Bank Branches as Smart Environments: Introducing a Cognitive Protection System to Manage Security and Safety

Salvatore Ammirato, Francesco Sofo, Alberto Michele Felicetti, Cinzia Raso

▶ **To cite this version:**

Salvatore Ammirato, Francesco Sofo, Alberto Michele Felicetti, Cinzia Raso. Bank Branches as Smart Environments: Introducing a Cognitive Protection System to Manage Security and Safety. 19th Working Conference on Virtual Enterprises (PRO-VE), Sep 2018, Cardiff, United Kingdom. pp.61-73, 10.1007/978-3-319-99127-6_6 . hal-02191178

HAL Id: hal-02191178

https://inria.hal.science/hal-02191178v1

Submitted on 23 Jul 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Bank Branches as Smart Environments: Introducing a Cognitive Protection System to Manage Security and Safety

Salvatore Ammirato[1], Francesco Sofo[2], Alberto Michele Felicetti[1], Cinzia Raso[1]

[1] Department of Mechanical Energy and Management Engineering, University of Calabria, Via P.Bucci, 87036 Rende (CS), Italy
{salvatore.ammirato. alberto.felicetti, cinzia.raso}@unical.it
[2] Faculty of Education, University of Canberra, ACT 2601, Australia.
{francesco.sofo}@canberra.edu.au

Abstract. Protection of Bank Branches (BBs) represents an interesting setting where potential benefits deriving from the introduction of IoT technologies can give best results in terms of operational performances. In this paper we present main results of an ERFD funded project aimed to redesign BBs as smart environments. First, we summarize main results of a multiple case study among Italian banking groups aimed to characterize the problem. Second, we propose main characteristics of a *cyber-physical-social space (CPSS)* specifically designed to facilitate the rise of a *smart BB.* Third, we introduce the architecture of a *cognitive protection system* designed to manage a network of BB CPSSs belonging to a banking group in order to improve both the degree of security and safety inside the branch environment, and the operational performances of security management processes.

Keywords: Internet of Things; Intelligent Protection System; Cyber-Physical-Social Space; cyber-physical security; case study.

1 Introduction

Over recent years, the "Internet of Things" (IoT) concept is gaining more and more popularity. Since Ashton first introduced this term in 1999, dealing with the introduction of RFiD sensors in supply chain management [1], the concept has been evolving representing a new paradigm in which the Internet extends into the real world embracing everyday objects [2].

At the core of the IoT there are the *smart objects* (SOs), which are physical things enhanced by electronic devices providing them with local intelligence and connectivity to the cyberspace [3]. Local intelligence means that SOs are able to sense/log/interpret what's occurring within the surrounding environment. SOs are building blocks for a *smart environment* where different kinds of SOs continuously work to make human interactions more comfortable and safer [4]. New research

directions argue that sensing and connection is not enough: SOs should have the capability to learn, think, and understand both physical and social worlds [5]. This emerging need to empower IoT with a "brain" for a higher level of intelligence leads to a new paradigm named *Cognitive Internet of Things* [5]. Cognition refers to the ability to be aware of the environment and the human interactions, be able to learn from the past actions and use it to make future decisions that benefit the network [6]. Thus a *cognitive information system* is able to modify its behaviour on the basis of experience, data analysis and interaction of smart and not SOs. This approach challenges the way networks and systems are designed and operate with humans. Current industrial trends and initiatives aim to "connect the unconnected", changing the way people and companies act every day in many key sectors, such as communications, health care, finance, education, transportation, manufacturing and agriculture [7]. An area that is becoming "a domain of major economic and social interest for the introduction of IoT" is the security domain [8]. Security of is a cutting edge issue gaining growing attention in recent years. Today, millions of connected devices are used to enhance protection levels of many types of infrastructures under the IoT paradigm [9].

