# Model-Based Development of Design Basis Threat for Physical Protection Systems

ISSE 2021 - 7th IEEE International Symposium on Systems Engineering, Proceedings

Tekinerdogan, Bedir; Ozcan, Kaan; Yagiz, Sevil; Yakin, Iskender

https://doi.org/10.1109/ISSE51541.2021.9582528

# Model-Based Development of Design Basis Threat for Physical Protection Systems

Bedir Tekinerdoğan
Information Technology
Wageningen University
Wageningen, The Netherlands
bedir.tekinerdogan@wur.nl

Kaan Özcan
ASELSAN
Ankara, Turkey
mkozcan @aselsan.com.tr

Sevil Yağız
ASELSAN
Ankara, Turkey
syagiz@aselsan.com.tr

İskender Yakın
ASELSAN
Ankara, Turkey
iyakin@aselsan.com.tr

*Abstract*— **Physical protection system (PPS) is developed to protect the assets or facilities against threats. A systematic analysis of the capabilities and intentions of potential threat capabilities is needed resulting in a so-called Design Basis Threat (DBT) document. A proper development of DBT is important to identify the system requirements that are required for adequately protecting a system and to optimize the resources needed for the PPS. In this paper we propose a model-based systems engineering approach for developing a DBT based on feature models. Based on a domain analysis process, we provide a metamodel that defines the key concepts needed for developing DBT. Subsequently, a reusable family feature model for PPS is provided that includes the common and variant properties of the PPS concepts detection, deterrence and response. The configuration processes are modeled to select and analyze the required features for implementing the threat scenarios. Finally, we discuss the integration of the DBT with the PPS design process.**

***Keywords— Physical Protection Systems, Systems Engineering, Design Basis Threat, Feature Modeling***

## I. Introduction

For the protection of areas, facilities, or assets additional systems are required to can deter potential attacks, detect these attacks and if needed provide a response. Such protection systems are called physical protection systems (PPS) [4][5][8] which include and integrate physical protection devices such as interior and exterior intrusion detection sensors, cameras, barriers, access control devices and response measures.

The development of a PPS requires an interdisciplinary, holistic approach as it is adopted in systems engineering [12]. Currently, an important trend in systems engineering is the focus on model-based systems engineering (MBSE) which focuses on creating and exploiting domain models as the primary means of information exchange between engineers, rather than using informal documents, as it is the case in the traditional conventional document-oriented approach [6][7][9]. Adopting an MBSE substantially supports the understanding of the design, enhances the communication of design decisions, and better analysis of the system before it is built.

For a given system that needs to be protected, various different PPSs can be designed based on the potential set of threats. To ensure that the right PPS is designed the conditions under which the protection system must perform need to be understood. To this end, an explicit description of the potential threats and the corresponding conditions of the system needs to be provided. The information related to threats can be based on various information sources, however this might not always be directly available and threats can change in due time. A PPS that is designed only for the current and limited set of threats may become very soon ineffective. In case the threats are not properly identified and not explicitly described it will be difficult to design the PPS for the required level of protection for a given system. Missing the threats (false negatives) might lead to severe consequences of the malicious attacks. On the other hand, identifying unnecessary threats can substantially increase the cost of PPS.

A design basis threat (DBT) is a well specified description of the threats for a confident protection level that is adequate. A DBT defines the scope of the PPS and supports an efficient allocation of resources for protection [2][8]. Further, the DBT defines a baseline against which the need for changes in physical protection can be evaluated.

In this paper we propose a MBSE approach for developing a DBT based on feature models. Feature models have been used to model the common and variant properties of a domain or a system. One of key advantages of a feature model is that it provides a formal model depicting the system configuration space of the selected domain. In the presented approach a reusable family feature model for PPS is provided that includes the common and variant properties of the PPS concepts detection, deterrence and response. Based on this feature model, the necessary features are identified and used for developing the DBT. We illustrate the approach for developing a DBT for a real industrial PPS.

