Use of Digital-Physical Security System in a Developing Country's Port: A Case Study of Ghana

Fred Amankwah-Sarfo

Use of Digital-Physical Security System in a Developing Country's Port: A Case Study of Ghana

Fred Amankwah-Sarfo

Department of Operations and Management Information Systems, University of Ghana Business School, Ghana,
famankwah-sarfo001@st.ug.edu.gh

Abstract. The purpose of this study is to understand how the use of digital-physical security (DPS) improves port security by enabling or constraining stakeholders' goals in a developing country. Information Systems (IS) research on digital-physical security has focused more on power networks, automotive, manufacturing, and healthcare sectors. Digital-physical security (DPS) research on ports in developing countries remains limited. Therefore, port security systems as a significant IS research is yet to receive the necessary attention. To address this gap, this study employed affordance theory as the analytical lens and qualitative interpretive case study as the methodology to the investigate use of digital-physical security for a port in Ghana. The research findings show that developing countries can use digital-physical security systems to improve port security. The findings have implication for research, practice, and policy. The originality of the paper lies in its focus on how a developing country can use digital-physical systems to improve port security as a significant IS research phenomenon.

Keywords: digital-physical security system, affordance theory, interpretive case study, developing country, developing country, Ghana.

1 Introduction

The purpose of this study is to understand how the use of digital-physical security system improves port security by enabling or constraining stakeholders' goals in a developing country. The efficiency of digital-physical systems and the effectiveness of port facilities are observed phenomena [1]. Digital-physical systems are the basic information technologies, organizational structures, the related services and facilities necessary for an enterprise or industry to function [2]. Moreover, the process of embedding digital capabilities and standards in organizational practices enables new social behaviors and/or regulations [3]and involves a heterogeneous mix of people and technologies built on an installed base [4].

In IS, digital-physical system can be defined as "a shared, open (and unbounded), heterogeneous and evolving socio-technical system (which we call installed base) consisting of a set of IT capabilities and their users, operations, and design" [5] and

the relationships between organized practices [6]. Research on digital-physical security system in different countries and universities has been conducted [7] in industrial control systems [8]. In interpretive research considerable attention has been paid to the evolution of digital-physical systems in the complex interdependencies between socio-technical elements ; networks of human and nonhuman actors; and the relationship between organized practices [6]. However, little empirical research exists on how digital-physical security improves organizational security by enabling or constraining of stakeholders' goals. Following this research gap, the research question motivating this study is: how do digital physical security systems improve security in a developing country's port? In addressing this question, the study employs Gibson's [9] affordance theory as the analytical lens, and an interpretive qualitative case study approach [10] to understand how the adoption of digital-physical security system improves port security in a developing country.

The Tema Port was chosen for this research as it is considered a typical developing country port which has recently deployed a digital-physical security system. Research on digital-physical security for ports is considered a significant e-government initiative for trade facilitation. Moreover, the use of digital-physical systems can help address security lapses at the port and thus require a need for research to help address inherent challenges. Results of this effort will help inform decision makers of emerging and available digital-physical technologies to enhance and improve existing capabilities, as well as to uncover potential challenges between security needs and enabling technologies. In sum, this study advances existing knowledge by offering rich insight into how and why a developing country's use of digital-physical system foster improvement of port security.

The remaining part of the paper is structured as follows: Section 2 reviews relevant literature on digital infrastructure and port community systems. Section 3 discusses the affordance theory as the theoretical lens for the data analysis. Section 4 presents the methodology for the data collection whilst Section 5 presents the case study description. Section 6 is the case analysis based on the selected theoretical foundation. Section 7 is the discussion of findings and finally, Section 8 concludes the paper with its contribution to knowledge and recommendation for further research.

2 Digital-physical security

Digital-physical security system refers to the integration of digital and physical components using modern sensors, computing and network technologies [11]. It is noted that these systems require communication, computation and control infrastructures with several separated components for the physical and IT "world" resources such as sensors, actuators, network nodes, computers and services [12].

