings (Section 7), the aim of this research was also to accomplish the following objectives: Identify an information technology best practice framework used for service management that can be integrated into the operational technology domain; To realize a theoretical framework that integrates operational technology with an information technology best practice framework; To outline the benefits that the operational technology domain can attain from implementing an information technology best practices in the 4IR. The abovementioned objectives have been accomplished by this research.

On contribution to theory, firstly, this research illustrates and concludes that IT best practices are integrable into the operational technology domain for service managing operational technology. However, the difference in perspectives between IT and OT in terms of confidentiality, integrity, security, and availability of systems must be taken into consideration. The adaptability of ITIL is possible because ITIL is not an authoritative framework but a flexible one, therefore, when service management is required in either IT or OT, the framework can be adopted as a guideline.

Secondly, the unified theoretical framework presented in Figure 3 highlights where ITIL fits into the operational technology system lifecycle which is the utilization and support phase. The integration of ITIL in OT to introduce a service management approach charts a path for other IT frameworks that can be explored for integration, for instance, the integration of OT into the broader enterprise through frameworks such as Zachman framework, TOGAF9, etc.

Thirdly, this research shows that data integration between various levels of the enterprise as indicated in Figure 4 and Figure 5, is one of the main pillars of Industry 4.0, particularly of the OT domain. The availability of data at all levels of the enterprise for systems such as Role-based Decision Support Systems (RB-DSS), ERP, MES, and MIS, is vital in providing relevant data and informing management in decision making.

Lastly, with the limited research literature in the IT and OT research community, this study contributes to the content and incite discussions and research regarding the management of new operational technologies that are brought forth by the onset of the 4IR. This research serves to ready the operational technology space for the technological disruptions that are on the horizon through technologies that enable smart manufacturing, cloud computing, BDA, etc.

On contribution to practice, the overall projected benefits and improvements brought to the management of OT operations by ITIL ITSM have been outlined with the unified theoretical framework and application case that resulted in a sample OT CMDB business process. Some of the benefits of applying ITSM in OT include the following: Advanced analytics and business intelligence through the implementation of service portfolio management; Enforcement of role-based decision-making supported by management information systems; Business process optimization and OT organization-wide process standardization; Integration of other IT frameworks to OT domain; and modernization of maintenance and operation of OT assets in the 4IR.

Additionally, the unified theoretical framework and the ITIL-OT mapping seek to outline that ITIL is adaptable to the OT domain as outlined by the mapping and can be extended. In industry or practice, IT personnel and OT personnel scarcely work in unison in collaboratory initiatives, this transdisciplinary study shows that through ITIL best practices people, processes, and technology can be unified to serve common organization-wide goals when relevant business processes in both disciplines are interfaced. Additionally, the collaboration between the disciplines is to a greater extent required in 4IR when managing enterprise-wide cybersecurity, data/information integration, and roll-out of other 4IR technologies in the OT domain. The critical success factors of implementing ITIL have also been outlined, and the main finding is that the approach must be socio-technical to overcome resistance to change by staff.

The limitations of this investigation are that the application of the findings from this research is only applicable to the operational technology domain. As mentioned, this study forms part of limited research in the field of IT/OT integration, mainly with regards to the adoption and adaptation of enterprise IT best practices such as ITIL in the operational technology space. From searching for databases such as IEEExplore, Emerald Insight, and Scopus, this research noted that there are very few published papers in this line of research. This limitation presented unmatched challenges to an extent that should this research had been a systematic literature review; the results would have indicated that there is a bare minimum close to no publications on the research topic compared to the topic of OT or industrial control systems cybersecurity.

On future work, countless amount of research publications focuses on operational technology cybersecurity management. This study opened a new undertaking, where researchers must start thinking about the implications of 4IR technologies on the management aspect of operational technology instead of focusing only on the technology aspect. Research on the 4IR in the OT domain focuses on technology trends such as IIoT, Internet of Everything (IoE), CPS, BDA, and blockchain, while the management aspect receives little to no attention. Researchers must look at ways to manage 4IR technologies in the OT domain to ensure the safe and efficient operation of OT assets. Furthermore, future work includes testing the unified theoretical framework and OT CMDB in a production environment, where CPS or/and IIoT are deployed to refine and expand the framework.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

Abe, S., Fujimoto, M., Horata, S., Uchida, Y., & Mitsunaga, T. (2016). Security threats of Internet-reachable ICS. *Paper presented at the 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)* (750-755). Tsukuba, Japan. https://doi.org/10.1109/SICE.2016.7749239

