Integrated process model for systems product line engineering of physical protection systems

Business Modeling and Software Design - 10th International Symposium, BMSD 2020, Proceedings
Tekinerdogan, Bedir; Yagiz, Sevil; Özcan, Kaan; Yakin, Iskender
https://doi.org/10.1007/978-3-030-52306-0_9

Integrated Process Model for Systems Product Line Engineering of Physical Protection Systems

Bedir Tekinerdogan[1(✉)], Sevil Yagiz[2], Kaan Özcan[2], and Iskender Yakin[2]

[1] Research, Information Technology, Wageningen University, Wageningen, The Netherlands
bedir.tekinerdogan@wur.nl
[2] Aselsan A.Ş., Ankara, Turkey
{syagiz,mkozcan,iyakin}@aselsan.com.tr

Abstract. A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent intruder attacks. Designing effective PPSs is not trivial and requires the consideration of multiple different concerns. Hence, several PPS methods have been proposed in the literature to design and analyze PPSs to realize the envisioned objectives. These methods have mainly considered the design of a single PPS. Yet, despite the differences, PPSs also share a common design and set of features and likewise can be developed using a systematic large scale reuse approach. Product line engineering (PLE) has been used in various application domains to exploit the potential for large scale reuse, and with this reduce the time-to-market, reduce the cost, and the overall quality of the developed systems. In this paper, we first report on the results of our study to explicitly model the process for developing PPSs. Subsequently, we present the integration of the PPS method with the current PLE method. For modeling the processes, we adopt the Business Process Modeling Notation (BPMN). The resulting method can be applied to the development of various PPSs while considering large-scale reuse.

Keywords: Physical protection systems · Systems engineering · Business process modeling · Product line engineering

1 Introduction

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent intruder attacks [4, 19]. PPSs have targeted the protection of various systems, including airports, rail transport, highways, hospitals, bridges, the electricity grid, dams, power plants, seaports, oil refineries, and water systems. Designing effective PPSs requires careful consideration of the requirements and the resources to provide the protection that is needed. Without a proper assessment and design, valuable resources on unnecessary protection might be wasted or, worse yet, fail to provide adequate protection at critical points of the facility. To avoid both limitations and risks, several PPS design methods have been proposed in the literature to design and analyze PPSs to realize the envisioned objectives.

B. Shishkov (Ed.): BMSD 2020, LNBIP 391, pp. 137–151, 2020.
https://doi.org/10.1007/978-3-030-52306-0_9

In general, a PPS provides *deterrence*, *detection*, *delay,* and *response* measures to protect against an adversary's attempt to complete a malicious act. As such, a PPS method considers these concerns explicitly and defines the steps for realizing these in the best possible manner. The existing PPS methods have been successfully applied to design effective PPSs. Yet, it can be observed that despite the differences, PPSs also share a common design and set of features, and likewise can be developed using systematic reuse approach. The current PPS methods, however, have targeted the development of a single system and did not consider the large scale reuse for developing various PPSs.

This paper considers the context of an industrial company that is indeed developing a broad range of PPSs. Each facility that needs to be protected is indeed unique, but on the other hand, also recurring development activities over the entire systems engineering life cycle can be observed. Obviously, there seems to be a large potential for reuse that will support the development process. Reuse has been an important goal in many industrial practices and also broadly addressed in the literature. While reuse was initially focused on a small scale, ad hoc reuse, currently, it is widely recognized that the broadest and the most valuable benefits are derived from a large-scale systematic reuse approach. This idea has culminated in the product line engineering (PLE) approach that indeed focuses on exploiting reuse over the whole lifecycle process [1, 11, 17]. Traditionally, a product line is defined as a set of systems sharing a common, managed set of features that satisfy the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. While PLE has initially focused on software reuse, the development paradigm is now applied in a broader systems engineering context, leading to the notion of systems product line engineering (SPLE). Despite earlier reuse approaches, SPLE aims to provide pro-active, pre-planned reuse at a large granularity (domain and product level) to develop applications from a core, shared asset base.

The benefits of adopting a product line approach have been analyzed and discussed before by several authors [9, 12]. Several studies show remarkable benefits of the organizations that are aligned with commonly held business goals including large-scale productivity gains, decreased time to market, increased product quality, decreased product risk, increased market agility, increased customer satisfaction, more efficient use of human resources, ability to effect mass customization, ability to maintain a market presence, and ability to sustain unprecedented growth.

The PLE process is agnostic to the domain and can be applied to developing a product line for any domain. Yet, for the development of PPSs, we also need to focus on the domain-specific PPS aspects. Hence an integrated PLE process for PPS is needed. To this end, our objective in this paper is to model the PPS method explicitly, and subsequently show the integration with the PLE process. For modeling the methods, we use the Business Process Modeling Notation (BPMN). The provided method is novel and can be applied to the development of various PPSs while considering large scale reuse.

