World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:17, No:7, 2023

Overview of Development of a Digital Platform for Building Critical Infrastructure Protection Systems in Smart Industries

Bruno Vilić Belina, Ivan Župan

***Abstract*—**Smart industry concepts and digital transformation are very popular in many industries. They develop their own digital platforms, which have an important role in innovations and transactions. The main idea of smart industry digital platforms is central data collection, industrial data integration and data usage for smart applications and services. This paper presents the development of a digital platform for building critical infrastructure protection systems in smart industries. Different service contraction modalities in Service Level Agreements (SLAs), Customer Relationship Management (CRM) relations, trends and changes in business architectures (especially process business architecture) for the purpose of developing infrastructural production and distribution networks, information infrastructure meta-models and generic processes by critical infrastructure owner demanded by critical infrastructure law, satisfying cybersecurity requirements and taking into account hybrid threats are researched.

***Keywords*—**Cybersecurity, critical infrastructure, smart industries, digital platform.

I. Introduction

MANY industries establish their digital platforms in order to implement concepts of smart industry and digital transformation. They have a role in innovations and transactions realizations [1]. They collect and analyze data from different industrial properties and devices, from tools and machines to warehouses and factories. These data are mainly available in digital ecosystems of other industries that work on complement solutions, such as industrial applications and services. Many platforms offer market positions to facilitate distribution and usage of applications in the large market of industrial consumers.

Two important roles of platforms, which make them successful are: acting as a technological base and market intermediary [2], [3]. Smart industries digital platforms use both. On the technological aspect of innovation platform, they enable creating complementary solutions from others by providing a stable core with standard interface and boundary resources from other parties [4], [5]. From the aspect of market intermediation, transaction platforms use relations between different parties, such as service providers and users, offering them a market position [6].

The main idea of smart industry digital platforms is central collection and integration of industrial data and their use in creating smart applications and services with the help of complementary industries [7], [8]. Smart industries digital platform locates in service layer of Internet of Things (IoT) or multilayer modular architecture of digital innovation [9], [10]. Hence, platform is mainly used as integration middleware [11] in terms of simultaneous provision of data storage and process capabilities of operating system for applications [12]. Under the service layer, which consists of digital platform, are located connectivity layer and device layer [13]. Device layer consists of all physical properties and objects, i.e., data acquisition sensors and actuators. The connectivity layer consists of everything required for data transfer to the platform and vice versa. In the application layer, which is located above the platform, i.e., the service layer, are developed applications that use collected data.

In this paper is presented overview of different contraction modalities in SLAs, trends and changes in business architectures (especially process business architecture) for the purpose of developing infrastructural preproduction and distribution networks, information infrastructure meta-models and generic processes by critical infrastructure owner demanded by critical infrastructure law, satisfying cybersecurity requirements and considering hybrid threats.

II. Service Level Agreement Modalities and Total Customer Relationship Management

A. Service Level Agreement

SLA is a contract between service provider and service customers, which guarantees service providing quality [14]. It is common in all domains of information technology, such as IoT, cloud computing, network and web services. The biggest challenges in IoT applications are: description of SLA terms (quality of service properties, SLA violation penalties), SLA terms monitoring and inclusion of SLA in all IoT layers.

SLA describes services delivered by provider, service provider and customer obligations and penalties in case of contract violation [15]. SLA concept is shown in Fig. 1 [16]. It ensures that the customer's quality of service (QoS) expectations are met and that each party sticks to their decisions. In case of interest conflict, SLA improves understanding of relations between each party of agreement. SLA serves the customer as a public declaration of service

B. Vilić Belina is with the University of Zagreb, Faculty of Electrical Engineering and Computing, 10 000 Zagreb, Croatia (corresponding author, phone: +385 95 9068 350; e-mail: bruno.vilic-belina@fer.hr).

I. Župan is with the University of Zagreb, Faculty of Electrical Engineering and Computing, 10 000 Zagreb, Croatia (e-mail: ivan.zupan@fer.hr).

provider what he agreed to provide. SLA serves provider as a record of what he obliged to provide to the customer [17].