DPS research is gaining interest in applications in electricity generation and distribution, medical and healthcare systems [13], automotive and manufacturing sectors [7]. Substantial amount of research work on DPS also referred to as cyber-physical sys-

tems and applications of dynamic infrastructures [14] exist. However, DPSs are vulnerable to potential security threats and disruption to the physical system [15]. Moreover, research has highlighted issues in the digital-physical security of WAMPAC (Wide-Area Monitoring, Protection and Control) [16].

In relation to power networks, studies show how the integration of digital technologies in smart grids enable efficient distribution of power [17]. These may however, come with security threats as a result of new data collection, communication, and information sharing capacities in the power system along with, vulnerabilities and associated cyber-physical attacks [7]. In relation to health, research on digital physical security has focused on interoperable medical devices, networking and coordination functionalities [18].

It is noted that digital physical security solutions enable plug-n-play secure communication which has been analyzed for intrusion detection of medical devices embedded in a medical cyber physical system [19]. In addition, cyber-security tools specifically designed for manufacturing allow communication among industrial machines [20] from posing threat to ensure products conformity and maintain the safety of equipment, employees, and consumers [7]. Attacks can alter a manufacturing system, resulting in impaired communication, functionality or reduced performance.

In relation to automotive [21], the digital-physical system protects against malicious design and interaction faults to guarantee correctness and reliable operation, a computer-mediated physical distributed complex systems have a significant impact [17]. Nonetheless, research specifically focusing on digital-physical security in developing countries remains limited. This study therefore seeks to extend the existing knowledge on digital physical security in developing countries.

3 Theoretical Foundation: Affordance Theory

The concept of affordance was introduced by ecological psychologist James Gibson (1977) to account for how various users may perceive or use the same object in different ways [22]. The foundational elements of affordance are (1) object; (2) observer; (3) environment; and (4) complementary relations between these elements [23]. Based upon the concepts of affordances: (1) affordances emerge in perception from the relation between these elements; they are not ‘in’ any of these elements per se; (2) affordances refer to action possibilities, that is, what the perceiver can do with the object; (3) affordances exist independent of the perceiver’s ability to perceive it; (4) affordances exist independent of need.

‘Affordance’ refers to the perceived and actual properties of a thing, primarily those functional properties that determine just how the thing could possibly be used [24]. An affordances perspective represents a relational approach to understanding how people interact with technology [25]. The perceived affordances are the opportunities

for action that the object enables the user to carry out and may be different depending on users context, competences, and objectives [26]. A conceptual definition of affordances broadly described as possibilities for action is the "multifaceted relational structure" [27] between an object/technology and the user that enables or constrains potential behavioral outcomes in a context [28].

In IS literature, affordance has been described as emerging from the relation between IT systems and organization systems and defined as "the possibilities for goal-oriented action afforded to specified user groups by technical objects" [27]. An affordance arises from the relation between a structure or object and a goal-directed actor or actors. [29]. When the object of study is information technology, and the question relates to how the introduction of that technology affects an organization, the more focused nature of the affordance concept is useful [29]. IS scholars have explained affordance actualization as the immediate-concrete outcome. Affordance actualization is the action taken by actors as they take advantage of one or more perceived affordances through their use of technology to achieve outcomes in support of organizational goals

Affordance theory from ecological psychology has received insufficient attention to the ontological status of affordances [29]. While affordance-based IS research has largely focused on how different visual cues support the perception of affordances, or how perceptual cues can be learned as social conventions, there is still much more to be learned by understanding the affordances themselves. To address this gap, this study adopts the interpretive paradigm to research into port security systems in a developing country. The underlying research paradigm of this study is based on subjective ontology and epistemology. This helps to understand how digital-physical security can be used to improve port security systems. The use of affordance theory for digital-physical port security systems research is important as it allows the understanding of how various actors perceive and use of digital infrastructure as an important aspect to improve port security systems.