The remainder of the paper is organized as follows. Section 2 presents the product line engineering process. Section 3 elaborates on the goals for process modeling. Section 4 presents the modeling PPS process. Section 5 shows how to integrate the PLE process with the PPS process. Finally, Sect. 6 concludes the paper.

2 Product Line Engineering

Developing PPS can be done using a single systems engineering or product line engineering approach. In the traditional single systems engineering approach in which no PLE is adopted, usually, a product portfolio can exist, but hereby systems are developed separately. This means that no PLE practices such as explicit commonality variability modeling, a product family architecture, and a shared asset base is adopted. The usually adopted process is shown in Fig. 1.

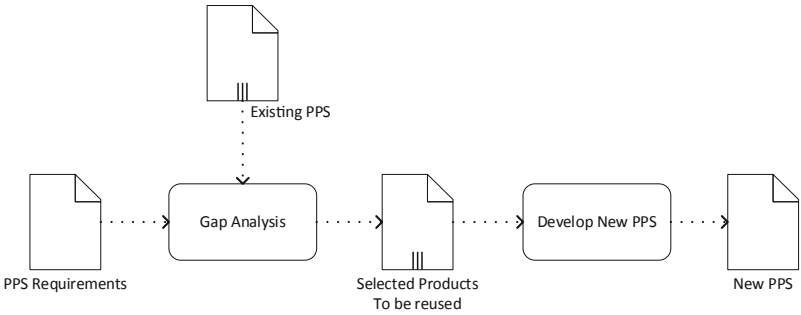

Fig. 1. Ad-hoc, non-PLE reuse strategy for developing PPS

The basic activity in this process is to identify among all the already manufactured or delivered systems, which is the closest one to the requirements and needs expressed formally (through PPS requirements) by a new potential customer. Then the selected engineering artifacts of the previously existing PPS are reused and modified in order to completely fulfill the requirements for the new PPS.

The traditional way of developing PPS fails to see and exploit the potential for reuse. Although PPSs are different, they still share the common structure and features. The larger the commonality is, the more reuse potential we can identify. This means that a company that targets the development of multiple PPS can adopt a smarter, reuse-based approach. Hence, a product line of PPS can be anticipated and developed from a common set of core assets in a prescribed way.

Compared to single system development, applying a product line engineering approach requires additional investments. The initial investment will result in a so-called *return on investment* (ROI). The adoption of product line engineering approach will usually pay off after the development of more than one product. This point is denoted as the *break-even point*. Although different PLE processes have been proposed, they share the same concepts of *domain engineering*, in which a reusable platform and product line architecture is developed, and *application engineering*, in which the results of the domain engineering process are used to develop the products. The overall development process is further controlled by a management process that consists of technical and organizational management. The typical common PLE process is shown in Fig. 2.

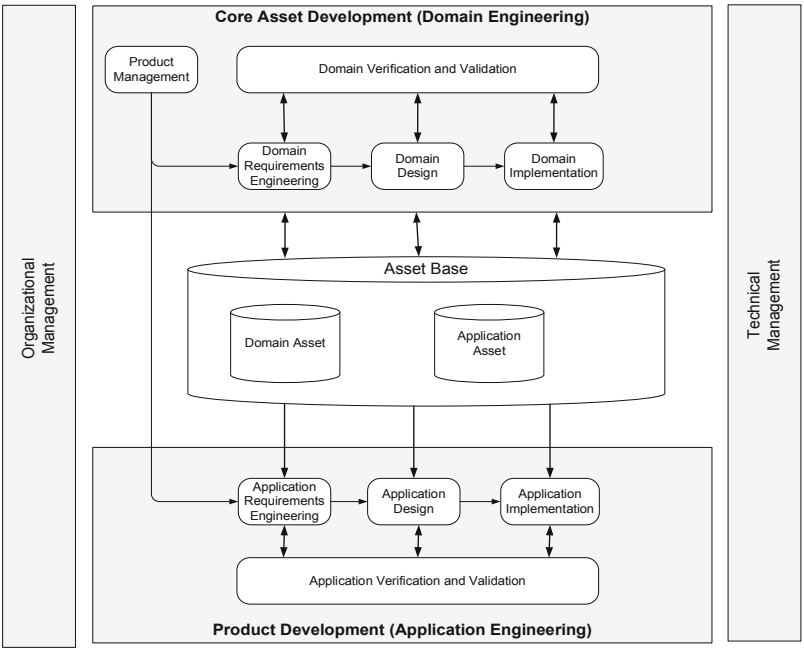

Fig. 2. PLE Process (adapted from: [15])

3 Adopted Design Approach

In this paper, we aim to model the PPS process and integrate this with the PLE process. In general, a process is defined as a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular set of customers. A business process model (BPM) is an abstract representation of a business process. Various objectives can be distinguished for developing explicit process models [15], including (1) Facilitate human understanding and communication (2) Support process improvement (3) Support process management (4) Automate process guidance (5) Automate execution support.