There are three types of SLA [18]. Customer oriented SLA places provided services, customer's requirements and expectations in one document. In a service-oriented SLA, the service provider places services in a catalog of services, where each service has its own set of SLA criteria that do not change the user's preferences. Multi-level SLA (ML-SLA) solves problems related to the agreements! integration in a multi-layer architecture and the limitation of flexibility due to the static nature of SLA in terms of QoS and price.

Fig. 1 SLA concept

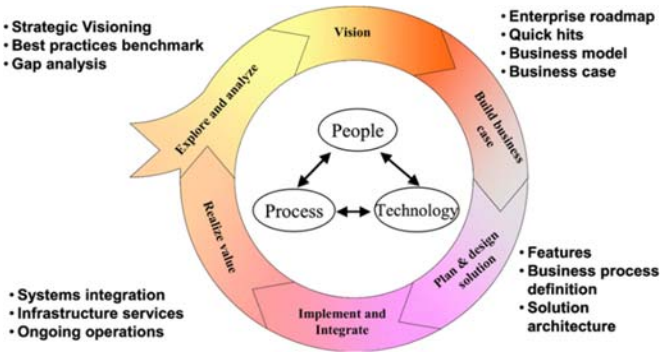

Fig. 2 CRM implementation framework

B. Customer Relationship Management

CRM system automates horizontal integration of business processes containing production (product configuration, contact management), marketing (telemarketing, campaign management) and customer service (services, call center) over multiple interconnected delivery channels [19], [20]. Many functional areas use CRM system implementation, e.g., customer support and services, sales and marketing [20]. Hahnke [21] describes the life cycle of CRM in three phases: integration, analysis and action.

The CRM life cycle starts with the integration of customer office system and centralization of customer data. It includes two related goals: providing a unique and complete view of each customer at every contact point and across all channels to the organization and employees in contact with customers and providing the user with a unique and complete view of the enterprise and its additional channels [22]. The result of this phase is a centralized source of all relevant user data, which increases efficiency and productivity of the user office [21].

The conceptual development framework of CRM is shown in Fig. 2. Research and analysis, visioning, business case building, solution planning and design, implementation, integration and value realization are six iterative processes included in typical CRM implementation [20]. The key perspectives of CRM are people, process and technology. Deliveries and services of main processes are also shown in Fig. 2.

III. Trends and Changes in Business Architectures for Development of Infrastructural Production and Distribution Networks

Business processes are fundamental in company management. Traditional software architecture is mostly applicable to unchangeable business processes. The first limitation is fixed and hidden process logic in applications, which makes it impossible to extract independent process logic. If the business process demands a change, it is necessary to reanalyze, redesign and reimplement the application software. Another limitation is difficulty in tracking the process between job requirements and system implementation. This means that there is no clear business process link between requirements and implementation [23], [24].

From an information point of view, enterprise logic can be divided into business logic and application logic [25]. Each belongs to a separate area and has its own organizational structure. In the traditional three-tier architecture, two logic systems can be integrated and are called business logic and application logic. They are located between the representation and application layer. With the need for changeable business processes, the lack of a three-tier architecture is obvious. Researchers have discovered a wide number of process-oriented architectures [26]-[28] aimed at business process reengineering or business process management, which has made techniques such as web services [29] and Enterprise Application Integration (EAI) popular [30]. These solutions are fully supported by workflow techniques and successfully separate process logic from application logic [30], [31]. Basic characteristic of workflow technique is focus on control logic of business processes, after which it manages application systems so that the business logic is self-contained.

Fig. 3 shows the business process-oriented software architecture (BPOSA) [32]. BPOSA has the following characteristics:

- Represents a service-based hierarchy and extends the traditional three-tier architecture by separating business logic from application logic.
- Separates process logic from business logic and adds an independent layer of business processes.
- Separates special enterprise business logic from application logic in business services layer.
- Has an application layer that consists of a business group program and a business object that performs a special function defined by business services.

