9th International Conference on Through-life Engineering Service
3-4 November 2020, Cranfield UK

A Multi-Level Analysis of the Implementation of Industrial Internet of Things: Challenges and Future Prospects

Sulaiman Rajab, Prateek Saxena*, Konstantinos Salonitis

Manufacturing department, School of Aerospace, Transport and Manufacturing, Cranfield University, MK43 0AL, UK

*Corresponding author. E-mail address: p.saxena@cranfield.ac.uk

Abstract

Industrial Internet of Things (IIoT) is still a new research area. The main emphasis of the IIoT literature is on identifying the challenges involved in implementation of the IIoT. This paper summarizes the literature on the barriers faced by any stakeholder aiming to adopt IIoT anywhere. After reviewing 31 empirical studies, three domains of factors have been identified, individual (skills, abilities and knowledge), institutional (organizational/management-related), and structural (technical and economic infrastructures). A total of eleven factors across the three dimensions have been extracted. The most important factors were the absence of human capital (limited individual soft and technical knowledge, skills and abilities), low information security experience leading to a high probability data leaks and high management resistance from employees and leaders. To strengthen information for successful IIoT implementation, this paper proposes the mandate of Security, Education, Training, and Awareness (SETA) initiatives for any stakeholder interested in IIoT adoption. A Causal loop diagram for the IIoT implementation is also developed and discussed in this work.

Keywords: Industrial Internet of Things; Challenges; Security Education and Training Awareness.

1. Introduction

New technological innovations over the last several decades have led to the initiation of the fourth industrial revolution, also known as industry 4.0 [1]. Also with the emergence of Industry 4.0, the industrial sectors are most impacted, contributing to the development of smart industries, goods, and services [2]. Industrial Internet of Things (IIoT) contributes to the widespread use of the internet in a business organization and is one of the nine key elements of Industry 4.0 [1]. Much of the available empirical literature discuss IIoT in highly developed economies like the United States, the United Kingdom, Australia, Singapore, Hong Kong, and China. This hinders the ability of interested stakeholders in adopting IIoT in many contexts [3] such as limited access to resources, non-specialized human capital and fragmented technological infrastructures; the case of many developing nations. Prior to the implementation of IIoT, stakeholders need to address areas of deficiencies or deal with potential barriers [4].

One dominant focus in the IIoT literature is the investigation of the challenges, obstacles and barriers facing stakeholders in implementing IIoT. Such barriers are not static and differ based on the availability of economic, social, cultural, and human capital. This makes each application of IIoT in manufacturing unique since it faces a different set of individual, institutional and structural barriers [5]. On another front, analyses of challenges of IIoT often concentrate on one level of analysis, technological systems-related factors, and ignore other equally important ones including individual and institutional [6]. Thus, a comprehensive multi-level investigation that summarizes individual, institutional, and structural factors hindering the IIoT implementation is warranted [7].

Prior research has concluded that specific individual skills, abilities and knowledge are correlated with a successful IIoT implementation [8]. Further, researchers have highlighted the significance of institutional, management and organizational variables in explaining IIoT desired application [9]. In addition, researchers have noted the requisite technological infrastructures necessary for the fruitful realization of IIoT in manufacturing [10].

It is estimated that the IIoT market is expected to reach approximately $124 billion by 2021 [14]. Over 90% of the information technology professionals, therefore, expect colossal investment and development in security and privacy apparatuses due to the rapid implementation of IoT across nearly all sectors. By 2020, Cisco has projected that 46% of machines will be connected. Some estimates posit that the IIoT will contribute $14 trillion to the global economy by 2030. Such statistics highlight the need for an immediate research and development in IIoT, particularly regarding its challenges and the investment (reaping

some of the potential benefits afforded by the technology in particular) [15].

The meta-analysis of the literature noted the information security awareness requiring an elevated level of training to prevent potential leaks. IIoT-related Security Education and Training Awareness (SETA) programs are likely to decrease information risks and improve compliance with internal, governmental, and international standards that have been shielding operations from potential leaks. SETA programs enhance individuals' attitudes, subjective norms, perceived behavioural control, and protective measures in order to avoid falling victims. IIoT SETA initiatives have ultimately enhanced three common challenges faced by the implementation of IIoT: human capital, human elements, and acceptance of change [11].