Bank Branches (BBs) represent an interesting setting where potential benefits deriving from the introduction of IoT technologies can be best exploited. In fact, a BB can be seen as a worksite where humans interact among them and smart objects to carry out multiple banking activities (operational, economic and financial). The presence of such characteristics enables, in principle, the shaping of a BB as a smart environment and its devices controlled by a cognitive information system. Unfortunately, the lack of sensible efforts in improving the BB protection system represents the main hindrance to a full transformation of a BB in a smart environment [10].

This paper reports results from the BaSS (Bank Security and Safety) project, funded under the EU ERFD program, which was aimed to support banking groups to design a *Cognitive Information System* able to improve:

- the degree of security and safety inside the branch environment
- the operational performances of security management processes

2 Theoretical Background

2.1 The BB Security Context

Bank branches are physical spaces that, traditionally, represent the contact points between banks and their customers. Even if the growth of on-line banking is an undoubtable trend, consumers being still more likely to use on-line channels for basic operations continuing to rely on bank branches for more complex financial transactions [11]. Money transactions are moving from bank counter to remote controlled platforms which are accessible via web (Internet/mobile banking) or placed close to the branch (ATMs) [12]. At the same time, the branch's physical layout is changing. Traditional "hard" security measures as visible security cameras, armour windows and metal detectors are going to be removed from customers' sight.

Although such measures are important to give protection to structures and people, they can generate a bad feeling of impending danger that can persuade customers to avoid entering in the branch or to stay within the branch the shortest possible time. It is evident that the aim to reduce the sense of anxiety in customers, is in contrast with the need to guarantee protection of people and properties against criminal attacks.

A criminal attack can be viewed as a sequence of actions happening in an interaction space, with the aim to obtain an unfair benefit and/or damage people or organizations [13]. The following table describes the categories of illegal actions (or *threats*) against BBs.

Table 1. Threats against BBs.

Threat	Description
T_1: Robbery	stealing from a bank while bank employees and customers are subjected to force, violence, or the threat of violence, putting the victim in fear.
T_2: Theft	the illegal taking of another's property.
T_3: Fraud	is the use of potentially illegal means to obtain money, assets, or other property owned or held by a bank institution.
T_4: Damage	intentional or unintentional harm to somebody's property.

FBI and EBF reports agree that criminal attacks against BBs are a problem that continues to take a toll on financial institutions and communities across the U.S. and Europe [14] [15]. Indeed, the growing number of attacks and their high rate of success prove that current protection measures are still not so efficacy and overall protection systems are far from the global security concept.

The occurrence of terroristic and criminal attacks at the international level, emphasized the role of security and strengthened the importance to monitor and control critical.

To improve degree of security and safety of people and goods inside a space an effective protection system is required. Conrath [16] defined protection as the set of measures that prevent or deter attackers from accessing to physical and logical resources and guidelines on how to design structures to withstand hostile acts. While in the past the emphasis was primarily addressed to the security of physical assets, today, businesses and public institution of all sizes and industries perceive a growing need to protect people and intangible assets, to preserve the continuity of their business processes. In this sense, new approaches in designing protection systems need to combine the security needs with those of operational freedom.

2.2 Smart Environment as Cyber-Physical-Social Systems

SOs are able to detect and interpret what is occurring in the surrounding environment (through an embedded sensor), interacting with other SOs, exchanging information with people and perform one or more actions through an actuator [17]. The integration of SOs within physical processes, by means of computation and networking features, shapes the so-called "cyber-physical system" (CPS) [18]. A CPS, which represents the technological layer of a smart environment, is able to

acquire and apply knowledge to offer context-based services to the environment [19]. A CPS integrates two main aspects:

- a cyberspace, that refers to the generalized information resources, including virtual and digital abstractions to achieve interconnections among cyber entities;
- and a physical space, that refers to the real world, in which physical objects are respectively perceived and controlled by sensors and actuators to establish interactions via the communication channels, remote collaboration, real-time localization, and autonomy maintenance [20].