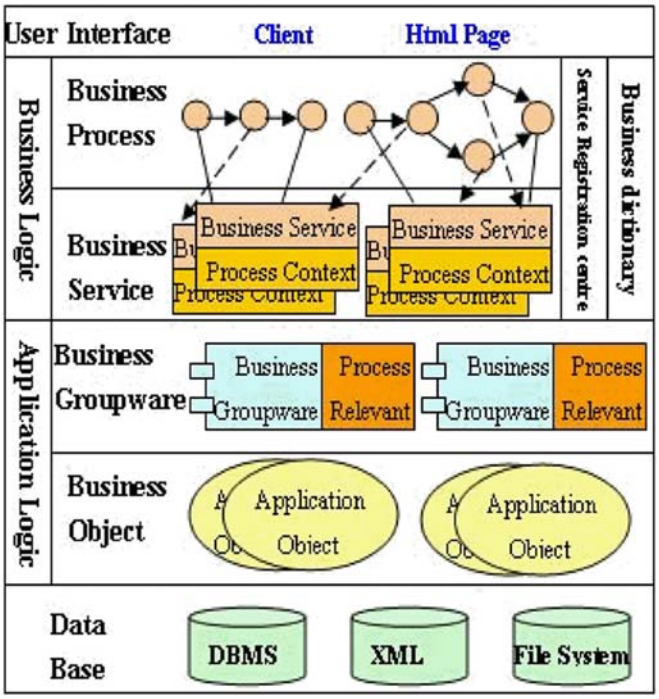

Fig. 3 BPOSA structure

Mobility as a Service (MaaS) is a popular example of new mobility systems and represents an innovative concept that has recently moved to providing door-to-door mobility services [33]. MaaS potentially improves accessibility and efficiency of transportation systems by identifying supply and demand patterns in detail. MaaS is believed to provide sustainable and user-oriented services and offers unique opportunities for gathering travel requests, smart use of existing systems, and supported or self-organizing travel services where interface automatically matches user demand with supply [34].

Many business architectures are designed to take advantage of the organizational and management structure of MaaS [35]. Business architectures are used to show different ways of distributing responsibility for business activities, e. g. production [36]. The suitability of each business architecture based on the type of services (complementary and substitute) is explained. For platforms that use mobility services, there are several types of service commission, which are defined and described in Table I and Fig. 4.

TABLE I
DEFINITION OF BUSINESS ARCHITECTURES EXPLOITING MAAS

	Description	Properties
VIa: Vertical integration of mobility services by travelers	Transport operators provide unique mobility services with an integrated distribution system, such as public transport or car rental companies. Transport operators have full control over production, supply, distribution and marketing. Vertical integration refers to the integration of the production and distribution of services in the service center of each transport operator.	Full control over distribution and marketing
VIb: Vertical integration of mobility services using a multimodal operator	The main difference is that one company provides several types of services. Distribution and marketing are integrated via transport operators that provide multiple types of services. The operator creates associations or owns other transport operators.	Full control over distribution and marketing Multiple services provided by one company
INTP: Intermediary platform	The provider of specific services as an intermediary takes over services from different transport operators, integrates them and sells them to passengers. Distribution and marketing are executed by intermediaries, not public transport operators.	No control over distribution and marketing
MSP: Multi-sided platform	Basic features enable direct interactions between members and associations from each side of the platform. Operators can remain responsible for important features of the services and delegate communication of services from user to the platform. Connecting to such a platform can be of interest to operators who want to gain access to many potential users. Travelers may also find it beneficial to connect to the platform as it reduces search and information costs for each transaction.	Partial control over distribution and marketing

IV. META-MODELS AND GENERIC PROCESSES FOR INFORMATION STRUCTURES DEMANDED BY CRITICAL INFRASTRUCTURES PROTECTION LAW

Some of the meta-models and generic processes for the information infrastructure of critical infrastructure owners required by the critical infrastructure protection law are Mobile Device Management (MDM), Reconfigurable Manufacturing System (RMS), Content Management System (CMS), Distribution Management System (DMS) and Connecting Europe Facility by Digital Signal Infrastructure (CEF DSI).

MDM systems mainly refer to the centrally supported management of a fleet of mobile devices (smartphones and tablets) and mobile applications by applying and securing predefined configuration settings [37], [38]. Gartner [39] considers MDM software as a policy tool for configuring and managing mobile devices. It also emphasizes that MDM services should guarantee the security of connectivity and transferred content. With the emergence of smart mobile devices, IoT has been on the rise in recent years and will very likely flood the market with millions of devices in coming years [40]. Zhang et al. [41] mention scalability, transparency and reliability as the main features that distinguish IoTs from classic internet. There are several IoT platforms currently available in the market, e.g., IBM Bluemix, Cumulocity, ARM mbed OS, etc. [42]. The transition raises the question of the differences and similarities between MDM and IoT device management as two different approaches [43].

