A Business Process and Data Modelling Approach to Enhance Cyber Security in Smart Cities

Josef Horalek, Tereza Otcenaskova, Vladimir Sobeslav(✉), and Petr Tucnik

Faculty of Management and Informatics, University of Hradec Kralove, Hradec Kralove, Czech Republic
{josef.horalek,tereza.otcenaskova,vladimir.sobeslav,petr.tucnik}@uhk.cz

Abstract. The term Smart City represents a strategic concept for a city or region that involves the use of modern technologies to influence the quality of life in the city. At the technological level, a wide range of IoT devices are used, which are interconnected through modern low-latency networks to enable the creation of intelligent applications with added value for their users. However, this relatively simple and noble idea represents a wide range of technologies and approaches, making the idea of ensuring Cyber Security in Smart Cities difficult. When implementing any technology in an organization, the processes, assets, and people that bring the technology to life, are crucial. The aim of this paper is to analyze the key capabilities, frameworks and standards that would facilitate and support the possibility of developing Smart Cities. The first part of the article introduces the issue of Cyber Security and Smart Cities. Subsequently, the key approaches for ensuring security in creating Smart Cities are analyzed. The final part presents the BPMN-SC data model based on business process model notation and key security standards while incorporating the specifics of Smart Cities.

Keywords: BPMN-SC Model · Business Process Modelling · Cyber Security · ISO 27001 · Smart Cities

1 Introduction

The term Smart City, which has become increasingly popular in recent years, refers to cities that use technologies to deliver services and solve problems that occur in the city. Essentially, a Smart City aims to optimize city functions, promote economic growth, and improve the quality of life of its citizens by using a variety of modern technologies, data collections and smart applications [16]. Thus, it is expected to make smarter, more efficient, and accessible services for citizens while ensuring the Cyber Security of modern technologies. There are many definitions that describe what Smart Cities are, but the key issue is that they encompass a wide range of technologies, smart devices, specialized protocols, utilization of mobile networks and Internet, cloud services, application development, big data processing issues and many more. According to the Berkley Center

P. Cong Vinh and H. Mahfooz Ul Haque (Eds.): ICTCC 2023, LNICST 586, pp. 70–84, 2024.
https://doi.org/10.1007/978-3-031-59462-5_5

for Long-Term Cyber Security (CLTC) and their survey of The Cybersecurity Risks of Smart City Technologies [1], the Internet of Things (IoT) and other smart technologies which are being used in Smart Cites are posing greater risks in aggregate than other technologies. Local officials and authorities should therefore consider whether cyber risks outweigh the potential gains of technology adoption on a case-by-case basis. Moreover, they should exercise particular caution when technologies are both vulnerable in technical terms and constitute attractive targets to capable potential attackers because the impacts of an attack are likely to be great. Deloitte [7] in their report 'Making smart cities cybersecure' defines three key factors that influence the cyber risk in Smart Cities.

1. Convergence between Information Technology (IT) and Operational Technology (OT) infrastructures on the boundary of the physical and cyber world. This represents for example the challenges and different views for the utilization of IoT sensors and actuators in physical and cyber environments.
2. Interoperability representing the coexistence band of frequent interactions between legacy and smart systems and platforms including the on-premise and cloud solutions.
3. Integration and comingling of services across domains through IoT and digital technologies.

It is important to mention that Smart Cities are far from being just about Information and Communication Technologies (ICT) but include a range of non-technological perspectives. People are key players, and in case of Smart Cities, it is mainly people who provide services to citizens. The legislative framework and the establishment of rules under which smart services are provided are also very important. Strategic planning at the city and regional level is also an integral part of this, to provide the means to realize community and policy objectives. The following Fig. 1 presents the key components of a sustainable Smart City, according to the European Innovation Partnership on Smart Cities and Communities research center [17].

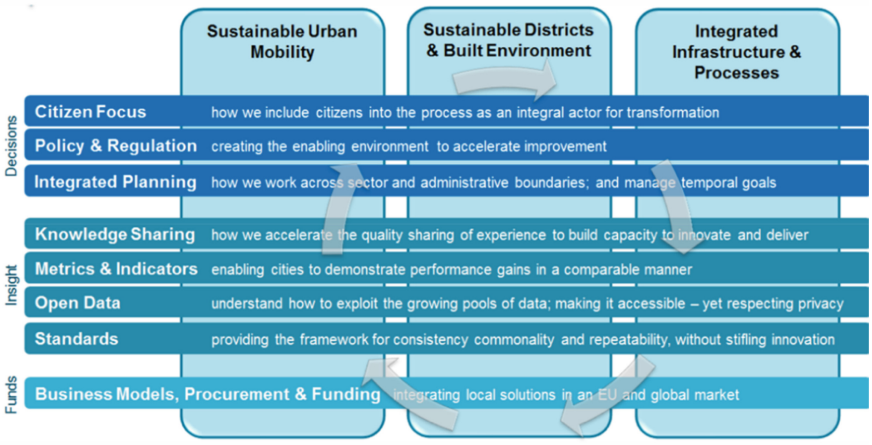

Fig. 1. Concept of Sustainable Smart City [26]