This paper presents the challenges when implementing IIoT. A multi-level analysis framework is a consideration of more than just a single level of analysis, and such an approach is therefore utilized in this investigation. More specifically, the analysis surveys recent literature on individual-level indicators that prevent the application of the best practices in IIoT. Three main domains of factors have been highlighted: low IIoT human capital, limited SETA workforce preparation, and resistance to change from traditional settings into IIoT contexts.

The organization of this paper is as follows. First, a literature review surveying the biases in existent IIoT literature is discussed. The challenges of implementing IIoT are then presented. Next, a detailed discussion on the individual, institutional, and structural preventing IIoT from taking a foothold is discussed. Finally, recommendations to overcome such challenges are suggested.

2. Critical Review of IIoT literature approach

The Internet of Things (IoT) refers to the machine-to-machine interconnectedness that is enabled through networks that exchange information and operate autonomously prior to making independent decisions without human interference [11]. In manufacturing, IoT aims to conserve resources, eliminate waste, and increase product quality while retaining high customer satisfaction rates (the same goals as of lean manufacturing). The application of IoT within the manufacturing world is referred to as the Industrial Internet of Things (IIoT), and smart factories constitute the most applicable implementation of IIoT within the manufacturing sector [12]. GE Digital predicts that 46% of the global economy will benefit from IIoT. In addition, their estimates suggest that IIoT will impact energy production and consumption considerably in the future [13].

Most analyses and investigations in the implementation of IIoT focus on the industrial world and have neglected the serious efforts to adopt the new technology [5]. One dominant focus of the IIoT research emphasizes the plethora of challenges that manufacturers face in implementing IIoT. Such barriers are not static and differ based on the availability of economic, social, cultural, and human capital. Therefore, manufacturing companies in different countries are likely to exhibit unique challenges that are rarely outlined in the IIoT literature. Simultaneously, analyses of IIoT challenges often concentrate on only one level of analysis (technological/systems-related factors) and ignores other equally important ones at both the institutional and individual levels [14].

Most analyses of IIoT challenges focus on technology-related factors preventing manufacturers from implementing it on their factory floors. In their analysis of IIoT barriers, Miazi et al. [16], concluded that four main areas needed to be addressed prior to any serious attempt to apply IIoT: technical factors, data centre availability, financial resources and security, and issues with privacy and trust. Notice that the three of the four areas emphasized by the researchers deal with technology-related variables and limited significance is awarded to institutional, social, organizational, and individual-level factors. Other authors have strictly examined the shortcomings of manufacturers' resources, processes, planning, and management, shedding light on the institutional domain of barriers while neglecting other important dimensions [7]. Further, only limited attempts have been made to blend a multi-level systematic analysis of IIoT challenges [17].

Most studies concerning IIoT challenges also assess the English language literature while leaving hundreds of papers (written in foreign languages such as Arabic, Japanese, or Turkish) without inspection. This excludes the potential of detecting both common and unique factors influencing the adoption and implementation of IIoT in these regions. Further, with the monolingual concentration of the research comes to a barrier to accessibility for the audiences themselves understudy, limiting the ability to actually apply the findings [6]. This is compounded with the seclusion of unpublished studies (such as dissertations and theses) from incorporation in previous studies, in a large part due to these language barriers, resulting in a failure to include solutions that may be applicable to addressing the limitations highlighted in the respective studies. The current analysis, therefore, surveys a broader spectrum of research that has been published in both peer-reviewed journals and unpublished outlets.

The methodology for the current research follows a critical literature review framework. First, the authors constructed research questions, outlined in Table 1. Second, the researchers constructed a list of phrases to be searched in major electronic databases. Third, a search of the journals' databases

was performed identifying relevant articles. Fourth, only those articles that featured challenges of IIoT were retained. Fifth, the authors read each paper carefully listing the identified factors. Sixth, a general typology of challenges was constructed where all identified challenges were classified into individual, structural and institutional. Seventh, the authors read each paper twice to ensure consistency of classification. Eighth, a comparison of classifications yielded perfect match indicating a high reliability of the classification technique. Below is a more nuanced explanation of the methodology.

A structured review process, outlined in Table 1, has been followed during the present investigation. The study attempts to answer three research questions (RQ):

- RQ1 = what are the individual level variables preventing IIoT from being adopted?
- RQ2 = what institutional level variables prevent IIoT from being adopted?
- RQ3 = what are the structural variables preventing IIoT from being adopted?