RMS takes advantage of Flexible Manufacturing System (FMS) and Dedicated Manufacturing System (DMS) using computing technologies (e.g., smart sensors, autonomous robots, automated material handling and computerized machines) [44]. Today's manufacturing sector is based on the fourth industrial revolution in which many smart technologies such as IoT, cloud computing, augmented reality, simulation,

blockchain, security protection systems, big data, horizontal and vertical system integration and additive manufacturing are being developed. Use of smart technologies is a strong driver for RMS to meet the demands of the digital manufacturing world.

CMS can be applied for web system cybersecurity. Exploitation of system core vulnerabilities or functional extension components are the most common causes of successful attacks [45]. Vulnerabilities can also be found in other software running on server. Using insecure Internet protocols may compromise the integrity or confidentiality of information. Malware on a device that accesses CMS management functions may be used to compromise an administrator's confidential data. The amount of administrator knowledge in the field of information security also plays a key role. This includes complexity of password and its storage. That is why a large amount of knowledge reduces the risk of an attacker succeeding in using social engineering methods.

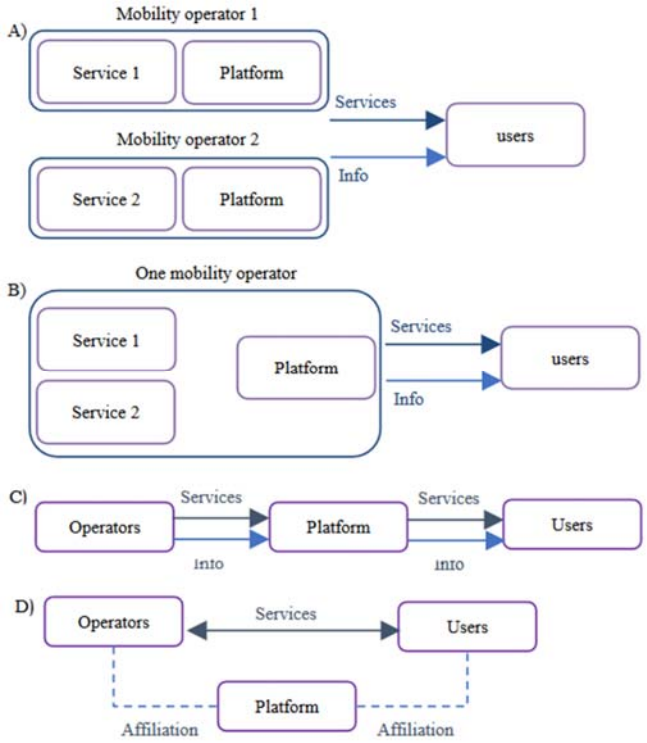

Fig. 4 Business architectures: (A) Via, (B) VIb, (C) INTP, (D) MSP

The purpose of this state is to develop methods for assessing and ensuring the cybersecurity of CMS-based web systems that allow creation of information technology to ensure cybersecurity of CMS. To achieve this, it is necessary to perform the following tasks:

1) Building an attack scenario model in the form of an attack tree. This model is based on the principle of creating a tree from the bottom up [46]. This construction uses the following scenarios: attacks with disclosure of an existing administrator password, attacks with the creation of a new administrator, attacks with authorization bridging. The main event in this tree is giving access to CMS administrator functions. Estimation of probability of the main event is possible using different types of scales [47].
2) Parameterization of the model. There are two options: a scale of fuzzy logical variables and a scale of five levels with selected indicators. It is possible to obtain estimation results in the interval [0, 1] using a numerical scale. To do this, each elementary event should be described over three realizations on a scale of 1 to 5 [46], [47].
3) Setting up a method to ensure CMS cybersecurity. The following countermeasures are assumed: use of two-factor authentication, staff training, use of HTTPS, use of VPN, protection of login and password searches, setting complex passwords and non-standard login, firewall installation and configuration. The combination of these measures is also possible. Unlike existing CMS-based web system cybersecurity provision measures [47], this method can minimize the percentage of attack success or the cost of services.
4) Development of information technology to ensure cybersecurity of CMS, shown in the form of an IDEF0-diagram in Fig. 5.