The remainder of the paper is organized as follows. In section 2 we present the background on PPS and model-based systems engineering. Section 3 presents the process for developing a PPS feature diagram. Section 4 presents the process for developing DBTs based on the feature diagram. Section 5, presents the related work. Finally, section 6 concludes the paper.

## II. Preliminaries

### A. *Physical Protection Systems*

Due to the interdisciplinary concerns developing a PPS typically requires a systems engineering approach. The traditional systems engineering lifecycle process is often presented as a V-model [9]. The left side of the V represents concept development and the decomposition of requirements into function and physical entities that can be architected, designed, and developed. The right side of the V represents the integration of these entities (including appropriate testing to verify that they satisfy the requirements) and their ultimate transition into the field, where they are operated and maintained.

Obviously, the systems engineering lifecycle process is agnostic to specific domains and as such is generic and less useful for modeling the specific concerns of a particular domain. In the case of a PPS this requires the domain specific steps to focus on the detection, delay and response measures to protect a system against an adversary's attempt to complete a malicious act. Fig. 1 shows the top-level activities for the PPS design process. In essence the PPS process consists of three key activities that include identifying the PPS objectives, designing the PPS, and evaluating the PPS. Determining the PPS objectives includes the facility characterization, the threat definition and the definition of the target that needs to be protected. Designing PPS focuses on three activities, detection, delay and response. The resulting PPS design should meet the defined objectives and operational, safety, legal, and economic constraints of the facility. The final step in the PPS lifecycle is the evaluation of the design PPS. Several techniques can be distinguished here, including Path Analysis, Scenario Analysis, and System Effectiveness Analysis [4][5].

The outcome of this process is 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.

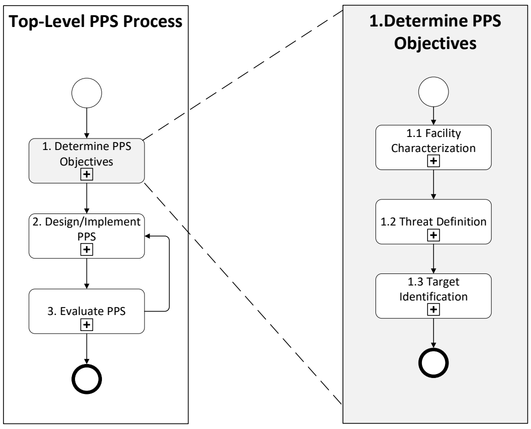
Top-Level PPS Process
1. Determine PPS Objectives
2. Design/Implement PPS
3. Evaluate PPS
1.Determine PPS Objectives
1.1 Facility Characterization
1.2 Threat Definition
1.3 Target Identification

Fig. 1. PPS Design Process with focus on PPS Objectives in which DBT is defined

### *B. Feature Modeling*

Feature modeling is an important domain modeling activity which is part of the domain analysis process. The goal of domain analysis is often to understand the key concepts of a domain and in the engineering process the guidance of the development of the system. It is defined as a systematic process for identifying, capturing and organizing domain knowledge about the problem domain with the purpose of making it reusable when creating new systems. The term domain refers to an area of knowledge or activity characterized by a set of concepts and terminology understood by practitioners in that area.

A feature model represents the domain by explicitly depicting the common and variant features. Hereby, a feature is defined as a system property that is relevant to some stakeholder and is used to capture commonalities or discriminate between. A feature model for a particular domain is often represented as a feature diagram, a tree with the root representing a domain or system, and its descendent nodes are features. Features can be mandatory, optional, or alternatives. The selection of the features in a feature diagram represents a feature configuration, which often refers to an instance of the system. Not all configurations are possible in practice, which are explicitly indicated using feature constraints. The most common feature constraints include *requires* or *mutex* that impose or exclude the selection of features, respectively.

## III. Metamodel and Method

In this section we will first present the metamodel for defining the key concepts, followed by the adopted method for developing DBTs.