An integral part of the Smart City concept is also data, which can be divided into sensitive data and open data. Sensitive data in the public administration domain include mainly personal data, which are protected by legislation, in the European Union (EU) for example by GDPR act [30]. Open data, on the other hand, represents data that are a sign of public sector transparency and provide citizens with a possibility to control the functioning state apparatus. Furthermore, these comprise also data freely available to citizens as a service [22]. According to the EU initiative and the Operational Implementation Plan for Smart Cities, the following key recommendations are essential [19]:

- Consistent use of standards, protocols and generic data formats that enable and support interoperability between different systems, avoid lock-in of specific out-doors and promote competition in the solutions developed.
- Ensuring access to third-party data (with full protection of personal data and trade secrets), thus creating support for the development and improvement of new applications.
- Leveraging existing infrastructures and enabling their unrestricted reuse for different purposes.

Apparently, the concept of Smart Cities covers a very broad spectrum of IT or OT technologies including energy, transportation, healthcare, and many others. The integration of next generation mobile networks or the use of the cloud to provide smart services to citizens - using open but also very sensitive data - opens new challenges in cyber security of Smart Cities. Given the widespread popularity of modern technologies, the question is not if, but how to protect services and data in Smart Cities. As already mentioned, a Smart City is far from being just about technology, but mainly about the people and processes in a city or region that shape the key services provided to citizens to improve their quality of life. The question is how to link these relatively separate principles into one homogeneous approach for enhancing the security of Smart Cities. The key to the successful implementation of the Smart Cities concept is to identify the specific needs and domains that characterize this area. Based on the domain model of use in the EU and with emphasis on the specifics in the Czech Republic [29], the Business Process Model for Smart Cities (BPM-SC) model is proposed. The BPM-SC is based on the business process model notation and the key security standards while considering the specifics of Smart Cities.

2 Related Works

The previous section highlighted the wide range of ICT that are used in the Smart City concept. However, it is not only technologies but also organizations, people, rules, processes, or data that together shape the smart services for citizens. Currently, a lot of technological approaches, standards, frameworks, methods, or technologies exist [10]. According to the Research on Information Security System of Smart City Based on Information Security Requirements [25], there are three important requirements the create information security: management requirements, technological requirements and lastly the construction and operation requirements. To fulfil the technological requirements in the area of Smart Cities, European Union Agency prof Cybersecurity (ENISA) recommends the use of security baselines [14]. As stated above, there is also a variety of

security standards which can help to ensure security from the organizational perspective. Smart Cities and Smart Regions are represented also by the people who provide the service to citizens, rules and laws, processes, data, and their interconnection. To ensure the security of complex organizations, it is very important to uncover the actors, entities, analyze the processes, data utilization and their interconnection to see the organization in a systematical and holistic way. For these purposes, the utilization of Business Process Modeling and Ontologies in various research and applications in this area occurs, for example [4, 9, 12, 24, 31]. From the above-mentioned reasons, the following approaches with respect to Smart City were selected.

2.1 Security Control Baselines

The first important and often used approach to enhance cyber security is the use of security baselines as a methodological support. This approach is mainly used when implementing IT/OT technologies for organizations of all sizes. According to NIST [8], it is mainly a set of information security controls that has been established through information security strategic planning activities to address one or more specified security categorizations. Security baselining is the process of capturing a point in time understanding of the current system security configuration. Establishing an easy means for capturing the current system security configuration can be extremely helpful in responding to a potential security incident [5, 13].

Security baselines do not cover the entire process of ensuring cyber security in an organization because they do not examine the organization in detail as a complex system that is defined by individual entities, their relationships or by defining the sensitivity of the data that are generated in such a system. Rather, they are about implementing best practices to enhance system security at the technology level. As we have already mentioned, smart technologies and their effective deployment make it possible to transform an ordinary city or region into a smart one. In the Smart City concept, it is advisable to use a security foundation defined by the manufacturer or a security strategy or best practices for the implementation of technologies. According to [18], technology systems and the use of security foundations can be categorized as follows:

- Physical environment security - prevent physical devices from being accessed or damaged under unauthorized conditions, to ensure the security of hardware devices.
- Network transmission security - mainly the establishment of cross network authentication and encryption mechanism between heterogeneous transmission networks, to prevent the security risks of cross isomerism network and enhance the transmission efficiency of information across the network.
- Host system security - in Smart City refers to the host security technology challenge in cloud computing environment and also the on-premise technologies related with the local installed IT/OT technologies which are deployed in the region or Smart City.
- Data resources security - large amount of collection, filtering and integration of business data and meticulous business analysis and association rules mining, enterprises or related data management departments can perceive their own network security situation.