In this paper, the primary goal of process modeling includes communication of the PPS process to different stakeholders, the guidance of the PPS process activities, means to analyze the progress and align the PPS process with the product line engineering process. Our focus is not on automated process guidance and/or automated execution of the process, although this could indeed be considered as a follow-up study.

The adopted design method is shown in Fig. 3. We start with two parallel activities that aim to identify the PLE methods and PPS methods. Both are modeled using BPMN. The final step is the integration of the PPS with the PLE method.

For the PPS methods, we have primarily consulted the methods of the following sources:

- ML. Garcia. Vulnerability Assessment of Physical Protection Systems. Amsterdam: Elsevier Butterworth-Heinemann; 2006 [3].

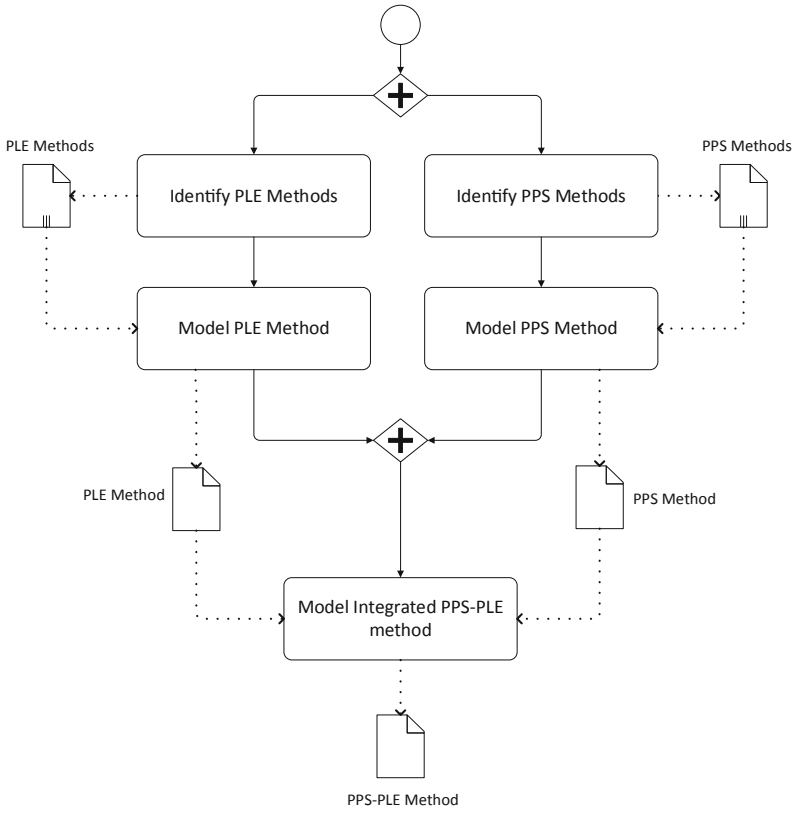

Fig. 3. Adopted design method for deriving integrated PPS-PLE process

- ML. Garcia. The Design and Evaluation of Physical Protection Systems. 2nd ed. Amsterdam: Elsevier Butterworth-Heinemann; 2008 [4].
- L. Fennelly. Effective Physical Security, Fifth Edition (5th. ed.). Butterworth-Heinemann, USA, 2016 [10].
- J.D. Williams, Physical Protection System Design and Evaluation, IAEA-CN-68/29, Vienna, 10–12 November 1997 [19].
- IAEA, Handbook on the Physical Protection of Nuclear Material and Facilities, IAEA-TECDOC-127, March 2000 [6].

For identifying the PLE methods, we have used the traditional methods as published in the PLE community. In this paper, we do not elaborate on the modeling of the PLE method [1, 11] since we have reported on these already in our earlier studies [14–16, 18].

4 PPS Process Model

PPS design is a systematic approach that employs, in particular, a systems engineering approach Systems engineering is an interdisciplinary approach to translating users'

needs into the realization of a system, its architecture, and design through an iterative process that results in an effective operational system [5, 7, 9]. Systems engineering applies over the entire life cycle, from concept development to final disposal. Systems engineering is an approach used to design and build complex systems and includes processes for defining requirements, designing systems, and evaluating designs. While systems engineering has focused on defining a systematic life cycle process to meet the quality requirements, reuse has largely been an implicit concern [8].