### *A. Metamodel for DBT*

Based on the domain analysis process several concepts can be identified that are important for the PPS domain and the DBT. The resulted metamodel is shown in Fig. 2.

A threat assessment is an analysis of the threats based on the acquired information and intelligence that anticipates on and describes the motivations, intentions and capabilities of these threats. The results of a threat assessment are described in the DBT. A DBT is a document that describes several threat scenarios. A threat scenario provides concrete information about the threat source, the threat event, the impact, the target, the vulnerability of the target, and the overall risk. The threat source can be natural or human, and internal or external. The threat can be intentional or unintentional.

The threat event can result in some impact on the target, which could have some degree of vulnerability. The impact can be related to security or safety. The vulnerability of the target refers to weaknesses or gaps in the protection of assets that can be exploited by threats in order to compromise the asset. Vulnerabilities can be physical or cyber (software) related. Risk is defined as the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. Altogether these will also define the baseline threat level, which is rated, for example as low, medium, high.

### *B. Method for Developing DBT*

The method developing DBT that is used in the threat assessment process is shown in Fig. 3.

We adopt a domain-driven approach [13] in which we use feature models to explicitly depict the common and variant features related to DBTs. The feature diagram will be discussed in the following sections. To support the configuration of the feature diagram, a specific process will be defined that can be used in the threat assessment process. This will result in a possible set of features that need further analysis. The analysis for the specific features is done based on existing intelligence or by deriving additional information. The results are written in the DBT that describes a set of scenarios together with their risk levels.

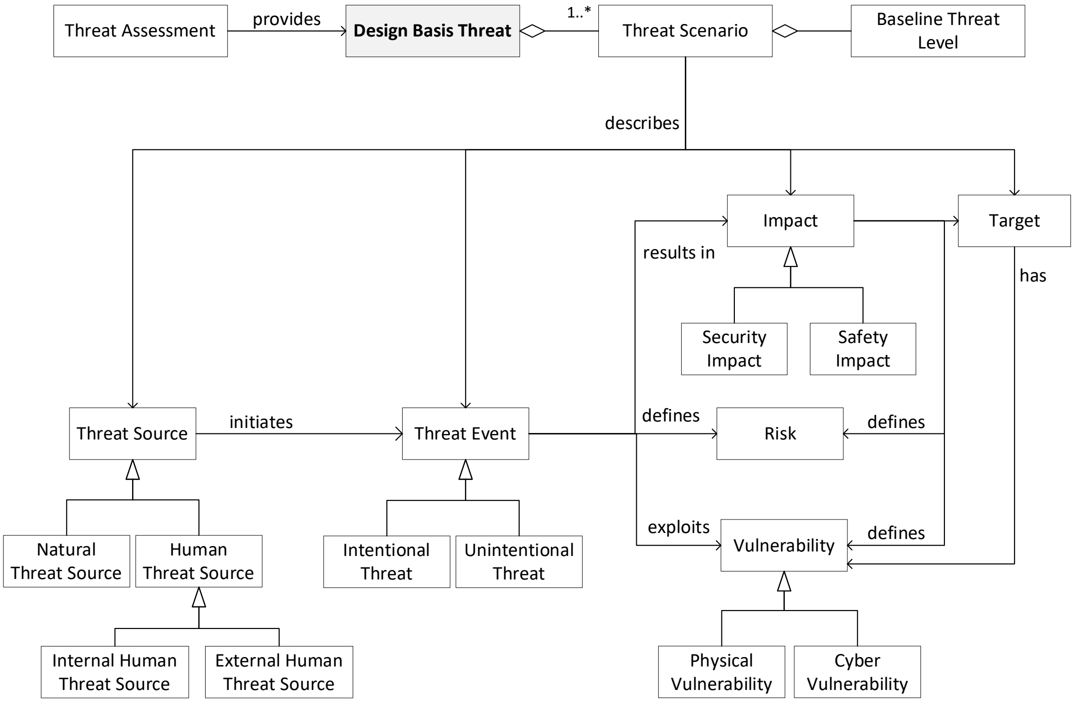

Fig. 2. Metamodel for Design Basis Threat (DBT)