Ahmad, N., Tarek Amer, N., Qutaifan, F., & Alhilali, A. (2013). Technology adoption model and a road map to successful implementation of ITIL. *Journal of Enterprise Information Management,* 26(5), 553-576. https://doi.org/10.1108/JEIM-07-2013-0041

Blumberg, M., Cater-Steel, A., Rajaeian, M.M., & Soar, J. (2019). Effective organisational change to achieve successful ITIL implementation. *Journal of Enterprise Information Management,* 32(3), 496-516. https://doi.org/10.1108/JEIM-06-2018-0117

Bustamante, F., Fuertes, W., Diaz, P., & Toulkeridis, T. (2016). A methodological proposal concerning to the management of information security in Industrial Control Systems. *Paper presented at the Ecuador Technical Chapters Meeting (ETCM)* (1-6). Guayaquil, Ecuador. https://doi.org/10.1109/ETCM.2016.7750821

Bustamante, F., Fuertes, W., Diaz, P., & Toulkeridis, T. (2017). Integration of IT frameworks for the management of information security within industrial control systems providing metrics and indicators. *Paper presented at the XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)* (11-21). Cusco, Peru. https://doi.org/10.1109/INTERCON.2017.8079672

Bryman, A., Bell, E., Hirschsohn, P., dos Santos, A., du Toit, J., & Masenge, A. (2014). *Research methodology: business and management contexts*. ISBN: 9780199076130.

Chapman, J.P., Ofner, S., & Pauksztelo, P. (2016). Key Factors in Industrial Control System Security. *Paper presented at the 41st Conference on Local Computer Networks (LCN)* (551-554). Dubai, United Arab Emirates. https://doi.org/10.1109/LCN.2016.90

Enose, N. (2012). A Unified management system for Smart Grid. *Paper presented at the Innovative Smart Grid Technologies (ISGT).* Kollam, Kerala, India. https://doi.org/10.1109/ISET-India.2011.6145400

Fan, X., Fan, K., Wang, Y., & Zhou, R. (2015). Overview of cyber-security of industrial control system. *Paper presented at the International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)* (1-7). Shanghai, China. https://doi.org/10.1109/SSIC.2015.7245324

Flick, U. (2009). *Designing Qualitative Research* (1st ed.). London: SAGE Publications.

Galloway, B., & Hancke, G.P. (2013). Introduction to Industrial Control Networks. *Communications Surveys & Tutorials,* 15(2), 860-880. https://doi.org/10.1109/SURV.2012.071812.00124

Garimella, P.K. (2018). IT-OT Integration Challenges in Utilities. *Paper presented at the 3rd International Conference on Computing, Communication and Security (ICCCS)* (199-204). Kathmandu, Nepal. https://doi.org/10.1109/CCCS.2018.8586807

Gartner (2018). Gartner. https://www.gartner.com/it-glossary/best-practice

Ghobakhloo, M. (2018). The future of manufacturing industry: a strategic roadmap toward Industry 4.0. *Journal of Manufacturing Technology Management,* 29(6), 910-936. https://doi.org/10.1108/JMTM-02-2018-0057

Isaksson, A.J., Harjunkoski, I., & Sand, G. (2018). The impact of digitalization on the future of control and operations. *Journal of Computers & Chemical Engineering,* 114, 122-129. https://doi.org/https://doi.org/10.1016/j.compchemeng.2017.10.037

ISO/IEC/IEEE-15288 (2015). *ISO/IEC/IEEE-15288.* https://www.iso.org/standard/63711.html

Jiang, J. (2017). An improved Cyber-Physical Systems architecture for Industry 4.0 smart factories. *Paper presented at the International Conference on Applied System Innovation (ICASI)* (918-920). Sapporo, Japan. https://doi.org/10.1109/ICASI.2017.7988589

Jie, P., & Li, L. (2011). Industrial Control System Security. *Paper presented at the Third International Conference on Intelligent Human-Machine Systems and Cybernetics* (156-158). *Zhejiang,* China. https://doi.org/10.1109/IHMSC.2011.108

Kannan, S.M., Suri, K., Cadavid, J., Barosan, I., Brand, M.v.d., Alferez, M., et al. (2017). *Towards Industry 4.0: Gap Analysis between Current Automotive MES and Industry Standards Using Model-Based Requirement Engineering.* Gothenburg, Sweden. https://doi.org/10.1109/ICSAW.2017.53

Kempter, S. (2019). *ITIL Process Maps.* https://wiki.en.it processmaps.com/index.php/ITIL_Implementation

Kossiakoff, A., Sweet, W.N., Seymour, S.J., & Biemer, S.M. (2011). *Systems Engineering Principles and Practice* (2nd ed.). John Wiley & Sons.