The following databases were used to locate and identify relevant studies for the review: Google Scholar, IEEE, ACM, and Scopus. This assessment has also focused on recently published works. Search terms included "Industrial Internet of Things," "challenges of IIoT," "Barriers to IIoT," and "IIoT implementation."

Table 1: Review Specifications.

Stage	Description
Research Question(s) Formulation	Questions Intended to be Answered
Location and Selection of Studies	Choice of Databases Time Specifications Inclusion Criteria Specification Identification of search terms
Synthesis of Studies	Thematic analysis
Analysis of Studies	Identification of research gaps
Reporting Results	Classification in Figurative and Tabular formats

A total of 31 empirical papers were reviewed and classified into three domains of barriers for IIoT implementation as Figure 1 illustrates. It is worth noting that individual factors were highlighted in more papers than the structural, as well as institutional factors. A closer examination in Figure 2 reveals that most papers were concerned with the human capital factor as a barrier to IIoT implementation.

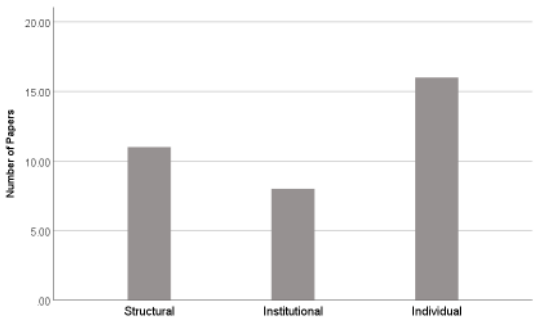

Fig. 1. Number of Reviewed Articles Base on Identified Barriers to IIoT.

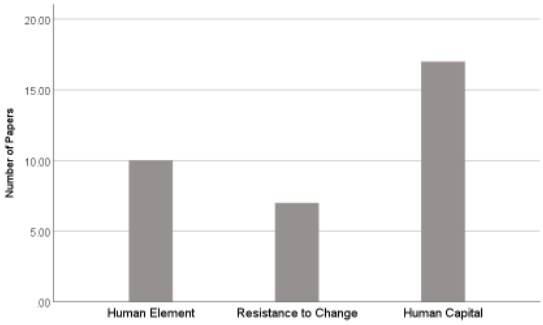

Fig. 2. Number of Reviewed Articles by Individual Barrier to IIoT implementation.

3. Challenges of IIoT.

Figure 3 illustrates the challenges faced during the implementation of IIoT. Notice that the factors are distributed across three broad categories of analysis that are important for the successful adoption and implementation of IIoT. The challenges can broadly be categorized into Structural, Institutional and Personal level challenges. Each of the challenge is discussed thoroughly in the subsequent sections.

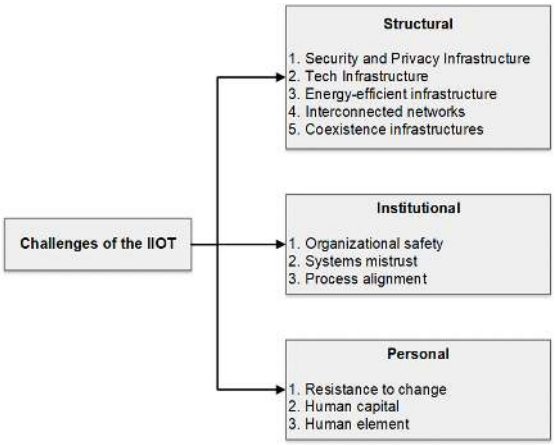

Fig 3. Challenges of the IIoT.

3.1 Individual-Level Challenges

3.1.1 Resistance to change.

Resistance to change, originating from manufacturers, stakeholders, and investors, constitutes one of the main challenges facing the implementation of IIoT today. Fear of job loss in the traditional manufacturing setting and the creation of an entire class based on cyber employment forms another primary barrier for the application of IIoT technologies, principles, and practices [8]. Kamble et al. concluded that employment disruptions and foreseen job replacements that will be brought about by the implementation of IIoT constitute the most important barriers for adopting IIoT [18]. Studies have also indicated that employees are usually resistant to the change, sticking to traditional work strategies that pose serious threats to information security and privacy. New compliance policies and standards for cybersecurity, therefore, need to be taught, practiced, monitored and enforced. These standards also need to fit the expectations, attitudes, and norms of the workforce. Ethical training should also precede any technical or cybersecurity educational program [19]. Ultimately, employees need to learn the value of change and to be exposed to the threats of cybersecurity through simulations in order to better safeguard the vulnerabilities of their systems. A need for implementation frameworks that consider and foresee the resistance is evident. Such frameworks have been developed for other organization wide initiatives, such as the introduction of lean [31].