- Application services security - The security of application services is mainly to consider the security increase, reinforcement, and transformation of the application systems, and to provide a unified support platform for the security protection functions of the cloud computing center and the region.

2.2 Security Standards and Frameworks

In the domain of standards and regulations for the domain of cyber security, there are two leading organizations, namely Cybersercurity and Infrastructure Security Agency (CISA) for United States area, and ENISA for the states in EU. CISA is an organization established by the US Department of Homeland Security and ENISA was established by order of the European Parliament and the Council of Europe (management is appointed by the Council). Both agencies provide recommendations, tools, and support for improvement of cybernetic security of organizations and states.

The main difference is geographical and legislative context in which they function. CISA has competencies to do inspections and audit critical infrastructure while ENISA is an independent body of EU Council and has no authority to enforce its recommendations or certify products and services. For technical standards and frameworks, CISA uses NIST. NIST, among other activities, defines NIST Cybersecurity Framework. ENISA uses the international standard ISO/IEC 27001 as a framework for defining requirements and procedures, which set out the requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS) and serves as an audit control framework. ISO/IEC 27002 provides detailed additional guidelines for application and control of security standards. The importance of agency ENISE increased with the implementation of Directive (EU) 2022/2555 of the European Parliament and of the council on measures for a high common level of cyber security across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [8].

NIS2 is legislation of EU in the area of cybernetic security and follows the original directive of NIS from 2016 which strengthens legal measures for increasing the overall level of cyber security in EU by stating: readiness of member states, risk management requirements, and incident reporting for subjects providing important or basic services, cooperation, and co-ordination between member states and EU, sanctions, and supervision. The directive also extends the range of entities that must comply with cyber security rules to other areas such as energy, transport, healthcare and digital infrastructure. NIS2 Directive also allows member states to impose fines on subjects up to 10 million EUR or 2% of worldwide turnover for previous fiscal year (depending on which one of those is higher) if they violate measures for cyber security risks control and/or obligations for cyber security incidents reporting. NIS2 Directive also assigns the set of new tasks to ENISA, for example development and maintenance of European registry of vulnerabilities which will contain information about known SW/HW vulnerabilities and recommendations for their handling. The Secretariat of the European Cyber Crisis Contact Organisation Network (CyCLONe), which will coordinate responses to large-scale cross-border cyber incidents or crises, also provides support to Member States in implementing and complying with the European Commission's zero-tolerance requirements in their national legal systems. CyCLONe is using its expertise in the field of cyber

security, in particular for entities providing essential or basic services in the context of NIS2 Directive, and supporting the harmonization of risk management and incident reporting requirements for entities ensuring essential or basic services in the context of NIS2 Directive.

Based on the aforementioned, it is obvious that both CISA and ENISA define general frameworks. In case of ENISA, these are to be implemented into national legislation of EU member states and through regional administration manage their control and enforcement. Both agencies create process and technical frameworks which ease the implementation, control and monitoring for affected organizations. The practice shows that the individual measures allowing achievement of proper cyber security levels are similar and defined on the basis of ISO/IEC 27001:2013 and NIST Cybersecurity Framework (CSF) at the same time. This proves their high rate of mutual similarity.

2.3 Ontological Engineering

There are various approaches to data modelling relating to cyber security. Among others, the ontology-based approaches help to identify the vulnerabilities [20]. Various ontological frameworks can be implemented too [18, 20, 27, 28]. Mozzaquarto et al. [18] emphasize that IoT being used in Smart Cities is facing many cybersecurity challenges and attacks. To eliminate these issues, they propose the improvements resulting from the ontological analysis identifying the ontology-based cybersecurity framework. This framework reflects the model-driven methodology considering the organizational processes as well as monitoring and ensuring the adaptation of the environment. Salnitri et al. [23] prove the ontology usage through the combination of BPMN-Query language and the Reference Model of Information Assurance & Security (RMIAS) comprising the high-level security ontology as a baseline. De Nicola and Villani [6] introduce various types of Smart City ontologies and justify their relevance for crisis management including numerous aspects of security. Moreover, in pursuit to increase system's security capability, Chergui and Benslimane [3] use the BPMN extension based on complete cyber security ontology for modelling of the security requirements. The abovementioned efforts might be umbrellaed by Unified Cyber Ontology (UCO) which represents „foundation for standardized information representation across the cyber security domain/ecosystem" [11]. This concept together with Cyber-investigation Analysis Standard Expression (CASE) provide significant community-developed and community-recognized tool for interoperability and cyber investigation. It helps to create flexible as well as explicit data models. The ontological approaches ensure particular advantages such as:

- misinterpretation and ambiguity elimination
- consistency and possibility to reuse the concepts and structures
- portability among domains and technologies
- integrity of representation [2, 11]

2.4 Business and Data Modelling

Business environment and its processes can be modelled by various tools. In connection to data which represent from the security perspective one of the most critical assets, the

very efficient tool is BPMN (Business Process Model and Notation) [21, 23]. BPMN is a standardized modelling tool and defines three types of diagrams: (i) collaboration diagram, (ii) conversation diagram, and (iii) choreography. The most frequently used is collaboration diagram which also contains the most important semantic elements. It allows modelling of business process workflows and possible interactions with external entities via B2B, B2C, B2G etc. relationships.