4 Research Setting and Methodology

Generally, qualitative research seeks an in-depth understanding of a research phenomenon This study's methodology was qualitative, interpretive case study [30-34, 43]. Generally, the qualitative research seeks an in-depth understanding of a research phenomenon [35] involving human and social interpretations, experiences and action. Based on a qualitative research approach, the interpretive case study in information systems seeks to understand interactions between information technologies and their social contexts.

As a result, the underlying research paradigm of this study is based on subjective ontology and epistemology on the assumption that the research phenomenon under study and the knowledge output are both socially constructed rather than objectively given [36, 37]. In line with this philosophy, this study considers interpretive case

study as suitable to understand how the use of digital-physical security system improves port security by enabling or constraining stakeholders' goals in a developing country. Data collection occurred over a period f six months, from September 2017 to March 2018. In line with the interpretive case study tradition [34], we gathered qualitative data from multiple sources, including interviews, observations and websites, field notes, and documentary materials. Interviews are one of the most important sources of case study information and are an efficient method to gather rich insights.

In line with this philosophy, this study considers interpretive case study as suitable for making sense of the digital infrastructure for port security systems. The data collection occurred in two main stages. The first was a stage of familiarization to develop an understanding of the context of the study, the technology employed, and the actors involved. This was achieved by observing meetings, demonstration sessions, tests and training sessions to build an understanding of the digital infrastructure for the port security systems.

The interview guide was semi-structured [38] and lasted between 30 minutes and 1 hour. Some of the interview sessions were audio recorded, subject to the informed consent of the interviewee. Interviews were subsequently transcribed for more detailed analysis. Initial data analysis occurred alongside data collection [39] and based on Hermeneutics cycle. In line with interpretive tradition, data analysis took place concurrently with the data collection [34],The data analysis was aided by affordance theory concepts of enabling affordance and constraining affordance to analyze the case findings.

5 Case Description

This study was conducted in Tema Port. The port is located in the south eastern part of Ghana, along with the Gulf of Guinea. The port serves both as a loading and unloading port for goods and a major transit point for land-locked countries to the north of Ghana. The port receives an average of 1,650 vessel calls per year. Stretching over 3.9 million square meters of land area, a high level of security is a major priority. This means that certain areas of the port can be inaccessible all the time as far as patrolling is concerned and therefore could lead to stealing of cargo from the cargo containers. It could also be prone to smuggling of weapons and arsenal into the country and issues of stowage and illegal immigration. The digital port security system which was put in place helps to provide multiple solutions.

5.2 Port Security

As a major entry point to countries, seaports are targets for unauthorized activities such as sabotage, terrorist threats, piracy, cargo theft, and smuggling. It is vital that ports are given security infrastructure and surveillance strategies and technologies that limit illegal activities and minimize threats and facilitate trade as well as enhance the

ability to assess cargo for risk, examine high-risk shipments at the earliest possible point, and increase the security of the supply chain.

Port security is the defense, laws and treaty enforcement, and counterterrorism activities that fall within the port and maritime domain. It includes the protection of the seaports themselves, the protection and inspection of the cargo moving through the ports, and maritime security. The port security manager observed:

Our security is made of systems that work together to combat unlawful activities. The systems comprise an interrelated part to achieve a goal. For security to thrive, various systems must work to complement each other. These are electronic, personnel, procedures and physical barriers.

These systems are mutually re-enforcing and interdependent meaning where one falls short, the other should complement. Whenever a breach of security occurs, the electronic system gives the earliest possible warning, the human being gives the quickest possible response, procedures give the fairest possible control and the physical barriers give the longest possible delay for a security breach to occur.
The deputy port security manager stated:

The possible threat of terrorist attacks and the increasingly sophisticated activities of organized criminal gangs have heightened the focus on electronic security. The result is increasing requirements for these high security and mission critical systems to be continuously available with no downtime.

The electronic security system at the Tema Port has an underlying technology infrastructure with following capabilities: virtualization-ready with a wide range of support for different applications; continuous availability of technologies is critical and consolidated to a shared set of server resources, unplanned downtime is not an option. There are many ways to mitigate the risk of unplanned downtime, with a high available or fault-tolerant solution which is easy to deploy and easy to service in the event of a failure.