3.1.2 Human capital.

The demand for skilled employees, combined with shortages in staff necessary to operate IIoT platforms in manufacturing, comprises a challenge for potential smart manufacturers. Khan and Turowski, identified the need for advanced training in data analytics, networking, and engineering as being of utmost importance for successfully achieving the transition into smart manufacturing [20]. Vogelsang et al., also identified a set of barriers related to the skills and individual profiles of workers in IIoT. The missing skills included the absence of necessary IT skills and appreciation for IIoT, the absence of process compatibility with technical knowledge, and the lack of overall technical appreciation for the role of technology [3].

The quality of instruction, certification, and assessment in cybersecurity protocols, standards, and programs, has been weak. This has resulted in the creation of only a limited pool of talented and qualified individuals and teams that are capable of securing industrial systems against cybercriminals [16]. Investment in advanced certification programs in cybersecurity has also been fragmented, often being an individual's endeavour rather than a systematic effort by national governments or manufacturing firms [7].

3.1.3 The human element in information security.

Aside from advanced security protocols and algorithms, human education and training in information security are also highlighted among the most important factors in successfully implementing IIoT [9]. Human errors, be they intentional or inadvertent, are the leading culprits behind information breaches and the chief drivers of phishing attacks. Investigations have so far emphasized the lack of an appropriate information security culture across organizations in the world, which necessitates prompt investment in education and training programs [19].

SETA programs are seldom found in the manufacturing sector. The workforce is therefore rarely trained in the technological and human tactics utilized to secure networks and information systems. When they are implemented, SETA programs have not been uniformly taught, monitored, or evaluated [11]. This generates a situation where employees lack the appropriate knowledge of responses that are proper during specific cybersecurity incidents [9]. Further, individuals joining the manufacturing sector have not developed the awareness and practices necessary for shielding their firms' or operations' essential cyberinfrastructure [19].

3.2 Institutional-Level Challenges

3.2.1 Process Alignment.

Process alignment refers to unifying all processes, measurement frameworks and business operations under a single rubric. Another barrier highlighted by the researchers is the lack of process flexibility and alignment with the IIoT infrastructure. Choi et al. reviewed and summarized the literature for the barriers that manufacturers are facing when adopting and implementing IIoT technologies [17]. From the perspective of a digital manufacturing vendor, the authors suggested that the focus should be on the functionality and specificity of the system. Vendors tend to map out processes, giving each actor a single, well-defined, task. This neglects the interdependence of tasks or each locations' work culture. Often, employees (or knowledge personnel) in manufacturing do perform distinct tasks and utilize various software creating an asynchronous environment that makes it harder on everyone engaged in production to follow information, products and services flow. To achieve a better implementation of IIoT, this behaviour needs to be modified. Further, from the manufacturing perspective, digital manufacturing could help streamline everything in the factory.

Nevertheless, the available data is insufficient in most cases and originates from different sources, thereby preventing a comprehensive and well-integrated system. Further, each work unit is

typically concerned only with its own work product, which prevents the development of a comprehensive performance measurement system that could be adopted by the manufacturer to ascertain the extent to which the IIoT or digital manufacturing actually works. Another barrier has been the presence of many varieties of software, practices, and a general lack of standardized work culture that appreciates the potential benefits of IIoT [21].

3.2.2 Systems Mistrust.

A less noticeable challenge (though of major significance to the implementation of IIOT in manufacturing) is mistrust among smart digital devices. Since machines are autonomously receiving, processing and generating orders, they are engaged in a collaborative work relationship. Evidence indicated that digital devices at times do not cooperate with each other for a variety of reasons including potential suspicion of fraudulent behaviour. Jeong et al. [22] identified a related challenge in the security of IIoT operations within smart factory settings where computing devices form mistrust via malicious behaviours. They argued that, in many cases, devices may manipulate data transmitted to systems in order to increase their share of resources, thereby inhibiting the smooth operation of the entire production system. The suggestion is made, therefore, that further research should be conducted in order to address this issue while facilitating the creation of a standardized, predictable, and error-free system operation within the smart factory [22].