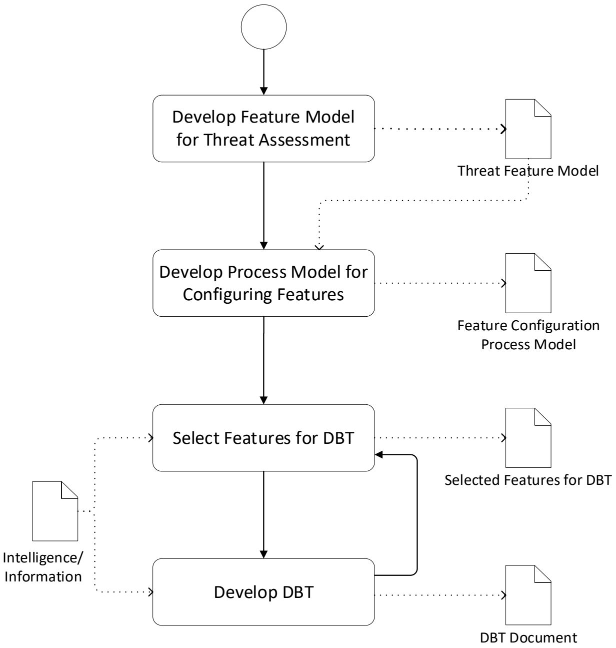
Develop Feature Model for Threat Assessment
Threat Feature Model
Develop Process Model for Configuring Features
Feature Configuration Process Model
Select Features for DBT
Selected Features for DBT
Intelligence/ Information
Develop DBT
DBT Document

Fig. 3. Method for developing DBT

## IV. Feature Model PPS

Before the analysis on the various threats, often the properties of the target (e.g. facility or asset) are analyzed. This is needed to clarify and understand what is being protected and the surrounding environment. An improper characterization will lead to either overprotecting a target or fail to adequately protect the target. Overprotection will lead to unnecessary waste of resources and increase the cost. Inadequate protection will leave the target vulnerable to potential adversarial attacks. The exact description of the target is also one of the key elements of a DBT.

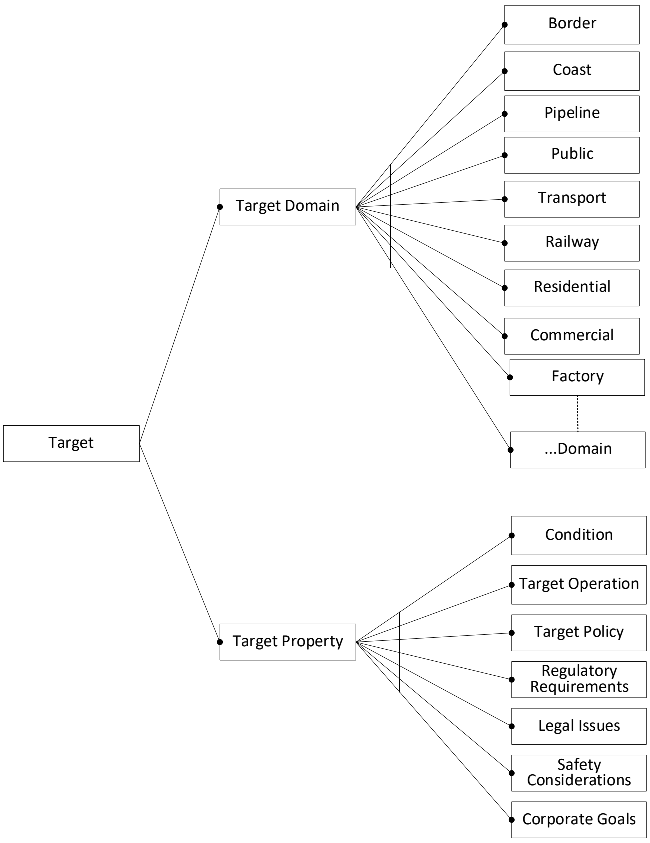

Fig. 4.Feature Diagram for PPS Domains (adapted from:[17])

Fig. 4 shows the feature diagram for the target feature, which has two sub-features target domain and target properties. The feature target domain is open-ended and more domains can be added. Each target domain will have different threats and will require different protection.