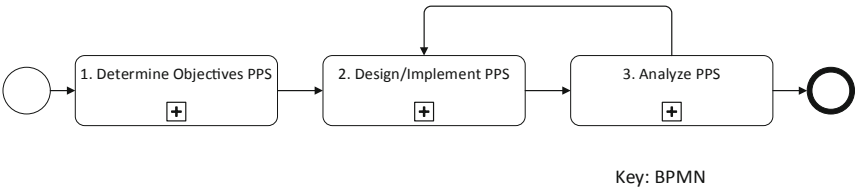

Fig. 4. Design and evaluation process for physical protection systems

Based on the identified PPS methods, we can state that the design of each PPS includes a predefined set of activities, including the determination of PPS objectives, the design and implementation of a PPS, the evaluation of the design, and if needed, a redesign or refinement of the system. The overall process is shown in Fig. 4, which can be considered as an instance of a systems engineering process that has been adapted to the design of a PPS. The shown process can be applied to the case of a new PPS design, or to an adaptation and enhancement of an existing PPS.

In the following, we elaborate on the process using explicitly developed process models.

4.1 Determine PPS Objectives Process

Figure 5 shows the activities for determining the objectives of a PPS. To formulate these objectives, the designer must (1) characterize the facility, (2) identify the targets, and (3) define the potential threats. In parallel, the designer should identify and check the legal and regulatory requirements that are required by the corresponding state laws or standardization organizations. We elaborate on these steps in the following sub-sections.

4.1.1 Facility Characterization Process

The facility characterization process is shown in Fig. 6. The characterization of the facility focuses on the entity that needs protection. Before any design decisions concerning the level of protection needed, in this step, it is aimed to provide an understanding of what is being protected and the surrounding environment.

The results of this step will help identify constraints, document existing protection features, and reveal areas and assets that may be vulnerable. The major areas of investigation for facility characterization that have been defined in the PPS methods include:

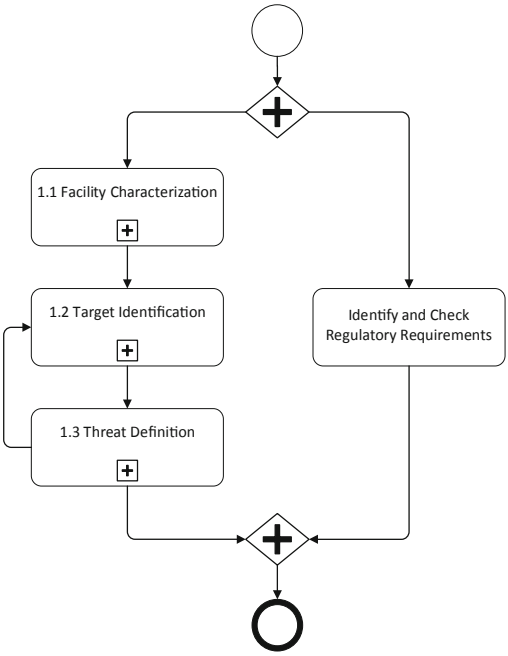

Fig. 5. Process for *determine objectives* physical protection systems

- *physical conditions*
  The physical conditions such as site boundary, location of the facility, access points, existing physical protection features, and other infrastructure details.
- *facility operations*
  The adopted processes in the facility, such as operating conditions (working hours, off-hours, emergency operations), and the types and numbers of employees.
- *facility policies and procedures*
  The written and unwritten policies and procedures used at a facility.
- *regulatory requirements*
  All facilities responsible for some regulatory authority, such as the local fire department, safety, and health regulators, and federal agencies.
- *legal issues*
  cover liability, privacy, access for the disabled, labor relations, employment practices, proper training for guards, the failure to protect, and excessive use of force by guards, to list only a few.
- *safety considerations*
  issues related to safety
- *corporate goals and objectives*
  the goals and objectives of the corporation or facility regarding the protection

Characterization of the facility thus requires both a thorough analysis of the facility and the processes within the facility, together with the identification of any existing physical protection features.