In the context of data modeling, BPMN distinguishes between (smaller) data objects with potential indication of input/output semantics, and data stores, used for larger databases. An interesting phenomenon when modeling work with data artifacts is that almost every activity can be connected to some kind of data objects. It is therefore important to choose an appropriate level of abstraction to keep diagrams transparent and comprehensive. Data objects are more frequently used in workflows and therefore will be mainly addressed in this sub-section.

The data objects are perceived as static entities in BPMN. While there obviously are changes being made, which can be indicated by input/output indicators when needed, data object internal state itself is encapsulated. The change is described by properly named activities (tasks or sub-processes), connected to the respective data objects. Internal dynamics of data objects is not being represented and security-related attributes of data, that can be very important, require use of some form of specialized BPMN extension for the security domain. This is discussed in more detail in sub-Sect. 3.2 of this paper.

While there are some limitations in BPMN when modelling data dynamics, notation allows us to identify process owners by use of elements of pools and lanes. The “pool” usually refers to larger part of the organization or some external entity, “lanes” identify individual actors whose responsibilities are processes shown within the respective lane. As the workflow is under way (which can be imagined as a movement of imaginary token through the diagram), the model reader can see clearly how the responsibility is shared between individual actors. From the cyber security point of view, this is quite advantageous, since the roles and responsibilities of individual users can be more easily identified, and access control mechanisms and strategies adjusted as needed.

The identification of process owners is also related to data objects security [15]. The diagram captures who owns the process working with data object and such actor also bears responsibility for the data object safety. Moreover, processes can be influenced by occurrence of events (of internal or external origin) or messages from external entities such as during B2B communication. Specialized “message flow” connector element is used here to capture B2B interactions and can hold information about the communication in its description. However, more detailed attributes related to data object safety again require the use of specialized BPMN extension, see sub-Sect. 3.2.

3 Business Process and Data Model Approach for Smart Cities

This chapter refers to the Smart Cities Domain and based on this introduces the BPMN metamodel extension with security-related elements. Moreover, the data type categorization including the measures to protect them.

3.1 Smart Cities Domain Model in the Czech Republic and Smart Cities Specifics

For the description of the current state-of-the-art of the domain model for Smart Cities in the Czech Republic, mostly general scientific methods were used. First, the available materials, especially academic articles, norms, laws, and standards, were reviewed. On the basis of this review and the analysis of national documentation, the domain model of Smart Cities in the Czech Republic was developed and published [29] (Fig. 2).

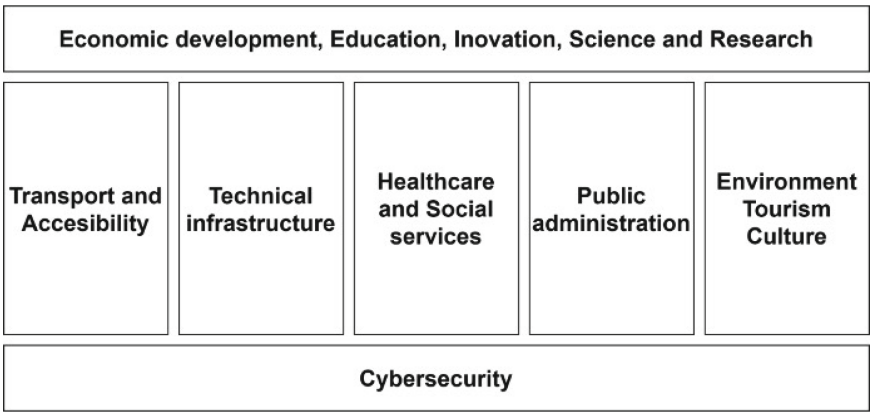

Fig. 2. Smart City Functional Domains [29]

This model is generally accepted by the professional public as a conceptual domain model of Smart Cities in the Czech Republic. Based on it, the Business Process Model representing basic data flows and process relationships was created. This model is supported by requirements for cyber security according to NIS2 requirements, respectively to the implementation of requirements from ISO/IEC 27001. The basic principle is that in individual functional domains security requirements are implemented. These are perceived as a process of control according to PDCA (Plan, Do, Check, Act). This is implemented not only to the domain model as a whole but also in the context of individual domains. This process approach allows us to fulfill criteria of ISO/IEC 27001 and especially areas of Appendix A of this standard, namely A.6 Organization of information security, A.7 Human resource security, A.8 Asset management, A.17 Information security aspects of business continuity management, and A.18 Compliance with requirements. Other criteria, mostly of technical nature, are influenced by the processes and technologies specific for the specific domain.