To support the identification and analysis of the important features, the process model as shown in Fig. 5 is adopted.

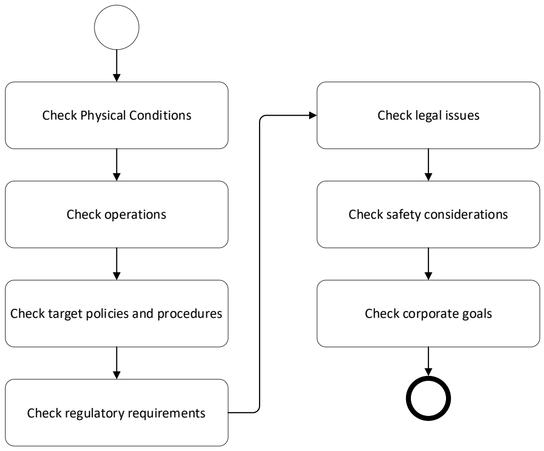
Check Physical Conditions
Check operations
Check target policies and procedures
Check regulatory requirements
Check legal issues
Check safety considerations
Check corporate goals

Fig. 5. Facility Characterization Process

The analysis of the feature diagram using the corresponding process results in the identification of the key elements of the target that are vulnerable or could be attacked. The target property addresses different concerns such as condition, facility operations, policy, regulatory requirements, legal issues, safety considerations and corporate goals. The DBT will include an instantiation of Table 1.

TABLE 1. Table in the DBT for describing the target element

| *Target Element* | *Description* |
|---|---|
| Physical conditions | E.g. site boundary, location of the facility, access points, existing physical protection features, and other infrastructure details |
| Target operations | The adopted processes such as operating conditions (working hours, off hours, emergency operations), and the types and numbers of employees. |
| Policies and procedures | The written and unwritten policies and procedures used. |
| Regulatory requirements | All facilities responsible to some regulatory authority, such as, 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 |

Fig. 6. shows the feature diagram for threats. A detailed description can also be found in our earlier study [17]. Each threat is characterized by the threat source, the adversary group, adversary tactics, adversary actions, adversary motivation and adversary capability. As shown in the figure, threat sources can be hackers, criminals, terrorists, extremists and natural threat sources. Adversaries can be grouped into different groups including insiders, outsiders, and outsiders collaborating with insiders.