3.2.3 Organizational Safety Controls.

Cybersecurity, safety, and privacy have remained as significant impediments to the implementation of IIOT in modern manufacturing [9]. Khan and Turowski [18] noted that the increase in resource-sharing has posed a serious threat to manufacturers' comparative advantages. Manufacturers fear the loss to their competitors of critical information and customized solutions and therefore will be increasingly hesitant to collaborate with others over IIOT. The authors further identified information breaches as one of the most potentially damaging factors preventing manufacturers from adopting IIOT capabilities. The last thing a company desires is the loss of private information or its assets, either cyber or physical. Therefore, stakeholders oftentimes are hesitant to make the transition into IIOT enabled technologies and platforms within manufacturing settings.

3.3 Structural-Level Challenges

3.3.1 Technical Infrastructure.

One of the most widely cited challenges in implementing IIOT in the manufacturing sector is the lack of technological infrastructure. Moktadir et al. explored the implementation of IIOT in the leather industry of Bangladesh by using a multi-criteria method for discovering the most pressing challenges. They found that manufacturers lack necessary software and hardware applications, as well as machinery, that supports the various capabilities and potential of IIOT [23]. Similarly, Khan and Turowski, identified (based on in-depth interviews and questionnaire data obtained through their case research) the need for developing robust data collection and analytics systems as one of the most pressing challenges facing manufacturers and production systems [20]. Kamble et al. further indicated that the high costs associated with the instalment of the infrastructure and implementation of IIoT were prohibitive [18]. Vogelsang et al. also identified a similar set of technical barriers (including the lack of appropriate infrastructure, security, and the use of heterogeneous and ineffective technologies) when implementing IIoT [3].

3.3.2 Energy-Efficient Infrastructures.

IIOT application to the manufacturing sector consumes significant amounts of energy, thus presenting several challenges to manufacturers. Sensors placed on machines and devices require power, so consistent supplies of low-energy sustainable batteries (that can be an expensive endeavour on the part of the manufacturer) must be undertaken [24]. Wireless Sensor Networks are also required in an IIOT environment, which in turn necessitates the establishment of a densely networked machine-to-machine environment. This makes data transfers easier and faster; however, it consumes a large amount of energy [25]. Further, research and development in green networking proves to be essential for a successful implementation of the IIOT

3.3.3 Interconnected Networks Availability.

IIOT application requires a reliable, fast, and timely-bound extensive network. This requirement is an expensive investment, rarely scalable, and difficult to deploy. Most manufacturers in the developing world lack the sufficient funds to establish robust networks quickly to power their operations[10]. Solutions for adapting to the external and internal disturbances facing IIOT networks that have been proposed by researchers have typically been framed by using centralized architectures, which are not scalable [13].

3.3.4 Coexistence Infrastructure.

IIOT application scalability to manufacturing environments is also limited due to the issue of coexistence [26]. Implementation of IIOT requires many devices to work simultaneously within a proximal environment, creating the challenge and risk of interference. While numerous solutions have been attempted to keep interference at a minimum, the dense, expensive, and complex IIOT environment will inevitably create problems for functional performance and operability of devices due to its triggering of machine-to-machine interventions. Also, the memory required by a successful IIOT deployment is unmet with currently proposed frameworks and models [27]. This creates the need to develop an interoperable IIOT environment where devices manage to share data both reliably and timely.

3.3.5 Security and Privacy Infrastructure.

Privacy and security present the most important challenges to IIOT applications. Conventional methods of cryptography have failed to secure the complex, coexistent, IIOT environment. More sophisticated solutions are therefore required, which by definition utilizes more resources, computation, and overhead investment [28]. The legal environment, with complex compliance structures and privacy protection layers for the information of customers, manufacturers, suppliers, and all other parties involved in an IIOT environment, also frighten potential IIOT investors [29]. Ultimately, IIOT requires advanced, technically sound, and validated security protocols coupled with highly competent legal teams, all of which require further financial and human investments.