Two main functional elements characterize a CPS [21]:

- Advanced connectivity ensuring real-time data acquisition from the physical world and information from the cyber space;
- intelligent data management, analytics and computational capability that construct the cyberspace

Basing on the CPS paradigm, applications have been developed to assist people activities in many domains which become smart environments: transportation and logistics [21], smart buildings [22], smart health [23], etc.

New approaches tend to consider human factors as an integrant part of the CPS instead of placing them outside its boundaries. In this sense, many authors proposed the concept of Cyber-Physical-Social System (CPSS) [24] [25]. CPSS extends the concept of CPS, including the so-called "social space" domain, featuring human participation and interaction among humans as well as human-computer interaction. Hence, it is possible to characterize a CPSS as comprising the following components:

- Social Space (SS): the human space containing human actors, relationships and user's interconnected device (Internet of People – IoP)
- Cyberspace (CS): the software based systems and the underlying infrastructures and platforms providing services to the users (Internet of Services – IoS)
- Physical Space (PS): the physical world of interconnected SOs, including sensors, actuators and gateways (Internet of Object – IoO).

When coupled, the above-mentioned components led to the definition of the following subsystems characterizing a CPSS:

- Human Computer Interaction (HCI): The human is not just an operator in a smart environment, but he/she continuously interact with SOs/devices to get mobiquitous services.
- Cyber social space (CSS): virtual worlds, social networks and internet based services allowing synchronous and asynchronous relationship among humans.
- Cyber Physical Space (CPS): integration of software based systems, platforms, networking infrastructures and interconnected SOs and devices providing context based services.

As stated in [25], CPSS appears to be an advanced version of the IoT paradigm where social attributes are considered to address the integration of computation, networking and physical processes aching the interfusion of the cyber–physical space and social space.

From an operational point of view, the design of a CPSS can benefit of the recent advances in mechatronics which led to a new generation of multipurpose sensors, known as *indirect or synthetic sensors* [26]. According this approach, single physical sensor can detect different characteristics from the same signal, instead of requiring

the use of many sensors. The ultimate embodiment of this approach would be a single general-purpose sensor able to digitize an entire building. This kind of sensors can be attached to a variety of objects, and without modification, sense many facets [27][28]. Synthetic sensors overcome traditional limitations of limited sensing functionality, limited large scale interoperability and failure to provide complex interpretations of implicit assumptions [29].

3 Methodology

With the aim "*to develop technology-based solutions to important and relevant business problems*", the present study follows the design research paradigm proposed in [30]. As stated in [31], a design science research process can be summarized on the following three steps: problem identification, solution design and validation.

The first step was aimed to highlight characteristics and weaknesses of the protection systems currently adopted by banking groups to protect security and safety of their branches. The framework methodology we have used at this step is based on a multi-methodological development approach that include a systematic literature research and review and interviews with experts. Literature review was intended to create a complete understanding of the BB security domain and IoT field of study. Moreover, we performed semi-structured interviews with a sample of convenience of six respondents who were working for primary Italian banking groups as security managers at the time of the study. The data gathering for the case study has been carried out in Italy during the last three months of 2016. The interviews were based on pre-defined open questions dealing with organizational and technological characteristics of the current protection systems. The second step of the methodology was aimed to propose an architecture for a *cognitive protection system* for BBs able to manage protection through a redesign of the BBs. In particular, we introduce a logical model of BB under a CPSS perspective and the architecture the architecture of the *Intelligent Protection System – IPS,* a cognitive platform designed to manage BB security. Third step consisted in testing activities in order to experiment it inside a BB context.

4 The Italian BB Case Study

4.1 The BB Protection Systems

Measures to protect the BB environment can be classified according to the desired effect to a criminal attack: prevention and reaction.

Prevention measures are static measures intended to prevent/obstacle harms to bank assets discouraging the potential criminals by doing the attack. Three typologies belong to this category: traditional "hard" measures (structural measures such as armour windows, armed guards, armour-plated doors, time lock doors); "soft" or psychological measures (i.e: transparent glasses or display panels which gives

information about the presence of security controls, etc.), and "technological" measures used to identify and enable/hinder people entering BB environment or interacting with ATMs, (e.g., secure ID generator, credit card; biometric data) [16].