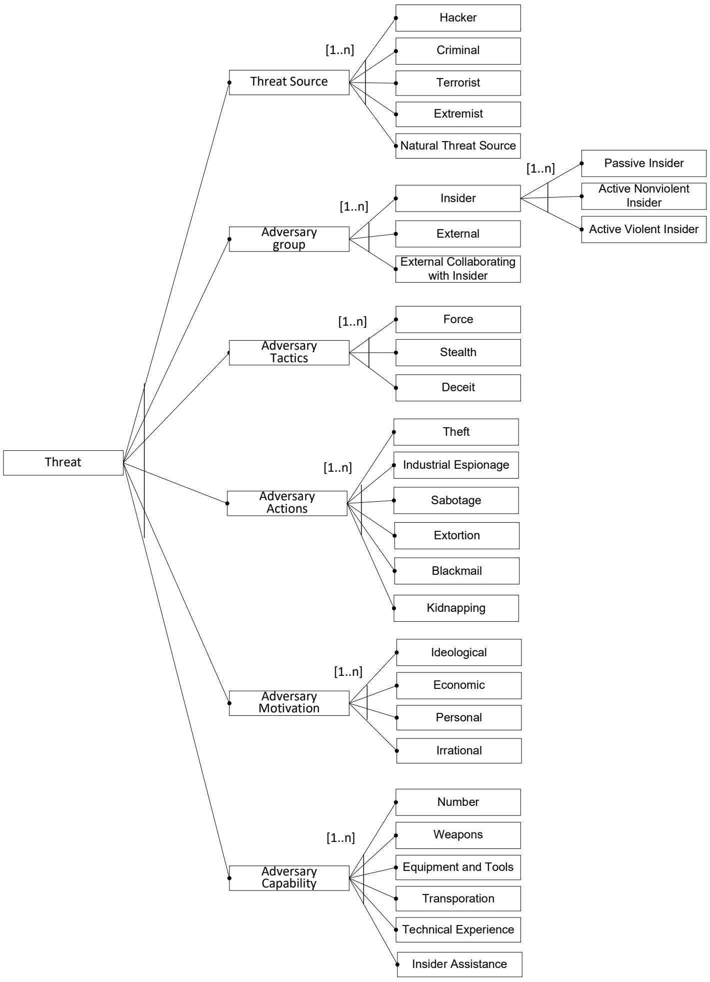

Fig. 6. Feature Diagram for PPS Threats and Risks (adopted from: [17])

Different classes of adversaries include outsiders, insiders, and outsiders working in collusion with insiders. The range of tactics of adversaries includes force, stealth, deceit or any combination of these. Different adversary actions can be distinguished including theft, industrial espionage, sabotage, extortion, blackmail and kidnapping. The motivation of an adversary can be ideological, economic, personal or irrational. Finally, adversaries may have different capabilities including the number of adversaries, the used weapons, the equipment and tools, the transportation means, the technical experience and insider assistance.

Again this feature diagram is analyzed, the features are selected, and for each selected feature the DBT describes the specific threat scenario and the concrete details. The DBT will use the table template as shown in

TABLE 2. Table in the DBT for describing the Threats

| *Element* | *Description* |
|---|---|
| Threat Source | The threat sources that can exploit a vulnerability, intentionally or unintentionally, and as such lead to a security or safety impact. |
| Threat Event | Description of the threat event initiated by the threat source |
| Likelihood | The chance that the threat event will happen |
| Impact | The impact of the threat event in case it happens |
| Target | The target of the adversarial attack |
| Vulnerabilities | The description of the weaknesses of the target system which thus make a threat possible and potentially even more dangerous. |
| Risk | The calculated overall risk given the likelihood of the threat to happen and the vulnerabilities of the target |

## V. PPS Dessign Based on DBT

The DBT is developed based on the feature model and the supporting processes that help to identify the key features. The DBT in its turn, is used as an input for the design of the PPS (Fig. 7). The DBT provides a characterization of the target and the threat scenarios, which define the threats, the vulnerabilities, the impact in case of a successful attack, and the potential risks. This information is used to guide the selection of the detection and deterrence elements for developing the PPS.

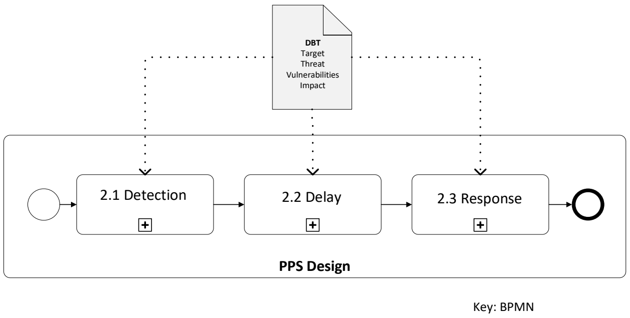

Fig. 7. PPS Design Activities

The design process will result in a PPS design that ensures the protection level to cope with the threat scenarios as identified in the DBT. Each threat will have a different risk level and thus, design decisions will be made based on this information. In addition to the aspects described in the DBT the design process should also take into account the operational, safety, legal, and economic constraints of the facility