IDEF diagrams consist of the following elements:

- Rectangles showing functions (information flow processing processes) that are performed using IT application.
- Horizontal arrows showing the flow of data, specifically input and output data.
- Vertical arrows pointing from top to bottom describe control inputs.
- Bottom-up vertical arrows describing decision support tools used in IT implementation.

DMS drives Distribution Service Operator (DSO), thereby enabling real-time controlling and monitoring of distribution network, typically from the DSO's control room [48]. DSOs evaluate different smart grid solutions for Fault Location, Isolation and Service Restoration (FLISR) systems where the key issue is how to implement cybersecurity and data protection.

The fastest FLISR solutions work locally on a predefined autonomous area of distribution network as shown in Fig. 6. Local FLISR controllers are collectively authorized to perform shutdown and reclosure operations until service is restored. Only the interrupt status is returned to Supervisory Control and Data Acquisition (SCADA) system, describing the new autonomous area technology which describes the new autonomous area topology.

Since messages sent to the SCADA system are status messages, SCADA system can protect itself from local FLISR domains by accepting only status messages. This implies that this solution is less vulnerable to cyberattacks than solutions that look to DMS to change violators.

If the sensor data were managed in a local FLISR solution, wrong commands could be sent to the violators, but the problem would not spread because autonomous area only sends status to the central SCADA system.

In the case of physical topology changes affecting FLISR functionality, local FLISR solutions require manual

reconfiguration. This means that such solutions will be less dynamic.

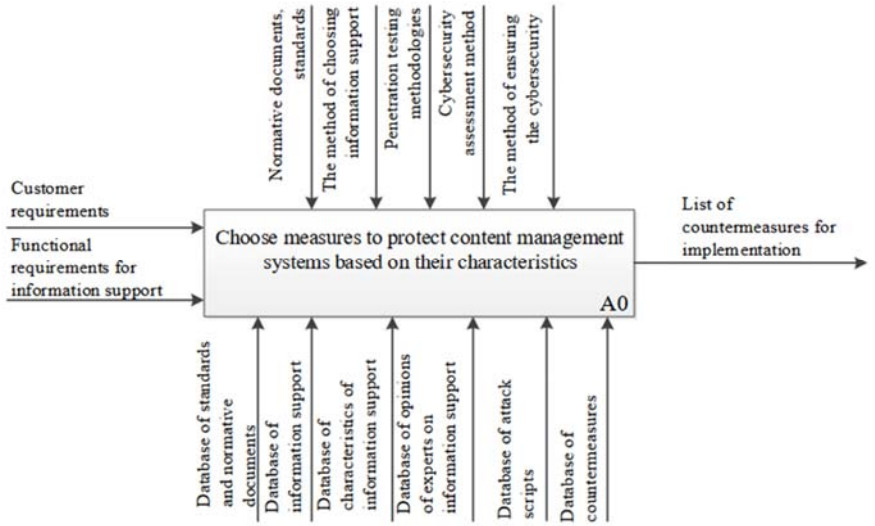

Fig. 5 IDEF0-diagram showing information technology for ensuring cybersecurity of CMS

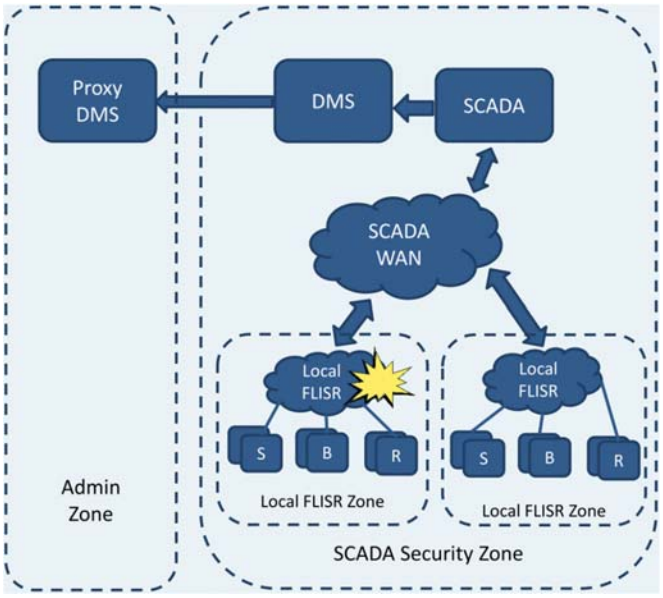

Fig. 6 Local FLISR

Centralized FLISR solution where the intelligence resides within the DMS requires DMS to actively manipulate violators in the SCADA network as the red arrow shows in Fig. 7.