Reaction measures require the activation (automatic or human driven) of a countermeasure further to a risky event (i.e.: sound alarm, systems for tracing money, emergency calls to law-enforcement, etc.) [32]. Traditional ways to recognize suspect behaviours comes from perimetric/volumetric sensors and from two "analogic" systems that continuously monitor the environment: the armed guards and video-surveillance system. In both cases humans, directly (the armed guards) or indirectly (the security guard looking at the video streaming from the control room) present on the scene are charged to pay attention to suspect behaviours of people who could attack the BB.

Unfortunately, interviews agreed that security measures are characterized by low efficacy and by outdated and stand-alone mechanisms. Traditional "hard" security measures clash with commercial purposes of BBs. Protection measures currently adopted cannot constantly monitor the environment properly: traditional camera surveillance systems are characterized by low effectiveness due to the tiredness and the alienation of operators because of the repetitive nature of the job. Moreover, protection measures are incapable of retaining, storing and communicating data about their state in order to examine the contexts of BB. If available, contextual information could be used to support and enhance the ability to execute specific countermeasures by providing information and services tailored to the security needs.

4.2 Towards a New Concept of BBs as CPSSs

As emerges from interviews, the growing interest of criminals in attacking BB is directly related to the persistent use of obsolete security technologies that, moreover, are a source of organizational inefficiencies, high costs and are characterized by long reaction times and scarce level of effectiveness.

The transformation of a BB in a smart environment can allow, in principle, to overcome these critical issues, improving security process performances and effectiveness against criminal attacks. In the following sections we summarize main characteristics of a CPSS specifically designed to facilitate the rise of a *smart BB*. In the so-called *BB CPSS*, protection measures, both smart and non-SOs, are capable of interacting among them and with humans through a digital network, to improve the BB security and safety management. Inside the BB CPSS, the cyber domains of communication and computing are combined with the dynamics of physical objects and their interaction with human actors proper of a BB setting [19]. After, we introduce the architecture of the *IPS - Intelligent Protection System* – which is the cognitive protection system designed to manage a network of BB CPSSs belonging to a banking group in order to improve both the degree of security and safety inside the branch environment, and the operational performances of security management processes.

4.2.1 The Logical Model of a BB CPSS

Each BB environment is characterized by the presence of a set of context entities, intended as physical or conceptual objects which interact among them [33]. According to Ning's view [25], it is possible to identify the subsystems which compose the BB CPSS and, for each of them, types of context entities interact inside:

- Social Space (SS): all the human actors which interact inside a BB. Four category of human entities are identified: customers, employees, attackers and guards.
- Cyberspace (CS): the local component of the IPS, that is a software based systems able to manage the security and safety operational process which happen inside a BB.
- Physical Space (PS): physical SOs and non SOs involved in security and safety processes.

The following table provide a description of the main context entities of a BB modelled as a CPSS.

Table 2. Main context entities of a BB modelled as a CPSS.

Space	Entity	Entity detail	Description
SS	People	P_1: Customer	a person who is utilizing one or more of the services provided by the bank.
		P_2: Employee	a person who works for a bank institution under a contract of employment.
		P_3: Attacker	a person who is performing a criminal action to obtain an unfair benefit and to damage someone or something.
		P_4: Guard	outsourced contractor monitoring for potential threats to BB, on-site (e.g. armed guard) and remotely (security guard inside the control room).
CS	IPS		A web platform based on a client-server architecture able to manage security and safety process within a BB
PS	Bank assets	BA_k	the set of tangible and intangible goods that are threatened by criminal attacks.
	Weapons		any device used with intent to inflict damage or threaten people, structures, or systems
	Safety and security systems	Non SOs	static measures intended to prevent/obstacle harms to bank assets discouraging the potential criminals by doing the attack (e.g. structural measures such as armour windows, armed guards, armour-plated doors, time lock doors).
		SOs	SOs that leverage on IoT features to provide security and safety services. These systems require the activation (automatic or human driven) of a countermeasure further to a risky event. Such systems are based on HCI or machine-to-machine interactions