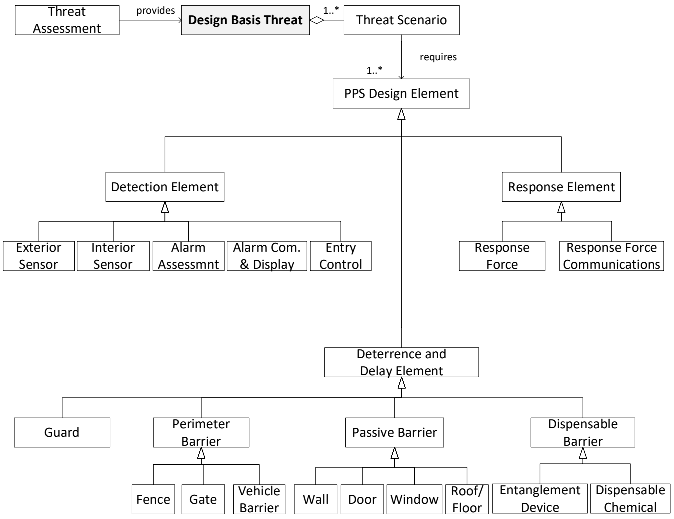

Fig. 8. Relation from DBT and Threat Scenario to PPS Design Elements

Several PPS methods have been proposed in the literature. While they differ in the details, there is a common consensus on the inclusion of the three key activities of 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 time needed for detection and response should be within a length of time that is less than the time required for completing the adversary task. Each threat scenario in the DBT will have different expected time periods for the detection, the delay and the response. The more threat scenarios are involved the more complicated the design process. Fig. 8 shows the metamodel depicting the relation from threat scenarios to design elements.

To derive a proper design several design principles are usually taken into account, such as defence in depth, graded approach, balanced protection, and robustness [7][8][11]. Defence 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 high probability of effective protection against the range of threats. The selection of the PPS design elements as well as the specific design principles will be largely guided by the findings as described in the DBT.

## VI. Related Work

The design of PPS has been addressed by several studies which describe the steps to design and evaluate a PPS [4][5][8].

As part of a larger part we have also focused on formalizing the method for PPS. In [16] we have focused on the product line engineering (PLE) [18][19] of PPSs. Although PLE is agnostic to a particular system the development of PPSs require domain-specific aspects to achieve the required protection. To provide a PLE-based

PPS method we have modelled the PLS process and PLE process using the BPMN. Subsequently, we have proposed an integrated PLE method that can be used to develop PPSs. In [18] we have provided a model-based systems product line engineering approach that integrates and applies PLE and model-based development for PPS.

In this paper we have focused on the earlier stages of the PPS method and discussed the DBT method, which was not addressed before. We have proposed the development of feature diagrams that can be used to support the threat assessment and the development of a DBT. An earlier study has provided a broader feature-driven analysis of PPSs [17].

The DBT is used for the requirements analysis of PPS which is subsequently used to design the PPS for the required protection. In this paper we did not focus on the design of PPSs. This has been addressed in earlier studies such as in [14][15][19]. In [14] we have provided a systems engineering architecture framework that provides a coherent set of viewpoints for modelling PPSs. This has been further used in [15] to design a product line architecture for PPS.

Related to PPS and perhaps part of a PPS is an intrusion detection system (IDS), which has also been extensively discussed in the literature [1][2][10]. An IDS monitors a network or system for malicious activity or policy violations. In case of an intrusion or violation activity, this is typically reported either to an administrator or collected centrally using a security information and event management system. The latter combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms. In the PPS, the detection functionality largely uses the techniques as proposed by IDS and IDPS (intrusion detection and prevention system). A related study in this context could be the detailed feature modelling for IDS.