One of the most difficult challenges in operating a digital physical security system is understanding and resolving operational issues. Digital technology greatly reduces the complexity of systems. This means that an end-to-end view of the entire security system (devices, applications, and hardware) decrease the challenges of identifying and even preventing issues before occurring. The deputy port security manager explained that:

Port security is a part of the maritime security which comes under International Maritime Organization (IMO) and the International Ship and Port Facility Security Code introduced in the year 2002 as a part of the Safety of Life at Sea (SOLAS) convention. Apart from these two organizations, a lot of port security measures are incorporated from the United Nation's own marine security enforcement agenda.

In line with the international ship and port security (ISPS) code, Tema Port has high security measures to prevent acts of terrorism and other security threats. An electronic gating system and security surveillance optical character recognition cameras, as well as CCTV's, have been installed. The head of port security explained:
All these have created a haven in our navigational waters and port operational areas giving shippers a great sense of security. Major Security Initiatives by the Ghana Ports and Harbours Authority, Electronic Gate Systems, ISPS, and Maritime Security (MARSEC) level 1 compliance in both commercial ports.

The new Meridian Port Services terminal is designed to run automated and semi-automated processes, enabled by digital technologies at the various stages of the terminal operations, to facilitate and save valuable time, a secure online portal enables initial registration of customers. The online portal is used to make appointments through the "Truck Appointment System" (TAS) for visit to the MPS Terminal at their convenience. Each customer has access to a dashboard containing personal information and available containers.

The Truck Appointment System and online portal are opened 24 hours a day, 7 days a week and avoid waiting times compared to a manual process. The TAS communicate in real-time with a centralized and high-available Digital Terminal Operating System (DTOS) to retrieve and validate all data. An importer reiterated:

Once an appointment is confirmed your registered truck driver is welcomed at our MPS Terminal and allowed to enter based upon biometric fingerprint validation. Using this advanced technology in the early stage of your visit allows MPS Terminal and Tema Port to grant access only to those truck drivers who are registered and authorized.

This ensures that visitors, staff, facility, and cargo is kept safe and is fully compliant with The International Ship and Port Facility Security (ISPS) code. Besides performing identity checks, this biometric validation is used in parallel to confirm the validity of appointment through the Digital Truck Appointment System (DTAS). This will avoid traffic congestion and waiting times. When trucks enter the port premises an automated workflow is initiated. Automated access portals read the truck license plate using the License Plate Recognition (LPR). In addition to the LPR, each truck is identified through a unique and tamper proof identification sticker based upon RFID technology.
A terminal operator stated:

> *The automated portals are equipped Digital Optical Recognition Cameras to recognize: Container Number; IMO Hazard Codes; Number of Containers loaded; Presence of seals; IMDG Classification.*

All data is captured and verified in real time when the truck drives through the automated portals, without stopping, towards the Terminal gates. By the time the truck reached the Terminal gates, all captured data is processed, and the weight is taken

through automated weighbridges. The truck is automatically identified through RFID and can proceed to its destination at the container yard. Soon as the truck driver is on its way to his destination in the yard the eRTG operator will be automatically informed through the digital terminal operating system, upon arrival the visiting truck will be served by the operator. An officer at the CCTV central control room stated that:

The electronic gate is used to control access to the restricted areas of the port. All vehicles (personal and truck) entering the restricted area must be screened before access is granted. Using cameras, proximity readers, magnetic-stripe readers, biometrics, OCR readers, cameras, and microphones all vehicles and persons are screened, and equipment information are captured and stored.

All port users must have an identification card, a valid visitor card, or a valid driver's license to enter the restricted area. The visitor will present a form of ID to one of the devices and then authentication of said ID is done; providing all requirements to allow entry is complete access is granted. If access is granted, a gate pass is issued for the individual(s) inside the vehicle. A gate pass for trucks is a paper printout of the time, date, name of the driver, and list of equipment brought into the restricted area. For cars, an electronic gate pass is created capturing similar information. This system also allows trucking companies to review their gate transaction logs and balances via the internet.