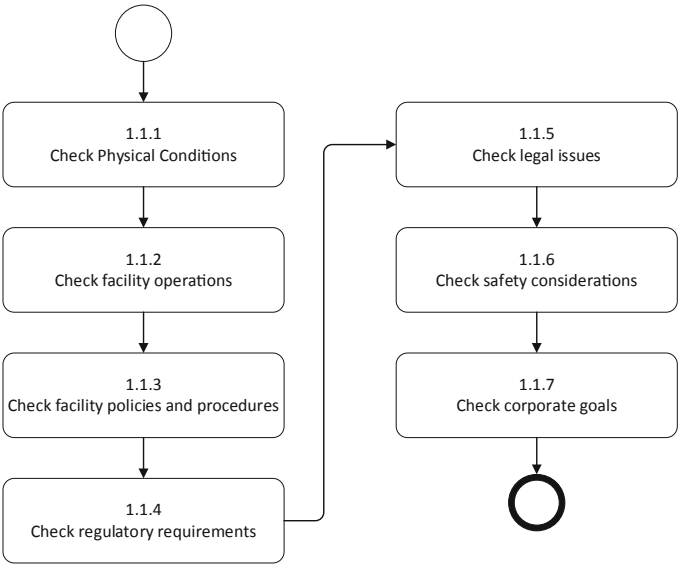

Fig. 6. Facility characterization process

4.1.2 Target Identification Process

The target identification process is shown in Fig. 7. The aim of this process is to identify what to protect without yet considering the potential threats or the means to provide physical protection. This elaborates on the facility characterization process and requires a thorough review of the facility and its assets. Two types of targets can be distinguished, primary targets, and secondary targets. Primary targets may be the physical assets inside the facility and include electronic data, people, or anything that could impact business operations. Secondary targets are the assets that can be attacked to reduce system effectiveness and/or facilitate an attack. The target identification process focuses on the identification of both types. The two techniques for target identification are a manual listing of targets and the use of logic diagrams to identify vital areas [3]. In manual listing, all significant targets to be protected are listed. When the facility is, however, too complex for manual identification of targets, logic diagrams can be used instead of or as a complementary technique. One type of logic diagram called a fault tree graphically represents the combinations of components and events that can result in a specified undesired state [13].

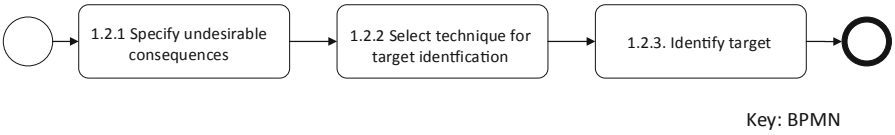

Fig. 7. Target identification process

4.1.3 Threat Definition Process

Facility characterization is followed by the threat definition process that aims to analyze and describe the threats for the corresponding facility and the identified targets.

The threat definition process is shown in Fig. 8. The methodology for *threat definition* consists of three basic parts: (1) List the information needed to define the threat (2) Collect information on the potential threat (3) Organize the information to make it usable. Hereby, the first step aims to identify and describe the information regarding the class of adversary, the range of tactics of the adversary, the range of the adversary's tactics, and the adversary's capabilities [4]. Different classes of adversaries include outsiders, insiders, and outsiders working in collusion with insiders. The range of tactics of adversaries includes deceit, force, stealth, or any combination of these. As defined by Garcia [4], deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system; and stealth is any attempt to defeat the detection system and enter the facility covertly.

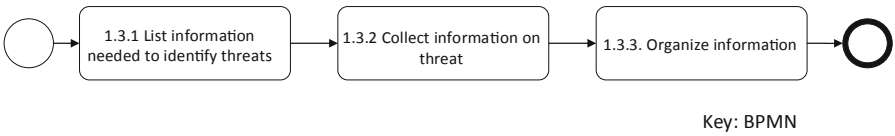

Fig. 8. Threat definition process

4.2 Design PPS Process

Once the PPS Objectives have been defined, the design process can be started. Figure 9 shows the top-level activities for the PPS design process. The outcome of the PPS design process is a PPS design that should meet the defined objectives and operational, safety, legal, and economic constraints of the facility. The design process is structured according to the primary functions of PPS, that is, *detection* of an adversary, *delay* of that adversary, and *response* by security personnel (guard force). All these three functions are essential functions of an effective PPS and must be performed in the order of *detect, delay, response.* Further, the overall period should be within a length of time that is less than the time required for completing the adversary task.

To derive a proper design, several design principles are usually taken into account, such as *defense in depth, graded approach, balanced protection*, and *robustness* [2, 3, 6]. *Defense in depth* implies the usage of a combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised. *Graded approach* implies the application of physical protection measures that are proportional to the potential consequences of a malicious act. *Balanced protection*, defines a method to use comparably effective physical protection measures. Finally, *robustness* requires the inclusion of redundancy and diversity in the PPS design to ensure a high probability of effective protection against the range of threats. In the following sub-sections, we elaborate on the steps of the design process.

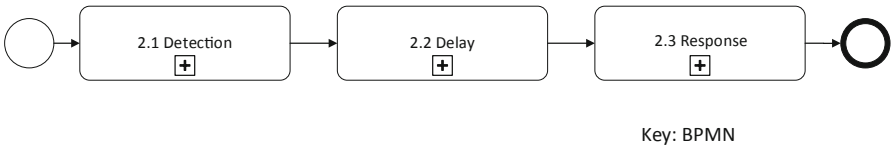

Fig. 9. PPS design process

4.2.1 Detection Process

Detection includes the discovery of an adversary action that is covert or overt. The process for detection is shown in Fig. 10. To detect an adversary action, typically, a sensor reacts to a stimulus, an alarm is initiated, and a report is sent and displayed. The alarm is assessed, and a decision is made, whether it was a false alarm or a real adversary action. Here it is necessary that an alarm is followed by an alarm assessment. Otherwise, this is not considered detection. For realizing the detection, interior and exterior sensors are designed. Detection also includes entry control which allows entry to authorized personnel only and detects the attempted entry of unauthorized personnel or material. The effectiveness of the detection function is defined by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