Volpentesta et al. [34] proposed that every action performed by context entities inside a smart environment affects their state. Interactions between entities can be sensed, interpreted and mediated through IoT based protection systems. In certain cases, a subset of actions performed by humans in a BB can be recognized as

threatening and may trigger a sequence of security service actions (e.g. a countermeasure) involving people (attackers, customers, employees) physical goods, as well safety and security systems. We define "security patterns" the sequence of actions involving context agents within a bank branch in order to detect of a threat.

In order to model security pattern, we used the following formalism. Let us consider S_k the set of all possible statuses of a Bank Asset BA_k and A_k a non-empty set of actions that can be performed on BA_k. We assume that any action $a \in A_k$, performed by an actor P_i-, determines a status change (from $s_{i,k}$ to $s_{j,k}$, $i \neq j$, $s_{i,k}$ $s_{j,k}$ $\in S_k$) of a Bank Asset BA_k. Each actor P_i is allowed to perform a set of activities $A_{k,i}$, where $A_{k,p} \subseteq A_k$.

The triple BA_k (S_k, A_k, $P(A_k)$) univocally identifies the interaction graph $G_{BAk}(N(S_k), E(A_k, P(A_k)))$, where $N(S_k)$ is the set of nodes, and $E(A_{k,p})$ is the set of arcs determining the transaction from a node to another, due to an action a $\in A_k$, performed by an actor P. A dangerous situation is detected when a transaction from a node n_x to n_y is due to an action A_k such that $a \epsilon A_k$ and $a \notin A_{k,p}$. A security pattern for a resource is a path p on the graph G_{BAk}. Continuous interactions along the graph shape the logical model of the BB CPSS. Security patterns constitute the building blocks of a security infrastructure, in the sense that any security infrastructure comes out from a combination of some security patterns. Unlike traditional security systems, where sensors are only capable of detecting simple actions in an environment (eg motion sensors), the IPS allows security management procedures based on complex and structured events. For example, traditional sensors are able to sense simple events like "*a strongbox is open*" or "*a human with a metal object is crossing the BB entering door*" recognizing them as dangerous events. The IPS sensors are able to sense primary events and learn, reason, and more effectively interact with humans inside a BB, leveraging on machine learning algorithms to process the data collected and recognize only real dangerous situations. Appropriate machine learning algorithms enable the IPS to combine security patterns to infer secondary events. More formally, let P_{BAk}. be the set of admissible patterns on G_{BAk}, (i.e. a sequence of actions considered not dangerous for BA_k's safety and security), the IPS recognizes a threat when it identifies an interaction such that $p \notin P_{BAk}$. In the previous example, the IPS recognizes that strongbox is open due to authorized scheduled refilling activities (p_1) and the armed human is a guard already authorized to enter the BB (p_2). Since both p_1 and $p_2 \in P_{BAk}$, both are "false positives" threats and the IPS do not activate any reaction measure.

4.2.2 The Architecture of the IPS

The IPS is able to manage many BBs as remote controlled CPSSs in order to both increase the degree of security and safety of the branches and reduce operational and management costs of the banking group protection system. We defined a logical and technological model allowing the remote management of the BB CPSSs, able to handle data coming from synthetic sensors, video surveillance (passive safety), and real-time reports from employees and sensors (active safety). The network architecture of the IPS is described below.

- Local Nodes: A local node is a local protection unit of a BB charged to manage and control the BB CPSS. Local nodes make use of computer vision and

synthetic sensors technologies, able to carry out the local management of the signaling, comprising the correlation with the state of other software subsystems. Any local nodes interact with the central node.