## VII. Conclusion

Physical protection systems (PPS) have been broadly discussed and applied for the protection of areas, facilities, or assets. Designing PPS requires the understanding of the key threat scenarios based on which the resources will be allocated to implement the required protection level. The design basis threat is a document that explicitly describes the threats, the targets, the vulnerabilities, the impact, and the overall risks. For different PPSs different DBTs need to be developed. We have proposed a model-based development approach for DBT. For developing the required models, we have applied domain analysis and derived the metamodel, the feature diagrams, and the process models for identifying the required features for the required protection. The metamodel was very useful in defining the key concepts and their relations. The feature model provides a comprehensive overview of the features and supports the threat assessment to identify the features that need to be taken into account for realizing the required protection. The presented approach complements and builds on our earlier work on physical protection systems. We have applied a model-based approach for developing DBT and the overall system. In our future work, we will focus on the adoption of executable models to automatically generate the DBT and the other relevant models in the PPS development process.

## References

[1] S. Axelsson, Intrusion Detection Systems: A Survey and Taxonomy, 2000.

[2] Development, Use and Maintenance of the Design Basis Threat, IAEA, IAEA Nuclear Security Series No. 10, Vienna, 2009.

[3] L. Fennelly. Effective Physical Security, Fifth Edition (5th. ed.). Butterworth-Heinemann, USA, 2016.

[4] ML. Garcia. Vulnerability assessment of physical protection systems. Amsterdam: Elsevier Butterworth-Heinemann; 2006.

[5] ML. Garcia. The design and evaluation of physical protection systems. 2nd ed. Amster-dam: Elsevier Butterworth-Heinemann; 2008.

[6] Guide to the Systems Engineering Body of Knowledge (SEBoK), October 2016.

[7] H.G. Gurbuz, B. Tekinerdogan. Model-based testing for software safety: a systematic mapping study. Software Quality J ournal26, 1327–1372. https://doi.org/10.1007/s11219-017-9386-2, 2018.

[8] Handbook on the Physical Protection of Nuclear Material and Facilities, IAEA, IAEA-TECDOC-127, March 2000.

[9] INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th Ed.. John Wiley & Sons, 2015.

[10] NIST (National Institute of Standards and Technology) – Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007.

[11] SEBOK 2016, Guide to the Systems Engineering Body of Knowledge (SEBoK).

[12] System Engineering Handbook, A Guide For System Life Cycle Process and Activities, 2015

[13] B. Tekinerdogan & M. Aksit. Classifying and evaluating architecture design methods, in: Software Architectures and Component Technology, Springer, pp3-27, 2002.

[14] B. Tekinerdogan, K. Özcan, S. Yagiz, I. Yakin. Systems Engineering Architecture Framework for Physical Protection Systems, International Symposium on Systems Engineering (ISSE), Vienna, Austria, October 12-14, 2020.

[15] B. Tekinerdogan, I. Yakin, S. Yagiz, K, Özcan. Product Line Architecture Design of Software-Intensive Physical Protection Systems, International Symposium on Systems Engineering (ISSE), Vienna, Austria, October 12-14, 2020.

[16] B. Tekinerdogan, S. Yagiz, K. Özcan, I. Yakin. Integrated Process Model for Systems Product Line Engineering of Physical Protection Systems, In: Shishkov B. (eds) Business Modeling and Software Design. BMSD 2020. Lecture Notes in Business Information Processing, vol 391 (ISBN: 978-3-030-52305-3). Springer, 2020.

[17] B. Tekinerdogan, K. Özcan, S. Yagiz, I. Yakin. Feature-Driven Survey of Physical Protection Systems, 11th Complex Systems Design & Management (CSD&M) conference, Paris, 2020.

[18] B. Tekinerdogan, K. Özcan, I. Yakin, S. Yagiz. Model-Based Systems Product Line Engineering of Physical Protection Systems, NCOSE 31st Annual International Symposium 2021, Jul 17, 2021 - Jul 22, 2021.

[19] E. Tüzün, B. Tekinerdogan, M.E. Kalender, S. Bilgen. Empirical Evaluation of a Decision Support Model for Adopting Software Product Line Engineering, Information and Soft-ware Technology, Elsevier, Vol. 60, Pages 77–101, 2015.

[20] Williams, J.D., Physical Protection System Design and Evaluation, IAEA-CN-68/29, 1997.