6 Case Analysis

In this section, the concepts of affordance theory are used for the case analysis. Digitalization denotes a complex transformation, where the physical and the digital are entwined and configured in new ways. From the case description, the port security system is the digital infrastructure that enables truckers, terminal operators and security personnel to use a digital port security system from the relationship between these goal-oriented actors.

The concepts of affordance were used to explain digital port security processes. The key principles of affordance theory are enabling and constraining affordances. The concepts of affordance are a technical object (digital technology), actor groups, and their goals were used to analyze the case findings.

6.1 Enabling Affordance of Digital Port Security System

From the case description, the digital infrastructure for the port security system enables port stakeholders to achieve intended goals. Table 1 shows a summary of the enabling affordance of the digital port security system. The next section detail how digital port security system enables truckers, security personnel and terminal operators achieve the goals. The electronic gate system enables control access to the restricted areas of the port by ensuring that visitors to the port have pre-authorized

clearance from the port security office. Truck drivers use the digital truck appointment system to book appointment to specific parts of the port to load/off load cargo.

Port security personnel use the digital optical recognition cameras to identify authorized users of the port and CCTVs allow port authorities to monitor in real time critical positions within the port. The footages of the CCTV are transmitted via the intranet to a central monitoring room for monitoring and analysis. The e-gate and CCTV are embedded with digital transmission chips and together with the network connectivity, hardware and storage devices constitute the digital-physical security system.

Table 1: Enabling Affordance of Digital Infrastructure for Port Security System

Affordance	**Digital technology**	**Actors**
access control	electronic gate systems	port users *goal: authorized access*
booking	digital truck appointment system	truck operators *goal: schedule appointment*
identification	digital optical recognition cameras	security personnel *goal: authorization*
surveillance	CCTV	Port authority *goal: real time recording*

6.2 Constraining affordance of digital Infrastructure for port security system

The constraining affordances are an unauthorized access smuggling. Table 2 is a summary of the constrains of the digital port security system.

The electronic gate prevents unauthorized persons from accessing the port facility. This is achieved by authorized card holder slotting digital card at the point of entry. The 3 D scanners constrain smuggling of illegal items by importers who may want to outwit port authorities from detecting such goods. The goal of pilfers is to have unauthorized access into the electronic gating (E-Gate) system that allows only biometrically verified persons into the port space. The e-gate, therefore, serves as a constrain against pilfering.

Table 2: Constraints of Digital Infrastructure for Port Security System

Constraints	**Digital technology**	**Actors**
unauthorized access	electronic gate systems	unauthorized persons *goal: pilfering*
smuggling	3D scanners	security personnel *goal: smuggling*

7 Discussion

The section discusses how the research question is answered using affordance as the theoretical lens. It is important to state that the digital port security system is a technical object with component parts [40]. In line with the research question of how the use of digital-physical security system for the port security enabled or constrained stakeholders' goals as shown in table 1 and table 2 above. The study sought to achieve this by examining the literature on digital-physical security systems and conducting empirical research at Ghana's Tema port.

From the case study, the port security system is conceptualized as a digital-physical security system which enables interactions between stakeholders to achieve goals [41] whilst restricting unauthorized activities [42]. The interactions between these actors and the digital-physical security system identified in the case study raise interesting issues for discussion, however, based on the research question and the affordance theory, the affordance, and constraints for the port security system a developing country are discussed.

This study has sought to achieve this by explaining affordance and constrains resulting from the digital port security system and its stakeholders. The research findings show that developing countries can use port security to enable (1) access control (2) booking (3) identification and (4) surveillance. Whilst the port security system also prevents unauthorized access and smuggling. To obtain authorized access to the port, temper-proof biometric identity card at the office of the port security is issued to authorized users. Hence on arrival at the gate, the truck driver showed the card to the electronic gate sensor for the gates to be automatically open.