4. Global Complexity

The implementation of IIOT into manufacturing today is not straight-forward. Rather, it is complex and filled with uncertainty, making its smooth and robust implementation into today's manufacturing settings difficult [8]. Sjödin, et al. [30] noted that the implementation of IIOT is a problem of systemic change, where one shift in an element (like production) is expected to alter other elements of the system (thereby creating unintended changes, whether in the technologies adopted or processes implemented). Further, many manufacturers lack the necessary knowledge or requirements that are essential for the instalment of smart factories and manufacturing systems. Exploratory research of factories that have implemented smart manufacturing in Sweden have ultimately found that the lack of vision toward smart manufacturing among stakeholders, uncertainties created by technological complexities, difficulties in digitization, fast-paced changing environments, lack of appropriate planning, and absence of cross-collaboration among stakeholders in factories constitute the main barriers toward applying IIOT to manufacturing [30]. Meanwhile et al found that a lack of comprehending the benefits associated with IIoT is the most important challenge faced by manufacturers in implementing IIoT [18].

5. Modelling of the IIoT implementation –A System Dynamics perspective

In order to understand and visualize the interdependency of the variables, a Causal Loop Diagram (CLD) is developed. A CLD diagram consists of the nodes and the edges. All the variables responsible for the IIoT implementation are represented with the nodes. The relation between two variables is shown with an edge. A relationship can further be classified as a positive or a negative relation, but this is not within the scope of this work.

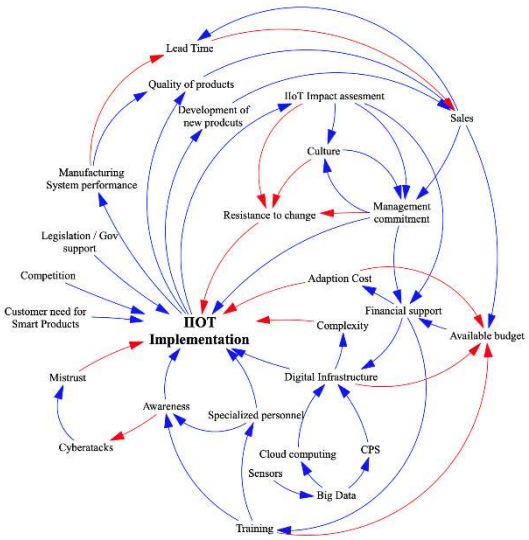

Fig. 4. Causal Loop Diagram for IIoT implementation

Figure 4 demonstrates the relationships between individual, instructional and structural factors involved in the implementation of the IIoT. As it is evident from CLD, Sensors have an influence on the big data, which is further related to the cloud computing and CPS. Each of them are linked to the digital infrastructure which is also linked to the financial support and the complexity in implementation of the IIoT.

6. Limitations

Figure 5 outlines the limitations of Security Education, Training, and Awareness (SETA) programs ignored by the cybersecurity literature reviewed in this paper. To be effective, SETA must conform to standard empirically supported instructional design practices. Those include the meticulous specification of topics to be covered, duration of courses, mediums of materials' delivery, and pilot testing. Further, SETA programs oftentimes suffer from low top management support

devoted elsewhere in manufacturing organizations. This is associated with the lower levels of funding, recognition of cybersecurity as an imminent threat, and decreased personnel dedication to protecting the manufacturing infrastructure. In addition, when SETA protocols are administered, they are not appropriately monitored, evaluated, or enforced. Such limitations need to be voiced more by advocates for cybersecurity in the manufacturing sector. More importantly, the solution to such problems lies in the harnessing of top management support, the implementation of instructional design universal principles, and consistent evaluation, as well as swift enforcement of rules associated with breaches' instances.