3.2 A Proposal of Abstract BPM-SC Based on Smart City Domain Model

One of the effective approaches to design, re-engineer, analyze, or understand internal functioning of the organization is BPMN (Business Process Model and Notation) analysis. In its standard version, it allows capturing of process workflows, especially in the most frequently used collaboration diagram. For the security-related issues, other BPMN diagrams, namely conversation diagram and choreography diagram, have only

limited value since most semantics is provided by elements in collaboration diagram. Moreover, the standard notation is enhanced by the extension of graphical elements to capture aspects specific for the security domain.

The review of research papers done in this area shows that security extensions content to BPMN metamodel quite vary, depending mainly on the level of detail preferred by individual authors. Particular differences include the work with data-related artifacts, roles and permissions given to individual actors and process owners, and representation of security requirements/goals. The used terminology - or rather simply naming - of individual extension components also vary, making the situation somehow less transparent. There are security standards/norms that can be used as a basis for identification of security components for incorporation into BPMN metamodel [3, 21, 23, 32]. In this case, the most relevant standard for EU context is ISO/IEC 27001 (and related standards) describing information security and management.

The BPMN core elements are shown in Fig. 3. From the security perspective, especially two groups of elements are important more than the others: participants and data artifacts. The former is used for identification of actors with the responsibility for processes, the latter should be protected by properly set security management strategy.

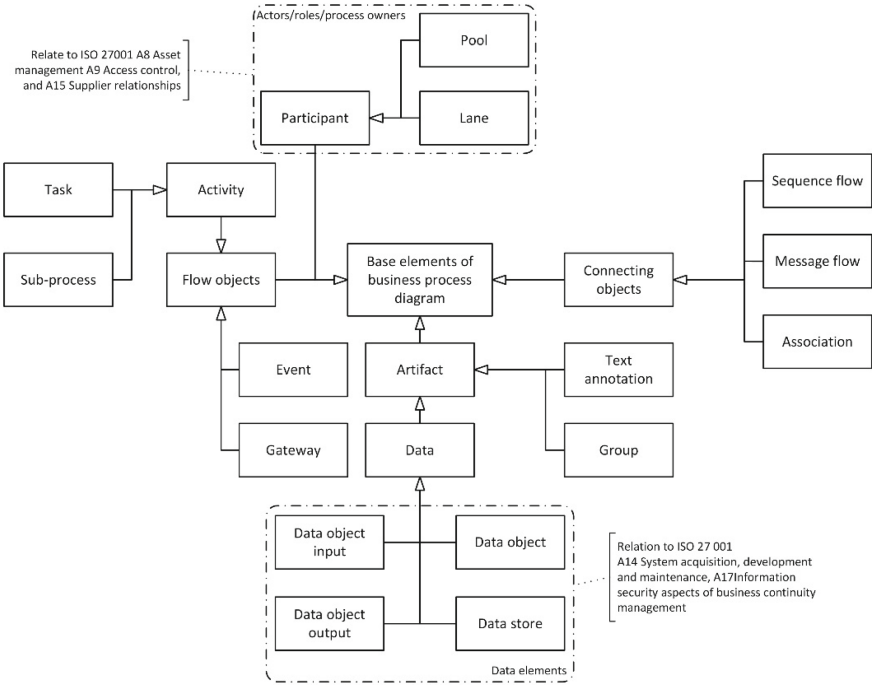

Fig. 3. Standard BPMN Metamodel Elements. Source: authors.

The proposed BPMN extension which considers the requirements of ISO/IEC 27001 standard is shown in Fig. 3. The security data model based on the BPMN metamodel standard, intended for the Smart City area and applicable to defined functional domains,

was designed with regard to the fulfillment of process and technical measures not specified in NIS2. These fulfil the recommendations of Annex A of ISO 2700 standard, which serve as a basic security framework. A fundamental principle of cyber security is the determination of the assets value. Critical assets in Smart City domain are represented mainly by data and information creating the data sets. One of the most used principles for determining the data assets value is based on the confidentiality, integrity, availability (CIA) triad. The specific classification of sub-parameters is determined by the asset manager. Generally, the usage of the evaluation scale containing an even number of values can only be only recommended. Even though such scale would eliminate the "middle"/neutral values. In the proposed security data model, these are gray-colored items entered into the security goal section.