8 Conclusion

The purpose of this study was to understand how the use of digital-physical system improves port security by enabling or constraining stakeholders' goals in a developing country. The paper's originality lies in its affordance theory-based explanation of how digital-physical security improves to port security. The improved outcomes are a result of digital-physical security enabling or constraining stakeholders' goals. The findings have implications for research, practice, and policy. For research, affordance theory is considered useful for studying digital infrastructure phenomena involving heterogeneous actor groups. For practice, digital infrastructure can significantly help streamline port security systems. For policy, port digital infrastructure can help improve the efficiency of port security. The study is limited as a single case study in one developing country. However, from an interpretive perspective, the findings are ap-

plicable to other countries with similar settings. Future research can focus on digital infrastructure for export.

References

1. Vaio, A. Di, Varriale, L.: AIS and Reporting in the Port Community Systems : An Italian Case Study in the Landlord Port Model. In: Reshaping Accounting and Management Control Systems. pp 153–165 (2017)
2. Tilson, D., Lyytinen, K., Sørensen, C.: Digital infrastructures: The Missing IS Research Agenda. Inf. Syst. Res. 21, 748–759 (2010). 3. Edwards, P.N., Jackson, S.J., Bowker, G.C., Knobel, C.P.: Understanding infrastructure: Dynamics, tensions, and design. (2007)
4. Bygstad, B., Hanseth, O., Siebenherz, A., Ovrelid, E.: Process innovation meets digital infrastructure in a high-tech hospital. Proc. Eur. Conf. Inf. Syst. 2017, 1–14 (2017)
5. Hanseth, O., Lyytinen, K.: Design theory for dynamic complexity in information infrastructures: the case of building internet. J. Inf. Technol. 25, 1–19 (2010)
6. Star, S.L., Ruhleder, K.: Steps toward an ecology of infrastructure: Design and access for large information spaces. Inf. Syst. Res. 1, (1996)
7. Lu, T., Zhao, J., Zhao, L., Li, Y., Zhang, X.: Towards a framework for assuring cyber physical system security. Int. J. Secur. its Appl. 9, 25–40 (2015). 8. Syed, D., Chang, T.-H., Svetinovic, D., Rahwan, T., Aung, Z.: Security for Complex Cyber-Physical and Industrial Control Systems: Current Trends, Limitations, and Challenges. In: Pacific Asia Conference on Information Systems (2017)
9. Burrell, M.: Burrell and Morgan ' s. Sociol. J. Br. Sociol. Assoc. 3, 380–381 (1979)
10. Walsham, G.: Doing interpretive research. Eur. J. Inf. Syst. 15, 320–330 (2006).
11. Zeadally, S., Jabeur, N.: Cyber-Physical System Design with Sensor Networking Technologies. Institution of Engineering and Technology (2016)
12. Teslya, N., Smirnov, A., Levashova, T., Shilov, N.: Ontology for resource self-organisation in cyber-physical-social systems. In: International Conference on Knowledge Engineering and the Semantic Web. pp 184–195. Springer (2014)
13. Kim, K.-D., Kumar, P.R.: An overview and some challenges in cyber-physical systems. J. Indian Inst. Sci. 93, 341–352 (2013)
14. Sandkuhl, K.: Feature Models as Support for Business Model Implementation of Cyber-Physical Systems. Int. Conf. Inf. Syst. Dev. (2018)
15. Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A.: Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges. Neurocomputing. 338, 101–115 (2019). 16. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L.: Cyber-physical systems and their security