- Central Node: A control room that collects signals from each CPSS (local node), and is able to implement prevention or reaction risk protocols [35]. The central node uses embedded technologies in order to recognize each kind of threat.

The IPS is a cognitive system since it is able to recognize the types of ongoing events in each BB and suggest (or automatically adopt) in real time a set of appropriate countermeasures. The IPS continuously updates and upgrades its security patterns since it is able to learn from past criminal attacks, adopted countermeasures and effects of such adoption. The IPS integrates efficient models and algorithms allowing the "unstructured events" video surveillance, in order to minimize the number of *false positive* alarms and to minimize the number of not identified risky situations. Smart cameras can be equipped with computer vision able to recognize human behaviour.

The IPS data-processing architecture is based on a web-based multi-tier solution which makes use of an interprocess communication mechanisms typical of enterprise-type solutions.

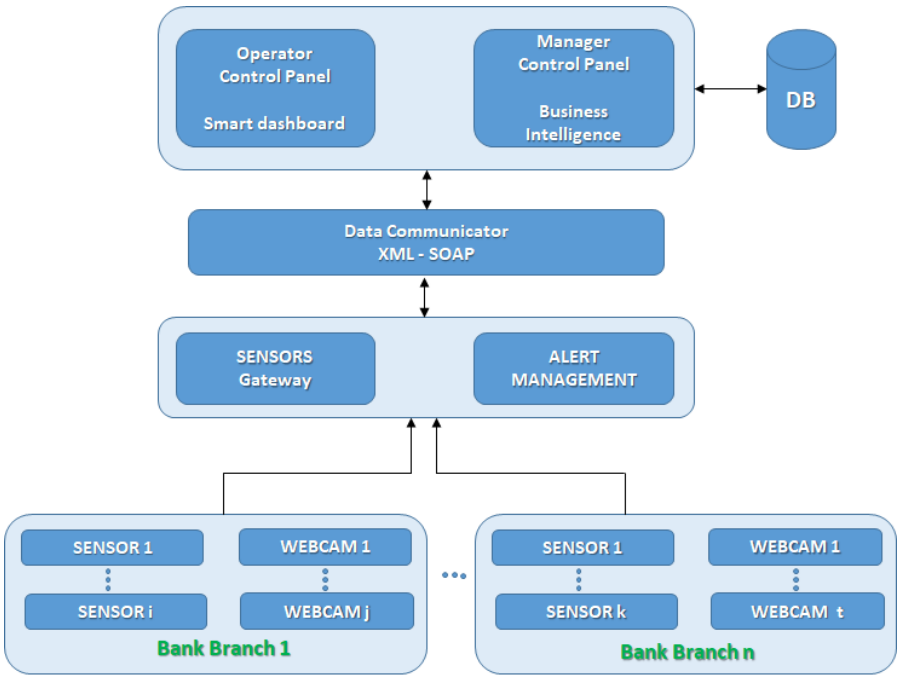

Fig. 1. The network architecture of the IPS

Figure 1 shows the different components of the IPS and how information flows occur from the BB CPSSs to the control room.

- **Sensor gateway**: a network device able to collect heterogeneous data from sensors.

- **Alert management**: represent all the alarm warnings generated by the sensors (break-in, intrusion, etc.) that are sent as a textual list to the control panel
- **Data Communicator**: transmission communication protocol among the recognition systems (which filter the alarms by assigning them a level of danger) and the platform that will display them on the control panel. This communication is based on XML / RPC web services.
- **Technical Operator Panel**: web interface for technical operators in order to manage security activities at an operational level.
- **Operator Manager Panel**: Management interface to analyse statistical data and setting up change to the security platform.
- **DB**: is the Data Base where will be saved all the events and decisions taken. Naturally it contains the whole knowledge base of the system on the security measures, security patterns and the risk model.

The human interaction with security services is mediated by a ubiquitous computing system and every smart object in the environment can potentially give either an input to the IPS or an output to each person inside the smart environment. In fact, the interaction is not centralized in a single device, but it involves a person, a potentially huge set of smart objects distributed in the real world, and many security services running on the system.