After evaluating particular data sets, it is necessary to determine their type. With regard to the focus of the security data model on Smart City, an analysis of occurring data types was carried out, especially during the designing of Smart City functional domains model [29]. Consequently, these data types were categorized. This resulted in five-point data scale of data types.

1. Public data – represented by publicly available data, e.g. in the data portals of the authorities ready for end processors/users. This category requires necessarily to keep the corresponding integrity.
2. Sensitive - represented typically by sensitive data appearing especially during their creation and processing. These are not intended for publication or before their publication, it is necessary to set rules and technologies for their protection, not only at the level of integrity, but also at the confidentiality level.
3. Confidential – this is non-public data subject to higher protection than Sensitive data. These include e.g. information about organizations established by the government, such as financial statements or internal methodologies. None of this data could have an impact in areas of financial, reputational, or also security risks.
4. Critical – this category includes data from the field of energy management, internal IT systems, financial and accounting systems, etc. Here, special emphasis is put on preserving their integrity, confidentiality, but especially availability, as this type of data also helps to regulate partial services of the entire Smart City environmental system.
5. Regulatory – these data with the highest protection, which is given not only by cyber security requirements, but also by other relevant legislative acts such as the GDPR regulation, the protection of healthcare systems, etc. Breach of the security of this information has legal consequences in the form of financial fines/reimbursements, restriction of the activity of the provided service or loss of license.

In order to fulfill security measures, it is necessary to implement appropriate technical measures based on technology-oriented measures resulting from recommendations of ISO 27001. This means setting of the appropriate level according to A.10 Cryptography. When implementing the cryptography protection, it is necessary to consider the data storage length with regard to the estimated the impenetrability of sub-algorithms. It is also critical to implement means and technologies for A.9.4 System and application access control, which form the basic security measures to ensure data confidentiality. An integral but sometimes underestimated are measures guaranteeing A.11 Physical

and environmental security. This is not only a centrally controlled system of physical access to the spaces where data is stored, but also to the spaces, where the data is created and managed. It is also necessary to set appropriate measures to secure personal computing systems where data is found in the form of PCs, laptops, mobile phones, tablets, but also external storage media. With regard to the use of the proposed model for the Smart City area, which is based on data communications, it is both logical and necessary step to mention the measures in the area of A.13 Communications security. The aim is to ensure an adequate level of integrity and availability of data assets. This is a measure based on the security of the layers of the TCP/IP architecture both in the area of MAN, LAN and WAN networks. All these measures must be tested before their deployment, but also within their life cycle, using appropriate test data. Therefore, the requirements from A.14.3 Test data are also included in this category. All technical orientation measures would be inefficient if the incident management system according to A.16 Information security incident management was not implemented. Without this measure, security is blind and does not allow effective response to potential security incidents. All of the beforementioned technical-oriented security measures have a wide range of specific implementations, which provide fulfilment of several described parts within one technological solution. Nevertheless, only as a whole, they form an effective technological assurance of cyber security over classified data.

After the evaluation and classification of data sets, it is absolutely to determine the authorization for operations with these data from the security point of view. The CRUD (Create, Read, Update, Delete) approach used in UML modeling represents a suitable model for data type determination. To manage these operations, it is necessary to set up organizationally oriented measures based on the ISO 27001 standard, among which A.8 Asset management and A.9 Access control are. Their aim is to establish, enforce, check and adjust access to data assets. During this process, it is absolutely necessary to use the principle of minimal corrections established on the basis of user roles and groups, including the introduction of more level approval of authorizations above standard access. Furthermore, a group of measures A.14 System acquisition, development and maintenance, A.15 Supplier relationships and A.17 Information security aspects of business continuity management should be deployed. There are all connected with the determination of penetrations and principles for maintaining the continuity of activities, which is often affected by supply chains, system development and maintenance. Establishing these rules, considering the access to data, is one of the most important components for ensuring the integrity and confidentiality of data, its classification and value. It is a complex security solution based on precisely defined organizational measures and process management, which are followed by technological solutions.

The security data model introduced above, based on the BPMN metamodel standard, thus provides a unique connection among the standard measures listed in ISO 27001, the process concept of their implementation and process control of an organization or complex of organizations from the point of view of data sets. It represents a unique model that enables the security manager to provide a process view for the company's board of directors and at the same time a data-oriented view for the system specialists responsible for the selection and implementation of necessary technologies (Fig. 4).