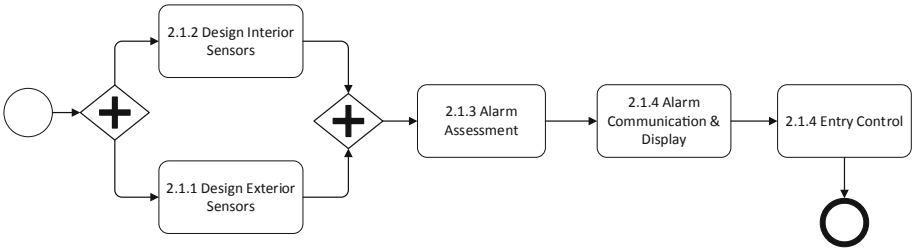

Fig. 10. PPS design process – detection

The measures of the effectiveness of entry control are throughput, false acceptance rate, and false rejection rate. Throughput is defined as the number of authorized personnel allowed access per unit time, assuming that all personnel who attempt entry are authorized for entrance. False acceptance is the rate at which false identities or credentials are allowed entry, while the false rejection rate is the frequency of denying access to authorized personnel.

4.2.2 Delay Process

Delay implies the slowing down of a detected adversary attack. Once the adversary is detected, it is important to delay the adversary so that the response force can interrupt the attack before the goal is achieved. Delay can be realized by human personnel, barriers, locks, and activated delays. Since it is not feasible to provide a response force at every attack point, some type of adversary delay is needed. The process for the delay in PPS is shown in Fig. 11. In essence, it includes two parallel steps *provide active barriers* and

provide passive barriers. Active barriers can, on command, stop or delay an adversary from accomplishing the objective. For example, a door or security barrier is active because it can be moved to allow access but keeps adversary agents outside. Passive barriers are relatively immovable, and no manual or electronic action is required for the barrier to perform its function.

After an adversary has been detected, delay elements will prevent completion of the adversary act, provide delay until an adequate response force can arrive. The adversary may be, of course, delayed prior to detection, but this has no value to the effectiveness of the PPS since it does not provide additional time to respond to the adversary. Delay before detection is primarily a deterrent [4].

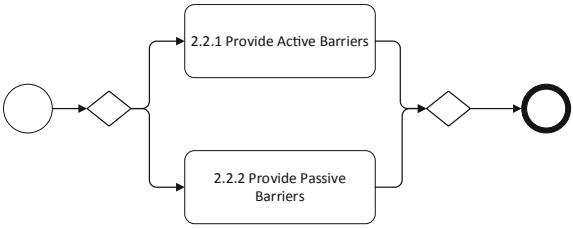

Fig. 11. PPS design process – delay

4.2.3 Response Process

The response function consists of the actions taken by the response force to prevent adversary success and can include both *interruption* and *neutralization.* Interruption is the activity of a sufficient number of response force personnel at the appropriate location to stop the adversary's progress. For this, it is needed to communicate the accurate information about adversary actions to the response force and select and deploy the response force. Neutralization includes the actions and effectiveness of the responders after interruption. Two major categories of response forces can be distinguished, immediate on-site response (timely response) and after-the-fact recovery. The use and combination of these forces will depend on the needs and objectives of a facility and the potential targets. An important metric is the response time that defines the time between receipt of a communication of adversary action and the interruption of the adversary action. Figure 12 shows the design process for the PPS response activity. It includes two steps, the design of the response force and the corresponding communication.

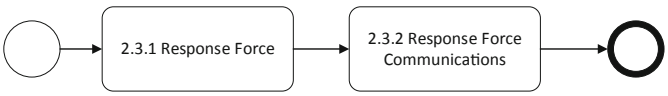

Fig. 12. PPS design process – response

4.3 Evaluate PPS Process

The final step in the design process is the evaluation of the design PPS. The process for this is shown in Fig. 13. Several techniques can be distinguished here, including Path Analysis, Scenario Analysis, and System Effectiveness Analysis. For more details about these approaches, we refer to [3, 4, 10].

The outcome of this process a system vulnerability assessment. The analysis of the PPS design can lead to either to the conclusion that the design is feasible and effectively achieves the protection objectives, or it will still identify unnoticed weaknesses. In the first case, the design and analysis process is completed. However, if the PPS does not fulfill the objectives for effective protection, then a redesign will be considered. This might also need to reconsideration or adaptation of the initial PPS objectives. This cycle continues until the analysis results show that the protection objectives are met. Note that the overall process of design and redesign is typically an iterative and incremental lifecycle process approach rather than a waterfall life cycle.