issues. Comput. Ind. 100, 212–223 (2018). doi:10.1016/j.compind.2018.04.017
17. El, Z., Kaabouch, N., El, H., El, H.: Cyber-security in smart grid : Survey and challenges. Comput. Electr. Eng. 67, 469–482 (2018).
18. Venkatasubramanian, K.K., Vasserman, E.Y., Sokolsky, O., Lee, I.: Security and interoperable-medical-device systems, part 1. IEEE Secur. Priv. 10, 61–63 (2012)
19. Mitchell, R., Chen, R.: Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. IEEE Trans. Dependable Secur. Comput. 12, 16–30 (2015)
20. Wells, L.J., Camelio, J.A., Williams, C.B., White, J.: Cyber-physical security challenges in manufacturing systems. Manuf. Lett. 2, 74–77 (2014)
21. Wasicek, A., Derler, P., Lee, E.A.: Aspect-oriented modeling of attacks in automotive cyber-physical systems. In: 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC). pp 1–6. IEEE (2014)
22. Fayard, A.-L., Weeks, J.: Affordances for practice. Inf. Organ. 24, 236–249 (2014)
23. Burlamaqui, L., Dong, A.: The Use and Misuse of the Concept of Affordance. Des. Comput. Cogn. DCC. 7–12 (2014). doi:10.1007/978-3-319-14956-1_17
24. Salomon, G.: Distributed cognitions: Psychological and educational considerations. Cambridge University Press (1997)
25. Treem, J.W., Leonardi, P.M.: Social Media Use in Organizations: Exploring the Affordances of Visibility, Editability, Persistence, and Association. 8985, (2016).
26. Vaast, E.: Social media affordances and governance in the workplace : An examination of organizational. J. Comput. Commun. 19, 78–101 (2013). doi:10.1111/jcc4.12032
27. Faraj, S., Azad, B.: The materiality of technology: An affordance perspective. Mater. Organ. Soc. Interact. a Technol. world. 237, 258 (2012)
28. Evans, S.K., Pearce, K.E., Vitak, J., Treem, J.W.: Explicating Affordances: A Conceptual Framework for Understanding Affordances in Communication Research. J. Comput. Commun. 22, 35–52 (2017). doi:10.1111/jcc4.12180
29. Volkoff, O., Strong, D.M.: Critical Realism And Affordances : Theorizing It-Associated Organizational Change Processes1. MIS Q. 37, 819–834 (2013)
30. Iivari, J., Hirscheim, R., Klein, K.H.: Beyond Methodologies: Keeping up with Information Systems Development Approaches through Dynamic Classification. In: Proceedings of the 32nd Hawaii International Conference on System Sciences, IEEE (1999)
31. Walsham, G.: Interpretive case studies in IS research: nature and method. Eur. J. Inf. Syst. 4, 74–81 (1995)
32. Myers, M.., Klein, H.K.: A Set of Principles for Conducting Critical Research in Information Systems. MIS Q. 35, 17–36 (2011). doi:10.2307/249410
33. Walsham, G.: Interpretive case studies in IS research: nature and method. Eur. J. Inf. Syst. 4, 74–81 (1995).
34. Walsham, G.: Doing interpretive research. Eur. J. Inf. Syst. 15, 320–330 (2006). doi:10.1057/palgrave.ejis.3000589

35. Miles, M.B., Huberman, A.M., Saldana, J.: Qualitative Data Analysis. A Methods Sourcebook. (2016)
36. Myers, M..: Qualitative Research in Business and Management. Sage (2013)
37. Orlikowski, W.J., Baroudi, J.J.: Studying Information Tech- nology in Organizations: Research Approaches and Assump- tions. Inf. Syst. Res. 2, 1–28 (1991)
38. Myers, M.., Newman, M.: The qualitative interview in IS research : Examining the craft. 17, 2–26 (2007).
39. Walsham, G.: Doing interpretive research. Eur. J. Inf. Syst. 15, 320–330 (2006)
40. Glowalla, P., Rosenkranz, C., Sunyaev, A.: Evolution of IT Use: A Case of Business Intelligence System Transition. Icis. 1–19 (2014)
41. Leonardi, P.M.: When does technology use enable network change in organizations? A comparative study of feature use and shared affordances. MIS Q. 749–775 (2013)
42. Dini, A.A., Wahid, F., Sæbo, Ø.: Affordances and constraints of social media use in eParticipation: perspectives from Indonesian politicians. (2016)
43. Choudrie, J, & Dwivedi, Y.K. "Investigating the research approaches for examining technology adoption issues." Journal of Research Practice 1.1 (2005): 1, available at http://jrp.icaap.org/index.php/jrp/article/viewFile/4/7.