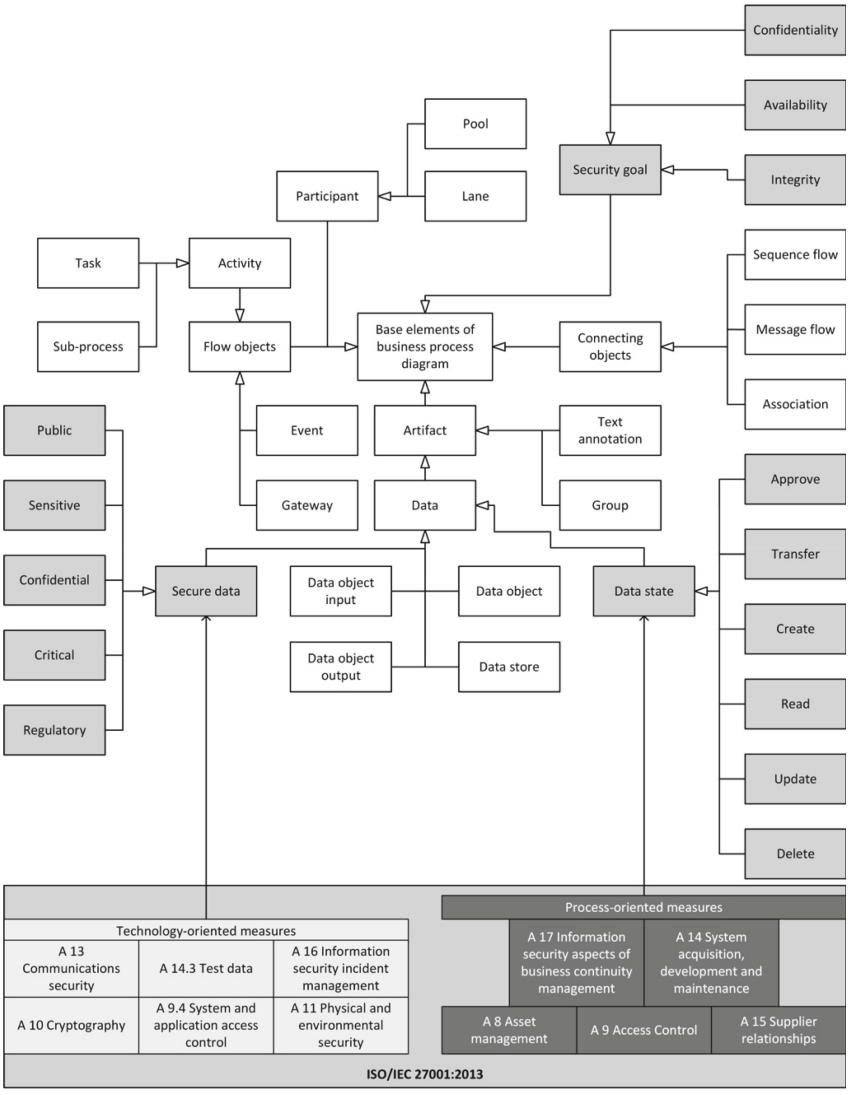

Fig. 4. BPMN Metamodel Extension with Security-related Elements. Source: authors.

4 Conclusion

The use of modern technologies, ubiquitous high-speed networks and smart applications is leading to the gradual adoption of the Smart City concept. As it was analyzed in this paper, the concept of Smart Cities not only represent a wide range of technologies, but also people and organizations, that provide services to citizens, play a very important role. The Smart City concept with the characteristic use of a broad spectrum of technologies, integration of processes and uncovering the interconnections, represents essentially a complex system that is not easy to secure because the standard e-government services

are enriched by OT technologies, sensor networks, cloud solutions, open data and many others. For the above reasons, the aim of this paper was to analyze the key approaches that would facilitate and support the possibility of developing Smart Cities with an emphasis on cyber security. In each part of the article, a key approaches that can be used to enhance the security of a Smart City or region were presented. These included security baselines, relevant norms and standards, ontologies, but also business process modelling. BPMN approach allows to see the cyber security in a holistic way and describe the Smart City or region as a complex system that needs to be decomposed into individual entities, establishing their relations, and defining data assets that need to be protected. Within the ARTISEC project (see the Acknowledgement), which is focused on the creation of a data model with an emphasis on the use of artificial intelligence for cyber security, an abstract data model, meta-model respectively, was created. This meta-model is based on the extension of the BPMN notation with the specifications of the internationally recognized security standard ISO27001, while considering the specifics of the Smart City concept. These specifics are based on the model of functional domains and the use of Smart Cities in EU, particularly in the Czech Republic. The key output of this paper is the BPM-SC data model that can be implemented in the specific areas and functional domains of a Smart City. As a future work within the ARTISEC project, the BPM-SC data model will be utilized on selected e-government/IT and OT technology domains and the results will be verified.

Acknowledgement. The financial support of the project "Application of Artificial Intelligence for Ensuring Cyber Security in Smart City" (ARTISEC), n. VJ02010016, granted by the Ministry of the Interior of the Czech Republic is gratefully acknowledged.