Decentralized FLISR solution relies on a central analysis function located in a DMS or a dedicated system that assists the logic in the local FLISR domain to perform all steps in FLISR. If the central analysis function resides in DMS, it will introduce the same security issues as with centralized FLISR solutions. From a security point of view, there is no difference between centralized and decentralized solutions.

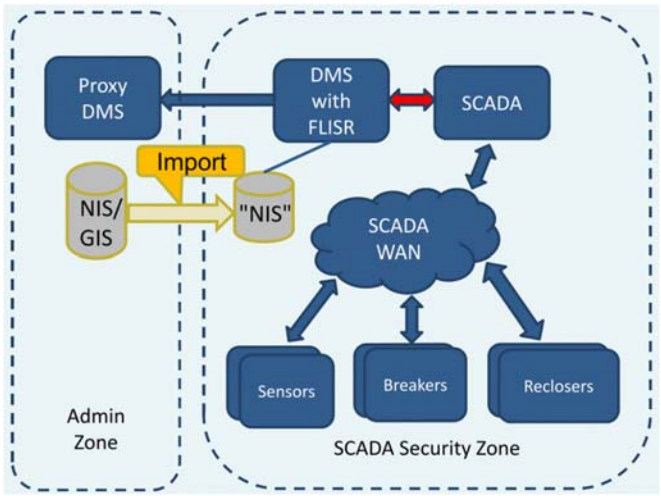

Fig. 7 DMS-based FLISR

CEF is a financial instrument that serves for additional investments in construction and improvement of the existing transport, energy and telecommunications structure. Members can finance projects from CEF in the fields of transport, energy and telecommunications.

CEF Telekom is a part of CEF and facilitates cross-border interaction between public administrations, industries and citizens by implementing DSI and broadband network [49]. CEF-funded projects help to create a European system of interoperable and interconnected digital services that support the Digital Single Market.

The goals of the CEF Telekom program are:

- Accelerating the implementation of high-speed and ultra-fast broadband networks.
- Promoting the interconnectedness of the interoperability of national online public services (measurability, percentage

of citizens and business entities using online public services, cross-border availability of services) and their access.

The European Commission annually adopts the Sectoral Annual Work Program with the aim of further development of infrastructural digital services. Digital services infrastructure provides trans-European interoperable services for citizens, businesses and/or public bodies. It consists of basic and generic services platforms. The building blocks are priority infrastructures of digital services. They are used to finance projects of basic sufficiently technically and operationally developed services.

V. Conclusion

In this paper is presented an overview of smart industries digital platform with critical infrastructure protection components. Different SLA modalities, CRM relation, trends and changes in business architectures (especially process business architectures) for development of infrastructural production and distribution networks (such as MaaS), meta-models and generic processes for informational infrastructure by critical infrastructure owners demanded by critical infrastructure protection law, satisfying cybersecurity and hybrid requests. In conclusion, digital platforms gather service contraction, customer relations improvement, modeling of business architectures and different components that contribute to cybersecurity and hybrid threats elimination.

Acknowledgment

The research presented in this paper is part of EU IRI 2 project “Development of a digital platform for Building Critical Infrastructure Protection Systems in Smart Industries – CIP 4 SI” project nr. KK.01.2.1.02.0204. funded by the European Structural and Investment Funds.

References

[1] M. Cusumano, D. Yoffie, and A. Gawer. *The future of platforms*. MIT Sloan Management Review, 2020.

[2] A. Gawer. "Bridging differing perspectives on technological platforms: Toward an integrative framework." *Research policy* 43.7 (2014): 1239-1249.

[3] M. Schreieck, M. Wiesche, and H. Krcmar. "Design and governance of platform ecosystems–key concepts and issues for future research." (2016).