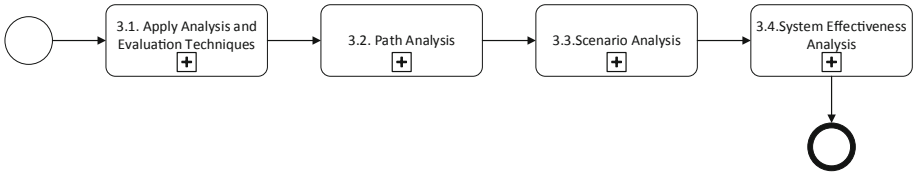

Fig. 13. PPS evaluation process

5 Integration of PLE and PPS Processes

In Sect. 2, we have provided the SPLE process, which we have also modeled in our earlier work [14–16, 18]. The previous section has provided an explicit process model for PPS. The SPLE process is, in general, domain agnostic, and can thus be applied to multiple application domains, and as such, fails to address domain-specific process concerns. On the other hand, the PPS process focuses on the development of a single PPS and does not explicitly consider reuse. To provide a systematic product line engineering for PPS, we have integrated both processes, which is shown in Fig. 14.

In essence, the dominant process model is the two-life cycle process of the PLE process consisting of a domain engineering process and an engineering process. In the domain engineering process, the core assets for the PPSs that are envisioned can be developed. In a sense, this does not change the conventional domain engineering process steps. The domain requirements engineering will result in a family requirements specification, the domain design will provide the product line architecture, and the domain implementation will provide the necessary implementation of the identified core assets for the PPSs.

The PPS method, shown on the right part of the figure, is integrated with the application engineering process, which starts by identifying the objectives and requirements of a particular PPS. These objectives and requirements, however, are not developed from

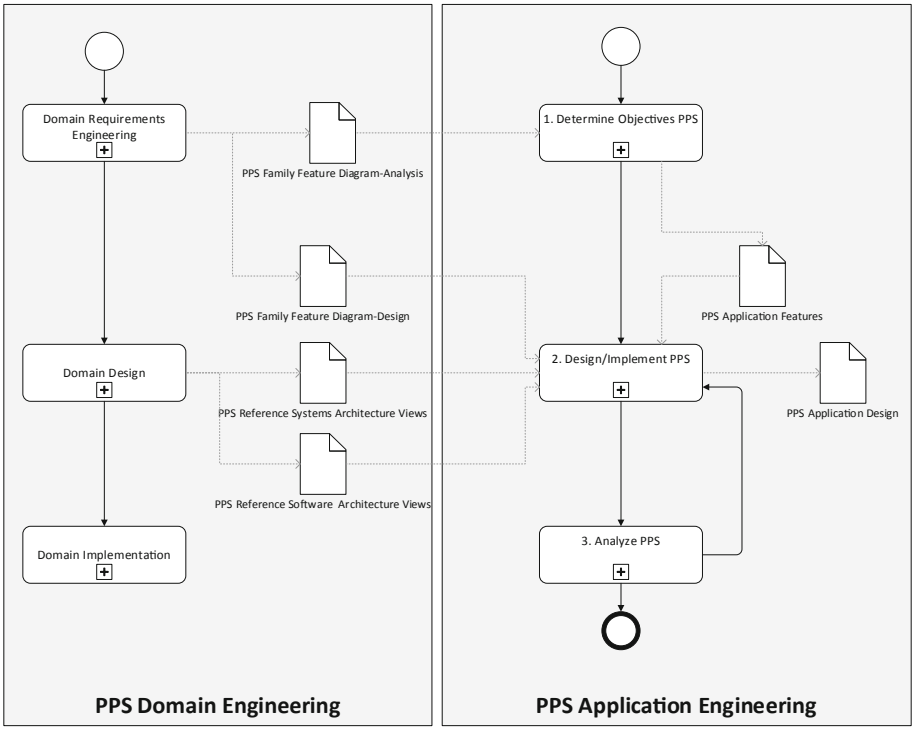

Fig. 14. PPS design process integrated within the PLE process

scratch but reused from the reusable asset base that is the result of the domain engineering process. Similarly, the design process follows the exact same process steps that we have described in the previous section but will primarily reuse the assets and the design that is needed for developing the PPS. Finally, the analysis of the PPS is based on the evaluation of the designed PPS.

Before, we stated that we wish to provide large scale systematic reuse for developing PPS. This is, in particular, necessary if a company is developing multiple different PPSs, which are based on a common product line architecture and a substantially large part of commonality. One could state that this could be just developed using conventional PLE methods. However, in particular, PPS design requires very domain-specific specific steps regarding the design of deterrence, detection, delay, and response actions. As such, it is needed to represent not only the artifacts but also the PPS process steps in the PPS product line engineering. The method shown in Fig. 14 accomplishes both goals. On the one hand, it ensures that the key concern of PPS that is protection is properly addressed. On the other hand, it helps to develop PPSs faster, with lower cost, and higher quality.