References

1. Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/publication/smart-cities/. Accessed 31 Mar 2023
2. Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H., Nelson, A.: Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. Digit. Investig. **22**, 14–45 (2017)
3. Chergui, M.E., Benslimane, S.M. (eds.) A valid BPMN extension for supporting security requirements based on cyber security ontology. In: 8th International Conference on Model and Data Engineering (MEDI), Marrakesh, Morocco (2018)
4. Computer Security Resource Center. https://csrc.nist.gov/publications/detail/sp/800-53b/final. Accessed 31 Mar 2023
5. Conrad, E., Misenar, S., Feldman, J.: Chapter 8 - domain 7: security operations (e.g., foundational concepts, investigations, incident management, disaster recovery). In: Conrad, E., Misenar, S., Feldman, J. (eds.) CISSP Study Guide. 3rd edn. Syngress, Boston, pp. 347–428 (2016)
6. De Nicola, A., Villani, M.L.: Smart City Ontologies and Their Applications: A Systematic Literature Review. Sustainability **13**(10), 5578 (2021)
7. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf. Accessed 31 Mar 2023

8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (2022)
9. Dong, N., Zhao, J., Yuan, L., Kong, Y.: Research on information security system of smart city based on information security requirements. J. Phys. Conf. Ser. **1069**, 012040 (2018)
10. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Accessed 31 Mar 2023
11. Unified Cyberontology. https://unifiedcyberontology.org. Accessed 31 Mar 2023
12. ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements (2013)
13. ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management. International Organization for Standardization (2013)
14. Kaspersky Daily. https://www.kaspersky.com/blog/cybersecurity-ontology/40404/. Accessed 31 Mar 2023
15. Kokolakis, S., Demopoulos, A., Kiountouzis, E.: The use of business process modelling in information systems security analysis and design. Inf. Manag. Comput. Secur. **8**, 107–116 (2000)
16. Manville, C., Kotterink, G.B.: Mapping Smart Cities in the EU. EPRS: European Parliamentary Research Service, Belgium (2014)
17. Maschio, I.: European Innovation Partnership on Smart Cities and Communities. European Comission (2023)
18. Mozzaquatro, B., Agostinho, C., Goncalves, D., Martins, J., Jardim-Goncalves, R.: An ontology-based cybersecurity framework for the Internet of Things. Sensors **18**(9), 3053 (2018)
19. Open Data. https://opendata.gov.cz/informace:kontext:smart-city. Accessed 31 Mar 2023
20. Pastuszuk, J., Burek, P., Ksiezopolski, B. (eds.) Cybersecurity ontology for dynamic analysis of IT systems. In: 25th KES International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES), Szczecin, Poland (2021)
21. Rodriguez, A., Fernández-Medina, E., Piattini, M.: A BPMN extension for the modeling of security requirements in business processes. IEICE Trans. Inform. Syst. **E90-D**(4), 745–752 (2007)
22. Massink, R., Manville GCJCJMJKPRKTALMW, C., Bas, K.: Mapping Smart Cities in the EU. European Parliamentary Research Service (2014)
23. Salnitri, M., Dalpiaz, F., Giorgini, P.: Designing secure business processes with SecBPMN. Softw. Syst. Model. **16**(3), 737–757 (2017)
24. San Martín, L., Rodríguez, A., Caro, A., Velásquez, I.: Obtaining secure business process models from an enterprise architecture considering security requirements. Bus. Process Manage. J. 28(1), 150–177 (2022)
25. Silicon Labs. https://pages.silabs.com/rs/634-SLU-379/images/Preparing_for_Next-Gen_Cyber_Attacks_on_IoT.pdf. Accessed 31 Mar 2023
26. Staalduinen van, W., Bond R., Dantas, C., Jegundo, A.L.: Smart Age Friendly Cities, Age Friendly Smart Cities. European Comission, Futurium (2022)
27. Syed, R.: Cybersecurity vulnerability management: a conceptual ontology and cyber intelligence alert system. Inf. Manage. **57**(6), 103334 (2020)
28. Temple, W.G., Wu, Y., Cheh, C., Li, Y., Chen, B., Kalbarczyk, Z.T., et al.: CyberSAGE: the cyber security argument graph evaluation tool. Empir. Softw. Eng. **28**(1), 18 (2022)
29. Urbanik, P., Horalek, J.: Design of the Smart City Domain Concept in the Czech Republic, pp. 803–814. Hradec Economic Days, University of Hradec Kralove (2023)

30. Vojkovic, G.: Will the GDPR slow down development of smart cities?. In: IEEE 2018 41st InternationalConvention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatja, Croatia, pp. 1295–1297 (2018)
31. Wang, Z., Zhu, H., Liu, P., Sun, L.: Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecurity **4**(1), 1–21 (2021)
32. Zareen, S., Akram, A., Khan, S.A.: Security requirements engineering framework with BPMN 2.0.2 extension model for development of information systems. Appl. Sci. **10**(14), 4981 (2020)