[4] C. Y. Baldwin, and C. J. Woodard. "The architecture of platforms: A unified view." *Platforms, markets and innovation* 32 (2009): 19-44.

[5] A. Ghazawneh, and O. Henfridsson. "Balancing platform control and external contribution in third-party development: the boundary resources model." *Information systems journal* 23.2 (2013): 173-192.

[6] G. G. Parker, M.W. Van Alstyne, and S. P. Choudary. *Platform revolution: How networked markets are transforming the economy and how to make them work for you*. WW Norton & Company, 2016.

[7] D. Beverungen, et al. "Conceptualizing smart service systems." *Electronic Markets* 29.1 (2019): 7-18.

[8] L. Schermuly, et al. "Developing an industrial IoT platform–Trade-off between horizontal and vertical approaches." (2019).

[9] YOY. Henfridsson, and K. Lyytinen. "The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research." *Information Systems Research* 21.4 (2010): 724-735.

[10] E. Sisinni, et al. "Industrial internet of things: Challenges, opportunities, and directions." *IEEE transactions on industrial informatics* 14.11 (2018): 4724-4734.

[11] J. Guth, et al. "Comparison of IoT platform architectures: A field study based on a reference architecture." *2016 Cloudification of the Internet of Things (CIoT)*. IEEE, 2016.

[12] D. Hodapp, et al. "Business models for internet of things platforms: empirical development of a taxonomy and archetypes." (2019).

[13] T. Pauli, E. Fielt, and M. Matzner. "Digital industrial platforms." Business & Information Systems Engineering 63.2 (2021): 181-190.

[14] S. Noureddine and B. Meriem, "ML-SLA-IoT: an SLA Specification and Monitoring Framework for IoT applications," 2021 *International Conference on Information Systems and Advanced Technologies (ICISAT)*, 2021, pp. 1-12

[15] I.U. Haq, A. A. Huqqani, and E. Schikuta. "Hierarchical aggregation of service level agreements." *Data & knowledge engineering* 70.5 (2011): 435-447.

[16] B. Lee and G. Lee, "Service Oriented Architecture for SLA Management System," *The 9th International Conference on Advanced Communication Technology,* 2007, pp. 1415-1418

[17] L. Wu, and R. Buyya. "Service level agreement (SLA) in utility computing systems." *Performance and dependability in service computing: Concepts, techniques and research directions*. IGI Global, 2012. 1-25.

[18] M. K. Halili, and B. Çiço. "Towards custom tailored SLA in IaaS environment through negotiation model: An overview." *2018 7th Mediterranean Conference on Embedded Computing (MECO)*. IEEE, 2018.

[19] Jun Wu, "Customer relationship management in practice: A case study of hi-tech company from China," *2008 International Conference on Service Systems and Service Management*, 2008, pp. 1-6

[20] A. Mishra, and D. Mishra. "Customer Relationship Management: implementation process perspective." *Acta Polytechnica Hungarica* 6.4 (2009): 83-99.

[21] J. Hahnke, (2001), The Critical phase of the CRM lifecycle. Without CRM analytics, your customer won't even know you're there, www.hyperion.com

[22] J. Galimi, "Strategic analysis report: CRM IT requirements and strategies for Payer Organizations." *Gartner Group* (2000).

[23] J.K. William, T.C.T. James, "Business Process Change: A Study of Methodologies, Techniques, and Tools", *MIS Quarterly*, 1997, 21(1): 55-80

[24] G.L. Li, "Win by Process-Optimization and Reengineering of Business Process", Development Press of China, Beijing, 2005

[25] T. Erl, "SOA Conception, Technology and Design", China Machine Press, Beijing, 2007S. P. Bingulac, “On the compatibility of adaptive controllers (Published Conference Proceedings style),” in *Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory*, New York, 1994, pp. 8–16.

[26] L. Aversano, T. Bodhuin, M. Tortorella, "Assessment and Impact Analysis for Aligning Business Processes and Software Systems", *SAC* 2005: 1338-1343

[27] W.M.P. van der Aalst, A.H.M. ter Hofstede, et al," Business Process Management: A survey", *Business Process Management Proceedings*, Springer-Verlag Berlin, 2003, pp:1-12.