5 Conclusions

Several authors highlighted the need for an integrated approach to managing physical security [36]. Physical protection systems leverage not only on technologies, but integrate people, procedures and equipment for the protection of goods or services against theft, sabotage or any action aimed at harming people or property, implying the need for an integrated methodological approach. Physical security of people and spaces (e.g. workplace, private and public areas), is becoming increasingly important, and requires comprehensive and integrated solutions, characterized by ease of configuration and immediacy of use.

The availability of a new generation of multipurpose and low-cost sensors enabled the opportunity to easily redesign physical spaces as smart environments. In order to exploit this opportunity, there is a need to design appropriate platforms able to manage and process data deriving from sensors. Thanks to the recent technological developments, it has become possible to integrate physical networks of SOs with cognitive systems where applications can use such an intelligent infrastructure to carry out data analytics, process optimization and decision support. In particular, we propose to deal with the traditional physical security issue of BBs under a CPSS perspective. The technological infrastructure of a BB can be modelled as a CPSS where smart and non-SOs used as protection measures, can interact among them and with humans through a digital network. Moreover, the introduction of an effective and tailored Intelligent Protection System is responsible to manage an analyze data acquired to synthetic sensors.

The IPS we proposed combines a high level of security and safety within a bank branch to a more rapid access to the physical structure and an increased positive

feeling requested by the customers. The non-invasive sensor network designed within the platform realizes a more comfortable environment through the elimination from the customer's sight of protective elements of a crime, such as bars, revolving doors, gunmen, etc., which, although currently necessary to prevent robberies, increase the sense of anxiety. This is in line with the changing of commercial banking needs, whose marketing functions are pushing to let bank branches be more and more similar to selling point of other industries.

Ongoing studies are testing a prototype of the IPS in order to experiment it inside a BB context.

References

1. Ashton, K.: That “internet of things” thing. RFID Journal, 22(7), 97–114 (2009)
2. Mattern, F., & Floerkemeier, C.: From the Internet of Computers to the Internet of Things. In: From active data management to event-based systems and more, Springer Berlin Heidelberg (2010), 242-259.
3. Kopetz, H.: Real-time systems: design principles for distributed embedded applications. Springer Science & Business Media (2011).
4. Cook, D., & Das, S. K.: Smart environments: Technology, protocols and applications (Vol. 43). John Wiley & Sons, (2004).
5. Wu, Q., Ding, G., Xu, Y., Feng, S., Du, Z., Wang, J., & Long, K.: Cognitive internet of things: a new paradigm beyond connection. IEEE Internet of Things Journal, 1(2), 129-143, (2014).
6. Al-Turjman, F. M.: Information-centric sensor networks for cognitive IoT: an overview. Annals of Telecommunications, 72(1-2), 3-18 (2017).
7. Sadeghi, A. R., Wachsmann, C., & Waidner, M.: Security and privacy challenges in industrial internet of things. In: Proceedings of the 52nd annual design automation conference, ACM, (2015) 54.
8. Del Giudice, M.: Discovering the Internet of Things (IoT) within the business process management: A literature review on technological revitalization. Business Process Management Journal, 22 (2), 263-270, (2016).
9. Alvi, S. A., Afzal, B., Shah, G. A., Atzori, L., & Mahmood, W.: Internet of multimedia things: Vision and challenges. Ad Hoc Networks, 33, 87-111 (2015).
10. Tinnilä, M.: Efficient service production: service factories in banking. Business Process Management Journal. 19(4), 648-661 (2013).
11. Bank Seta: THE BANK OF THE FUTURE: innovative solutions to meet the challenges of the new environment. Technical report, Wits Business School (2014).
12. Sofo, F., Berzins, M., Ammirato, S., & Volpentesta, A. Investigating the relationship between consumers' style of thinking and online victimization in scamming. *JDCTA*, *4*(7), 38-49 (2010).
13. Matthews, R., Pease, C., Pease, K: Repeated bank robbery: themes and variations .(2001).
14. EBF: Physical security report 2015. Technical report, European banking federation (2016)
15. FBI: BANK CRIME STATISTICS – 2015. Technical report, U.S. Department of justice federal bureau of investigation Washington (2016).
16. Conrath, E. J.: Structural design for physical security: State of the practice. ASCE Publications (1999).
17. García, C. G., Meana-Llorián, D., G-Bustelo, B. C. P., Lovelle, J. M. C.: A review about Smart Objects, Sensors, and Actuators. International Journal of Interactive Multimedia and Artificial Inteligence, 4 (2017).