Kozlova, E., Hasenkamp, U., & Kopanakis, E. (2012). Use of IT Best Practices for Non-IT Services. *Paper presented at the Annual SRII Global Conference* (725-734). San Jose, CA, USA. https://doi.org/10.1109/SRII.2012.85

Lema-Moreta, L., & Calvo-Manzano, J. (2018). A proposal for implementation of ITIL incident management process in SMEs. *Paper presented at the Second Ecuador Technical Chapters Meeting (ETCM)* (1-5). Salinas, Ecuador. https://doi.org/10.1109/ETCM.2017.8247494

Lewandowski, D., Pareschi, D., Pakos, W., & Ragaini, E. (2018). Future of IoTSP - IT and OT Integration. *Paper presented at the 6th International Conference on Future Internet of Things and Cloud (FiCloud)* (203-207). Barcelona, Spain. https://doi.org/10.1109/FiCloud.2018.00037

Limanto, A., Khwarizma, A.F., Rumagit, R.Y., Pietono, V.P., Halim, Y., & Liawatimena, S. (2017). A study of Information Technology Infrastructure Library (ITIL) framework implementation at the various business field in Indonesia. *Paper presented at the 5th International Conference on Cyber and IT Service Management (CITSM)* (1-4). Denpasar, Indonesia. https://doi.org/10.1109/CITSM.2017.8089244

Mahy, Y., Ouzzif, M., & Bouragba, K. (2017). Supporting ITIL processes implementation using business process management systems. *Paper presented at the Third International Conference on Systems of Collaboration (SysCo)* (1-4). Casablanca, Morocco. https://doi.org/10.1109/SYSCO.2016.7831338

Mathew, S., & Pretorius, J.H.C. (2017). Critical success factors for instrumentation and control projects within the power industry in South Africa. *Paper presented at the International Conference on Industrial Engineering and Engineering Management (IEEM)* (608-613). Singapore, Singapore. https://doi.org/10.1109/IEEM.2017.8289963

Medoh, C., & Telukdarie, A. (2016). *Enhancing Enterprise Resource Planning and Manufacturing Execution System Efficiency with Simulation-Based Decision Support.* Johannesburg, SA.

Pantoni, P.R., Mossin, A.E., & Donarires, S.O. (2007). Configuration Management for Fieldbus Automation Systems. *Paper presented at the International Symposium on Industrial Electronics* (1844-1848). Vigo, Spain. https://doi.org/10.1109/ISIE.2007.4374886

Persse, J. (2012). *The ITIL Process Manual Key Processes and their Application* (1st ed.). Van Haren Publishing.

Pollard, C., & Cater-Steel, A. (2009). Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study. *Journal of Information Systems Management,* 26(2), 164-175. https://doi.org/10.1080/10580530902797540

Quayzin, X. (2011). Are best practices really best practice?. *Paper presented at the 6th IET International Conference on System Safety.* Birmingham, UK. https://doi.org/10.1049/cp.2011.0271

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2013). *Research Methodology.* New York: Cornel University.

Ray, P.D., Harnoor, R., & Hentea, M. (2010). Smart power grid security: A unified risk management approach. *Paper presented at the 44th Annual 2010 IEEE International Carnahan Conference on Security Technology.* San Jose, CA, USA. https://doi.org/10.1109/CCST.2010.5678681

Robinson, N. (2005). IT excellence starts with governance. *Journal of Investment Compliance,* 6(3), 45-49. https://doi.org/10.1108/15285810510659310

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *Paper presented at the Second Asia International Conference on Modelling & Simulation (AMS)* (749-753). Kuala Lumpur, Malaysia. https://doi.org/10.1109/AMS.2008.145

Sharifi, M., Ayat, M., Rahman, A., & Sahibudin, S. (2008). Lessons learned in ITIL implementation failure. *Paper presented at the International Symposium on Information Technology.* Kuala Lumpur, Malaysia. https://doi.org/10.1109/ITSIM.2008.4631627

Sopko, M., & Winegardner, K. (2007). Process control network security concerns and remedies. *Paper presented at the Cement Industry Technical Conference Record.* Charleston, SC, USA, 26-37. https://doi.org/10.1109/CITCON.2007.358984

Vavra, J., & Hromada, M. (2015). An evaluation of cyber threats to industrial control systems. *Paper presented at the International Conference on Military Technologies (ICMT)* (1-5). Brno, Czech Republic. https://doi.org/10.1109/MILTECHS.2015.7153700

Yang, W., & Zhao, Q. (2015). Cyber security issues of critical components for industrial control system. *Paper presented at the Chinese Guidance, Navigation and Control Conference* (2698-2703). Yantai, China. https://doi.org/10.1109/CGNCC.2014.7007593