[28] Object Management Group, "Enterprise Collaboration Architecture (ECA) Specification", 2004

[29] K. Raman, P. Marco, R. Marco, "A Framework for Integrating Business Processes and Business Requirements", *EDOC* 2004, pp: 9-20

[30] P. Johannesson, B. Wangler, et al, "Application and Process Integration Concepts, Issues, and Research Directions". *Systems Engineering Symposium CAiSE 2000*, Springer Verlag, 2000.

[31] C.F. Strnadl, "Aligning Business and IT: The Process-Driven Architecture Model", *Computer as a Tool*, 2005. Volume: 2, pp: 1048-1051

[32] Q. Yao, J. Zhang and H. Wang, "Business Process-Oriented Software Architecture for Supporting Business Process Change," *2008 International Symposium on Electronic Commerce and Security*, 2008, pp. 690-694

[33] P. Jittrapirom, V. Caiati, A. M. Feneri, M. J. Alonso-González, S.Ebrahimigharehbaghi, and J. Narayan, “Mobility as a Service : a critical review of definitions, assessments of schemes, and key challenges,” *Urban Plan.*, vol. 2, no. 2, 2017.

[34] J. Sochor, I. C. M. Karlsson, and H. Strömberg, “Trying Out Mobility as a Service: Experiences from a Field Trial and Implications for Understanding Demand,” in 95th Annual Meeting of the *Transportation Research Board*, Washington, D.C., January 10-14, 2016., 2016.

[35] S. Ebrahimi, F. Sharmeen, and H. Meurs. "Innovative business architectures (BAs) for Mobility as a Service (MaaS)-exploration, assessment, and categorization using operational MaaS Cases." *97th annual meeting of transportation research board. Washington DC*. 2018

[36] G. Versteeg and H. Bouwman, "Business architecture: A new paradigm to relate business strategy to ICT," *Inf. Syst. Front.*, vol. 8, no. 2, pp. 91–102, 2006.
[37] D. Beimborn, and M. Palitza. "Enterprise app stores for mobile applications-development of a benefits framework." (2013).
[38] K. Ortbach, T. Brockmann, and Stefan Stieglitz. "Drivers for the adoption of mobile device management in organizations." (2014).
[39] P. Redman, J. Girard, and L.O. Wallin. "Magic quadrant for mobile device management software." *Gartner G00211101.–2011* (2011).
[40] T. Xu, J. B. Wendt, and M. Potkonjak. "Security of IoT systems: Design challenges and opportunities." *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2014.
[41] Z. K. Zhang, M. C. Y. Cho, and S. Shieh. "Emerging security threats and countermeasures in IoT." *Proceedings of the 10th ACM symposium on information, computer and communications security*. 2015.
[42] T. Takalo. "Should IoT Device Management be automated? Accessed on: 25 August, 2017." (2016).
[43] J. F. Gomes, et al. "Cybersecurity Business Models for IoT-Mobile Device Management Services in Futures Digital Hospitals." *Journal of ICT Standardization* 5.1 (2017): 107-128.
[44] A. Singh, P. Gupta, and M. Asjad. "Reconfigurable manufacturing system (rms): Accelerate towards industries 4.0." *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*. 2019.
[45] O. Morozova, et al. "Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks." *Radioelectronic and computer systems* 4 (2021): 145-156.
[46] A. Strielkina, et al. "Modeling and availability assessment of mobile healthcare IoT using tree analysis and queueing theory." *Dependable IoT for human and industry modeling, architecting, implementation* (2018): 105-126.
[47] M. Khanna, et al. "A Multi-Objective Approach for Test Suite Reduction During Testing of Web Applications: A Search-Based Approach." *International Journal of Applied Metaheuristic Computing (IJAMC)* 12.3 (2021): 81-122.
[48] M. G. Jaatun, M. E. Gaup Moe and P. E. Nordbø, "Cyber Security Considerations for Self-healing Smart Grid Networks," *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2018, pp. 1-7, 1982, p. 301
[49] https://carina.gov.hr/istaknute-teme/eu-fondovi/financijski-okvir-2014-2020/instrument-za-povezivanje-europe-connecting-europe-facility-cef/6775 - accessed 22nd July 2022.