18. Lee, E. A.: Cyber physical systems: Design challenges. In: 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), IEEE, (2008) 363-369.
19. Monostori, L.: Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia CIRP, 17, 9-13 (2014).
20. Volpentesta, A. P., Muzzupappa, M., & Ammirato, S. Critical thinking and concept design generation in a collaborative network. In *Working Conference on Virtual Enterprises,* Springer, Boston, MA. (2008) 157-164.
21. Lee, J., Bagheri, B., Kao, H. A.: A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23 (2015).
22. Felicetti, C., De, R., Raso, C., Felicetti, A. M., Ammirato, S.: Collaborative smart environments for energy-efficiency and quality of life. International Journal of Engineering and Technology 7(2), 543-552 (2015) .
23. Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., Alamri, A.: Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Systems Journal (2015).
24. Zeng, J., Yang, L. T., Lin, M., Ning, H., & Ma, J.: A survey: Cyber-physical-social systems and their system-level design methodology. Future Generation Computer Systems (2016).
25. Ning, H., Liu, H., Ma, J., Yang, L. T., & Huang, R.: Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology. Future Generation Computer Systems, 56, 504-522. (2016)
26. Lloret, J., Canovas, A., Sendra, S., & Parra, L.: A smart communication architecture for ambient assisted living. IEEE Commun. Mag, 53(1), 26-33 (2015).
27. Grill, T., Polacek, O., & Tscheligi, M.: Conwiz: The contextual wizard of oz. Journal of Ambient Intelligence and Smart Environments, 7(6), 719-744 (2015)
28. Laput, G., Zhang, Y., & Harrison, C.: Synthetic sensors: Towards general-purpose sensing. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, ACM (2017) 3986-3999.
29. Tripolitsiotis, A., Prokas, N., Kyritsis, S., Dollas, A., Papaefstathiou, I., and Partsinevelos, P.: "Dronesourcing: a modular, expandable multi-sensor UAV platform for combined, real-time environmental monitoring", International Journal of Remote Sensing. Vol. 38, No. 8-10, 2757-2770 (2017).
30. Hevner, R. H., March, S. T., Park, J., & Ram, S: Design science in information systems research. MIS quarterly, 28(1), 75-105, (2004).
31. Offermann, P., Levina, O., Schönherr, M., Bub, U.: Outline of a design science research process. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology ACM (2008).
32. Baker, P. R.: Physical Protection Systems. In: Baker, P. R. & Benny, D. The Complete Guide to Physical Security. CRC Press (2012)
33. Wojciechowski, M., & Xiong, J.: A user interface level context model for ambient assisted living. In International Conference on Smart Homes and Health Telematics, Springer, Berlin, Heidelberg (2008) 105-112.
34. Volpentesta, A. P., Felicetti, A. M., & Ammirato, S.: Intelligent Food Information Provision to Consumers in an Internet of Food Era. In Working Conference on Virtual Enterprises, Springer (2017) 725-736.
35. Volpentesta, A. P., Ammirato, S., & Palmieri, R. Investigating effects of security incident awareness on information risk perception. *International Journal of Technology Management*, *54*(2/3), 304-320. (2011).
36. Garcia, M. L.: Design and evaluation of physical protection systems. Butterworth-Heinemann. (2007).