6 Conclusion

In this paper, we have focused on the design of PPS systems. In contrast to the single system perspective that is adopted in current PPS methods, we have discussed the adoption

of product line engineering that aims to develop systems based on large scale systematic reuse. Several practical and important benefits can be identified here that justify this decision, including reduced time-to-market, reduced cost, and increased quality. However, the current PPS methods do not adopt such a large product line or product family focus. On the other existing PLE methods are agnostic to the domain of the products and, as such, lack the required focus on the specific process steps, such as that in PPS methods. With this observation and triggered by a real industrial context and objectives, we have provided an approach that integrates the PPS method with the PLE method. For this, it was needed to explicitly model PPS methods. The design of PPS is discussed in detail in several books, and we have also benefited from these sources, however, nowhere in the sources, the method has been explicitly modeled. Hence the method that is modeled using the BPMN approach can be considered novel in this perspective. Further, we have shown how to integrate the PPS with the PLE method. For this, the PLE method has been considered as the dominant decomposition of the process consisting of two life cycle processes, domain engineering, and application engineering. The domain engineering process is largely the same as in conventional PLE. However, the application engineering process has been adjusted with respect to the needs of the PPS process steps. Both in the PLE literature and PPS literature, this integration has not been discussed before. This study will be continued in the future by applying it to the design of real PPSs.

References

1. Clements, P., Northrop, L.: Software Product Lines: Practices and Patterns. Addison-Wesley, Boston (2002)
2. Drago, A.: Methods and techniques for enhancing physical security of critical infrastructures, Ph.D. thesis, University of Naples, March 2015
3. Garcia, M.L.: Vulnerability Assessment of Physical Protection Systems. Elsevier Butterworth-Heinemann, Amsterdam (2006)
4. Garcia, M.L.: The Design and Evaluation of Physical Protection Systems, 2nd edn. Elsevier Butterworth-Heinemann, Amsterdam (2008)
5. Guide to the Systems Engineering Body of Knowledge (SEBoK), October 2016
6. IAEA: Handbook on the Physical Protection of Nuclear Material and Facilities, IAEA-TECDOC-127, March 2000
7. Walden, D.D., Roedler, G.J., Forsberg, K.J., Hamelin, R.D., Shortell, T.M. (eds.): INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th edn. Wiley, New York (2015)
8. INCOSE Product Line Engineering International Working Group. http://www.incose.org/ChaptersGroups/WorkingGroups/analytic/product-lines. Accessed October 2017
9. International Council on Systems Engineering (INCOSE), INCOSE Systems Engineering Handbook, Ver. 3.2, INCOSE-TP-2003-002-03.2, January 2010
10. Fennelly, L.: Effective Physical Security, 5th edn. Butterworth-Heinemann, Oxford (2016)
11. Pohl, K., Böckle, G., van der Linden, F.: Software Product Line Engineering – Foundations, Principles, and Techniques. Springer, Heidelberg (2005). https://doi.org/10.1007/3-540-28901-1
12. Schmid, K., Verlage, M.: The economic impact of product line adoption and evolution. IEEE Softw. **19**(4), 50–57 (2002)
13. Tekinerdogan, B., Sozer, H., Aksit, M.: Software architecture reliability analysis using failure scenarios. Elsevier J. Syst. Softw. **81**(4), 558–575 (2008)

14. Tekinerdogan, B., Ozkose Erdogan, O., Aktug, O.: Supporting incremental product development using multiple product line architecture. Int. J. Knowl. Syst. Sci. (IJKSS) **5**(4), 1–16 (2014)
15. Tekinerdogan, B., Duman, S., Gümüşay, Ö., Durak, B.: Devising integrated process models for systems product line engineering. In: 2019 International Symposium on Systems Engineering (ISSE), Edinburgh, United Kingdom (2019)
16. Tekinerdogan, B., Duman, S., Caner, H., Durak, B.: Customizing a feature ontology for product line engineering within a system-of-systems context. In: 2019 International Symposium on Systems Engineering (ISSE), Edinburgh, United Kingdom (2019)
17. Tüzün, E., Tekinerdogan, B., Kalender, M.E., Bilgen, S.: Empirical evaluation of a decision support model for adopting software product line engineering. Inf. Softw. Technol. **60**, 77–101 (2015)
18. Tüzün, E., Giray, G., Tekinerdogan, B., Macit, Y.: Modeling software product line engineering with essence framework. Int. J. Inf. Technol. **11**(1), 99–109 (2018)
19. Williams, J.D.: Physical Protection System Design and Evaluation, IAEA-CN-68/29, Vienna, 10–12 November 1997