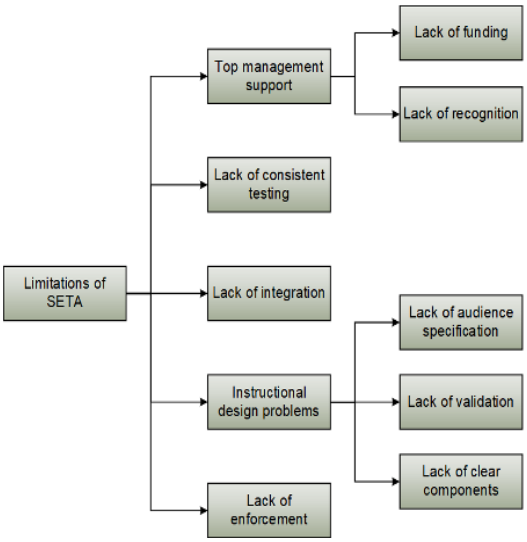

Fig. 5. Limitations of SETA

7. Conclusions and Future Work

This investigation has summarized the most common and recurring challenges facing the implementation of IIoT more comprehensive level of analytical approach that was applied in order to generate the individual, institutional, and structural factors composing the overarching barriers which prevent manufacturers from deploying IIoT. Eleven factors were ultimately extracted from the extant literature, with 3 individual, 3 institutional, and 5 structural challenges. Despite the additional weight that structural variables have been awarded by earlier studies, human capital and institutional process related factors have been seen to carry an equal significance when altering manufacturers' decision to adopt and implement IIoT. Future research should, therefore, focus on including studies from more linguistic backgrounds in addition to the English currently dominating this field of inquiry. Further, a more comprehensive and disaggregated analysis that dissects each category conceptualized in this research should be undertaken to better identify barriers obstructing the implementation of IIoT. More specific case studies should also be encouraged in order to generate detailed information about particular contexts (i.e. countries or industries). Future studies should focus on the process of IIoT implantation. This can be done by applying qualitative research techniques like process tracking. This method enables researchers to identify the milestones constructing a process or leading to an outcome. It allows the identification or critical junctures, decisions, and stockholders.

Implications for through-life-engineering are numerous. First, the improvement of human capital enhances the design, manufacturing, and functioning capabilities of IIoT products. Second, the deployment of IIoT advanced technologies including data analytics and cloud computing facilitates the scalability of high-valued products manufacturing scalability, perfection, and delivery to customers. Third, aligning all complex processes involved in the production of high-valued products within the IIoT framework decreases defects, variability, and design/production related complications. Fourth, increasing human's information security practices in IIoT facilities result in fewer instances of privacy invasions for high-valued digital products, and their usage over the customer's lifespan.

Understanding IIoT challenges in the world carry varied benefits. First, the investors learn how to allocate limited resources before making any critical decisions concerning making their facilities smart. Second, policymakers learn about the areas of need and improvement to funnel monetary and logistic support to improve conditions for smart manufacturing. Third, existing enterprises become more alert to the problems facing manufacturers and introduce preventive measures like information security training for their employees avoiding disastrous outcomes. Fourth, employees in manufacturing firms are aware of existing challenges and make strides to ameliorate their skills, abilities, and knowledge making manufacturing more effective and efficient.

References

[1] Saxena, P., Papanikolaou, M., Pagone, E., Salonitis, K., & Jolly, M. R. (2020). Digital manufacturing for foundries 4.0. In Light Metals 2020 (pp. 1019-1025). Springer, Cham.
[2] Stock, T., & Seliger, G. (2016). Opportunities of sustainable manufacturing in industry 4.0, Procedia Cirp, 40, 536-541.
[3] Vogelsang, K., Liere-Netheler, K., Packmohr, S., & Hoppe, U. (2019, January). Barriers to Digital Transformation in Manufacturing: Development of a Research Agenda. In Proceedings of the 52nd Hawaii International Conference on System Sciences.
[4] Liao, Y., Loures, E., & Deschamps, F. (2018). Industrial Internet of Things: A systematic literature review and insights. IEEE Internet of Things Journal, 5(6), 4515-4525.
[5] Adly, A. (2019). Technology trade-offs for IIoT systems and applications from a developing country perspective:

case of Egypt. In The Internet of Things in the Industrial Sector (pp. 299-319). Springer, Cham.

[6] Arnold, C. (2017). The Industrial Internet of Things from a Management Perspective: A Systematic Review of Current Literature. Journal of Emerging Trends in Marketing and Management, 1(1), 8-21.

[7] Kim, Y., Cho, N., & Jang, H. (2018). Trends in Research on the Security of Medical Information in Korea: Focused on Information Privacy Security in Hospitals. Healthcare informatics research, 24(1), 61-68.

[8] Kusiak, A. (2018). Smart manufacturing. International Journal of Production Research, 56(1-2), 508-517.

[9] Atlam, H., & Wills, G. (2020). IoT Security, privacy, safety and ethics. In Digital Twin Technologies and Smart Cities (pp. 123-149). Springer, Cham.

[10] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 101, 1-12.

[11] Ashton, K. (2009). That 'internet of things' thing. RFID journal, 22(7), 97-114.

[12] Lee, C., Zhang, S., & Ng, K. (2017). Development of an industrial Internet of things suite for smart factory towards re-industrialization. Advances in manufacturing, 5(4), 335-343.

[13] Sun, W., Liu, J., & Yue, Y. (2019). AI-enhanced offloading in edge computing: when machine learning meets industrial IoT. IEEE Network, 33(5), 68-74.

[14] El-Mawla, N., Badawy, M., & Arafat, H. (2019). IoT for the Failure of Climate-Change Mitigation and Adaptation and IIoT as a Future Solution. World, 6(1), 7-16.

[15] Bayshore Networks, 2017, IIoT: 8 Fun Facts, Accessed: 02:01:2020. [Online]. Available: https://www.bayshorenetworks.com/blog/iiot-fun-facts

[16] Miazi, M., Erasmus, Z., Razzaque, M., Zennaro, M., & Bagula, A. (2016, May). Enabling the Internet of Things in developing countries: Opportunities and challenges. In 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV) (pp. 564-569). IEEE.

[17] Choi, S., Jun, C., Zhao, W., & Do Noh, S. (2015, September). Digital manufacturing in smart manufacturing systems: contribution, barriers, and future directions. In IFIP International Conference on Advances in Production Management Systems (pp. 21-29). Springer, Cham.

[18] Kamble, S., Gunasekaran, A., & Sharma, R. (2018). Analysis of the driving and dependence power of barriers to adopt industry 4.0 in Indian manufacturing industry. Computers in Industry, 101, 107-119.

[19] Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Computers & Security, 80, 211-223.

[20] Khan, A., & Turowski, K. (2016). A Perspective on Industry 4.0: From Challenges to Opportunities in Production Systems. In IoTBD (pp. 441-448).

[21] Kang, H., Lee, J., Choi, S., Kim, H., Park, J., Son, J., & Do Noh, S. (2016). Smart manufacturing: Past research, present findings, and future directions. International journal of precision engineering and manufacturing-green technology, 3(1), 111-128.

[22] Jeong, S., Na, W., Kim, J., & Cho, S. (2018). Internet of things for smart manufacturing system: Trust issues in resource allocation. IEEE Internet of Things Journal, 5(6), 4418-4427.

[23] Moktadir, M., Ali, S., Kusi-Sarpong, S., & Shaikh, M. (2018). Assessing challenges for implementing Industry 4.0: Implications for process safety and environmental protection. Process Safety and Environmental Protection, 117, 730-741.

[24] Han, G., Que, W., Jia, G., & Zhang, W. (2018). Resource-utilization-aware energy efficient server consolidation algorithm for green computing in IIOT. Journal of Network and Computer Applications, 103, 205-214.

[25] Boubiche, D., Pathan, A., Lloret, J., Zhou, H., Hong, S., Amin, S., & Feki, M. (2018). Advanced industrial wireless sensor networks and intelligent IoT. IEEE Communications Magazine, 56(2), 14-15.

[26] Al-Turjman, F., & Alturjman, S. (2018). Context-sensitive access in industrial internet of things (IIoT) healthcare applications. IEEE Transactions on Industrial Informatics, 14(6), 2736-2744.

[27] Mumtaz, S., Alsohaily, A., Pang, Z., Rayes, A., Tsang, K., & Rodriguez, J. (2017). Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. IEEE Industrial Electronics Magazine, 11(1), 28-33.

[28] Choo, K., Gritzalis, S., & Park, J. (2018). Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities. IEEE Transactions on Industrial Informatics, 14(8), 3567-3569.

[29] Bajramovic, E., Gupta, D., Guo, Y., Waedt, K., & Bajramovic, A. (2019). Security Challenges and Best Practices for IIoT. In INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik–Informatik für Gesellschaft (Workshop-Beiträge). Gesellschaft für Informatik eV.

[30] Sjödin, D., Parida, V., Leksell, M., & Petrovic, A. (2018). Smart Factory Implementation and Process Innovation: A Preliminary Maturity Model for Leveraging Digitalization in Manufacturing Moving to smart factories presents specific challenges that can be addressed through a structured approach focused on people, processes, and technologies. Research-Technology Management, 61(5), 22-31.

[31] Almanei M., Salonitis K., Tsinopoulos C. (2018) "A conceptual lean implementation framework based on change management theory", Procedia CIRP, Vol. 72, pp. 1160–1165